FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Bezpečnostní analýza SOHO směrovačů
Student:	Jakub Kaloč
Vedoucí:	Ing. Josef Kokeš
Studijní program:	Informatika
Studijní obor:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	Do konce zimního semestru 2020/21

Pokyny pro vypracování

Seznamte se s metodikami bezpečnostní analýzy a bezpečnostními standardy se zaměřením na síťové prvky.
Proveďte rešerši volně dostupných softwarových nástrojů pro penetrační testování.
Zformulujte metodiku pro provedení základní bezpečnostní analýzy SOHO směrovače vzhledem k útokům z vnitřní sítě uživatele. Analyzujte možnosti překonání bariéry mezi vnitřní a vnější sítí, např. útočný javascriptový kód ve webové stránce.
Vyberte několik běžně používaných SOHO směrovačů a otestujte je podle vytvořené metodiky.
Diskutujte své výsledky, v případě nalezení zranitelností navrhněte obranná opatření.

Seznam odborné literatury

Dodá vedoucí práce.

prof. Ing. Pavel Tvrdík, CSc.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 28. února 2019

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalárska práca

Bezpečnostní analýza SOHO směrovačů

Jakub Kaloč

Katedra počítačových systémů
Vedúci práce: Ing. Josef Kokeš

14. mája 2019

Poďakovanie

Chcel by som poďakovať Ing. Josefovi Kokešovi, vedúcemu mojej práce, za cenné rady, veľkú ochotu a čas, ktorý mi venoval pri písaní tejto práce. Ďalej by som chcel poďakovať mojim rodičom za spätnú väzbu k obsahovej aj jazykovej stránke textu, ktorú mi poskytovali počas vytvárania tejto práce.

Prehlásenie

Prehlasujem, že som predloženú prácu vypracoval(a) samostatne a že som uviedol(uviedla) všetky informačné zdroje v súlade s Metodickým pokynom o etickej príprave vysokoškolských záverečných prác.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Sb., autorského zákona, v znení neskorších predpisov a skutočnosť, že České vysoké učení technické v Praze má právo na uzavrenie licenčnej zmluvy o použití tejto práce ako školského diela podľa § 60 odst. 1 autorského zákona.

V Prahe 14. mája 2019 .....

České vysoké učení technické v Praze
Fakulta informačních technologií

Odkaz na túto prácu

Kaloč, Jakub. *Bezpečnostní analýza SOHO směrovačů*. Bakalárska práca. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2019.

Abstrakt

Cieľom práce je zoznámiť čitateľa s problematikou bezpečnostného testovania smerovačov a niektorými rozšírenými zraniteľnosťami smerovačov, vrátane prekonávania bariéry medzi lokálnou sieťou a internetom. Práca zároveň aplikuje vybudované teoretické zázemie a testuje niekoľko SOHO smerovačov bežne distribuovaných internetovými poskytovateľmi.

V teoretickej časti práca predstavuje vybrané technické štandardy relevantné pre bezpečnosť sieťových prvkov. Následne je predstavený koncept bezpečnostného testovania a viaceré klasifikácie testov. S využitím predstavených informácií práca popisuje konkrétnu metodiku bezpečnostného testovania smerovačov a rozoberá celý postup jeho priebehu.

V praktickej časti sa predstavená metodika aplikuje na vybrané smerovače a použije sa na otestovanie vybraných zraniteľností. Výsledky testovania sú analyzované v záverečnej časti práce.

Kľúčové slová analýza zraniteľností smerovačov, informačná bezpečnosť, smerovač, bezpečnostné štandardy, penetračné testovanie, útoky na smerovače, výsledky bezpečnostného testovania, testovacie nástroje, Kali Linux

Abstract

The aim of this thesis is to inform the reader about the issues of router security testing and some common router vulnerabilities, including overcoming the barrier between the local area network and the internet. The paper applies the acquired theoretical information to perform security testing on some SOHO routers commonly distributed by internet providers.

The theoretical part of this paper describes the technical standards which are relevant for the security of network devices. The following part of the thesis defines the fundamentals of security testing and various classifications of security test. The particular methodology of router security testing and its whole procedure are both defined and described in the thesis based on the presented background information.

The practical part of this paper demonstrates the use of the methodology of router security testing and is used to perform security tests of some of the chosen vulnerabilities. The results are described in the final part of this paper.

Keywords router vulnerability analysis, cybersecurity, router, cybersecurity standards, penetration testing, attacks on routers, results of security tests, penetration testing tools, Kali Linux

Obsah

Úvod **1**
Motivácia k vytvoreniu práce 1
Ciele práce 1
Štruktúra práce 2

1 Štandardy a kybernetická bezpečnosť **3**
1.1 International Organization for Standardization 4
1.1.1 Norma ISO/IEC 27000 5
1.1.2 Norma ISO/IEC 27001 6
1.1.3 Norma ISO/IEC 27033 6
1.2 Common Criteria 8
1.2.1 Kľúčové pojmy definované v Common Criteria 9
1.2.2 Úrovne EAL 11
1.3 Bezpečnostné štandardy v Českej republike 12

2 Bezpečnostné testovanie **13**
2.1 Druhy testov z hľadiska rozsahu 13
2.1.1 Skenovanie zraniteľností 14
2.1.2 Penetračné testy 14
2.1.3 Social engineering 15
2.2 Druhy testov podľa znalosti informácií o systéme 16
2.2.1 Black box testy 16
2.2.2 White box testy 17
2.2.3 Gray box testy 18
2.3 Druhy testov z pohľadu prístupu 18
2.3.1 Fyzický prístup 18
2.3.2 Prístup z lokálnej siete 19
2.3.3 Prístup z internetu 19
2.4 Druhy testov z pohľadu automatizácie 20

2.4.1 Automatizované testy 20
2.4.2 Manuálne testy 20
2.5 Druhy testov z pohľadu dopadu na systém 21
2.5.1 Deštruktívne testy 21
2.5.2 Nedeštruktívne testy 21

3 Metodika bezpečnostného testovania smerovačov 23
3.1 Fáza plánovania – Pre-engagement 24
3.1.1 Určenie rozsahu testovania 24
3.1.2 Zber dokumentácie a informácií 24
3.1.3 Preskúmanie zraniteľností odhalených v minulosti . . . 24
3.1.4 Určenie úrovne náročnosti testov 25
3.1.5 Určenie pravidiel 25
3.2 Fáza testovania – Engagement 26
3.2.1 Prieskum 26
3.2.2 Analýza zraniteľností 26
3.2.3 Využitie zraniteľností 26
3.3 Fáza vyhodnotenia – Post Engagement 27
3.3.1 Vrátenie prostredia do pôvodného stavu 27
3.3.2 Dokumentácia nájdených zraniteľností 27
3.3.3 Vyhodnotenie vážnosti zraniteľností 27
3.3.4 Odporúčania na odstránenie zraniteľností 28

4 Zraniteľnosti smerovačov 29
4.1 Útoky na služby vzdialenej administrácie 29
4.1.1 Útoky na Telnet 29
4.1.2 Útoky na SSH 30
4.1.3 Útoky na HTTP 31
4.2 Útoky na UPnP 32
4.2.1 Komponenty UPnP 33
4.2.2 Fungovanie UPnP 33
4.2.3 Útoky na UPnP z lokálnej siete 34
4.2.4 Útok UPnProxy 34
4.2.5 Útok do vnútornej siete pomocou UPnP 35
4.3 Útok na WPA2-PSK 35
4.3.1 WPA2 PSK Handshake 36
4.3.2 Prelomenie WPA2-PSK 37
4.4 WiFi denial of service 38
4.5 Útok DNS Rebinding 38
4.5.1 Politika rovnakého pôvodu v prehliadačoch 39
4.5.2 Scenár útoku 39

5 Praktické testovanie 41
5.1 Fáza plánovania – Pre-Engagement 41

5.1.1 Určenie pravidiel testovania 41
5.1.2 Zber dokumentácie a informácií 42
5.1.3 Určenie rozsahu testovania 42
5.1.4 Prieskum zraniteľností odhalených v minulosti 42
5.1.5 Softwarové testovacie prostredie 42
5.1.6 Testovacie nástroje 43
5.2 Fáza testovania – Engagement 45
5.2.1 Prieskum 45
5.2.2 Analýza zraniteľností 47
5.2.3 Prevedenie útokov 47
5.2.4 Prelamovanie WPA2-PSK 47
5.2.5 Útok na SSH 48
5.2.6 Útok na Telnet 49
5.2.7 Útok na HTTP 49
5.2.8 Útok na UPnP z vnútornej siete 51
5.3 Fáza vyhodnotenia – Post-Engagement 52
5.3.1 Vrátenie prostredia do pôvodného stavu 53
5.3.2 Zraniteľnosť WPA2-PSK 53
5.3.3 Zraniteľnosť SSH 54
5.3.4 Zraniteľnosť Telnet 55
5.3.5 Zraniteľnosť HTTP 56
5.3.6 Zraniteľnosť UPnP 57

Záver **61**

Literatúra **63**

A Zoznam použitých skratiek **71**

B Obsah priloženého CD **75**

Zoznam obrázkov

1.1 Stručná história Common Criteria 9

2.1 Schéma black box testovania 17
2.2 Schéma white box testovania 18

4.1 Varovanie pred neplatným certifikátom 32
4.2 Schéma priebehu 4-way Handshake 36

5.1 Časť výpisu nástroja Hydra 49
5.2 Časť výpisu nástroja Hydra 49
5.3 Časť výpisu komunikácie so smerovačom Zyxel 50
5.4 Časť výpisu komunikácie so smerovačom ADB 51
5.5 Ukážka pridaného záznamu do smerovača Draytek 52
5.6 Časť komunikácie tlačiarne so zariadením v internete 52

Zoznam tabuliek

5.1 Výsledky skenovania smerovača Zyxel 46
5.2 Výsledky skenovania smerovača DrayTek 46
5.3 Výsledky skenovania smerovača ADB 46
5.4 Časť výpisu nástroja Airodump-ng 48
5.5 Odhalené heslá bezdrátových sietí 48

Úvod

Smerovač je sieťové zariadenie, ktoré zariaďuje prenos dát medzi počítačovými sieťami. Kategória SOHO (Small Office / Home Office) smerovačov je určená pre siete vytvárané v domácnostiach alebo menších podnikoch. Oproti modelom určeným na spravovanie väčších sietí sa tieto prístroje vyznačujú nízkou cenou, oveľa väčšou dostupnosťou na trhu, ale aj obmedzenejšou funkcionalitou.

Motivácia k vytvoreniu práce

V dnešnej dobe sa takmer v každej bežnej domácnosti alebo malom podniku nachádza SOHO smerovač, cez ktorý prechádzajú všetky dáta užívateľov pristupujúcich na internet. S príchodom IoT sa do sietí spravovaných SOHO smerovačmi pripájajú rôzne zariadenia ovládateľné cez sieť.

Rozšírenosť použitia týchto zariadení vyvoláva otázku: Nakoľko zabezpečené sú SOHO smerovače a ako bezpečne sa môžu užívatelia cítiť pri využívaní sietí, ktoré sú týmito smerovačmi spravované? Práve táto otázka sa stala motiváciou k vytvoreniu tejto práce.

Ciele práce

Hlavným cieľom práce je zhodnotenie bezpečnosti vybraných SOHO smerovačov. To je dosiahnuté splnením viacerých vedľajších cieľov, ktoré sú:

- oboznámenie sa s existujúcimi bezpečnostnými štandardmi;
- získanie informácií o existujúcich klasifikáciách bezpečnostných testov;
- sformulovanie metodiky bezpečnostného testovania smerovačov;

- preskúmanie známych zraniteľností, ktoré sa môžu vyskytovať na SOHO smerovačoch;
- aplikovanie navrhnutej metodiky a otestovanie rôznych zraniteľností.

Na základe testovania spomenutého v poslednom bode je možné analyzovať nájdené zraniteľnosti a zhodnotiť bezpečnosť testovaných SOHO smerovačov. Práca takto prináša predstavu o aktuálnom stave zabezpečenia na menších lokálnych sieťach a reálne zneužívaných zraniteľnostiach smerovačov.

Štruktúra práce

Práca sa v prvej kapitole zaoberá bezpečnostnými štandardami, pričom sú predstavené najznámejšie štandardizačné organizácie, ktorých štandardy sú dnes všeobecne platné a používané na celom svete. Pozornosť je upriamená na existujúce bezpečnostné štandardy, špeciálne štandardy, ktoré sa zaoberajú bezpečnosťou v rámci počítačových sietí a bezpečnosťou jednotlivých sieťových prvkov.

Druhá kapitola práce predstaví viaceré klasifikácie bezpečnostných testov podľa rôznych kritérií. Ujasní sa, prečo má zmysel zavádzať jednotlivé rozdelenia bezpečnostných testov a v rámci jednotlivých rozdelení budú porovnané výhody a nevýhody testov spadajúcich do danej kategórie.

Kapitola číslo tri popisuje metodiku bezpečnostného testovania smerovačov. Využíva poznatky z predošlých kapitol a vytvára návod na celý priebeh bezpečnostného testovania smerovačov používaných v kanceláriách a domácnostiach. Predstaví, na aké fázy sa testovanie rozdeľuje a aké kroky je potrebné v jednotlivých fázach podniknúť.

Štvrtá kapitola je venovaná najznámejším a najbežnejším zraniteľnostiam SOHO smerovačov. Zatiaľ čo v predošlej kapitole sa predstavuje štruktúra bezpečnostných testov, táto kapitola dodáva ich náplň. Ukazuje sa, akým rôznym rizikám a zraniteľnostiam podliehajú SOHO smerovače a ako sa dajú zneužiť.

V poslednej kapitole sa prakticky použije metodika z kapitoly číslo tri a otestujú sa tri rôzne SOHO smerovače, ktoré sú dnes distribuované do domácností poskytovateľmi internetu. Testovať sa budú vybrané zraniteľnosti zo štvrtej kapitoly. V kapitole sú analyzované výsledky testovania a nájdené zraniteľnosti.

Kapitola 1

Štandardy a kybernetická bezpečnosť

Technický štandard alebo technická norma je dokument vytvorený ako konsenzus uznávaných autorít a expertov, ktorý popisuje parametre, vlastnosti a charakteristiky produktov, prípadne pravidlá pracovných postupov a aktivít. Cieľom vytvárania týchto dokumentov je zabezpečenie konzistencie podstatných vlastností produktov a služieb. Technická norma bežne vzniká pod záštitou nejakej štandardizačnej organizácie, prípadne súkromného subjektu, kde sa stretne skupina odborníkov, aby vypracovali návrh. Potom, čo sa návrh stane oficiálnym dokumentom, začne sa jeho uvádzanie do praxe. [1] Práve podľa toho, kto vytvára tieto dokumenty, sa bežne členia na:

- medzinárodné štandardy
- národné štandardy
- regionálne štandardy
- priemyselné štandardy

Medzinárodné a regionálne štandardy nie sú spravidla záväzné, slúžia viac ako odporúčanie, napriek tomu ide o najrozšírenejší druh štandardov. Tieto dokumenty slúžia aj ako predlohy pri vytváraní jednotlivých národných a priemyselných noriem, kde sa základ prispôsobí potrebám súkromného subjektu alebo zákonom v danom štáte. [2]

Národné štandardy sa obyčajne uplatňujú výhradne na území konkrétneho štátu, kde ich vydávajú a spravujú kompetentné inštitúcie. Existujú však štandardy, ako napríklad FIPS alebo ANSI v USA, ktoré sa aj napriek tomu, že sú národné štandardy, používajú vo veľkom rozsahu aj mimo hraníc štátu. Na rozdiel od medzinárodných a regionálnych štandardov, národné štandardy

zvyknú byť prijímané legislatívou, čím sa stávajú na území daného štátu právne záväzné. [1], [2]

Priemyselné štandardy sú vyvíjané súkromnými subjektami a podobne ako národné štandardy zvyknú čerpať z medzinárodných štandardov a upravovať si ich pre vlastné potreby. Tieto normy sú záväzné v rámci organizácie, poprípade podniku, ktorý ich prijal, pre všetkých zamestnancov. Štandardy, ktoré vytvoria veľké subjekty, sa často stanú nevyhnutnosťou pre tie menšie, aby zaručili kompatibilitu svojich produktov a dokázali sa udržať na trhu. V minulosti sa mnoho priemyselných noriem stalo natoľko rozšírenými a populárnymi, až ich prijali za svoje medzinárodné štandardizačné organizácie. Príkladom niečoho takého sú protokoly SSL/TLS, ktoré boli v minulosti vyvíjané spoločnosťou Netscape a v neskorších verziách boli publikované ako RFC dokumenty. [2]

Existuje veľké množstvo štandardov, ktoré sa zaoberajú informačnými technológiami. Nasledujúce časti kapitoly popisujú rôzne štandardizačné inštitúcie pôsobiace v oblasti IT a nimi publikované štandardy zaoberajúce sa kybernetickou bezpečnosťou.

1.1 International Organization for Standardization

Medzinárodná organizácia pre normalizáciu (anglicky International Organization for Standardization, skrátene ISO) je mimovládne zoskupenie národných normalizačných organizácií. Informácie o tejto organizácií v tejto časti dokumentu sú čerpané primárne z [3]. Každý štát zastupuje práve jedna v ňom pôsobiaca štandardizačná organizácia, ktorá zároveň reprezentuje ISO v danej krajine. ISO je všeobecne považovaná za organizáciu, ktorá vytvára a publikuje nové štandardy, nie sú to však jediné typy dokumentov, ktoré táto organizácia vydáva. Všeobecne sa dajú produkty ISO rozdeliť do týchto kategórií: [4], [5]

ISO štandardy sú hlavným produktom organizácie. Publikujú sa pod názvom vo formáte `ISO[/IEC][/ASTM] IS nnnnn[-p]:[yyyy] Title`, kde údaje v hranatých zátvorkách sú nepovinné, `nnnnn` je číslo dokumentu, `Title` je názov dokumentu, `-p` označuje časť daného dokumentu a `yyyy` označuje rok vydania. Skratky `IEC` pre *International Electrotechnical Commission* a `ASTM` pre *American Society for Testing and Materials* označujú dokumenty, ktoré vznikli v spolupráci s týmito organizáciami. Skratka `IS` (International Standard) slúži na odlíšenie kategórie produktu organizácie.

Technické špecifikácie (ISO/TS) sa vzťahujú na prácu, ktorá je stále v technickom rozvoji alebo sa očakáva, že sa v budúcnosti stane ISO štandardom. Technická špecifikácia je publikovaná pre okamžité použitie a zároveň

za účelom spätnej väzby, na základe ktorej sa môže dokument upravovať a transformovať, aby mohol byť publikovaný ako ISO štandard. Dokumenty tohoto typu sa uverejňujú pod rovnakým názvom ako ISO štandardy, ale *IS* je zamenené za *TS*.

Technické správy (ISO/TR) obsahujú iný typ informácií ako predošlé dva typy dokumentov. Môžu obsahovať dáta z prieskumov, vysvetlenia alebo odporúčania. Publikujú sa pod názvom rovnakého formátu ako ISO štandardy, ale *IS* je zamenené za *TR*.

Verejne prístupné špecifikácie (ISO/PAS) sú publikované ako reakcia na urgentné potreby trhu a reprezentujú konsenzus expertov v pracovnej skupine alebo organizácii. Podobne ako ISO/TS sú publikované s cieľom získať spätnú väzbu a stať sa neskôr ISO štandardom. Verejne prístupné špecifikácie majú však životnosť obmedzenú na 6 rokov, po ktorej sa buď musia stať ISO štandardom alebo zaniknú.

International Workshop Agreements (IWA) sú vytvárané na pracovných stretnutiach organizácií alebo aj súkromných subjektov a nie celou ISO technickou komisiou. Štandardy kategórie IWA sa môžu týkať akejkoľvek problematiky. Podobne ako pri ISO PAS, tieto publikácie majú životnosť 6 rokov, po ktorej sa osvedčia a stanú sa z nich ISO štandardy alebo zaniknú.

ISO návody a príručky slúžia na informovanie čitateľov. Ponúkajú informácie o štandardoch a sférach, kde sa štandardy uplatňujú. Môžu popisovať, ako ISO štandardy pomáhajú robiť prácu lepšie, bezpečnejšie a efektívnejšie.

V rámci informačných technológií sa ISO venuje širokému spektru tém a vydáva dokumenty zaoberajúce sa každým odborom informatiky.

Prvé štandardy, ktoré sa venovali informačnej bezpečnosti boli *ISO/IEC 17799:2000*. Tieto dokumenty vychádzali z predtým existujúcich britských štandardov *BS 7799* publikované organizáciou *British Standards Institution*. Postupom času normy týkajúce sa informačnej bezpečnosti pribúdali, až sa rozhodlo vyhradiť pre ne samostatnú radu 27000. Štandard *ISO Guide 83* z roku 2012 popisuje jednotnú štruktúru a pravidlá pre začlenenie dokumentov do tejto rady. Vybrané normy z tejto rady sú popísané v nasledujúcich podkapitolách. [6]

1.1.1 Norma ISO/IEC 27000

Norma *ISO/IEC 27000:2018* je základná norma tejto rady prvýkrát vydaná v roku 2009, ktorá obsahuje terminologický slovník a zavádza všetky pojmy,

ktoré sú používané v ďalších dokumentoch tejto série. V rámci informačnej bezpečnosti sa používa množstvo pojmov a často sa stáva, že v literatúre alebo dokumentácii rôzni autori používajú rovnaké pojmy v rozdielnom kontexte alebo nevystihnú presne to, čo daný pojem znamená. Toto môže spôsobovať zmätenie čitateľom, ale môže to ovplyvniť celé hodnotenie bezpečnosti a certifikáciu systému. Práve toto bolo motiváciou zjednotiť pojmy na jednom mieste spolu s jednoznačnou definíciou a vymedzením každého termínu. [7]

1.1.2 Norma ISO/IEC 27001

Prvá verzia tejto normy pochádza z roku 2005 a priamo vychádza z britskej normy BS 7799-2, tá posledná a aktuálna verzia je z roku 2013. Cieľom tejto normy je pomôcť s návrhom, nasadením a udržiavaním efektívne fungujúceho systému riadenia bezpečnosti. Implementáciu celého systému riadenia bezpečnosti alebo jeho časti je možné nechať otestovať a získať *certifikát ISO/IEC 27001*. Táto norma obsahuje aj prílohy *A.13.1* a *A.13.2*, ktoré sa zaoberajú bezpečnou komunikáciou. [8]

1.1.2.1 Príloha A.13.1

Táto príloha popisuje požiadavky kladené na bezpečnostné mechanizmy za účelom ochrany informácií a prvkov, ktoré ich spracovávajú. V rámci celkového zabezpečenia systému je nutné splniť požiadavky tejto prílohy, pokiaľ je cieľom získať certifikáciu *ISO 27001*. Príloha ohsahuje tri časti, v ktorých sa píše, že sieť má byť spravovaná a kontrolovaná za účelom ochrany informácií. Od prevádzkovateľa alebo majiteľa je požadované, aby vynaložil patričné prostriedky a úsilie na zabezpečenie ochrany, pričom treba zvážiť najmä nasadenie firewallu, verifikáciu koncových zariadení, intrusion detection, intrusion prevention, access control listy a segregáciu siete na fyzickej aj logickej úrovni. [9]

1.1.2.2 Príloha A.13.2

Príloha A.13.2 sa zaoberá prenosom informácií. Cieľom tejto prílohy je udržať dôvernosť informácií prenášaných v rámci organizácie alebo pri kontakte s externou entitou ako dodávateľ či zákazník. Prenos informácií v tomto dokumente nie je obmedzený len na elektronickú komunikáciu, ale ustanovujú sa všeobecné zásady a praktiky, ktoré je potrebné dodržiavať pri akomkoľvek komunikačnom médiu. [9]

1.1.3 Norma ISO/IEC 27033

Norma *ISO/IEC 27033* vznikla úpravami a modernizáciou pôvodnej normy *ISO/IEC 1828*. Cieľom tejto normy je poskytnúť podrobné rady a informácie ohľadne bezpečnostných aspektov spravovania, prevádzkovania a prepájania

sietí. Dokument sa vzťahuje na bezpečnosť a správu sieťových zariadení, sieťových služieb, aplikácií a používateľov siete. Celá norma je rozdelená na 6 častí a je relevantná pre kohokoľvek, kto navrhuje, vlastní, prevádzkuje alebo používa sieť. [10]

1.1.3.1 Norma ISO/IEC 27033-1:2015

Norma *ISO/IEC 27033-1:2015* je oporou pre ďalšie časti normy *ISO/IEC 27033*. [10] Obsahuje:

- slovník pojmov relevantných pre sieťovú a informačnú bezpečnosť;
- prehľad a informácie o tom, čo je možné nájsť v nasledujúcich častiach;
- informácie na vytvorenie si prehľadu o konceptoch spojených s bezpečným prevádzkovaním sietí;
- návody na identifikáciu a analýzu bezpečnostných rizík a na základe tejto analýzy definuje požiadavky na zabezpečenie siete;
- popis požiadaviek z triády *CIA* (confidentiality – dôvernosť, integrity – integrita, availability – dostupnosť) a pridáva k nim reliability – spoľahlivosť a non-repudiation – nepopierateľnosť.

1.1.3.2 Norma ISO/IEC 27033-2:2012

Druhá časť normy ISO/IEC 27033 obsahuje návody a pokyny pre dizajn a implementáciu sieťovej bezpečnosti. Definuje bezpečnostné architektúry sietí a implementácie takýchto architektúr, ktoré zabezpečia sieťovú bezpečnosť primeranú prostrediu, do ktorého sú nasadzované. [10], [11]

1.1.3.3 Norma ISO/IEC 27033-3:2010

Tretia časť normy ISO/IEC 27033 popisuje hrozby a riešenia problémov spojených s prevádzkovaním siete. Pre rôzne návrhy sietí sa v tomto dokumente nachádzajú popisy konkrétnych hrozieb a popis techník a protiopatrení, aby sa týmto hrozbám predišlo. [10]

1.1.3.4 Norma ISO/IEC 27033-4:2014

V štvrtej časti normy ISO/IEC 27033 sa nachádzajú návody na zabezpečenie komunikácie medzi sieťami. Pokiaľ dochádza ku komunikácii medzi dvomi sieťami, v každej sa nachádzajú brány, body, cez ktoré všetky dáta v rámci komunikácie medzi danými sieťami prechádzajú. Dokument popisuje rôzne prostriedky ako analyzovať tok dát prúdiaci cez brány a zabezpečiť tento bod pomocou firewallov, IPS (Intrusion Prevention System) alebo aplikačných

firewallov. Vysvetľuje sa v ňom, ako by mali tieto technológie analyzovať a kontrolovať dátový tok s využitím metód ako filtrovanie paketov, NAT, analýza a filtrovanie obsahu dát, SPI (Stateful Packet Inspection), application proxy. [10], [11]

1.1.3.5 Norma ISO/IEC 27033-5:2013

Piata časť normy ISO/IEC 27033 rozširuje štandard ISO/IEC TR 13335. Dokument sa zaoberá zabezpečením sieťovej komunikácie a vzdialeného prístupu pomocou virtuálnej privátnej siete – VPN. Uvádza a popisuje viaceré druhy vzdialeného prístupu a protokoly, ktoré je možné nasadiť. Zároveň je možné nájsť rozbor hrozieb pre VPN, ktorý však nie je kompletný. Nachádzajú sa tam informácie o Denial of Service útokoch, preniknutí skrz VPN, ale chýbajú tam informácie ohľadom neautorizovaného monitorovania toku dát, úmyselnom poškodzovaní dát alebo vkladaní falošných dát. Cieľovou skupinou sú najmä administrátori, ktorí používajú alebo sa chystajú používať tento typ pripojenia a potrebujú radu ohľadne bezpečného nastavenia a prevádzkovania. [10], [11]

1.1.3.6 Norma ISO/IEC 27033-6:2016

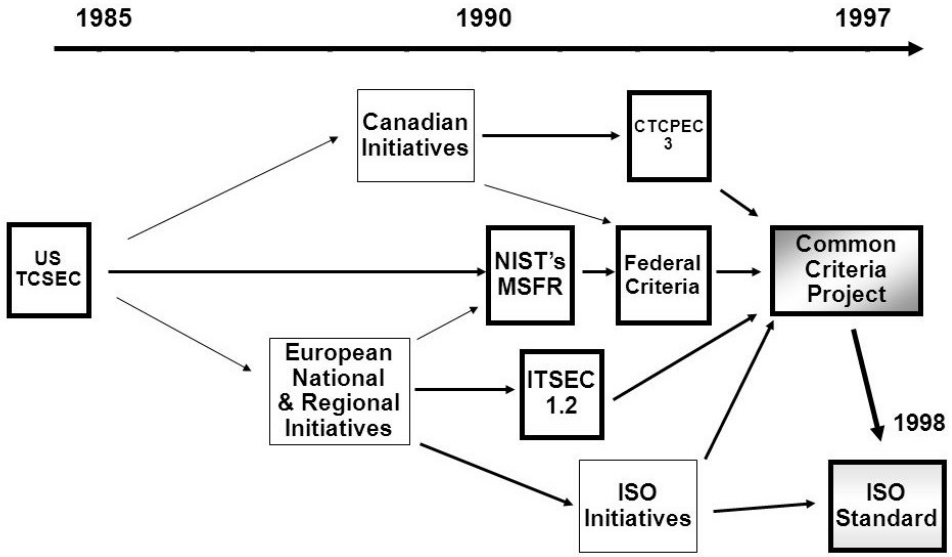
Posledná časť normy ISO/IEC 27033 sa zaoberá zabezpečením bezdrátových sietí ako napríklad WiFi, Bluetooth alebo mobilných sietí. Ponúka základné rady ohľadom bezpečného používania týchto sietí a zoznam hrozieb a scenárov útokov. [10]

1.2 Common Criteria

Pred dvadsiatimi rokmi existovali v rámci celého sveta mnohé štandardy a frameworky na vyhodnocovanie bezpečnosti produktov a technológií v oblasti IT. V Európe boli používané ITSEC štandardy vyvíjané Francúzskom, Nemeckom, Holandskom a Britániou, v rámci USA sa používali TCSEC štandardy (publikované v auguste 1983), často nazývané ako *Orange Book* a v Kanade boli zase CTCPEC štandardy, ktoré boli odvodené z TCSEC štandardov. V strede 90tych rokov začali vyššie spomínané štáty spolupracovať na vytvorení jednotných štandardov na posudzovanie bezpečnosti IT produktov. Cieľom bolo vyhnúť sa niekoľkonásobnému testovaniu produktov, ktoré prechádzali medzinárodným trhom, ktoré bolo predtým nevyhnutné. V roku 1994 boli publikované dokumenty Common Criteria verzia 1.0 ako výsledok snahy o zjednotenie predošlých štandardov.

V snahe o výraznejšie medzinárodné presadenie a zvýšenie počtu participujúcich krajín sa Common Criteria v roku 1999 stali ISO štandardom s identifikátorom ISO/IEC 15408. Ten zodpovedá verzii 2.1 dokumentu Common

Criteria. Dnes je aktuálna verzia 3.1 revízia 5, ktorá bola vydaná v apríli 2017 a vo svete ju podporuje celkovo 26 krajín. [12], [13]



Obr. 1.1: Stručná história Common Criteria podľa [14]

Common Criteria (CC) je zbierka medzinárodne uznávaných technických štandardov, ktoré poskytujú framework umožňujúci posudzovanie a vyhodnocovanie bezpečnosti produktov a technológií v oblasti IT. [15] Medzi hlavné ciele CC patrí:

- zabezpečenie, že vyhodnocovanie bezpečnosti produktov v oblasti IT prebieha podľa prísnych a konzistentných štandardov, čo prispeje k zvýšeniu dôvery v bezpečnosť týchto produktov;
- odstránenie potreby duplikátneho testovania rovnakých IT produktov v rámci sveta;
- zlepšenie efektívnosti a zníženie nákladov na vyhodnocovanie bezpečnosti a certifikácie IT produktov.

1.2.1 Kľúčové pojmy definované v Common Criteria

Terminológia zavedená a používaná v dokumentoch Common Criteria je esenciálna pre pochopenie a používanie frameworku. Nasledujúca časť práce rozoberá kľúčové pojmy, s ktorými CC pracuje.

1.2.1.1 TOE

CC sú veľmi flexibilné pokiaľ ide o to, čo sa vyhodnocuje a testuje. Preto zavádza pojem *Target of Evaluation* (TOE), ktorým označuje cieľ testovania. Môže ísť o software, hardware, firmware, vrátane návodov na používanie a prevádzkovanie. TOE môže byť jeden konkrétny IT produkt, jeho časť alebo dokonca aj niekoľko skombinovaných produktov. [16] Medzi najčastejšie príklady TOE patria:

- softwarové aplikácie,
- operačné systémy,
- softwarové aplikácie v kombinácii s operačným systémom a pracovnou stanicou,
- čipové karty,
- integrovaný obvod,
- kryptografické koprocesory,
- lokálna sieť vrátane všetkých staníc, serverov a sieťových prvkov.

1.2.1.2 ST

Security Target, alebo skrátene ST, je dokument, ktorý vymedzuje rozsah TOE a špecifikuje jeho detaily. Dokument ST obsahuje kompletný a podrobný popis bezpečnostných problémov daného TOE, vrátane hrozieb, funkčné bezpečnostné požiadavky a požiadavky na garanciu úrovne bezpečnosti. ST vytvára výrobca alebo predajca daného produktu. [16]

1.2.1.3 PP

Zatiaľ čo ST popisuje špecifické TOE, dokument nazývaný *Protection Profile* (PP) je vytváraný za účelom popísať typ TOE a všeobecné bezpečnostné požiadavky, ktoré sú na dané TOE kladené. Preto môže byť jeden PP použitý pre mnoho rôznych ST v rámci rôznych, nezávislých testovaní. Príkladom pre PP môže byť firewall, antivirus, operačný systém... [16]

1.2.1.4 EAL

Evaluation Assurance Level, skrátene EAL, je stupnica hodnotiaca garanciu zabezpečenia daného TOE. Rozpätie tejto stupnice je od 1 do 7, pričom čím vyšší level TOE dosiahne, tým väčšiu dôveru poskytuje, že jeho bezpečnostné prvky sú implementované spoľahlivo a efektívne. Spolu s vyššími úrovňami pribúda množstvo testov, a teda rastie cena testovania aj náklady na vytvorenie TOE, ktorý má spĺňať danú úroveň. Je dôležité si uvedomiť, že EAL

nevypovedá priamo o bezpečnosti TOE, ale o úrovni a rozsahu testov. Informácie o EAL v tomto odstavci a jednotlivých úrovniach, ktoré sú opísané v nasledujúcom texte, sú čerpané z [17].

1.2.2 Úrovne EAL

EAL1 je úroveň, kde sa robí funkčné testovanie, aplikovateľné na TOE, kde je požadovaná istota v korektné fungovanie, ale bezpečnostné hrozby nie sú vážne. Testuje sa najmä správanie sa TOE a jeho rozhraní v porovnaní s dodanou dokumentáciou.

EAL2 je úroveň, kde sa robí štruktúrne testovanie a vyžaduje si oproti EAL1 aj spoluprácu vývojára. Ten musí dodať potrebnú dokumentáciu, ktorá by mala obsahovať popis bezpečnostnej architektúry, spraviť testy funkčnosti a dodať ich výsledky. Okrem testov je robená aj analýza zraniteľností ukazujúca odolnosť voči útokom.

EAL3 je úroveň, kde sa robí metodické testovnie s kontrolou, ktoré vie poskytnúť svedomitému vývojárovi istotu v bezpečnostné prvky zakomponované už v návrhu TOE, bez nutnosti robiť závažné zmeny v architektúre. Testy sú oproti EAL2 podrobnejšie, s väčším pokrytím a zameraním na bezpečnostné procedúry a mechanizmy.

EAL4 je úroveň, kde sa metodicky navrhuje, testuje a kontroluje TOE. Pri návrhu sa dbá na zaužívané bezpečnostné praktiky, ktoré však nevyžadujú znalosti alebo zručnosti špecialistu. EAL4 je najvyššia úroveň, kedy je ekonomicky prijateľné robiť zásadné zmeny v už existujúcom produkte tak, aby spĺňal túto úroveň. Vďaka omnoho rozsiahlejším testom, podrobnejšej dokumentácii a požiadavkám na bezpečnostné mechanizmy zvyšuje táto úroveň oproti predošlej dôveru v zabezpečenie. Práve na tejto úrovni sú testované bežné, komerčné, operačné systémy ako Windows alebo niektoré Linuxové distribúcie.

EAL5 je úroveň, kde sa vyžaduje semi-formálny návrh a testovanie. Okrem použitia bežných bezpečnostných praktík vývojárom je vývoj TOE podporený základnými technikami vyžadujúcimi vzdelanie špecialistu. Takýto TOE je väčšinou už od začiatku navrhovaný tak, aby dosiahol úroveň EAL5, čo sa spája s mierne zvýšenými nákladmi na vývoj. V porovnaní s EAL4 je vďaka semi-formálnemu návrhu a viac štrukturovanej architektúre možná lepšia analýza bezpečnostných rizík a testovanie zahŕňa aj základné penetračné testy. Túto úroveň dosahuje mnoho bežných čipových kariet.

EAL6 je úroveň, kde sa vyžaduje semi-formálne overený návrh a testovanie. Pri návrhu sú použité pokročilé techniky vyžadujúce odborné vedomosti

a v rámci testovania sú zahrnuté dôkladné a rozsiahle penetračné testy. Pre túto skutočnosť sú náklady na návrh a vývoj značne zvýšené. Táto úroveň je vyžadovaná u TOE, ktoré chránia cenné aktíva alebo sú nasadené v rizikových a chúlostivých miestach, kde sú zvýšené náklady oprávnené. Už od začiatku navrhovania je nutné brať do úvahy, že TOE má dosiahnuť úroveň EAL6. Túto úroveň dosahujú niektoré čipové karty a systémy reálneho času. [18]

EAL7 je najvyššia úroveň, ktorá vyžaduje formálne overený návrh a testovanie. Podobne ako pri EAL6 je potrebné zvážiť, či zvýšenie nákladov spojené s dosiahnutím tejto úrovne je opodstatnené. Praktické využitie EAL7 je značne obmedzené na TOE s úzko zameranou bezpečnostnou funkcionalitou. EAL7 dosahujú jednosmerné komunikačné systémy – dátové diódy. [18]

1.3 Bezpečnostné štandardy v Českej republike

V rámci Českej republiky je za tvorbu, vydávanie a distribúciu noriem zodpovedná *Česká agentura pro standardizaci*, skrátene ČAS. Normy vydávané ČAS sa nazývajú české technické normy (ČSN) a zaradením patria medzi národné normy. Dokumenty vydávané ČAS sú buď pôvodné české technické normy alebo prevzaté Európske či medzinárodné normy. [19], [20]

Pôvodné české technické normy tvoria približne 10 % z celkovej ročnej produkcie noriem v ČR. Ich názov je vo formáte `ČSN triediaci_znak`, napr. ČSN 73 4301. [20], [21]

Prevzaté európske a medzinárodné normy tvoria zvyšných 90 % ročnej produkcie noriem v ČR. Prijatím takýchto noriem sa rušia pôvodné normy, ktoré sa stávajú zastaralé alebo sú konfliktné s novoprijatými dokumentami. Tieto normy sa označujú sa ako `ČSN číslo_prevzatej_normy triediaci_znak`, napr. ČSN ISO 11083 (757424). Niektoré európske a medzinárodné normy sa preberajú v originálnom jazyku a iné sa prekladajú do češtiny. [20], [21]

Triediaci znak sa skladá zo šiestich číslic vo formáte `XX YYZZ` a slúži na klasifikáciu noriem v rámci tried a skupín. Dvojčíslie `XX` označuje triedu 1 až 99, ktoré pomenúvajú všeobecné kategórie, kam norma môže spadať. Dvojčíslie `YY` označuje skupinu v rámci triedy, ktorá viac špecifikuje problematiku, ktorou sa dokument zaoberá. Posledné dvojčíslie `XX` je poradové. [20]

Technické normy zaoberajúce sa informačnými technológiami spadajú do triedy číslo 36 – elektrotechnika a do skupín 90–99. Najpodstatnejšie normy, ktoré rozoberajú sieťovú bezpečnosť, sú prevzaté ISO normy zo série ISO/IEC 27000, ktoré boli popísané v kapitole 1.1.1, napríklad ČSN ISO/IEC 27033 (369701). [22]

Kapitola 2

Bezpečnostné testovanie

Bezpečnostné testovanie je proces, ktorého úlohou je odhaliť chyby v bezpečnostných mechanizmoch systémov, počítačových zariadení, hardwarových komponentov, sietí alebo aplikácií (ďalej len testovaných objektoch). [23] Tieto testy simulujú reálne útoky a pokusy o kompromitáciu systému s cieľom analyzovať zraniteľnosti, softwarové alebo hardwarové nedostatky a možné následky v prípade prekonania testovaných bezpečnostných mechanizmov.

Celý proces testovania prebieha z pohľadu potenciálneho útočníka, ktorý sa snaží zneužiť nedostatky v zabezpečení s cieľom získať neoprávnený prístup k informáciám, sfalšovať informácie alebo zneprístupniť testovaný objekt, prípadne jeho časti, užívateľom. Výsledky, nálezy a návrhy protiopatrení na zvýšenie zabezpečenia sa následne spíšu do správy, ktorá je prezentovaná subjektu, ktorý o testy požiadal. [23]

Je dôležité si uvedomiť hneď na začiatku, že tieto testy nikdy nezaručia, že v testovanom objekte neexistujú zraniteľnosti, ktoré by sa dali zneužiť, ani nepotvrdia, či je systém absolútne bezpečný. [23] Bežne sa testujú len vybrané typy útokov a zraniteľností, pričom záleží na rozsahu testov, koľko toho pokryjú. Nič však nezaručuje, že útočník neodhalí a nevyužije zraniteľnosť, ktorá nebola testovaná, alebo že je útočník inovatívny a nepríde s úplne novým útokom, na ktorý neboli testy zamerané, lebo sa o existencii zraniteľnosti nevedelo.

2.1 Druhy testov z hľadiska rozsahu

Pri bezpečnostnom testovaní je podstatné vymedzenie rozsahu testov kvôli jednoduchšiemu rozvrhnutiu postupu testovania a rozdelenia testov na menšie, preveditelné časti. Druhý dôvod takéhoto vymedzovania sú financie. Každý, kto chce nechať nejaký testovaný objekt podrobiť bezpečnostným testom,

si kladie iné nároky na celkovú bezpečnosť, pričom väčší rozsah testov je spravidla spojený s vyššou cenou testovania.

2.1.1 Skenovanie zraniteľností

Skenovanie zraniteľností spočíva v hľadaní už známych zraniteľností v rámci testovaného objektu. V prípade lokálnej siete sa skenujú sieťové zariadenia ako napríklad smerovače alebo prepínače, hľadajú sa otvorené porty, ktoré by bolo potenciálne možné zneužiť na útok, testuje sa firewall ... Iné testy skúmajú predvolené heslá alebo chýbajúce bezpečnostné aktualizácie. Tieto testy sú zväčša automatizované a existujú rôzne špecializované nástroje, ktoré pracujú s databázou známych zraniteľností. Vzhľadom na to, že sa pravidelne objavujú nové možnosti útokov a popisujú sa nové zraniteľnosti, je nutné udržiavať tieto testovacie nástroje aktualizované a skenovanie pravidelne opakovať.

Výsledky skenovania sú spísané do správy, ktorá je potom podaná na zhodnotenie kompetentnému administrátorovi alebo testerovi. Správa nezhodnocuje vážnosť nálezov a ani nezaručuje, že všetky nájdené problémy sú skutočne hrozby. [24] Skenovacie nástroje môžu napríklad nájsť slabé heslo v databáze, ale nevedia zhodnotiť, či by jeho prezradením bola ohrozená funkčnosť systému, alebo len bežného užívateľského účtu bez vyšších privilégií. Iný prípad je, keď skenovacie nástroje nahlásia možnú zraniteľnosť, tester ju preverí a zhodnotí, že nie je možné toto miesto zneužiť. Pre tieto dôvody je nutné správy preveriť, zhodnotiť vážnosť každého nálezu a prípadne zabezpečiť nápravu.

2.1.2 Penetračné testy

Na rozdiel od predošlého skenovania zraniteľností, penetračné testy simulujú reálne útoky na testovaný objekt (tzv. white hat hacking – etické testovanie) pričom sa tester snaží získať prístup k dátam, zvýšiť si privilégiá alebo testovaný objekt vyradiť z prevádzky. [24] Pred penetračnými testami zvykne prebehnúť skenovanie zraniteľností, ktoré môže slúžiť ako počiatočný bod útokov. Potom pomocou jednej alebo kombináciou viacerých zraniteľností sa prevedie útok na systém so snahou prelomiť čo najviac bezpečnostných mechanizmov. Po ukončení útoku prebehne analýza vážnosti a dopadu útoku. Výsledkom je správa, v ktorej sa popisuje, čo umožnilo útok uskutočniť, priebeh útoku, dopad na testovaný objekt (aké dáta sa dajú získať, na ako dlho sa dá objekt vyradiť z prevádzky...) a návrh nápravy zraniteľnosti.

Penetračné testy nie je potrebné robiť tak často ako skenovanie zraniteľností. [24] Je len niekoľko momentov, kedy je ich nutné vykonať:

- pri uvedení testovaného objektu do prevádzky;

- pri zavádzaní nových komponentov a rozširovaní;
- po veľkých zmenách a softwarových aktualizáciách;
- po odhalení prelomenia alebo úniku informácií.

Zatiaľ čo na skenovanie zraniteľností stačí vedieť používať automatizované nástroje a posudzovať vážnosť nálezov, pri penetračných testoch je vyžadovaná hlboká znalosť fungovania systému a kreativita. To sa premietne do času, ktorého je treba niekoľkokrát viac ako na skenovanie zraniteľností. Keďže potrebné znalosti na kvalitné penetračné testovanie sú značne rozsiahle, obyčajne sa najíma tretia strana, ktorá sa špecializuje na túto problematiku a zhromažďuje ľudí s potrebnými znalosťami.

2.1.3 Social engineering

Celkom iným smerom sa uberajú testy a útoky zamerané na metódy Social Engineeringu. Priamym cieľom útokov nie je testovaný objekt, ale ľudia, ktorí majú k nemu prístup alebo ho spravujú. Ide o spôsob manipulácie týchto ľudí k tomu, aby vykonali akciu, ktorá kompromituje bezpečnosť testovaného objektu alebo snahy získať od nich užitočné informácie, čo taktiež v konečnom dôsledku povedie ku kompromitácii bezpečnosti aj veľmi kvalitne zabezpečeného testovaného objektu. [25] Existuje viacero spôsobov ako získať citlivé informácie, medzi tie najrozšírenejšie patria tieto:

- phishing
- baiting
- impersonation

Phishing je technika, ktorá vedie k získaniu citlivých alebo osobných údajov ako prihlasovacie údaje, PIN kód k platobným kartám, číslo kreditnej karty, rodné číslo... [25] Pomocou elektronickej komunikácie (e-mail, správy na sociálnej sieti) pošle útočník odkaz na falošnú stránku, ktorá je však takmer identická s tou, za ktorú sa vydáva. Po tom, čo sa adresát skúsi prihlásiť alebo zaregistrovať na podvrhnutú stránku, útočník získa prihlasovacie údaje adresáta, ktoré môže ďalej zneužívať.

Baiting je metóda, ktorej základnými predpokladmi sú zvedavosť alebo chamtivosť ľudí. Útočník niekde na vhodné miesto podstrčí návnadu v podobe USB alebo CD, ktoré je neoznačené a nálezca si ho vezme a zapojí do počítača. Druhým scenárom je, že USB/CD je označené nejakým známym logom a názvom softwaru a nálezca si ho znova zapojí do počítača s tým, že dostane zdarma nový software. Hneď po zapojení do zariadenia sa nainštaluje malware, ktorý môže fungovať ako trójsky kôň, vytvoriť bránu z internetu

do lokálnej siete a odovzdať kontrolu útočníkovi bez toho, aby o tom nálezca vedel. [25]

Impersonation je vydávanie sa za inú osobu s cieľom získania neoprávneného prístupu alebo privilegovaných informácií. [26] Medzi bežné podvody patrí vydávanie sa za administrátora alebo správcu siete, systému alebo webovej aplikácie a požadovanie prihlasovacích údajov pod zmyslenou zámienkou. Ďalšou možnosťou je vydávanie sa za zamestnanca firmy s cieľom získať prístup do firemnej siete.

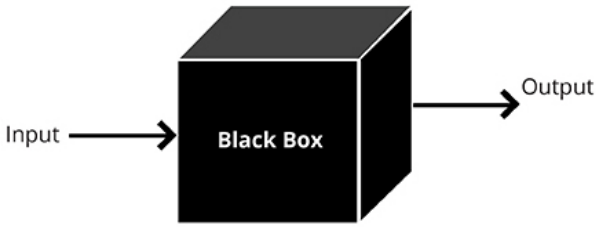
Aby testovaný objekt prešiel úspešne bezpečnostnými testami tohoto typu je potrebné dodržiavať viacero zásad. Najdôležitejšou je správne rozvrhnutie privilégií – každý užívateľ má mať minimálne potrebné privilégiá, aby v prípade zneužitia jeho osobných údajov nedošlo k veľkej škode. Administrátorov aj bežných užívateľov či zamestnancov je potrebné informovať o týchto útokoch, aby si boli vedomí rizík a následkov. Zatiaľ čo bežným užívateľom mnohokrát stačí posielať informačné e-maily o tom, že nemajú nikdy nikomu dávať svoje prihlasovacie údaje, užívateľom s vyššími privilégiami je vhodné poskytnúť školenie venované tejto problematike.

2.2 Druhy testov podľa znalosti informácií o systéme

Je bežné, že mnoho útokov by nebolo možné realizovať bez znalostí špecifických informácií o testovanom objekte, jeho implementácii alebo nasadení. Aby bolo testovanie dostatočne komplexné, je potrebné uvažovať aj nad možnosťami, že útočník sa (napríklad metódami sociálneho inžinierstva alebo pomocou iného útoku) dostal k informáciám, na ktoré nemal oprávnenie. Práve preto sa pre každý test vytvára model, v ktorom sa na začiatku určí, aké informácie má a nemá útočník k dispozícii. Bežne platí, že čím viac má útočník informácií o testovanom objekte, tým sú jeho útoky efektívnejšie zamerané a tým väčšiu šancu má na úspešný útok. Testy môžeme všeobecne rozdeliť do troch hlavných kategórií, podľa toho, koľko vieme o testovanom objekte na začiatku.

2.2.1 Black box testy

Pri black box testoch sa k celému testovanému objektu stavia ako ku čiernej krabičke, do ktorej tester nevidí a nič o nej nevie. Nemá prístup k dokumentácii systému alebo zariadenia, nie je mu známa implementácia a ani vnútorná štruktúra. Jediné, čo mu je známe je, čo má celý systém robiť a ako sa má správať.



Obr. 2.1: Schéma black box testovania dostupná z [27]

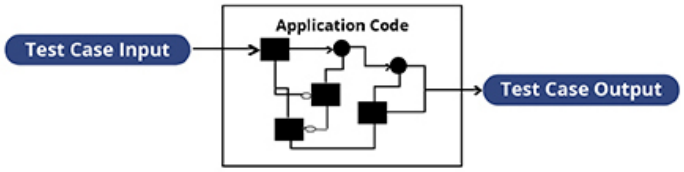
[28] Počas black box testov sa tester snaží odhaliť najmä tieto nedostatky a zraniteľnosti:

- chyby grafického rozhrania,
- chyby pri inicializácii alebo ukončení,
- chybné výstupy pre korektné vstupy,
- chybné reakcie na nekorektné vstupy.

Zatiaľ čo niektoré nedostatky môžu byť len užívateľsky nepríjemné, iné môžu vážne ohroziť celý systém. Predpokladajme zadanie príliš dlhého alebo zložitého vstupu do systému, vďaka ktorému systém zlyhal, poprípade mu trvá niekoľko minút spracovať náš vstup. Takéto správanie otvára možnosti pre útoky typu Denial of Service (podrobnosti v kapitole 4.4). Ďalším príkladom môže byť, že po chybnom vstupe systém poskytne chybovú hlášku (ako napríklad chybový výpis priamo z databázy), na základe ktorej je možné vyvodiť nové informácie o systéme, ktoré predtým neboli známe ani k dispozícii.

2.2.2 White box testy

White box testy sú presným opakom black box testov. To znamená, že všetky potrebné informácie o testovanom objekte sú prístupné. K dispozícii je dokumentácia, je známa implementácia, a to až do takej miery, že je plný prístup k zdrojovému kódu a je známa celá vnútorná štruktúra, ktorá bežnému užívateľovi prístupná nie je. [29]



Obr. 2.2: Schéma white box testovania dostupná z [30]

White box testy sú komplexnejšie a časovo aj vedomostne náročnejšie ako black box testy. Vyžadujú si znalosť programovacieho jazyka, vďaka ktorej je možná podrobná analýza kódu. [29] Z tejto analýzy potom tester dostane možné nedostatky, ktoré potom môže testovať ako pri black box testoch, ale tentoraz už s vstupmi cielenými na slabé miesta. Prístup ku všetkým potrebným informáciám o testovanom objekte umožní komplexnejšie testy, ktoré môžu odhaliť chyby, ktoré by boli pri black box testoch ťažko nájditeľné.

2.2.3 Gray box testy

Posledný typ testov z hľadiska znalosti informácií o testovanom objekte sú gray box testy. Ide o kombináciu predošlých dvoch typov testov, teda máme prístup k informáciám, ako napríklad použité algoritmy, časti vnútornej štruktúry (napríklad použitý typ databázy) alebo dokumentácia, ale zďaleka nemáme prístup ku všetkým informáciám. To nám umožňuje vytvárať oveľa efektívnejšie zamerané testy ako pri black box testoch na základe limitovaných informácií, ktoré nám boli poskytnuté. Tieto testy môžu zahŕňať aj metódy reverzného inžinierstva a použitie dynamickej analýzy kódu na zistenie hraničných hodnôt alebo preskúmanie chybových výpisov. [31]

2.3 Druhy testov z pohľadu prístupu

Každý útok má inú sadu predpokladov, a teda aj každý test bude mať iné počiatočné predpoklady. Nasledujúca podkapitola je zameraná na to, ako sa budú testy líšiť podľa toho, aký je prístup k testovanému objektu.

2.3.1 Fyzický prístup

Prvým možným typom prístupu k testovanému objektu je fyzický prístup. Predpokladáme, že testerovi aj potenciálnemu útočníkovi je umožnené manipulovať s hardwarovými časťami testovaného objektu, a teda je aj možné pripájať do portov rôzne periférie. Medzi najrozšírenejšie hrozby dnes patrí pripájanie USB kľúčov, ktoré spustia priamo na zariadení, v ktorom sú

pripojené, škodlivý kód, poprípade keylogger, alebo tzv. USB Killery, ktoré do zariadenia vypustia elektrický impulz s vysokým napätím, čím trvalo fyzicky poškodia zariadenie. [32] V prípade, že je k zariadeniu pripojený celý počítač, môže dôjsť k neoprávnenému získaniu privilégií – napríklad pripojenie počítača k smerovaču, kde síce je zabezpečená vzdialená administrácia, ale konzolový prístup nie je zabezpečený vôbec alebo len slabo.

2.3.2 Prístup z lokálnej siete

V prípade, že je umožnený prístup do lokálnej siete, je možné vidieť zariadenia do nej pripojené, a teda sú známe IP adresy týchto zariadení. Lokálna sieť je pre mnohých užívateľov aj administrátorov vnímaná ako bezpečná zóna, ktorá je zabezpečená proti útokom z internetu a zároveň je zabezpečený prístup do siete silným heslom. Kvôli tomu skoro všetky zariadenia ponúkajú konfiguráciu s vyšším stupňom dôvery k zariadeniam v rovnakej sieti. Ak však útočník prelomí heslo (ak nebolo dostatočne silné), získa heslo nejakými metódami sociálneho inžinierstva alebo už mal prístup do siete predtým (zamestnanec/bývalý zamestnanec má prístupy do firemnej siete), tak môže všetky útoky realizovať z lokálnej siete, ktorá je však považovaná za bezpečnú zónu, takže zabezpečovacie mechanizmy nebudú veľké.

2.3.3 Prístup z internetu

V porovnaní s predošlými dvomi typmi prístupov, prístup z internetu neviaže útočníkov na určitú geografickú lokáciu, ale môžu útočiť kdekoľvek zo sveta. Tým sa samozrejme zvyšuje počet potenciálnych útočníkov a teda aj riziko nájdenia nejakej zraniteľnosti, ktorá nebola nájdená počas testov. Na druhej strane, lokálne siete a zariadenia v nich sú oveľa viac chránené a nedôverčivé pri komunikácii so subjektami z internetu. Veľakrát je nutné prekonávať viacero zábran, ktoré potenciálne útoky buď komplikujú alebo sa snažia cielene testovaný objekt chrániť.

Pokiaľ útočník chce útočiť z internetu do lokálnej siete, stretne sa s prvým takýmto problémom, a to NAT (preklad sieťových adries). Je normálne, že zariadenia v lokálnej sieti nemajú verejné IP adresy, ale len gateway má jednu verejnú adresu, cez ktorú prechádza všetka sieťová premávka smerujúca z/do lokálnej siete. Útočník teda nevie, aké majú cieľové zariadenia IP adresy. NAT je všeobecne považovaný za prirodzený firewall, avšak neplní jeho úlohu. Firewall slúži ako filter a kontrola samotného toku dát pomocou špecifických pravidiel, ktoré si aj sám užívateľ vie nastaviť, NAT len robí preklad IP adries a portov, bez hlbšej kontroly samotných dát a pôvodne ani nebol navrhnutý ako bezpečnostný mechanizmus. Druhou prekážkou, ktorá sa nasadzuje medzi lokálnu sieť a internet je práve spoinaný firewall. Aby sa teda potenciálnemu útočníkovi znížili šance na úspech ešte viac, pridávajú sa ďalšie bezpečnostné

prvky ako napríklad proxy server.

Dnes funguje väčšina sietí na IPv4 protokole, avšak postupne sa pre nedostatok adries prechádza na IPv6. Keďže v IPv6 je 2^{128} IP adries, nie je potrebné mať jednu verejnú adresu pre bránu, ale každé zariadenie v sieti dostáva svoju verejnú IPv6 adresu. Týmto sa stráca zmysel pokračovať s prekladom sieťových adries, ale zároveň s tým aj zmizne prirodzená ochrana pred útočníkmi, keďže je jednoduchšie zistiť adresy zariadení, ktoré sú pripojené do lokálnej siete. Na druhej strane, bežnou praktikou je v IPv6 vytvárať najmenšie siete o veľkosti /64, čo zodpovedá 18 446 744 073 709 551 616 adresám. [33] Týmto sa pre automatické nástroje stráca využitie, pretože je príliš časovo náročné poslať požiadavky na také množstvo adries a čakať na odpovede. Zároveň je pre útočníka komplikované ostať pri toľkých požiadavkách nepovšimnutý firewallom, ktorý môže bežať na sieti.

Ak sa útočník nepotrebuje dostať do lokálnej siete, problém s NAT zmizne, avšak stále môže pretrvávať problém s firewallom. V tomto scenári sa útočník buď snaží vytvoriť DoS alebo DDoS útoky na systém a zneprístupniť ich pre iných užívateľov alebo sa snaží zneužiť neošetrené miesta pre užívateľský vstup s rôznymi následkami vedúcimi zväčša k získaniu privilegovaných dát.

2.4 Druhy testov z pohľadu automatizácie

Počas bezpečnostného testovania sa vykonáva veľké množstvo testov pre viacero rôznych scenárov útokov, niektoré sú veľmi jednoduché a slúžia väčšinou na kontrolu základných vlastností, iné sú pomerne komplikované. Preto je vhodné rozlišovať testy, ktoré sa dajú automatizovať, a tie, ktoré sa naopak automatizovať nedajú, lebo vyžadujú špecifický prístup.

2.4.1 Automatizované testy

Ak je potrebné opakovane spúšťať veľké množstvo testov, napríklad pri testovaní vstupov alebo sily hesiel, je veľmi neefektívne spúšťať každý test ručne. Preto sa vytvárajú testovacie skripty s dopredu preddefinovanými dátami a hodnotami, ktoré sa mnohokrát spúšťajú a automaticky vyhodnocujú. Hlavnou výhodou takéhoto testovania je šetrenie času. Na druhej strane, ak sa chcú takéto testy uskutočniť, je potrebné mať vhodný testovací nástroj, vstupné dáta a k nim očakávané výstupné dáta. [34]

2.4.2 Manuálne testy

Niektoré testy nemožno automatizovať alebo by bola automatizácia príliš zložitá a náročná na realizáciu, lebo výstupy si vyžadujú ľudské vyhodnotenie a zváženie ďalšieho postupu, ktorý sa môže na základe rôznych výsledkov

výrazne líšiť. Manuálne testovanie má však viacero nevýhod oproti automatizovanému. Keďže si tieto testy vyžadujú individuálny prístup, tak sú značne časovo náročné, čo prináša zvýšenie celkových nákladov na testovanie. Ďalšou nevýhodou je, že testy nie sú úplne spoľahlivé, keďže ich nevyhodnocuje počítač a môže dôjsť k pochybeniu človeka. [34]

2.5 Druhy testov z pohľadu dopadu na systém

Každý útok na systém má svoj cieľ a tieto ciele je možné dosiahnuť rôznymi cestami, ktoré môžu a nemusia zanechať následky na cieľovom systéme. Na základe tejto myšlienky existuje nasledujúce delenie bezpečnostných testov.

2.5.1 Deštruktívne testy

Deštruktívne testy sú charakteristické tým, že po ich skončení zanechajú na systéme následky. Systém alebo jeho časti môžu byť pri takýchto testoch úplne odstavené, nedostupné alebo prestanú fungovať správne. [35] Toto môže nastať z dvoch dôvodov:

- cieľom testu alebo útoku je znefunkčniť systém – testovanie robustnosti systému alebo analyzovanie možných preveditelných DoS útokov;
- primárnym cieľom testu alebo útoku je získanie alebo falšovanie informácií, ale v priebehu došlo k znefunkčneniu systému alebo jeho častí.

Deštruktívne testy si pred ich prevedením vyžadujú podrobnú analýzu dopadov na systém, zmapovanie následkov a plán nápravy škôd, ktoré budú testami spôsobené. Mnohokrát sa testuje už nasadený systém, ktorý je v prevádzke a je veľmi nežiadúce systém odstaviť, poprípade zasiahnuť testovaním bežných užívateľov. Práve pre tieto dôvody sú tieto testy značne nákladné a ich prevedenie vie byť komplikované.

2.5.2 Nedeštruktívne testy

Na druhej strane nedeštruktívne testy nijakým spôsobom systém nepoškodia. Cieľom útokov je získanie alebo falšovanie privilegovaných informácií, avšak ani v priebehu samotného útoku nie je nutné vykonať žiadnu akciu, ktorá by zanechala na systéme následky. Tento typ testov je preferovaný, keďže testovanie môže prebiehať na nasadenom systéme bez toho, aby vážne ovplyvnil užívateľov, ale nemožno takýmito testami preveriť všetky bezpečnostné riziká, preto je žiadúce kombinovať oba typy testov.

Kapitola 3

Metodika bezpečnostného testovania smerovačov

Vykonávanie bezpečnostných testov pozostáva zo sady viacerých úloh, ktoré si vyžadujú odborné znalosti a výsledky musia garantovať istú mieru bezpečnosti na základe vykonaných testov. Preto nie je bežné, aby si spoločnosti alebo jednotlivci vykonávali tieto testy sami, ale požiadajú o vykonanie bezpečnostných testov subjekt, ktorý sa na to špecializuje. Takýmito subjektami sú väčšinou firmy, ktoré robia rôzne bezpečnostné testy a audity rôznych informačných systémov, aplikácií alebo aj hardwarových komponentov.

Na realizáciu bezpečnostných testov sa vytvárajú rôzne metodiky, ktoré slúžia ako návod. Tieto návody šetria mnoho času (spolu s ním aj financií), ktorý by musel byť inak zakaždým strávený vymýšľaním priebehu a náplne testovania. Priebeh testovania rôznych objektov je podľa danej metodiky konzistentný a pokiaľ je metodika kvalitná a stane sa rozšírená, tak certifikát, ktorý testovaný objekt získa, vypovedá o garantovanej úrovni bezpečnosti aj používateľom tohoto objektu.

Nasledujúca kapitola predstavuje metodiku, pomocou ktorej je možné vykonať bezpečnostné testy smerovačov. Priebeh takéhoto bezpečnostného testovania sa člení do troch hlavných fáz:

- fáza plánovania – Pre-engagement,
- fáza testovania – Engagement,
- fáza vyhodnotenia – Post engagement.

V ďalšom texte je postupne rozobratá každá z troch fáz testovania spolu s postupom, kde je popísané, čo je potrebné vykonať v jednotlivých fázach na to, aby testovanie prebehlo úspešne. [36]

3.1 Fáza plánovania – Pre-engagement

Predtým, než sa začne samotné testovanie, je potrebné, aby sa medzi všetkými zúčastnenými stranami (zadávateľ, tester, užívateľ) vymenili viaceré podstatné informácie. Určujú sa pravidlá testovania, rozsah testovania a tester zbiera informácie o testovanom objekte. [36] Na základe týchto informácií sa vytvorí plán ako postupovať v ďalšej fáze.

3.1.1 Určenie rozsahu testovania

Pri určovaní rozsahu testovania zadávateľ spolu s testerom analyzujú sieť, hľadajú kritické miesta, prístupové body do siete a identifikujú dôležité systémy pracujúce v danej sieti. Po uistení sa, že žiadne podstatné komponenty siete neboli prehliadnuté, sa vymedzí, ktoré budú zahrnuté do testovania. [36]

3.1.2 Zber dokumentácie a informácií

Akonáhle je známe, čo všetko sa bude testovať, zadávateľ by mal sprístupniť testerovi všetku dokumentáciu popisujúcu testované komponenty. [36] Toto zahŕňa dokumentáciu smerovača, sieťových prvkov, firewallov, aplikácií a služieb bežiacich na sieti, dokumentáciu architektúry siete... Pokiaľ nie je možné z akýchkoľvek dôvodov poskytnúť nejakú dokumentáciu, je potrebné testerovi oznámiť všetky relevantné informácie o komponentoch, ich implementácii a očakávanej funkcionalite. Na základe získaných informácií je možné identifikovať potenciálne slabé miesta a pripraviť cielenejšie penetračné testy.

3.1.3 Preskúmanie hrozieb a zraniteľností odhalených v minulosti

V kapitolách 2.1.1 a 2.1.2 sa píše, že bezpečnostné testy sa nevykonávajú jednorázovo. Pri vykonávaní nových testov je vždy potrebné zobrať do úvahy výsledky posledného testovania a zakomponovať preverenie opravy zraniteľností nájdených v minulosti. [36] Pri hrozbách a zraniteľnostiach, ktoré neboli opravené, sa následne analyzujú riziká a možné dopady.

Druhá vec, ktorú tester berie do úvahy, sú problémy a zraniteľnosti nahlásené zadávateľom. [36] Je možné, že od posledných testov bolo na testovaný objekt zaútočené, poprípade samotný zadávateľ odhalil zraniteľnosť alebo nekorektné správanie niektorej časti testovaného objektu.

Okrem toho je povinnosťou testera byť informovaný o novonájdených zraniteľnostiach za obdobie od posledného testovania, ktoré sa týkajú testovaného objektu alebo jeho komponentov.[36]

3.1.4 Určenie úrovne náročnosti testov

V ďalšom kroku zadávateľ predostrie svoju predstavu, do akej hĺbky chce robiť testy a akú úroveň spoľahlivosti očakáva. Táto predstava je konzultovaná s testerom, ktorý zadávateľa usmerňuje a vďaka tejto komunikácii sa určia hranice a hĺbka, do akej sa bude testovať. [36] Tester následne na základe týchto informácií určí, aké zraniteľnosti sa budú testovať a aké druhy testov (rozoberané v kapitole 2) budú použité.

3.1.5 Určenie pravidiel

Poslednou, ale rovnako podstatnou činnosťou v prvej fáze, je určovanie pravidiel, podľa ktorých bude prebiehať fáza 2. Na základe týchto pravidiel získa tester od zadávateľa autorizáciu na napádanie testovaného objektu a využívanie jeho zraniteľností za účelom testovania a zadávateľ získa prehľad o tom, čo sa bude s testovaným objektom diať počas týchto testov. [36] Medzi najdôležitejšie otázky, ktoré je potrebné vyjasniť, patrí:

- V akom čase budú prebiehať testy? – Je rozdiel, ak testy prebiehajú počas maximálneho vyťaženia testovaného objektu a môžu ovplyvniť mnoho užívateľov alebo počas minimálneho vyťaženia.
- Ako naložiť s citlivými údajmi, pokiaľ budú odhalené počas testovania?
- Ak tester potrebuje do siete pripojiť vlastné zariadenia, aké požiadavky musí spĺňať toto zariadenie?
- Budú počas testu citlivé údaje prístupné niekomu inému ako testerovi?
- Budú užívatelia informovaní o prebiehajúcom testovaní? – Pokiaľ áno, môže to značne ovplyvniť výsledky testov zameraných na sociálne inžinierstvo.
- Aké kroky tester podnikne, ak objaví minulé alebo stále aktuálne napadnutia testovaného objektu? – Napríklad pokiaľ je nájdený spustený škodlivý kód.
- Môže si tester dovoliť vyradiť testovaný objekt z prevádzky? Ak áno, aký čas má na opätovné uvedenie do prevádzky.
- Môže tester komunikovať s užívateľmi systému? – Možné poškodenie reputácie zadávateľa, ak by sa tester vydával za reálneho útočníka.
- Môžu byť vykonané testy, ktoré vedia zmeniť funkčnosť alebo výzor systému?

3.2 Fáza testovania – Engagement

V tejto fáze dochádza k samotnému testovaniu. Každé prostredie, v ktorom prebieha test, je unikátne a používa rôzne technológie. Kvôli tomu je dôležité zvoliť vhodné nástroje na vykonanie testu, správna voľba nástrojov vie testy značne urýchliť, viď. kapitola 2.4. Samotné testovanie bežne prebieha v niekoľkých krokoch, ktoré na seba nadväzujú. [36]

3.2.1 Prieskum

Prvým krokom testov je prieskum, ktorého cieľom je za prvé overiť informácie získané zo zberu dokumentácie (3.1.2) a za druhé získať nové informácie, ktoré predtým neboli známe. [23] Celú fázu prieskumu pokrýva skenovanie zraniteľností popísané v kapitole 2.1.1.

3.2.2 Analýza zraniteľností

Na základe správy z predošlého kroku tester vyhodnocuje a identifikuje, ktoré zraniteľnosti sú potenciálne zneužiteľné. [23] Základné bezpečnostné testovanie končí týmto krokom a výstupom je správa s analýzou nájdených zraniteľností.

Pokiaľ testovanie pokračuje, zraniteľnosti sa následne prioritne ohodnotia podľa vážnosti a zostavia sa scenáre útokov. [23] Tie sa zostavujú na základe jednotlivých druhov testov ako boli popísané v kapitolách 2.2, 2.3 alebo v 2.5.

3.2.3 Využitie zraniteľností

Po zostavení scenárov útoku sa postupne každý jeden scenár testuje. Prebiehajú penetračné testy, tak ako sú popísané v kapitole 2.1.2, ktoré sa snažia dosiahnuť zneprístupnenie cieľa užívateľom, zmeny správania sa cieľa, získanie privilegovaných informácií alebo získanie vyšších oprávnení.

Ak sa podarí zneužiť nejakú zraniteľnosť, stále je možné, že oprávnenia testera budú značne limitované. Preto musí tester v mnohých prípadoch zvýšiť svoje oprávnenia, aby sa bolo možné dostať k privilegovaným informáciám. Zvýšenie oprávnení je možné docieliť viacerými spôsobmi, medzi inými aj crackovaním užívateľských hesiel, identifikovaním *shadow súboru* obsahujúceho prihlasovacie údaje, získať neoprávnený prístup metódami sociálneho inžinierstva...

Penetračný test môže, ale nemusí končiť dosiahnutím cieľov opísaných vyššie. Pokročilejšie a zložitejšie testy sa zameriavajú na udržanie si získaného prístupu. Skúšajú sa otvárať rôzne zadné dvierka, napríklad v podobe zriadenia nových prístupov cez sieť alebo vytvorením nových účtov s administrátor-

skými oprávneniami. Aby toto zostalo úspešne skryté pred administrátorom, je potrebné po sebe zahladiť stopy, napríklad premazaním prístupových logov alebo chybových správ spôsobených penetračným útokom. [23]

3.3 Fáza vyhodnotenia – Post Engagement

Po skončení testovania je potrebné vykonať niekoľko aktivít aj na strane zadávateľa, aj na strane testera. [36]

3.3.1 Vrátenie prostredia do pôvodného stavu

Počas testov je bežné, že sa vytvoria nové účty s užívateľskými, ale aj administrátorskými oprávneniami. Taktiež sa na uskutočnenie penetračných útokov alebo skenovanie zraniteľností používajú rôzne nástroje. Existenciu všetkých takto vytvorených účtov a programov je potrebné nahlásiť, resp. zahrnúť do správy, ktorá bude odovzdaná zadávateľovi. Všetky účty, nástroje a programy, ktoré boli nainštalované za účelmi testovania, sa následne odstránia zo systému, aby nemohli byť zneužité pre ďalšie útoky. [36]

3.3.2 Dokumentácia nájdených zraniteľností

Základný koncept dokumentácie nájdených zraniteľností popisuje, čo bolo testované, ako to bolo testované a aké boli výsledky testu. Táto správa obsahuje všetky nálezy, bez ohľadu na to, či daná zraniteľnosť je zneužiteľná s vážnymi následkami alebo nie. [36]

3.3.3 Vyhodnotenie vážnosti zraniteľností

Za účelom prioritizácie odstraňovania jednotlivých zraniteľností je potrebné každý nález analyzovať a ohodnotiť jeho vážnosť. Táto činnosť je vykonávaná testerom, avšak bežne sa používa niektorá zo štandardizovaných hodnotiacich metodík, aby bola zaručená konzistencia hodnotenia. [36] Medzi najznámejšie takéto metodiky patria:

- Common Vulnerability Scoring System (CVSS),
- Common Weakness Scoring System (CWSS),
- DREAD.

Najjednoduchšia z uvedených metodík je DREAD. Každá zraniteľnosť sa ohodnotí v nasledujúcich piatich kategóriách číslom od 1 do 10, kde 10 je najviac:

- **D**amage potential – Aké veľké škody môžu byť spôsobené?

- **R**eproducibility – Ako ľahko sa dá zopakovať proces využitia zraniteľnosti?
- **E**xploitability – Aké vedomosti a čas si vyžaduje využitie zraniteľnosti?
- **A**ffected Users – Aké množstvo užívateľov je zasiahnutých?
- **D**iscoverability – Ako ľahko je možné nájsť danú zraniteľnosť?

Výsledné hodnotenie je následne vypočítané ako aritmetický priemer hodnotení jednotlivých kategórií. [37]

Metodika CVSS funguje aktuálne vo verzii 3.0 a bola vyvinutá tak, aby reagovala na nedostatky metodiky DREAD. [37] Výsledné skóre zostáva s rovnakým rozsahom, aj keď výpočet je značne zložitejší a zásadne sa zvyšuje počet základných metrík z 5 (v DREAD) na 8 a znižuje sa škála hodnotenia jednotlivých metrík. Namiesto stupnice od 1 do 10 majú nové metriky dva až štyri stupne hodnotenia. Okrem týchto základných metrík existuje aj ďalších 14 dodatočných metrík slúžiacich na spresnenie výsledného skóre. [38]

U metodiky CWSS sú metriky rozdelené do troch hlavných skupín: Base Finding, Attack Surface a Enviromental. Každá skupina obsahuje viaceré metriky, ktoré sa ohodnotia a prepočítajú pomocou definovaných váh. V rámci skupiny Base Finding sa potom vypočíta výsledné skóre v rozsahu 0–100 a vo zvyšných dvoch skupinách sa rovnakou metódou vypočítajú skóre v rozsahu 0–1. Tieto tri skóre sa navzájom vynásobia a vyjde výsledné skóre v rozsahu 0–100. [39]

3.3.4 Odporúčania na odstránenie zraniteľností

Je na zadávateľovi, aby po testovaní uskutočnil opatrenia zaisťujúce, že všetky nájdené zraniteľnosti sa odstránia. Úlohou testera je zahrnúť do záverečnej správy odporúčania, ako tieto zraniteľnosti odstrániť. Po realizácii týchto opatrení je odporučené všetky upravené časti testovaného objektu znova podrobiť bezpečnostným testom, ktoré preveria kvalitu opráv. [36]

Kapitola 4

Zraniteľnosti smerovačov

Základným predpokladom pre vykonávanie bezpečnostného testovania je znalosť možných zraniteľností, ktoré budú testované. Bez tejto znalosti tester nemôže vykonať analýzu zraniteľností a ani zostaviť scenáre útokov, ktoré budú testované. Nasledujúca kapitola popisuje najbežnejšie zraniteľnosti vyskytujúce sa u SOHO smerovačov a v lokálnych sieťach.

4.1 Útoky na služby vzdialenej administrácie

Väčšina bezdrátových zariadení podporuje niekoľko bežných služieb, ktoré slúžia na administráciu a správu daného zariadenia. Medzi najtypickejšie služby patrí vzdialená administrácia pomocou protokolov HTTP alebo HTTPS, ktoré umožňujú administráciu zariadenia cez webové rozhranie. Tieto webové rozhrania často obsahujú bežné zraniteľnosti webových aplikácií, ako napríklad Cross-site request forgery, Cross-site scripting, Command injection alebo odchytávanie nechránených prihlasovacích údajov. [40]

Okrem administrácie cez HTTP a HTTPS sa bežne na zariadeniach vyskytujú služby Telnet, SSH alebo SNMP, ale bežní užívatelia smerovačov ich nevyužívajú a nechávajú tam nastavené slabé prihlasovacie údaje alebo dokonca pôvodné prihlasovacie údaje nastavené výrobcom. To otvára útočníkovi možnosť zaútočiť na danú službu hrubou silou a behom krátkeho času uhádnuť prihlasovacie meno a heslo. Akonáhle útočník získa takýmto spôsobom prístup, získa kontrolu nad zariadením.

4.1.1 Útoky na Telnet

Telnet je protokol pracujúci na aplikačnej vrstve TCP/IP, ktorý umožňuje obojsmernú interaktívnu komunikáciu medzi užívateľom a zariadením pomocou textového užívateľského rozhrania. Na prenos údajov používa transportný protokol TCP a obyčajne počúva na porte číslo 23. Zároveň je Telnet aj názov

aplikácie, ktorá realizuje komunikáciu medzi dvomi zariadeniami v sieti pomocou Telnet protokolu. [41] Tento protokol je dnes už málo používaný hlavne preto, že neumožňuje šifrovať komunikáciu medzi zariadeniami v sieti. Dnes sa práve preto často uprednostňuje protokol SSH, avšak na mnohých zariadeniach je Telnet stále podporovaný a povolený v štandardných nastaveniach. [40]

Existuje viacero spôsobov ako zaútočiť na smerovač, kde je povolený Telnet. Prvou a najjednoduchšou možnosťou je útok hrubou silou na prihlasovacie údaje. Keďže sa Telnet dnes už používa veľmi málo, často sa stane, že majiteľ alebo administrátor zabudol túto službu na smerovači úplne vypnúť, zmeniť pôvodné prihlasovacie údaje, poprípade použil len veľmi slabé heslo a bežne používané prihlasovacie meno. V takomto prípade môže útočník skúšať hádať prihlasovacie mená a heslá a za pomerne krátky čas získa prístup a kontrolu nad smerovačom.

Ďalšie riziko Telnetu vyplýva z faktu, že nešifruje komunikáciu. Predpokladom je byť v dosahu WiFi signálu smerovača v čase, keď sa administrátor prihlasuje pomocou Telnetu. Ktokoľvek, kto si dokáže nastaviť sieťovú kartu na svojom počítači do monitorovacieho módu, potom dokáže zachytiť komunikáciu, v ktorej sa nachádzajú v textovej forme prihlasovacie údaje alebo nastavenia smerovača. [40]

4.1.2 Útoky na SSH

Secure Shell, v skratke SSH, je názov pre kryptografický komunikačný protokol pracujúci na aplikačnej vrstve TCP/IP na porte číslo 22 a zároveň pre aplikáciu používajúcu tento protokol. Na prenos údajov využíva protokol TCP podobne ako Telnet. Bol navrhnutý ako náhrada za nezabezpečené protokoly ako Telnet alebo RSH a slúži na zabezpečenú sieťovú komunikáciu medzi dvomi zariadeniami vrátane vzdialeného prístupu, administrácie alebo prenosu súborov. [42]

Na začiatku spojenia pomocou SSH si najprv pomocou asymetrickej kryptografie s použitím Diffie-Hellmanovho algoritmu dohodnú obe strany spoločný šifrovací kľúč pre symetrické šifrovanie. [42] Keďže pri asymetrickej kryptografii nie je nutné zdieľať cez sieť šifrovací kľúč, aby sa mohli dáta šifrovať, tak sa komunikujúce entity dohodnú na spoločnom kľúči bez rizika odpočutia treťou stranou. Keď už majú obe strany spoločný kľúč, môžu prejsť na šifrovanie prenášaných dát symetrickou kryptografiou a zrýchliť tak komunikáciu.

Keďže komunikácia prebiehajúca pomocou SSH je šifrovaná, tak odchytávaním dát bez znalosti šifrovacieho kľúča nieje možné získať informácie o obsahu. Na autentizáciu užívateľa existujú v SSH viaceré metódy, ktoré

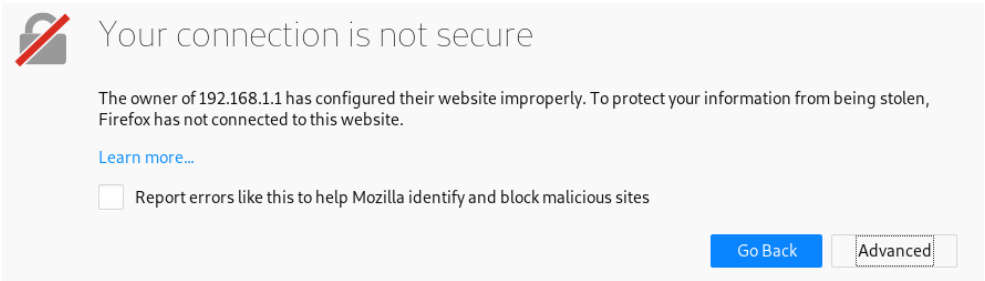
sú podrobne zdokumentované v RFC 4252. Na domácich smerovačoch sa vo všeobecnosti používa overovanie pomocou prihlasovacieho mena a hesla. To otvára priestor na útok hrubou silou. [40] Podobne ako pri Telnete, aj na SSH bežný užívateľ mnohokrát nezmení pôvodné prihlasovacie údaje alebo zvolí ľahko uhádnuteľnú kombináciu prihlasovacieho mena a hesla. Tomuto útoku je možné predísť, ak implementujeme SSH autentizáciu pomocou verejného kľúča, podrobne popísanú v RFC 4252. Na prihlásenie je v tomto prípade potrebná znalosť súkromného kľúča, ktorý pozná iba majiteľ konta. Privátny kľúč, ktorý má typicky 2048 alebo 4096 bitov, je pri dnešnej výpočtovej technike takmer nemožné uhádnuť pre časovú náročnosť. [43]

4.1.3 Útoky na HTTP

Hypertextový prenosový protokol, skrátene HTTP, je protokol na aplikačnej vrstve TCP/IP, ktorý slúži na prenos HTML dokumentov cez WWW. Protokol využíva transportný protokol TCP, ktorý obyčajne počúva na porte číslo 80 a funguje systémom požiadavka-odpoveď. V požiadavkách sa textovo popisujú požiadavky klienta, identifikácia požadovaného dokumentu, vlastnosti prehliadača atď. Server následne pošle v textovej forme požadovaný dokument alebo informáciu o zlyhaní požiadavky. [44] Keďže celá komunikácia prebieha bez šifrovania, tak dnes sa namiesto HTTP používa protokol HTTPS, ktorý zabezpečuje šifrovanie celej komunikácie. Ďalšie podrobnosti o HTTP je možné nájsť v RFC 7230.

Protokol HTTPS funguje podobne ako HTTP na základe protokolu TCP, počúva na porte číslo 443 a prenos dát šifruje pomocou protokolov SSL alebo TLS. [45]Týmto dokáže ochrániť komunikáciu pred odpočúvaním a útokmi typu Man-in-the-middle. Komunikácia sa začína procedúrou zvanou Handshake. Počas nej pošle server klientovi svoj certifikát, aby si klient overil integritu kľúča, čím sa zabráni podvrhnutiu iného kľúča treťou stranou. Klient má u seba databázu certifikačných autorít (ďalej CA), ktorým dôveruje, kde sa nachádzajú okrem iných údajov, ako napríklad dátum vydania a dátum platnosti, aj ich verejné kľúče. Nimi podpisujú verejné kľúče ďalších CA, verejné kľúče serverov alebo priamo dáta či stránky. Keďže dôveryhodné CA môžu podpísať kľúče iným CA, tak sa vytvoria reťazce dôvery. Aj keď klient nemá vo svojej databáze priamo CA, ktorú overuje, stačí mu overiť nejakú, ktorá sa nachádza vyššie v reťazci dôvery, a odtiaľ postupne overiť všetky ostatné podpisy v reťazci a zistiť či tento reťazec ostal neporušený. Toto je možné vďaka tomu, že server neposiela klientovi len svoj certifikát, ale aj všetky certifikáty, ktoré su vyššie v reťazci dôvery. Po overení certifikátu si server s klientom pomocou asymetrickej kryptografie dohodnú spoločný šifrovací kľúč pre ďalšiu komunikáciu. [46] Po skončení handshake sa môže začať šifrovaná komunikácia medzi serverom a klientom. Ďalšie informácie je možné nájsť v RFC 2818.

Na domácich smerovačoch je možné spravovať smerovač cez webový prehliadač pomocou protokolu HTTP alebo HTTPS. Je bežné, že staršie smerovače spravovanie cez HTTPS nepodporujú a dokonca aj pri prístupe na nové smerovače sa mnohokrát uprednostní protokol HTTP. Ak používateľ ručne zadá v prehliadači `https://ip_adresa_smerovača`, vo väčšine prípadov prehliadač zobrazí varovanie, ktoré informuje, že pripojenie nie je zabezpečené, varuje pred krádežou informácií a odporučí opustiť túto stránku. Tieto varovania sú dôsledkom toho, že aj keď smerovač podporuje HTTPS, tak má certifikát podpísaný sebou samým a nie dôveryhodnou certifikačnou autoritou. Keďže prehliadač nemá prečo rozoznať certifikačnú autoritu vytvorenú daným smerovačom, tak zobrazí spomínané varovania. Bežný užívateľ v tejto chvíli opustí zdanlivo nebezpečnú stránku a prejde na protokol HTTP, ktorý mu už pôjde bez problémov. Protokol HTTP však nešifruje komunikáciu, ak útočník odchytáva prenos dát medzi užívateľom a smerovačom, dostane sa k prihlasovacím údajom, ktoré buď nie sú chránené vôbec alebo sú chránené hashovacou funkciou. Ak sa podarí zistiť, ktorá hashovacia funkcia bola použitá, tak útočníkovi stačí spustiť slovníkový útok a ak je heslo slabé, tak ho útočník dostane.



Obr. 4.1: Varovanie pred neplatným certifikátom

4.2 Útoky na UPnP

Universal Plug and Play (UPnP) je sada sieťových protokolov, ktorá umožňuje hľadať iné zariadenia v sieti používajúce UPnP a automatizuje konfiguráciu a sieťovanie medzi nájdenými zariadeniami. S technológiou UPnP sa zariadenie vie dynamicky pripojiť do siete, obdržať IP adresu, oznámiť svoje schopnosti, zistiť, aké zariadenia sú pripojené do siete a aké majú vlastnosti. Komunikácia zariadení používajúcich UPnP je modelovaná ako peer-to-peer. UPnP je definované rozšírenými protokolmi (TCP/IP, HTML, XML, SSDP...) a je nezávislé na operačnom systéme, programovacom jazyku alebo fyzickom médiu. [47] Vďaka tomu je ľahko nasaditeľné do bežných sietí a na

veľmi širokú škálu sieťových zariadení, od smerovačov po inteligentné chladničky.

4.2.1 Komponenty UPnP

Základné stavebné bloky UPnP tvoria zariadenia, služby a kontrolné body. Informácie o jednotlivých komponentoch sú prevzaté z [47].

Zariadenie UPnP je súbor služieb a vnorených zariadení. Informácie o zariadení sú obsiahnuté v XML súbore, ktorý musí každé zariadenie povinne obsahovať. Tento súbor obsahuje podrobné informácie o službách, ktoré zariadenie poskytuje, jeho vnorených zariadeniach, popis zariadenia a zoznam vlastností – meno zariadenia, ikony... Na vyžiadanie vie zariadenie poskytnúť URL odkaz ukazujúci na tento súbor.

Služba v UPnP pozostáva zo stavovej tabuľky, riadiaceho servera a servera akcií. Stavová tabuľka popisuje stav služby pomocou stavových premenných. Riadiaci server dostáva požiadavky na akcie, ktoré vykoná, aktualizuje stavovú tabuľku a vráti odpoveď. Server akcií oznamuje udalosti, kedykoľvek sa stav služby zmení.

Riadiaci bod je ovládač schopný objavovať a ovládať iné zariadenia. Každé zariadenie by malo obsahovať riadiaci bod, aby bola zaručená komunikácia peer-to-peer. Po objavení nového zariadenia riadiaci bod vie:

- vrátiť popis zariadenia a zoznam jeho služieb;
- poskytnúť popis jednotlivých služieb;
- vykonať akcie na ovládanie služby;
- sledovať oznámenia o udalostiach využívaných služieb.

4.2.2 Fungovanie UPnP

Prvým krokom, ktorý má UPnP na starosti, je adresovanie. Každé zariadenie s DHCP klientom nájde DHCP server, od ktorého dostane IP adresu. Pokiaľ DHCP nie je k dispozícii, použije sa metóda Auto IP. Každé zariadenie môže mať okrem IP adresy svoje meno. To je využité, pokiaľ zariadenie podporuje DNS. [47]

Po získaní adresy je potrebné, aby zariadenie objavilo ostatné zariadenia v sieti využívajúce UPnP a oznámilo im svoju prítomnosť. To prebieha pomocou protokolu SSDP. Riadiaci bod pripojeného zariadenia pošle *search request* zatiaľ čo ostatné UPnP zariadenia počúvajú na multicastovom porte a po

obdržaní *search request* pošlú unicastovú odpoveď s informáciami o sebe. Podobne posiela informácie o sebe a svojich službách aj pripojené zariadenie. [47]

Akonáhle má riadiaci bod základné informácie o zariadení a jeho službách, môže mu posielať správy. Výmena správ prebieha pomocou protokolu SOAP a správy sú vo formáte XML. Pomocou nich môže získavať dodatočné informácie o ponúkaných službách a zadávať kontrolnému serveru príkazy. [47]

4.2.3 Útoky na UPnP z lokálnej siete

Takmer všetci výrobcovia implementujú UPnP do SOHO smerovačov a sieťových zariadení a vo východiskovom nastavení majú tieto zariadenia UPnP povolené. Hlavnou výhodou, ktorú UPnP prinieslo, je nulová konfigurácia zariadení, avšak to ide na úkor zabezpečenia. Pri UPnP nie je vyžadovaná žiadna autentizácia. [40] Jeden argument, prečo to je v poriadku, je, že v lokálnej sieti užívateľ dôveruje ostatným zariadeniam a nie je potrebné sa voči nim autentizovať, ale opak je pravdou. Technológia UPnP sa stala natoľko rozšírenou, že je používaná v rámci firemnej siete, v domácnostiach a na verejných miestach. Ktokoľvek, kto sa dostane do takejto siete, vie bez zábran získať kontrolu nad zariadeniami, ktoré majú UPnP povolené. Stačí ich po pripojení vyhľadať a začať im posielať riadiace príkazy. [40] Vďaka tomu si útočník môže streamovať obraz zo smart televízie, alebo keďže aj počítače môžu byť UPnP zariadením, je možné si otvoriť dieru vo firewalle a získať kontrolu nad cudzím počítačom.

4.2.4 Útok UPnProxy

Problém s UPnP sa netýka len lokálnych sietí. Niektoré chybné implementácie UPnP nerozdeľujú na smerovačoch sieťové rozhrania LAN a WAN. [48] V novembri 2018 bolo pomocou skenov adresného priestoru IPv4 zistené, že viac ako 3,5 milióna smerovačov implementuje UPnP počúvajúce na WAN rozhraní. [49]

Keďže UPnP nie je nijako zabezpečené, akonáhle vystavuje svoje služby do internetu, ktokoľvek ich vie začať využívať. Útočník je schopný pomocou SSDP výzvy zistiť, na akom porte UPnP počúva, aké obsahuje zariadenia a aké služby tieto zariadenia poskytujú. S týmito informáciami je možné vytvoriť jednoduché SOAP/XML požiadavky, ktoré modifikujú NAT tabuľku a vložia do nej nové riadky. [48] Toto sa dá využiť k viacerým útokom.

Prvou možnosťou je previesť útok zvaný UPnProxy. Myšlienkou je vložiť do NAT tabuľky záznam, ktorý presmeruje tok dát z útočníkovej IP adresy na ďalšiu verejnú IP adresu, a teda smerovač začne slúžiť ako proxy server. Rovnaký postup je možné aplikovať na niekoľkých zraniteľných zariade-

niach a presmerovávať tok dát medzi nimi. Takto je možné vytvárať reťazce proxy serverov. Tieto reťazce je možné zneužívať na ďalšie útočenie, kedy útočník takýmto presmerovaním ukrýva pôvod posielaných dát. [48] Vďaka tomu je možné spúšťať útoky, ktoré je veľmi obtiažne vystopovať naspäť k originálnemu útočníkovi.

4.2.5 Útok do vnútornej siete pomocou UPnP

Druhou možnosťou, ako zneužiť UPnP počúvajúce na WAN rozhraní, je vloženie záznamu do NAT tabuľky, ktorý presmeruje prichádzajúce dáta niekam do lokálnej siete. [48] Tým útočník prekoná prirodzenú bariéru medzi internetom a lokálnou sieťou, ktorú smerovač vytvára. Z lokálnej siete je možné následne napádať jednotlivé zariadenia, ktoré sú často chránené iba smerovačom, alebo je možné napádať smerovač samotný. Keďže z lokálnej siete je možné administrovať smerovače cez HTTP, po správnom presmerovaní a zadaní adresy smerovača sa útočník dostane na administratívnu stránku, kde sa môže skúšať prihlasovať. Pokiaľ sú na smerovači nastavené slabé administrátorské prihlasovacie údaje, útočník získa plný prístup k tomuto zariadeniu.

4.3 Útok na WPA2-PSK

Zariadenia komunikujúce cez WiFi prenášajú dáta pomocou rádiového signálu. To znamená, že okrem komunikujúcej stanice a prístupového bodu zachytia prenášané dáta aj všetci, čo sa nachádzajú v dosahu signálu. Protokol WiFi Protected Access II (WPA2) je bezpečnostný protokol popísaný v štandarde IEEE 802.11i a slúži na šifrovanie bezdrátovej komunikácie a autentizáciu. V rámci WPA2 existujú dva režimy – WPA2 Enterprise a WPA2 Personal, nazývaný aj WPA2-PSK. Režim WPA2 Enterprise používa RADIUS server na overenie identity užívateľov a je zväčša nasadzovaný v rámci väčších inštitúcií, zatiaľ čo WPA2 PSK používa na autentizáciu heslo a nasadzuje sa na lokálne siete menších inštitúcií a do domácností. [40]

Akonáhle sa užívateľ prihlási do siete s WPA2 PSK, jeho komunikácia je šifrovaná pomocou šifry AES. [40] Napadnúť túto komunikáciu je zložité, aj keď dnes je už známa zraniteľnosť KRACK (viac informácií o tejto zraniteľnosti je možné nájsť v [50]), ktorá dokáže prelomiť WPA2. Jednoduchšie a rozšírenejšie je napadnutie komunikácie ešte pred začiatkom samotného šifrovania a zistenie hesla. V rámci prihlasovania sa do siete si musí koncová stanica s prístupovým bodom (AP) vymeniť niekoľko informácií a dohodnúť sa na šifrovacom kľúči. Táto procedúra sa volá *4-way Handshake*. [40]

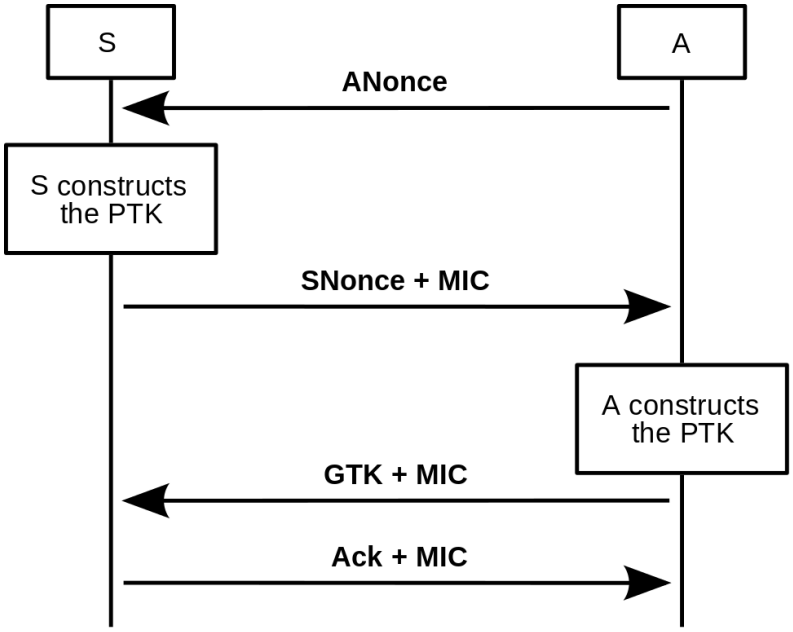
4.3.1 WPA2 PSK Handshake

Na začiatku komunikácie medzi prístupovým bodom (authenticator) a koncovým zariadením (supplicant) sa musí koncové zariadenie autentizovať a je potrebné vygenerovať šifrovacie kľúče na šifrovanie nasledujúcej komunikácie. Toto zaisťuje *4-way Handshake* pomocou výmeny 4 správ medzi prístupovým bodom a koncovým zariadením. Informácie o priebehu handshake sú čerpané z [51] a [52].

Na začiatku procedúry oba konce poznajú prihlasovacie heslo a spočítajú si Pre-Shared Key (PSK), ktorý závisí iba na SSID siete, do ktorej sa prihlasuje. Tento kľúč sa počíta pomocou funkcie na deriváciu kľúčov *PBKDF2*, konkrétne:

$$\text{PSK} = \text{PBKDF2}(\ \text{HMAC-SHA1, heslo, SSID, 4096, 256}\ )$$

Potom si obe strany vygenerujú nejaké náhodné číslo. Číslo vygenerované prístupovým bodom je označené Authenticator Number used once (ANonce) a číslo vygenerované koncovým zariadením sa označuje Supplicant Number used once (SNonce).



Obr. 4.2: Schéma priebehu 4-way Handshake dostupné z [53]

Prvú správu pošle prístupový bod koncovému zariadeniu a v nej svoje ANonce. V tomto momente je koncovému zariadeniu známa MAC adresa prístupového bodu (MAC(A)) a MAC adresa koncového zariadenia (MAC(S)).

Po prijatí prvej správy vie koncové zariadenie vygenerovať Pairwise Transient Key (PTK) ako:

PTK = PRF-HMAC-SHA-384(PSK, ANonce, SNonce, MAC(A), MAC(S))

Druhú správu posiela koncové zariadenie prístupovému bodu. Správa obsahuje SNonce a Message Integrity Code (MIC). MIC slúži ako kontrola integrity a vypočíta sa zo samotnej správy pomocou funkcie CBC-MAC, kde je ako kľúč použitý PTK. Prístupový bod má v tomto momente všetky informácie, aby si spočítal PTK. Potom z prijatej správy vypočíta svoj MIC a porovná ho s prijatým MIC. Pokiaľ sa tieto čísla rovnajú, tak prístupový bod má istotu, že má rovnaký PTK ako koncové zariadenie. Dôležité je uvedomiť si, že heslo ani PTK nikdy neboli prenesené po sieti. Následne prístupový bod náhodne vygeneruje Group Master Key (GMK) a Group Number used once GNonce a z nich odvodí Group Temporal Key (GTK), ktorý je používaný na šifrovanie multicastového a broadcastového prenosu.

Tretiu správu pošle prístupový bod koncovému zariadeniu. Obsahuje GTK zašifrovaný pomocou PTK a MIC správy. Koncové zariadenie rozšifruje GTK a skontroluje MIC. V tomto momente majú obe strany spoločný GTK aj PTK, ktoré môžu používať na šifrovanie.

Štvrtú správu posiela koncové zariadenie prístupovému bodu ako potvrdenie. V tejto správe sa nachádza len MIC, ktorý je po prijatí overený.

4.3.2 Prelomenie WPA2-PSK

Na zistenie prihlasovacieho hesla do siete je nevyhnutné odchytiť handshake popísaný v predchádzajúcom texte. Ten však prebieha, len keď sa koncové zariadenie pripája do siete. Aby sa minimalizovala doba čakania na odchytenie handshake, je možné cieľovú stanicu odpojiť zo siete. Tá sa bude snažiť pripojiť naspäť a pri tomto procese prebehne handshake.

Súbor štandardov IEEE 802.11 (WiFi) definuje služby poskytujúce funkcie, ktoré sú potrebné na LLC vrstve (vyššia časť dátovej vrstvy OSI modelu) na posielanie MAC Service Data Units (MSDUs) medzi dvomi entitami v sieti. Jedna z týchto funkcií je *Deauthentication*. Túto funkciu využíva zariadenie, ktoré chce ukončiť asociáciu s iným zariadením, a to tak, že odošle druhému zariadeniu deautentizačný rámec, čím mu oznámi, že ukončuje autentizáciu. Keďže nejde o požiadavku, ale o oznámenie, druhé zariadenie nemá na výber a ukončí asociáciu. Tieto rámce nie sú ani šifrované ani podpísané, takže pokiaľ útočník podvrhne smerovaču rámec s falošnou zdrojovou MAC adresou, odhlási iné zariadenie zo siete. [54]

Potenciálny útočník pozná SSID, počúvaním komunikácie zistí MAC(A) aj MAC(S) a odchytením prvých dvoch správ handshake zistí aj ANonce a SNonce. Neznáme útočníkovi ostáva PSK a PTK, ktoré však už je možné dopočítať so znalosťou hesla. [52]

Pokiaľ začne útočník skúšať rozšírené heslá slovníkovým útokom, tak pre dané heslo vie zakaždým dopočítať PTK. To sa síce nikdy po sieti neprenieslo, ale bolo použité ako kľúč k vypočítaniu MIC v druhej správe. Keďže má útočník odchytenú druhú správu, vie z nej a svojho PTK vypočítať svoj vlastný MIC. Ak je tento jeho MIC rovnaký ako ten v druhej správe, útočník vie, že heslo, ktoré použil na výpočet PTK, bolo správne prihlasovacie heslo do siete. [52] Útočník takto získa plný prístup do lokálnej siete, vie odšifrovať komunikáciu, ktorá bola predtým chránená WPA2 a ďalej útočiť na smerovač alebo iné zariadenia v sieti.

4.4 WiFi denial of service

V predošlej sekcii 4.3.2 je popísaná funkcia *Deauthentication* a ako ju zneužiť na odpojenie ľubovoľného zariadenia zo siete. Túto vedomosť je však možné zneužiť na trvalé odpojenie zariadenia zo siete. Pokiaľ útočník začne posielať deautentizačné rámce s dostatočne vysokou frekvenciou, tak zariadenie nebude môcť dokončiť handshake alebo sa v sieti udržať, lebo bude permanentne odpájané. [55]

V minulosti boli zistené prípady využívania tohoto útoku v rámci hotelov. Pokiaľ bola v hoteloch detekovaná cudzia sieť WiFi vytvorená napríklad mobilným prístupovým bodom, hotely začali blokovať pripojené zariadenia. Cieľom bolo donútiť návštevníkov platiť za internetové pripojenie poskytované hotelom. [56], [57]

4.5 Útok DNS Rebinding

Útok DNS Rebinding dovoľuje útočníkovi z internetu prekonať bariéru vytvorenú smerovačom, poprípade firewallom obete útoku a použiť ich internetový prehliadač ako proxy na komunikáciu so zariadeniami v lokálnej sieti. [58]

Tento útok obchádza bezpečnostný mechanizmus nazývajúci sa *Politika rovnakého pôvodu (Same-origin policy)* v prehliadačoch. [58]

4.5.1 Politika rovnakého pôvodu v prehliadačoch

Politika rovnakého pôvodu je bezpečnostný mechanizmus v internetových prehliadačoch, ktorý zabraňuje tomu, aby webové stránky z jednej domény posielali požiadavky na webové stránky inej domény. Teda pokiaľ užívateľ otvorí škodlivú stránku, tá by nemala byť schopná posielať požiadavky na stránku banky, kde je aktuálne užívateľ prihlásený. [58]

Dve URL adresy majú rovnaký pôvod, pokiaľ sa v nich zhoduje číslo portu, protokol a meno servera v rámci rovnakej domény. [59]

Prehliadač Internet Explorer implementuje tento mechanizmus odlišne. Do identifikácie rovnakého pôvodu sa nezahŕňa kontrola rovnakých portov. Druhou zmenou sú tzv. *Dôverné zóny*. Pokiaľ sa dve domény nachádzajú v dôvernej zóne, politika rovnakého pôvodu sa na ne vôbec neuplatňuje. [59]

4.5.2 Scenár útoku

Na prevedenie DNS Rebinding útoku je potrebné, aby si útočník zaregistroval doménu, napríklad `utocnik.net`. [60] Za každou doménou sa skrýva jedna alebo aj viacero IP adries, ktoré sú však pre človeka ťažko zapamätateľné. DNS servery zabezpečujú preklad ľahko zapamätateľných doménových mien na IP adresy. Aj útočník si pre svoju doménu spustí DNS server, ktorý bude mať úplne pod kontrolou. V rámci domény útočník vytvorí stránku so škodlivým kódom, napríklad `http://utocnik.net`. [60]

Ďalším krokom je donútiť obeť, aby si načítala útočníkovu stránku so škodlivým kódom. To je možné dosiahnuť napríklad s využitím Phishingu (2.1.3), pomocou reklám alebo perzistentných cross-site scripting útokov.

Akonáhle sa bude obeť snažiť načítať stránku `http://utocnik.net`, bude potrebovať zistiť jej IP adresu. Najprv sa pozrie do DNS cache, či sa tam nachádza záznam o stránke. Keďže ide o prvý prístup obete na stránku, tak nebude v DNS cache. Spýta sa teda svojho prednastaveného DNS serveru, ten stránku nebude poznať, ale bude sa ju snažiť zistiť od iných DNS serverov. Po chvíli hľadania a odkazovania medzi DNS servermi, dostane prednastavený server obete informáciu, že záznamy, ktoré obeť požaduje, vie poskytnúť útočníkov DNS server. Ten odpovie s reálnou IP adresou stránky `http://utocnik.net`, ale nastaví parameter Time To Live (TTL) na veľmi nízku hodnotu. [58] Tento parameter určuje ako dlho ostane záznam v DNS cache obete.

Obeť načíta stránku `http://utocnik.net`, ktorá obsahuje, okrem iného aj škodlivý JavaScript kód. Ten sa spustí v prehliadači obete. Pokiaľ je stránka

spravená tak, aby pôsobila legitímne a vierohodne, obeť nemusí vedieť, že sa na ňu útočí. Škodlivý kód začne posielať na `http://utocnik.net` rôzne HTTP požiadavky, podľa potreby útočníka. Keďže útočníkove DNS poslalo informáciu s krátkym TTL, v čase odosielania týchto požiadaviek sa v DNS cache obete už nenachádza informácia, akú IP adresu má `http://utocnik.net`. Služba DNS začne znovu zisťovať IP adresu útočníkovej stránky, ale tentoraz, keď sa obeť spýta útočníkovho DNS servera, ten odpovie s falošnou IP adresou, ktorá sa nachádza niekde vnútri lokálnej siete obete. Prehliadač obete túto adresu pri preklade použije a odošle útočníkove HTTP požiadavky do lokálnej siete. Z pohľadu prehliadača to vyzerá, že stále prebieha komunikácia s doménou `http://utocnik.net`, takže tejto komunikácii nebude nijako brániť. [58]

Útočník takto vie posielať do lokálnej siete UPnP požiadavky (4.2.2) alebo sa môže skúšať prihlásiť na smerovač pomocou najčastejšie používaných prihlasovacích údajov a získať kontrolu nad smerovačom.

Požiadavky je možné posielať naslepo na všetky adresy v štandardnom rozsahu používaných privátnych IP adries v lokálnych sieťach – 192.168.1.1 až 192.168.255.254. Druhou možnosťou je využitie zraniteľnosti *WebRTC leak*, pomocou ktorej je možné zistiť rozsah IP adries v lokálnej sieti skôr než škodlivý JavaScript kód začne posielať požiadavky. [58]

Kapitola 5

Praktické testovanie

V tejto kapitole prebehne bezpečnostné testovanie troch vybraných smerovačov podľa metodiky predstavenej v kapitole 3.

5.1 Fáza plánovania – Pre-Engagement

Bezpečnostného testovania sa účastnia 4 strany – zadávateľ, tester, užívatelia a poskytovateľ smerovačov. V tomto prípade je zadávateľ a tester jedna osoba. Pre účely testovania budú užívatelia simulovaní ako majitelia zariadení pripojených do siete.

5.1.1 Určenie pravidiel testovania

Priebeh testovania sa musí riadiť nasledujúcimi pravidlami:

- Podmienkou poskytovateľa smerovačov je utajenie informácií, ktoré by viedli k jednoznačnej identifikácii tohto internetového poskytovateľa. To sa týka aj špecifikácie modelov smerovačov alebo verzie ich firmware v rámci tohto textu alebo snímkov obrazovky v prílohách.
- Heslá zistené počas testovania nebudú utajované, pretože smerovače aj bezdrátové siete boli vytvorené za účelom demonštrácie testovania, a teda nedôjde k odhaleniu citlivých informácií reálnych užívateľov.
- Smerovače môžu byť počas testov odstavené útokmi, nemôže však vzniknúť trvalá škoda na smerovači (napr. zmazanie firmware), pre nutnosť vrátenia smerovačov poskytovateľovi.
- Smerovače budú počas testovania zraniteľné útokmi z internetu a budú ohrozené užívateľské zariadenia, špeciálne tlačiareň bežiaca na lokálnej sieti. Tieto zariadenia budú odpojené mimo momentov, kedy test vyžaduje prítomnosť daných zariadení na sieti.

- Pri prípadnom objavení aktuálne prebiehajúceho útoku vynaloží tester patričné prostriedky, aby tomuto útoku zamedzil.

5.1.2 Zber dokumentácie a informácií

Testovať sa budú tri smerovače od troch rôznych výrobcov – Zyxel, DrayTek a ADB. Ide o zariadenia, ktoré sú bežne dodávané do domácností alebo menších firiem internetovým poskytovateľom. K smerovačom nebola dodaná žiadna ďalšia dokumentácia o firmware, ktorý na nich beží, avšak je na ne administratívny prístup a s ním možnosť prezerania aplikácií, nastavení a logov. Aplikácie a služby ako napr. SSH, HTTP alebo UPnP sú zdokumentované v štandardoch a na oficiálnych stránkach.

Každý smerovač vytvára bezdrátovú sieť pomenovanú podľa značky daného smerovača, konkrétne `test-ZYXEL`, `test-DRAYTEK` a `test-ADB`. Na každej sieti bolo simulovaným administrátorom nastavené prístupové heslo. Každý smerovač je pripojený na internet a zároveň vytvára lokálnu bezdrátovú sieť. V každej sieti je pripojený okrem smerovača aj tester a pre potreby niektorých testov bezdrátová tlačiareň.

5.1.3 Určenie rozsahu testovania

Testované sú tri smerovače popísané v predchádzajúcej sekcii. Testovanie začne skenovaním siete a hľadaním potenciálnych zraniteľností. Skenovanie sa zameria najmä na otvorené porty a služby, ktoré na nich bežia. Výsledky skenovania sa zanalyzujú a prebehne penetračné testovanie. Penetračné testovanie sa zameria na zraniteľnosti služieb SSH, Telnet, HTTP, na prelamovanie hesla protokolu WPA2-PSK a na protokol UPnP.

Každý smerovač je primárne otestovaný v predvolených nastaveniach a prípadné zmeny nastavení budú popísané v scenároch útokov, ktoré tieto zmeny vyžadujú.

5.1.4 Prieskum zraniteľností odhalených v minulosti

Smerovače neboli v minulosti testované testerom, a teda nie je k dispozícii záznam o hrozbách a zraniteľnostiach nájdených v minulosti. Pri testovaní sa bude vychádzať výhradne z kapitoly 4 a zdrojov použitých na vypracovanie tejto kapitoly.

5.1.5 Softwarové testovacie prostredie

Na bezpečnostné testovanie je vhodné mať operačný systém dedikovaný na tieto účely. Takýto systém už obsahuje mnoho predinštalovaných nástrojov na skenovanie a penetračné testy a zároveň oddelí bežne používané prostredie

od toho, ktoré je určené na bežné použitie. Takýto operačný systém je možné spustiť na už nainštalovanom OS ako virtuálny stroj. Druhou možnosťou je nainštalovať ho priamo na počítač ako plnohodnotný OS.

Existuje viacero operačných systémov, ktoré slúžia na bezpečnostné testovanie. Niektoré zhromažďujú široké spektrum nástrojov a iné sú len úzko zamerané. Medzi najznámejšie systémy patria:

- Kali Linux
- Black Box
- Parrot Security

Pre účely testovania v rámci tejto práce bol vybraný operačný systém Kali Linux, ktorý je podrobnejšie popísaný v nasledujúcej sekcii.

5.1.5.1 Kali Linux

Kali Linux je linuxová distribúcia odvodená od Debianu, určená na penetračné testovanie a bezpečnostné audity. Vyvíjaný je od roku 2012 spoločnosťou *Offensive Security Ltd* ako náhrada systému BackTrack Linux. Kali Linux rozširuje distribúcie projektu Debian a pridáva niekoľko stoviek balíčkov, ktoré sa týkajú informačnej bezpečnosti. Aktuálne je Kali Linux považovaný za najrozšírenejší OS určený na bezpečnostné testovanie a má širokú aktívnu základňu užívateľov, čo umožnuje ľahko hľadať odpovede na prípadné problémy pri používaní systému, či nástrojov v ňom. Informácie o Kali Linuxe sú čerpané z [61], kde je možné nájsť podrobnejšie informácie, dokumentáciu a návody na používanie.

5.1.6 Testovacie nástroje

Nasledujúca časť kapitoly je venovaná nástrojom, ktoré sa použijú pri testovaní. Všetky popisované nástroje sú predinštalované v OS Kali Linux alebo zdarma dostupné na internete. Popisy nástrojov boli čerpané z oficiálnych stránok autorov uvedených na konci jednotlivých sekcií.

5.1.6.1 Nmap

Nástroj Network Mapper (Nmap) slúži na skenovanie a preskúmavanie sietí. Pomocou takzvaných raw paketov, ktoré sa doručujú na všetky porty na danej IP adrese, je schopný objavovať aktívne zariadenia na sieti a zistiť, ktoré porty majú otvorené a aké služby sú na nich aktívne. Pokiaľ je to možné, zistí, aký OS zariadenie používa a aká je verzia tohto OS alebo aké firewally má zariadenie aktivované. Ďalšie informácie o používaní tohto nástroja je možné nájsť na [62].

5.1.6.2 Wireshark

Wireshark je nástroj na analýzu sieťových protokolov s grafickým rozhraním. Umožňuje zachytávať všetku komunikáciu na danom sieťovom rozhraní, ukladať si zachytené dáta a analyzovať ich. Analýza je podporovaná mnohými funkcionalitami, medzi ktoré patria rôzne filtre zachytených paketov, možnosti usporiadavania zachytených dát a podpora dešifrovania dát v rámci rôznych sieťových protokolov. Dokumentáciu a ďalšie informácie o tomto nástroji je možné nájsť na [63].

5.1.6.3 Aircrack-ng

Nástroj Aircrack-ng slúži na prelamovanie WEP a WPA2-PSK kľúčov. Na prelamovanie WPA2, ktoré bude realizované vo fáze testovania (kapitola 5.2), používa Aircrack-ng slovník so skúšanými heslami a handshake zachytený pomocou nástroja Airodump-ng. Viac informácií o používaní tohto nástroja je možné nájsť na [64].

Názov Aircrack-ng zároveň označuje aj celý balík nástrojov, ktoré podporujú činnosť nástroja Aircrack-ng. Všetky nástroje v tomto balíku používajú ako rozhranie príkazový riadok a slúžia na analýzu bezpečnosti v rámci WiFi.

5.1.6.4 Airmon-ng

Sieťové rozhrania zachytávajú len pakety, ktoré sú určené pre ne a ostatné ignorujú. Ignorované pakety nie je možné potom zachytávať pomocou nástrojov ako Wireshark (kapitola 5.1.6.2) a ďalej s nimi pracovať. Aby sa tento problém odstránil, je možné prepnúť sieťové rozhrania do monitorovacieho módu, kedy prijímajú všetky dáta, ktoré vedia zachytiť. Na prepínanie sa medzi normálnym a monitorovacím módom slúži skript Airmon-ng, ktorý je zakomponovaný ako súčasť väčšieho balíčka nástrojov Aircrack-ng. Viac informácií o používaní tohto nástroja sa nachádza na [65].

5.1.6.5 Airodump-ng

Nástroj Airodump-ng je súčasťou balíčka nástrojov Aircrack-ng a slúži na zachytávanie rámcov protokolu 802.11 (WiFi). S týmto nástrojom je možné monitorovať bezdrátové siete a zariadenia v dosahu počítača, následne sa zamerať na konkrétnu sieť a odchytávať dáta. Nástroj špeciálne zobrazuje informácie o zachytení handshake a je vhodný na získanie dát pre nástroj Aircrack-ng (kapitola 5.1.6.3). Informácie o tom, ako používať tento nástroj, je možné nájsť na [66].

5.1.6.6 Aireplay-ng

Aireplay-ng je nástroj, ktorý vie injektovať pakety do bezdrátovej siete. Tieto pakety vie vytvárať s falošnými IP adresami alebo MAC adresami. Nástroj má zabudovaných niekoľko funkcionalít na prevedenie útokov ako deautentizácia klientov v bezdrátovej sieti alebo falošná autentizácia. Viac informácií je možné nájsť na [67].

5.1.6.7 Hydra

Nástroj Hydra slúži na automatizáciu útoku hrubou silou na prihlasovacie údaje. Podporuje viaceré protokoly, vrátane SSH a Telnet, kde sa skúša prihlasovať a pri úspechu vypíše použité prihlasovacie údaje. Na vstupe potrebuje slovník s prihlasovacími menami a heslami, ktoré postupne skúša. Nástroj umožňuje celý proces skúšania paralelizovať a tým značne skrátiť dobu čakania na výsledky. Dokumentáciu a samotný kód na stiahnutie je možné nájsť na [68].

5.1.6.8 Miranda

Nástroj Miranda funguje ako UPnP klient aplikácia, ktorá vie objavovať iné zariadenia s aktívnym UPnP v rámci siete a komunikovať s nimi. Pomocou tohto nástroja je možné získať informácie o funkcionalitách iných UPnP zariadení, prezerať ich pomocou interaktívneho a prehľadného rozhrania a posielať UPnP príkazy na iné zariadenia. Viac informácií je možné nájsť na [69].

5.2 Fáza testovania – Engagement

Nasledujúca časť práce dokumentuje priebeh skenovania siete, zostavenia scenárov útokov na základe analýzy zraniteľností a samotné penetračné testy. Podrobné snímky obrazoviek zachytávajúce zadávané príkazy, výpisy, použitie nástrojov a zachytené dáta je možné nájsť na CD, ktoré je priložené k tejto práci.

5.2.1 Prieskum

Počas prieskumu prebehlo pripojenie sa do každej z troch bezdrátových sietí `test-ZYXEL`, `test-DRAYTEK` a `test-ADB`. Pomocou nástroja `ifconfig` sa zistilo, že všetky smerovače používajú protokol DHCP a pridelili testerovmu počítaču IP adresu z rozsahu `192.168.1.0/24`.

Po prihlásení sa do bezdrátovej siete prebehlo skenovanie pomocou nástroja `Nmap`. Vďaka tomu bolo zistené, že všetky smerovače sa v rámci lokálnej siete, ktorú vytvárajú, nachádzajú na IP adrese `192.168.1.1`. Ďalej skenovanie odhalilo MAC adresy každého smerovača, otvorené porty na smerovačoch

a služby, ktoré na nich boli spustené. Výsledky skenovania portov sú zhrnuté v tabuľkách 5.1, 5.2 a 5.3.

Smerovač ADB a DrayTek majú spustenú službu HTTPS, ktorej funkčnosť bola preskúmaná. Na oba smerovače bolo skúsené najprv obyčajné prihlasovanie sa cez webové rozhranie. V oboch prípadoch bolo automaticky spustené prihlasovanie cez nešifrovaný protokol HTTP. V ďalšom kroku bolo vynútené použitie protokolu HTTPS zadaním `https://192.168.1.1`. V oboch prípadoch prehliadač zobrazil varovanie popísané v kapitole 4.1.3.

Tabuľka 5.1: Výsledky skenovania smerovača Zyxel

Zyxel	
Číslo otvoreného portu	Služba spustená na porte
21/tcp	ftp
22/tcp	ssh
23/tcp	telnet
53/tcp	DNS
80/tcp	http

Tabuľka 5.2: Výsledky skenovania smerovača DrayTek

DrayTek	
Číslo otvoreného portu	Služba spustená na porte
21/tcp	ftp
23/tcp	telnet
80/tcp	http
443/tcp	https

Tabuľka 5.3: Výsledky skenovania smerovača ADB

ADB	
Číslo otvoreného portu	Služba spustená na porte
53/tcp	DNS
80/tcp	http
443/tcp	https

Ďalšia fáza skenovania sa venovala UPnP. Už z predošlých výpisov si je možné všimnúť, že v rámci pôvodných nastavení táto služba nie je spustená. Za účelom zistenia, či UPnP počúva aj na internetovom rozhraní smerovača, bolo nutné túto službu spustiť. Na zistenie, či je UPnP chybne implementované a počúva na internetových rozhraniach boli využité služby, ktoré poskytuje

Gibson Research Corporation na stránkach [70]. Skeny ukázali, že ani na jednom smerovači nebolo zistené žiadne nežiadúce správanie a UPnP nereaguje na internetovom rozhraní.

5.2.2 Analýza zraniteľností

Smerovače Zyxel a DrayTek majú spustenú službu Telnet, čo prináša riziko odchytávania nešifrovanej komunikácie v prípade, že administrátor túto službu využíva. Pokiaľ naopak táto služba využívaná nie je, je možné, že sú nastavené slabé alebo pôvodné prihlasovacie údaje. V takomto prípade je možné službu napadnúť útokom hrubou silou a získať prístup na smerovač.

Smerovač Zyxel má spustenú službu SSH. Tá podobne ako Telnet, nesie so sebou riziko, že sú nastavené buď pôvodné alebo slabé prihlasovacie údaje a tým pádom môže byť zraniteľná útokom hrubou silou.

Všetky smerovače majú spustenú službu HTTP, čo prináša riziko odchytávania komunikácie a prihlasovacích údajov počas toho, ako je administrátor prihlásený na smerovači.

5.2.3 Prevedenie útokov

Na základe určeného rozsahu testovania a analýzy zraniteľností sa zostavili scenáre jednotlivých útokov, ktoré sa následne otestovali. Popis priebehu testovania jednotlivých zraniteľností zachytáva nasledujúca časť práce.

5.2.4 Prelamovanie WPA2-PSK

Na prelomenie WPA2-PSK a získanie hesla do siete sú potrebné nástroje Airmon-ng, Airodump-ng, Aireplay-ng a Aircrack-ng. Predpoklad k úspešnému prevedeniu útoku je aspoň jedno zariadenie prihlásené do bezdrátovej siete.

Prvým krokom bolo prepnutie sieťovej karty do monitorovacieho módu pomocou nástroja Airmon-ng. Následne bolo potrebné zistiť pomocou nástroja Airodump-ng, aké siete sa vyskytujú v dosahu. Ten zachytil celkovo 9 sietí v dosahu vrátane troch testovaných sietí, ktoré je vidieť na ukážke z výpisu 5.4. Zároveň zachytil aj niekoľko zariadení, ktoré boli pripojené na niektorú z týchto sietí.

Tabuľka 5.4: Časť výpisu nástroja Airodump-ng

BSSID	CH	ENC	AUTH	ESSID
8C:59:C3:8D:03:51	10	WPA2	PSK	test-ADB
C8:6C:87:73:AE:32	10	WPA2	PSK	test-ZYXEL
00:50:7F:BC:96:80	10	WPA2	PSK	test-DRAYTEK

Ďalšie kroky sa už vykonávali pre každú sieť samostatne, avšak postup zostal rovnaký. Najskôr sa vybrala konkrétna sieť (jej BSSID) a pomocou nástroja Airodump-ng sa začali zachytávať a ukladať všetky dáta prenášané cez túto sieť, ktoré sieťová karta zachytila. Ako bolo popísané v 4.3, nasledujúcim krokom bolo zachytiť handshake. Na to bol využitý nástroj Aireplay-ng, ktorý deautentifikoval zariadenie pripojené v sieti. Akonáhle sa zariadenie pripojilo naspäť, Airodump-ng zobrazil informáciu, že zachytil handshake.

Od momentu, kedy boli zachytené všetky handshake zo všetkých troch sietí, bolo len otázkou zložitosti hesla, či bude útok úspešný. Na zistenie hesla bol použitý nástroj Aircrack-ng, ktorý použil slovník s miliónom frekventovaných hesiel. Nástroj zisťoval heslo do každej zo sietí, tak ako je popísané v 4.3. Nakoniec sa zistilo, že všetky tri heslá sa nachádzajú v slovníku, a teda boli odhalené, ako je zobrazené v 5.5.

Tabuľka 5.5: Odhalené heslá bezdrátových sietí

názov siete	zistené heslo
test-DRAYTEK	1qazxsw2
test-ADB	staropramen
test-ZYXEL	maminka1

5.2.5 Útok na SSH

Predpokladom na prevedenie útoku na SSH je prístup do lokálnej siete, v ktorej sa smerovač nachádza. K dispozícii potrebuje tester nástroj Hydra a slovníky s často používanými prihlasovacími menami a heslami.

Smerovač Zyxel mal ako jediný aktívny port 22 a na ňom spustenú službu SSH. V tomto teste bola overovaná sila prihlasovacích údajov. Test prebiehal ako slovníkový útok hrubou silou s využitím nástroja Hydra. Tento nástroj odhalil, že na tejto službe zostal vytvorený pôvodný účet s prihlasovacími údajmi `login: admin` a `password: admin`. Po prihlásení sa pomocou týchto údajov bol získaný prístup k vzdialenej administrácii tohto smerovača.

```
[22][ssh] host: 192.168.1.1   login: admin   password: admin
```

Obr. 5.1: Časť výpisu nástroja Hydra

5.2.6 Útok na Telnet

Útočenie na Telnet bolo zamerané na útoky hrubou silou pomocou nástroja Hydra a slovníkov s často používanými prihlasovacími menami a heslami.

Ako prvý bol otestovaný smerovač Zyxel, pri ktorom bol nástroj Hydra schopný nájsť prihlasovacie údaje v rámci 100 najčastejších kombinácií mien a hesiel. Po prihlásení sa bol získaný administrátorský prístup na smerovač

```
[23][telnet] host: 192.168.1.1   login: admin   password: admin
```

Obr. 5.2: Časť výpisu nástroja Hydra

Druhý bol otestovaný smerovač DrayTek. Pri manuálnom pokuse o prihlásenie sa bolo zistené, že nie je vyžadované prihlasovacie meno a stačí skúšať heslo, čo zásadne znižuje počet kombinácií, ktoré bolo treba vyskúšať. Pomocou nástroja Hydra bolo zistené heslo `admin`, pomocou ktorého bolo možné prihlásiť sa do administrácie smerovača.

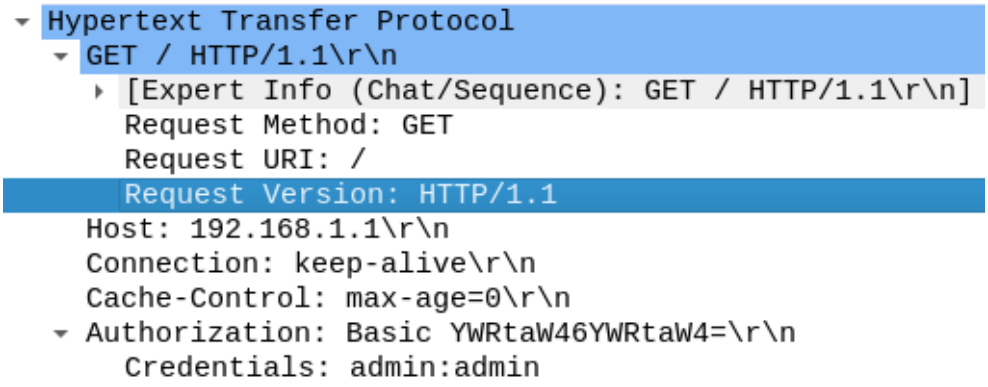
5.2.7 Útok na HTTP

Všetky tri smerovače poskytujú možnosť využívať vzdialenú administráciu cez protokol HTTP. Vďaka užívateľskému rozhraniu v internetovom prehliadači je tento spôsob administrácie rozšírený a preferovaný medzi užívateľmi a administrátormi. Úlohou testu bolo odchytiť komunikáciu užívateľa alebo administrátora, ktorý sa prihlasoval k administrátorskému účtu na smerovači a z odchytenej komunikácie zistiť prihlasovacie údaje.

Na prevedenie tohto útoku je potrebné poznať prihlasovacie heslo do siete a odchytávať v čase, kedy sa niekto prihlasuje do administrátorského účtu na smerovači. Aby bolo možné odšifrovať odchytenú komunikáciu, je nutné odchytiť handshake, ktorý prebehol medzi smerovačom a daným zariadením. To sa podarilo pri všetkých troch smerovačoch.

V odchytenej komunikácii na sieti `test-ZYXEL` bol odchytený paket obsahujúci nezašifrované prihlasovacie meno a heslo. Rovnako dopadlo odchytávanie na sieti `test-DRAYTEK`. Odchytené prihlasovacie údaje boli v oboch

prípadoch `login: admin` a `password: admin`. Výpis z Wiresharku 5.3 zobrazuje, ako vyzerali odchytené prihlasovacie údaje. Bez ohľadu na to, aké zložité by boli tieto prihlasovacie údaje, stále by boli odchytené v čitateľnej podobe a odhalené.



Obr. 5.3: Časť výpisu komunikácie so smerovačom Zyxel

Smerovač ADB sa ukázal ako bezpečnejšia voľba. V odchytenej komunikácii bolo nešifrované prihlasovacie meno. Heslo však bolo skryté pomocou neznámej hashovacej funkcie, tak ako to je možné vidieť na obrázku 5.4. Po analýze prihlasovacej stránky bola nájdená nasledujúca časť kódu v rámci prihlasovacieho formulára:

```
document.form.userPwd.value = CryptoJS.HmacSHA256(
                                document.form.origUserPwd.value,
                                document.form.nonce.value);
```

Z tohto bolo možné zistiť, že heslo prenášané po sieti je obrazom funkcie HMAC-SHA256, kde vstupná správa je prihlasovacie heslo a kľúč je náhodne vygenerované číslo Nonce. Toto číslo bolo tiež zachytené v rámci dát zobrazených na obrázku 5.4.

Pokiaľ sa heslo nachádza v slovníkoch hesiel, je možné spraviť útok hrubou silou, kedy sa počítajú obrazy HMAC-SHA256 všetkých hesiel v slovníku a porovnávajú sa s odchytenou hodnotou. To bolo spravené pomocou vytvoreného skriptu v jazyku Python3. Skript použil slovník s miliónom najbežnejších hesiel a zistil, že pôvodná, nehashovaná hodnota hesla bola `password:12345678`.

```
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
  ▸ Form item: "userName" = "admin"
  ▸ Form item: "origUserPwdShow" = "on"
  ▸ Form item: "language" = "EN"
  ▸ Form item: "login" = "Login"
  ▸ Form item: "userPwd" = "fe1cbe23ef655825d97e04d1fea181cd0e03dabe02b4d0e785ec2c06feff25b0"
  ▸ Form item: "nonce" = "1561503180"
  ▸ Form item: "code1" = "Q6iQL1VtO"
  ▸ Form item: "code2" = "MkT8b2Mns"
  ▸ Form item: "code3" = "bjQqYgn"
```

Obr. 5.4: Časť výpisu komunikácie so smerovačom ADB

5.2.8 Útok na UPnP z vnútornej siete

Na prevedenie útoku na UPnP bolo nutné aktivovať túto službu na všetkých troch smerovačoch. Cieľom útoku bolo zistiť, či je možné z lokálnej siete zneužiť UPnP na vytvorenie komunikačného tunela medzi lokálnou sieťou a internetom. Na demonštráciu funkčnosti bola pripojená do siete bezdrátová tlačiareň, na ktorú sa bolo cieľom pripojiť. Ďalej bolo potrebné zariadenie, ktoré bolo pripojené na internet, ale nie pomocou testovaného smerovača. Pri realizácii útoku boli použité nástroje Hydra a Wireshark.

Prvým krokom bolo objaviť pomocou nástroja Hydra zariadenia v sieti s aktivovanou službou UPnP. Po nájdení sa pomocou nástroja stiahol zo smerovačov XML súbor, ktorý popisuje možnosti UPnP na danom zariadení. Kompletné záznamy je možné nájsť na CD priloženom k tejto práci. Medzi zariadeniami sa na každom smerovači nachádzalo zariadenie s názvom `WANConnectionDevice`, ktoré poskytovalo službu `WANPPPConnection`. V rámci tejto služby bolo možné nájsť celkom 12 akcií, pričom medzi najpodstatnejšie pre účely tohto penetračného testu boli akcie:

- `AddPortMapping` – slúži na pridanie záznamov o mapovaní portov
- `GetGenericPortMappingEntry` – slúži na výpis existujúcich záznamov o namapovaných portoch
- `GetExternalIPAddress` – slúži na zistenie externej IP adresy
- `DeletePortMapping` – slúži na mazanie jednotlivých mapovaní portov

V ďalšom kroku bolo do záznamov všetkých troch smerovačov pridané mapovanie. Po vypísaní si záznamu pomocou `GetGenericPortMappingEntry` bolo možné vidieť, že záznam je uložený v smerovači, ako je ukázané na obrázku 5.5.

```
NewPortMappingDescription : print
NewLeaseDuration : 0
NewInternalClient : 192.168.1.16
NewEnabled : 1
NewExternalPort : 3333
NewRemoteHost :
NewProtocol : TCP
NewInternalPort : 80
```

Obr. 5.5: Ukážka pridaného záznamu do smerovača Draytek

Na smerovače DrayTek a Zyxel sa bolo možné po pridaní tohto záznamu pripojiť z internetu na tlačiareň v lokálnej sieti, ktorá mala na porte 80 spustenú webovú administráciu. Komunikácia tlačiarne a zariadenia v internete bola zachytená vo Wiresharku a časť zachytenej komunikácie je možné vidieť na obrázku 5.6.

Source	Destination	Protocol	Length	Info
192.168.1.16	194.154.249.74	TCP	146	80 → 49359 [SYN, ACK] Seq=0 Ack=1 Win=4096 Len=0
194.154.249.74	192.168.1.16	TCP	146	49359 → 80 [ACK] Seq=1 Ack=1 Win=16560 Len=0
194.154.249.74	192.168.1.16	HTTP	608	GET / HTTP/1.1

Obr. 5.6: Časť komunikácie tlačiarne so zariadením v internete

Smerovač ADB tiež umožnil pripojenie sa na tlačiareň, avšak na rozdiel od zvyšných dvoch smerovačov si ku každému záznamu vytvorenému cez protokol UPnP pridával poznámku o pôvode tohto záznamu. Akonáhle bola IP adresa, na ktorú sa záznam odkazoval, uvoľnená a potom pridelená znovu buď tomu istému alebo inému zariadeniu, smerovač tento záznam zmazal. Toto správanie výrazne znížilo trvácnosť tohto útoku, napriek tomu, že bol úspešný a do vnútornej siete, vytvorenej smerovačom ADB, sa bolo možné dostať z internetu.

5.3 Fáza vyhodnotenia – Post-Engagement

V nasledujúcej časti bezpečnostného testovania sa nachádza dokumentácia vrátenia prostredia do pôvodného stavu a rozbor jednotlivých penetračných testov. Rozbor každého testu obsahuje analýzu možných dopadov, vyhodnotenie vážnosti zraniteľnosti a odporúčania na jej odstránenie.

Na vyhodnotenie vážnosti zraniteľnosti bola boužitá metodika DREAD, ktorá je podrobne popísaná v 3.3.3. Formát vyhodnocovania je založený na formáte uvedenom v [37].

5.3.1 Vrátenie prostredia do pôvodného stavu

V rámci bezpečnostného testovania sa menili nastavenia smerovačov a bezdrátovej tlačiarne. Tlačiareň bolo nutné pripojiť naspäť do domácej siete. Každý zo smerovačov bolo nutné uviesť do pôvodného nastavenia, v ktorom boli zapožičané poskytovateľom – čo bolo v tomto prípade východzie nastavenie.

5.3.2 Zraniteľnosť WPA2-PSK

Testovaná zraniteľnosť spočíva v slabom hesle, ktoré sa nachádza v slovníku skúšaných hesiel. Útok môže mať vážne dopady, pokiaľ sa neoprávnenej osobe podarí dostať sa do firemnej siete, kde sa môžu nachádzať rôzne servery s nízkou úrovňou zabezpečenia. Ďalšie vážne ohrozené subjekty sú užívatelia pripojení na sieti. V rámci lokálnej siete majú počítače často zvýšenú úroveň dôvery k iným zariadeniam. Náročnosť napadnutia takýchto zariadení je značne znížená oproti náročnosti napadnutia z internetu.

5.3.2.1 Vyhodnotenie vážnosti zraniteľnosti

- **D**amage potential – Priamo tento útok nespôsobuje škody, môže však otvárať priestor pre ďalšie, škodlivejšie útoky. $\mathbf{D = 5}$
- **R**eproducibility – Po oboznámení sa s nástrojmi a s dostatočne rozsiahlym slovníkom hesiel je jednoduché útok kedykoľvek zopakovať za krátky čas. $\mathbf{R = 9}$
- **E**xploitability – Útok je pri zložitejšom hesle náročný na čas. Prehľadávanie veľkých slovníkov môže trvať rádovo hodiny až dni. Na druhej strane naučiť sa používať nástroje podľa podrobného návodu nie je príliš náročné. $\mathbf{E = 4}$
- **A**ffected Users – Ohrození vedia byť všetci užívatelia v sieti, ale len s predpokladom, že majú aj oni nastavenú vysokú dôveru k zariadeniam v lokálnej sieti. $\mathbf{A = 4}$
- **D**iscoverability – Zistiť, že sieť je takto zraniteľná je možné až po nájdení hesla v slovníku. Teda dopredu nie je vôbec istý úspech. $\mathbf{D_2 = 0}$

Výsledné skóre je:

$$\frac{D + R + E + A + D_2}{5} = \frac{5 + 9 + 4 + 4 + 0}{5} = 4,4$$

Výsledné skóre nie je príliš vysoké, takže náprava tejto zraniteľnosti nemusí byť najväčšou prioritou. Na druhej strane náprava tejto zraniteľnosti je jednoduchá a časovo nenáročná, preto sa odporúča ju odstrániť.

5.3.2.2 Odporúčania na odstránenie zraniteľnosti

Najjednoduchším protiopatrením je zabezpečenie siete dostatočne silným heslom, ktoré sa určite nenachádza v žiadnom zozname známych hesiel. Nevýhodou tohto riešenia je, že užívateľom sa bude zložité heslo výrazne horšie pamätať. To zapríčiní, že užívatelia si budú potrebovať heslo zapísať. V lepšom prípade použijú software na správu hesiel, ktorý im zároveň zabezpečuje aj ochranu. V horšom prípade hrozí riziko, že heslo niektorí, menej skúsení užívatelia, začnú zapisovať na papier, ktorý môže skončiť v rukách útočníka.

5.3.3 Zraniteľnosť SSH

Služba SSH na smerovačoch nebýva často využívaná, pretože bežný užívateľ uprednostní administráciu cez webové rozhranie. Napriek tomu bola služba aktivovaná a boli v nej ponechané pôvodné účty s ľahko uhádnuteľnými údajmi.

Po odhalení týchto údajov sa útočník vie zmocniť smerovača. Možnosti, ako toto zneužiť, sú široké. Jednou z možností je DoS útok spôsobený zneprístupnením siete pre všetkých užívateľov. To je možné docieliť zmenou prihlasovacieho hesla na sieť alebo úplným vypnutím siete. Pokiaľ by boli zmenené aj prihlasovacie údaje na administráciu smerovača, bolo by pre opätovné získanie kontroly nutné reštartovať smerovač do výrobných nastavení.

Pokiaľ by sa jednalo o firemnú sieť, bolo by možné odstaviť webové služby danej firmy. To by sa odrazilo na dobrom mene firmy a ušlých ziskoch v čase, kedy sú služby nedostupné.

Inou možnosťou, ako zneužiť tento útok, je presmerovanie komunikácie na útočníkove servery s podvrhnutými stránkami a získavanie dôverných údajov všetkých užívateľov siete.

5.3.3.1 Vyhodnotenie vážnosti zraniteľnosti

- **D**amage potential – Tento útok vie obmedziť všetkých užívateľov siete a priamo ohrozuje bezpečnosť všetkých zariadení, ktoré sú pripojené do lokálnej siete. **D = 10**
- **R**eproducibility – Po oboznámení sa s nástrojmi a s dostatočne rozsiahlym slovníkom hesiel je jednoduché útok zopakovať. V porovnaní s útokom na WPA2-PSK je jednoduchšie tento útok zopakovať, lebo nie je vyžadovaná prítomnosť iného zariadenia v sieti. **R = 10**
- **E**xploitability – Naučiť sa používať nástroje, ktoré skúšajú heslá, nie je náročné. Útok priemerne zaberie viac času ako útok na WPA2-PSK. Jednak treba skúšať okrem hesiel aj prihlasovacie mená. Za druhé musí byť každé heslo odskúšané reálnym pokusom o prihlásenie. **E = 2**

- **A**ffected Users – Ohrozené sú všetky zariadenia pripojené v lokálnej sieti. V porovnaní s útokom na WPA2-PSK útočník získa kontrolu nad smerovačom a môže vykonávať ďalšie útoky prostredníctvom smerovača. Nepotrebuje sa spoliehať na vysokú dôveru zariadení k iným zariadeniam v sieti. $\mathbf{A = 10}$

- **D**iscoverability – Zistiť, že sieť je takto zraniteľná, je možné len z vnútornej siete pomocou skenovacieho nástroja alebo pokusov na slepo. Po zistení, že služba je aktivovaná, záleží len na sile hesla, a teda úspech nie je dopredu istý. $\mathbf{D_2 = 0}$

Výsledné skóre je:

$$\frac{D + R + E + A + D_2}{5} = \frac{10 + 10 + 2 + 10 + 0}{5} = 6,4$$

Výsledné skóre je pomerne vysoké a odporúča sa zamerať sa na odstránenie tejto zraniteľnosti v čo najbližšej dobe.

5.3.3.2 Odporúčania na odstránenie zraniteľnosti

Služba SSH by mala byť deaktivovaná, pokiaľ ju administrátor alebo iní užívatelia nevyužívajú. Pokiaľ však je táto možnosť vzdialenej administrácie využívaná, je potrebné ju patrične zabezpečiť.

V prvom rade je nutné zmazať všetky prednastavené účty s jednoduchými prihlasovacími menami a heslami. Pokiaľ existujú používatelia s rôznymi privilégiami, je nutné im prideliť samostatné účty s rozdielnymi prihlasovacími údajmi.

Útok využil to, že účty mali slabé, resp. bežne používané prihlasovacie údaje. Pokiaľ sa nastavia dostatočne silné prihlasovacie údaje, bude časovo veľmi náročné, až nemožné uhádnuť prihlasovacie meno a heslo a tým predísť útoku. Zároveň je potrebné docieliť, aby všetci užívatelia dbali na bezpečné heslá. Tomu vie administrátor dopomôcť deaktivovaním prázdnych hesiel.

Ďalšou možnosťou zabezpečenia je zavedenie módu autentizácie pomocou verejného kľúča, kedy sa meno a heslo vôbec nepoužíva.

5.3.4 Zraniteľnosť Telnet

Útok na službu Telnet bol, podobne ako útok na SSH, spôsobený tým, že je služba aktivovaná s nezmazanými predvytvorenými účtami, napriek tomu, že sa bežne nevyužíva.

Telnet je dnes už zastaralá služba, ktorá aj napriek tomu, že podporuje autentizáciu pomocou mena a hesla, nepodporuje šifrovanie komunikácie. Útokom hrubou silou je možné predísť nastavením bezpečných prihlasovacích údajov, avšak vždy hrozí riziko, že niekto odchytí tieto údaje počas prihlasovania sa na smerovač. Takýmto odchytením získa útočník heslo, bez ohľadu na to, aké náročné by ho bolo hádať.

Keďže je služba Telnet určená na vzdialenú administráciu, následky tohto útoku sú rovnaké ako následky popísané v analýze útoku na SSH (5.3.3).

5.3.4.1 Vyhodnotenie vážnosti zraniteľnosti

Vážnosť tejto zraniteľnosti bola pre kategórie **D**, **R**, **A** a $\mathbf{D_2}$ ohodnotená rovnako ako zraniteľnosť SSH. Jednotlivé zdôvodnenia pre SSH platia aj pre Telnet. Keďže komunikácia cez Telnet nie je šifrovaná a tým pádom je možné komunikáciu odpočúvať, kategória **E** bola ohodnotená číslom 5. Výsledné skóre je:

$$\frac{D + R + E + A + D_2}{5} = \frac{10 + 10 + 5 + 10 + 0}{5} = 7$$

Výsledné skóre je vysoké a je odporúčané zamerať sa na odstránenie tejto zraniteľnosti v čo najbližšej dobe.

5.3.4.2 Odporúčania na odstránenie zraniteľnosti

Vzhľadom na zastaralosť služby Telnet a absenciu akéhokoľvek šifrovania prenosu dát je najbezpečnejšou možnosťou uistiť sa, že je služba Telnet deaktivovaná.

5.3.5 Zraniteľnosť HTTP

Všetky tri smerovače používali na webovú administráciu protokol HTTP, kde bolo možné odchytiť prihlasovacie údaje. S nimi získa útočník plnú kontrolu nad smerovačom a nad celou sieťou. Následky tohto útoku sú zhodné s následkami útoku na SSH, ktoré sú popísané v 5.3.3.

5.3.5.1 Vyhodnotenie vážnosti zraniteľnosti

- **D**amage potential – Získaním administrátorských prístupových údajov na smerovač sa útočník zmocní siete. S takou kontrolou vie útočník spôsobiť veľké škody aj firme, aj jednotlivým užívateľom. $\mathbf{D = 10}$
- **R**eproducibility – Útok nie je úplne ľahké zopakovať. Je potrebné vždy zachytiť handshake zariadenia, ktoré sa prihlasuje do administrátorského účtu na smerovači. Bez odchyteného handshake nie je možné odšifrovať odchytenú komunikáciu medzi zariadením a smerovačom. V prípade

smerovača ADB ešte analyzovať zachytené hashované heslo. To v porovnaní s útokom na SSH prácu komplikuje, a preto je výsledné skóre **R = 6**

- **E**xploitability – Naučiť sa používať nástroje, odchytávať dáta, je zložité ako odpočúvanie komunikácie cez Telnet. Útok na smerovač s hashovaním vyžaduje na zistenie hesla viac času ako len samotné odchytenie dát a vyčítanie prihlasovacích údajov. Preto pre smerovače DrayTek a Zyxel **E = 5** a pre smerovač ADB je hodnota **E = 3**
- **A**ffected Users – Ohrozené sú všetky zariadenia pripojené v lokálnej sieti. **A = 10**
- **D**iscoverability – Zistiť, že sieť je takto zraniteľná, je možné len z vnútornej siete pomocou skenovacieho nástroja. $\mathbf{D_2 = 5}$

Výsledné skóre pre smerovače Zyxel a DrayTek je:

$$\frac{D + R + E + A + D_2}{5} = \frac{10 + 6 + 5 + 10 + 5}{5} = 7,2$$

Výsledné skóre pre ADB je:

$$\frac{D + R + E + A + D_2}{5} = \frac{10 + 6 + 3 + 10 + 5}{5} = 6,8$$

Výsledné skóre je pomerne vysoké, najmä u smerovačov DrayTek a Zyxel. Odporúča sa zamerať sa na odstránenie tejto zraniteľnosti v čo najbližšej dobe.

5.3.5.2 Odporúčania na odstránenie zraniteľnosti

Najefektívnejším riešením zraniteľnosti, ktorá bola demonštrovaná, je deaktivovanie protokolu HTTP a zavedenie používania protokolu HTTPS, ktorý šifruje všetky posielané dáta. Nie všetky smerovače majú túto možnosť, avšak ak hrozí riziko odpočúvania na sieti, je vhodné zvážiť kúpu iných modelov smerovačov, ktoré HTTPS používajú. Protokolom HTTPS by sa zabránilo odchytávaniu aj silných aj slabých hesiel. Nevýhodou je udržiavanie platného certifikátu na smerovači, avšak to je možné riešiť vydávaním certifikátu na dlhšie časové obdobie a aktualizáciami neplatných certifikátov.

5.3.6 Zraniteľnosť UPnP

Útok na UPnP bol prakticky ukázaný v rámci vnútornej siete a výsledkom bolo otvorenie tunelu medzi lokálnou sieťou a internetom. Pokiaľ sa útočník dostane do vnútra siete, vie vystaviť internetu akékoľvek zariadenie v tejto sieti bez väčších ťažkostí. V rámci firiem to spôsobuje vážnu hrozbu pre firemné servery, ktoré bežia len na lokálnej sieti. V rámci domácností tento

útok ohrozuje bežných užívateľov alebo smart zariadení, ktoré sa môže útočník snažiť ovládať.

V kapitole 4.5 je popísaný jeden možný spôsob, ako spúšťať škodlivý kód z internetu v rámci lokálnej siete. Pokiaľ by tento útok bol spojený s útokom na UPnP, mal by rovnaké následky, ako keby bol užívateľ vo vnútornej sieti. Tým sa značne zvyšuje závažnosť zraniteľnosti UPnP, pretože skupina potenciálnych útočníkov sa rozširuje na užívateľov v celom internete.

5.3.6.1 Vyhodnotenie vážnosti zraniteľnosti

- **D**amage potential – Tento útok vie vážne ohroziť všetky zariadenia v lokálnej sieti, keďže je možné ich priamo vystaviť internetu **D = 10**
- **R**eproducibility – Po oboznámení sa s nástrojmi a problematikou je jednoduché spraviť útok kedykoľvek **R = 10**
- **E**xploitability – Naučiť sa používať nástroje, ktoré skúšajú heslá, nie je náročné. Útok nie je veľmi časovo náročný, pokiaľ útočník vie, čo robí a ako funguje protokol UPnP. Na rozdiel od útoku na SSH alebo HTTP, nie je nutné čakať a spoliehať sa na nájdenie hesla v slovníku, keďže pri UPnP nedochádza k žiadnej autentizácii. **E = 8**
- **A**ffected Users – Ohrozené sú všetky zariadenia pripojené v lokálnej sieti. **A = 10**
- **D**iscoverability – Zistiť, že sieť je takto zraniteľná, je možné z vnútornej siete pomocou skenovacieho nástroja alebo z vonkajšej siete s využitím skenovacích nástrojov, ako napríklad na stránke [70]. $\mathbf{D_2 = 7}$

Výsledné skóre je:

$$\frac{D + R + E + A + D_2}{5} = \frac{10 + 10 + 8 + 10 + 7}{5} = 9$$

Výsledné skóre je najvyššie spomedzi všetkých nájdených zraniteľností. Je vysoko odporúčané podniknúť kroky, ktoré odstránia túto zraniteľnosť.

5.3.6.2 Odporúčania na odstránenie zraniteľnosti

Pri uvádzaní smerovača do prevádzky je vhodné použiť skenovací nástroj, ktorý overí, či služba UPnP počúva na internetovom rozhraní. Pokiaľ to je tak, službu nie je možné bezpečne používať a je odporúčané ju deaktivovať. V prípade, že užívateľ chce využívať UPnP na lokálnej sieti, je vhodné zvážiť výmenu smerovača za model, ktorý nevystavuje službu UPnP do internetu.

V rámci vnútornej siete je vhodné UPnP deaktivovať tiež. Prvým dôvodom pre to je hrozba útoku z vnútornej siete, ktorý bol demonštrovaný v 5.2.8. Ľubovoľný užívateľ na sieti mohol otvoriť tunel do internetu a komunikovať so zariadeniami vo vnútornej sieti.

Druhým argumentom je fakt, že útok na UPnP z vnútornej siete sa stáva oveľa nebezpečnejším v kombinácii s útokom ako DNS rebinding (4.5). Vtedy neohrozujú bezpečnosť len útočníci vo vnútornej sieti, ale aj útočníci z celého internetu.

Záver

Cieľom práce bolo zhodnotenie bezpečnosti vybraných SOHO smerovačov. Tento cieľ mal byť dosiahnutý oboznámením sa s existujúcimi bezpečnostnými štandardmi, získaním informácií o existujúcich klasifikáciách bezpečnostných testov a navrhnutím metodiky bezpečnostného testovania smerovačov. Práca mala pokračovať preskúmaním známych zraniteľností, ktoré sa môžu vyskytovať na SOHO smerovačoch. Ďalej bolo cieľom práce aplikovanie navrhnutej metodiky a otestovanie vybraných zraniteľností.

Práca splnila hlavný cieľ, aj všetky vedľajšie ciele, ktoré boli na začiatku určené. V prvom rade bol uskutočnený prieskum technických štandardov zameraných na bezpečnosť sieťových prvkov a prieskum existujúcich kategorizácií bezpečnostných testov. Na základe tohto prieskumu bola sformulovaná metodika bezpečnostného testovania smerovačov.

Ďalšia časť práce sa zaoberala známymi zraniteľnosťami smerovačov. Pozornosť bola upriamená na útoky na služby vzdialenej administrácie smerovačov, protokoly UPnP a WPA2-PSK, a nakoniec na útok DNS Rebinding, ktorý prekonáva bariéru medzi lokálnou sieťou a internetom. Práca podrobne popísala, ako fungujú slabé miesta a ako je možné ich zneužiť na uskutočnenie útoku.

V praktickej časti boli otestované tri smerovače, ktoré sa bežne vyskytujú v domácnostiach alebo menších podnikoch. Testovanie prebiehalo podľa metodiky, ktorá bola predtým v práci sformulovaná.

V prvej fáze bezpečnostného testovania sa predstavili nástroje a testovacie prostredie, ktoré boli využívané počas testovania. Bol vytýčený rozsah testovania a určili sa pravidlá, podľa ktorých testovanie prebiehalo. Boli predstavené testované smerovače spolu so všetkými informáciami, ktoré o nich boli pred testovaním známe.

V druhej fáze bezpečnostného testovania prebehol prieskum zraniteľností a na všetkých smerovačoch boli identifikované potenciálne zraniteľné miesta. Tieto miesta boli následne otestované. Penetračné testy odhalili viaceré nedostatky v zabezpečení. Pri všetkých troch smerovačoch bolo možné dostať sa do administrácie smerovača a získať tak nad ním kontrolu. Heslá k prístupu do bezdrátovej siete zabezpečenej WPA2-PSK boli u každého smerovača zistené. Nakoniec prebehla demonštrácia útoku na UPnP, ktorý skončil úspešne a umožnil prístup na zariadenia v lokálnej sieti internetu.

V tretej fáze sa píše, aké kroky bolo potrebné uskutočniť na návrat testovaného prostredia do pôvodného stavu. U všetkých uskutočnených útokov sa analyzovali možné následky, vyhodnotila sa vážnosť nájdenej zraniteľnosti a boli poskytnuté odporúčania na nápravu tejto zraniteľnosti.

V budúcnosti je možné na prácu nadviazať niekoľkými spôsobmi. Prvým je analýza ďalších zraniteľností smerovačov. Všetky analyzované zraniteľnosti je možné následne otestovať a zistiť, či sú zrealizovateľné v praxi a akú hrozbu predstavujú. Ďalšou možnosťou je aplikovanie metodiky na iné smerovače a získanie informácií o stave väčšieho množstva SOHO smerovačov.

Literatúra

[1] International Organization for Standardization: *Standards in our world [internetová stránka]*. [online], [cit. 3. marca 2019]. Dostupné z: https://www.iso.org/sites/ConsumersStandards/1_standards.html

[2] Vondruška, P.: *Úvod do klasických a moderních metod šifrování ALG082 – Standardy a normy*. Technická zpráva, MFF UK. [online], 2004, [cit. 3. marca 2019]. Dostupné z: http://www.karlin.mff.cuni.cz/~tuma/nciphers/standardy_normy_s-1.pdf

[3] International Organization for Standardization: *ISO deliverables [internetová stránka]*. [online], [cit. 3. marca 2019]. Dostupné z: https://www.iso.org/deliverables-all.html

[4] International Organization for Standardization: *All about ISO [internetová stránka]*. [online], [cit. 3. marca 2019]. Dostupné z: https://www.iso.org/about-us.html

[5] International Organization for Standardization: *ISO: a global network of national standards bodies [internetová stránka]*. [online], [cit. 3. marca 2019]. Dostupné z: https://www.iso.org/members.html

[6] Iso27001security: *Timeline [internetová stránka]*. [online], [cit. 4. marca 2019]. Dostupné z: https://www.iso27001security.com/html/timeline.html

[7] Risk Analysis Consultants: *ISO/IEC 27000:2018 [internetová stránka]*. [online], [cit. 4. marca 2019]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27000

[8] Risk Analysis Consultants: *ISO/IEC 27001:2013 [internetová stránka]*. [online], [cit. 4. marca 2019]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27001

[9] ISMS.online: *ISO 27001 - Annex A.13: Communications Security [internetová stránka]*. [online], [cit. 5. marca 2019]. Dostupné z: https://www.isms.online/iso-27001/annex-a-13-communications-security/

[10] Iso27001security: *ISO/IEC 27033:2010 [internetová stránka]*. [online], [cit. 5. marca 2019]. Dostupné z: https://www.iso27001security.com/html/27033.html

[11] Risk Analysis Consultants: *ISO/IEC 27033 [internetová stránka]*. [online], [cit. 5. marca 2019]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27033

[12] Wallace, K.: *Common Criteria and Protection Profiles: How to Evaluate Information*. [online], 2003, [cit. 5. marca 2019]. Dostupné z: https://www.sans.org/reading-room/whitepapers/standards/common-criteria-protection-profiles-evaluate-information-1078

[13] Common Criteria: *History [internetová stránka]*. [online], [cit. 8. marca 2019]. Dostupné z: https://www.commoncriteriaportal.org/iccc/ICCC_arc/history.htm

[14] Ferris, M.; a i.: *A Security Business Case for the Common Criteria*. [online], [cit. 8. marca 2019]. Dostupné z: https://slideplayer.com/slide/6671286/

[15] Common Criteria: *About the Common Criteria [internetová stránka]*. [online], [cit. 8. marca 2019]. Dostupné z: https://www.commoncriteriaportal.org/ccra/index.cfm

[16] Common Criteria: *Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model*. [online], apríl 2017, [cit. 8. marca 2019]. Dostupné z: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[17] Common Criteria: *Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance components*. [online], apríl 2017, [cit. 8. marca 2019]. Dostupné z: https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

[18] Buček, J.: *HW Bezpečnost – HW bezpečnostní moduly, čipové karty*. [online], 2018, [cit. 13. marca 2019]. Dostupné z: https://moodle.fit.cvut.cz/pluginfile.php/72110/mod_resource/content/0/prednaska1.pdf

[19] Česká agentura pro standardizaci: *O nás [internetová stránka]*. [online], [cit. 13. marca 2019]. Dostupné z: http://www.agentura-cas.cz/o-nas

[20] Technické Normy: *České technické normy ČSN [internetová stránka]*. [online], [cit. 13. marca 2019]. Dostupné z: https://www.technickenormy.cz/tridy-norem-csn/

[21] Úřad pro technickou normalizaci, metrologii a státní zkušebnictví: *Co je to technická norma? [internetová stránka]*. [online], [cit. 13. marca 2019]. Dostupné z: http://www.unmz.cz/urad/co-je-to-technicka-norma-

[22] TECHNOR print, s.r.o: *Elektrotechnika [internetová stránka]*. [online], [cit. 14. marca 2019]. Dostupné z: http://www.technicke-normy-csn.cz/technicke-normy/elektrotechnika-36/

[23] Muniz, J.; Lakhani, A.: *Web Penetration Testing with Kali Linux*. Packt Publishing Ltd., september 2013, ISBN 978-1-78216-316-9.

[24] Barnett, P.: *Penetration Testing vs. Vulnerability Assessment*. [online], september 2018, [cit. 26. marca 2019]. Dostupné z: https://www.hitachi-systems-security.com/blog/penetration-testing-vs-vulnerability-assessment/

[25] Symantec employee: *What is social engineering? Tips to help avoid becoming a victim*. [online], [cit. 26. marca 2019]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

[26] My Security Awareness: *What is Impersonation in Social Engineering? [internetová stránka]*. [online], [cit. 27. marca 2019]. Dostupné z: https://mysecurityawareness.com/article.php?article=384&title=what-is-impersonation-in-social-engineering#.XLtpGpyxWV4

[27] Rongala, A.: *What is Black Box Testing: Advantages and Disadvantages*. [online], marec 2015, [cit. 27. marca 2019]. Dostupné z: https://www.invensis.net/blog/it/black-box-testing-advantages-disadvantages/

[28] Software Testing Fundamentals: *Black Box Testing [internetová stránka]*. [online], [cit. 27. marca 2019]. Dostupné z: http://softwaretestingfundamentals.com/black-box-testing/

[29] Software Testing Fundamentals: *White Box Testing [internetová stránka]*. [online], [cit. 28. marca 2019]. Dostupné z: http://softwaretestingfundamentals.com/white-box-testing/

[30] Rongala, A.: *What is White Box Software Testing: Advantages and Disadvantages*. [online], marec 2015, [cit. 28. marca 2019]. Dostupné z: https://www.invensis.net/blog/it/white-box-software-testing-advantages-disadvantages/

[31] Software Testing Fundamentals: *Gray Box Testing [internetová stránka]*. [online], [cit. 28. marca 2019]. Dostupné z: http://softwaretestingfundamentals.com/gray-box-testing/

[32] Hutter, D.: *Physical Security and Why It Is Important*. [online], jún 2016, [cit. 30. marca 2019]. Dostupné z: https://www.sans.org/reading-room/whitepapers/physical/physical-security-important-37120

[33] Ripe Network Coordination Centre: *Understanding IP Addressing and CIDR Charts*. [online], január 2011, [cit. 30. marca 2019]. Dostupné z: https://www.ripe.net/about-us/press-centre/understanding-ip-addressing

[34] Guru99: *Automation Testing Vs. Manual Testing: What's the Difference [internetová stránka]*. [online], [cit. 30. marca 2019]. Dostupné z: https://www.guru99.com/difference-automated-vs-manual-testing.html

[35] Guru99: *What is Destructive Testing? Techniques, Methods, Example [internetová stránka]*. [online], [cit. 30. marca 2019]. Dostupné z: https://www.guru99.com/destructive-testing.html

[36] Penetration Test Guidance Special Interest Group PCI Security Standards Council: *Information Supplement: Penetration Testing Guidance*. [online], september 2017, [cit. 2. apríla 2019]. Dostupné z: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

[37] Zahradnický, T.; Kokeš, J.: *Bezpečný kód – Úvod do bezpečného kódu, modelování hrozeb*. [online], február 2019, [cit. 2. apríla 2019]. Dostupné z: https://moodle.fit.cvut.cz/pluginfile.php/86748/mod_folder/content/0/bek01cz-Introduction_to_secure_code.pdf?forcedownload=1

[38] FIRST: *Common Vulnerability Scoring System Version 3.0 Calculator [internetová stránka]*. [online], [cit. 6. apríla 2019]. Dostupné z: https://www.first.org/cvss/calculator/3.0

[39] Common Weakness Scoring System: *Scoring CWEs*. [online], september 2014, [cit. 6. apríla 2019]. Dostupné z: https://cwe.mitre.org/cwss/cwss_v1.0.1.html

[40] Sak, B.; Ram, J. R.: *Mastering Kali Linux Wireless Pentesting*. Packt Publishing Ltd., február 2016, ISBN 978-1-78528-556-1.

[41] Postel, J.; Reynolds, J.: *TELNET PROTOCOL SPECIFICATION*. [online], máj 1983, [cit. 9. apríla 2019]. Dostupné z: https://tools.ietf.org/html/rfc854

[42] SSH Communications Security: *SSH (Secure Shell) [internetová stránka]*. [online], [cit. 10. apríla 2019]. Dostupné z: https://www.ssh.com/ssh/

[43] SSH Communications Security: *SSH Tectia® Server 5.5 for IBM z/OS*. [online], september 2007, [cit. 10. apríla 2019]. Dostupné z: https://www.ssh.com/manuals/server-zos-product/55/chooseauth-chapter.html

[44] Fielding, R.; Reschke, J.: *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*. Adobe. [online], jún 2014, [cit. 12. apríla 2019]. Dostupné z: https://tools.ietf.org/html/rfc7230

[45] Rescorla, E.: *HTTP Over TLS*. [online], 2000 máj, [cit. 13. apríla 2019]. Dostupné z: https://tools.ietf.org/html/rfc2818

[46] IBM: *Digital certificates [internetová stránka]*. [online], [cit. 17. apríla 2019]. Dostupné z: https://www.ibm.com/support/knowledgecenter/en/SSFKSJ_9.0.0/com.ibm.mq.sec.doc/q009820_.htm

[47] Microsoft Corporation: *Understanding Universal Plug and Play*. [online], jún 2000, [cit. 17. apríla 2019]. Dostupné z: https://www.cs.colorado.edu/~rhan/CSCI_7143_002_Fall_2001/Papers/

[48] Akamai: *UPnProxy: Blackhat Proxies via NAT Injections*. [online], marec 2018, [cit. 20. apríla 2019]. Dostupné z: https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-paper.pdf

[49] Constantin, L.: *Hackers Exploit UPnP in Routers to Expose Private Networks to Attacks*. [online], november 2018, [cit. 20. apríla 2019]. Dostupné z: https://securityboulevard.com/2018/11/hackers-exploit-upnp-in-routers-to-expose-private-networks-to-attacks/

[50] krackattacks: *Introduction [internetová stránka]*. [online], [cit. 23. apríla 2019]. Dostupné z: https://www.krackattacks.com/

[51] admin: *4-Way Handshake*. [online], január 2019, [cit. 25. apríla 2019]. Dostupné z: http://www.wifi-professionals.com/2019/01/4-way-handshake

[52] Novák, M.: *Odposlouchávání a prolamování Wi-Fi sítí zabezpečených pomocí WPA2*. [online], január 2017, [cit. 25. apríla 2019]. Dostupné z: https://www.root.cz/clanky/odposlouchavani-a-prolamovani-wi-fi-siti-zabezpecenych-pomoci-wpa2/

[53] Mikm: *The four-way handshake in 802.11i*. [online], január 2007, [cit. 25. apríla 2019]. Dostupné z: https://en.wikipedia.org/wiki/IEEE_802.11i-2004

[54] Geier, J.: *Overview of the IEEE 802.11 Standard*. [online], december 2001, [cit. 26. apríla 2019]. Dostupné z: http://www.informit.com/articles/article.aspx?p=24411&seqNum=7

[55] Noman, H. A.; Abdullah, S. M.; Mohammed, H. I.: *An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless 802.11 Networks*. [online], júl 2015, [cit. 26. apríla 2019]. Dostupné z: https://pdfs.semanticscholar.org/e41e/8f773e44232fb6ff3e4c827282b5cd50a735.pdf

[56] Deleon, N.: *FCC Fines Hotel Wi-Fi Provider for Blocking Personal Hotspots*. [online], august 2015, [cit. 27. apríla 2019]. Dostupné z: https://motherboard.vice.com/en_us/article/jp57qp/fcc-fines-freedom-hating-hotel-wi-fi-provider-for-blocking-personal-hotpsots

[57] Hetter, K.: *Marriott fined $600,000 by FCC for blocking guestsẂi-Fi*. [online], október 2014, [cit. 27. apríla 2019]. Dostupné z: https://edition.cnn.com/2014/10/03/travel/marriott-fcc-wi-fi-fine/index.html

[58] Dorsey, B.: *Attacking Private Networks from the Internet with DNS Rebinding*. [online], jún 2018, [cit. 30. apríla 2019]. Dostupné z: https://medium.com/@brannondorsey/attacking-private-networks-from-the-internet-with-dns-rebinding-ea7098a2d325

[59] Ruderman, J.: *Same-origin policy*. [online], marec 2019, [cit. 30. apríla 2019]. Dostupné z: https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

[60] Jackson, C.; a i.: *Protecting Browsers from DNS Rebinding Attacks*. [online], november 2007, [cit. 30. apríla 2019]. Dostupné z: https://crypto.stanford.edu/dns/dns-rebinding.pdf

[61] Hertzog, R.; O'Gorman, J.; Aharoni, M.: *Kali Linux Revealed*. Offsec Press, 2017, ISBN 978-0-9976156-0-9, [cit. 2. mája 2019]. Dostupné z: https://kali.training/lessons/introduction/

[62] Lyon, G.: *Nmap [internetová stránka]*. [online], [cit. 2. mája 2019]. Dostupné z: https://nmap.org/

[63] Wireshark: *About Wireshark [internetová stránka]*. [online], [cit. 3. mája 2019]. Dostupné z: https://www.wireshark.org/

[64] mister_x: *Aircrack-ng*. [online], október 2018, [cit. 3. mája 2019]. Dostupné z: https://www.aircrack-ng.org/doku.php?id=aircrack-ng

[65] mister_x: *Airmon-ng*. [online], máj 2019, [cit. 5. mája 2019]. Dostupné z: https://www.aircrack-ng.org/doku.php?id=airmon-ng

[66] mister_x: *Airodump-ng*. [online], október 2018, [cit. 5. mája 2019]. Dostupné z: https://www.aircrack-ng.org/doku.php?id=airodump-ng

[67] mister_x: *Aireplay-ng*. [online], november 2018, [cit. 5. mája 2019]. Dostupné z: https://www.aircrack-ng.org/doku.php?id=aireplay-ng

[68] vanhauser thc: hydra [internetová stránka]. [online], apríl 2019, [cit. 5. mája 2019]. Dostupné z: https://github.com/vanhauser-thc/thc-hydra

[69] The SourceSec Security Research Group: *SourceSec Security Research Group's Miranda UPNP Administration Tool*. [online], [cit. 5. mája 2019]. Dostupné z: https://code.google.com/archive/p/mirandaupnptool/

[70] Gibson Research Corporation: *Shields Up! [internetová stránka]*. [online], [cit. 5. mája 2019]. Dostupné z: https://www.grc.com/x/ne.dll?bh0bkyd2

Dodatok **A**

Zoznam použitých skratiek

AES Advanced Encryption Standard

ANSI American National Standards Institute

ASTM American Society for Testing and Materials

CA Certificate authority

CBC Cipher Block Chaining

CC Common Criteria

CD Compact Disc

CVSS Common Vulnerability Scoring System

CWSS Common Weakness Scoring System

CTCPEC Canadian Trusted Computer Product Evaluation Criteria

ČAS Česká agentura pro standardizaci

ČSN Česká technická norma

DDoS Distributed Denial of Service

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DoS Denial of Service

EAL Evaluation Assurance Level

FIPS Federal Information Processing Standards

GMK Group Master Key

GTK Group Temporal Key

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

IEC International Electrotechnical Commission

IEEE Institute of Electrical and Electronics Engineers

IoT Internet of things

IP Internet Protocol

IPS Intrusion Prevention System

IS International Standard

ISO International Organization for Standardization

IT informačné technológie

ITSEC Information Technology Security Evaluation Criteria

IWA International Workshop Agreements

LAN Local Area Network

MAC Media Access Control Address

MIC Message Integrity Code

NAT Network address translation

Nonce Number used once

OS operačný systém

OSI Open Systems Interconnection

PAS Publicly Available Specification

PIN Personal Identification Number

PP Protection Profile

PSK Pre-Shared Key

PTK Pairwise Transient Key

RFC Request for Comments

RSH Remote Shell

SPI Stateful Packet

SNMP Simple Network Management Protocol

SOAP Simple Object Access Protocol

SOHO Small Office Home Office

SSDP Simple Service Discovery Protocol

SSH Secure Shell

SSID Service Set Identifier

ST Security Target

TCP Transmission Control Protocol

TCSEC Trusted Computer System Evaluation Criteria

TOE Target of Evaluation

TR Technical report

TS Technical standard

TTL Time to Live

UPnP Universal Plug and Play

USA United States of America

USB Universal Serial Bus

VPN Virtual Private Network

XML Extensible Markup Language

WAN Wide Area Network

WEP Wired Equivalent Privacy

WPA Wi-Fi Protected Access

WWW World Wide Web

Dodatok **B**

Obsah priloženého CD

- `readme.txt` ..... stručný popis obsahu CD
- `testy` ..... adresár s dátami z testovania
  - `dictionaries` ..... adresár so slovníkmi prihlasovacích mien a hesiel
  - `explore_network` ..... adresár s výsledkami prieskumu siete
  - `other_info` ..... adresár s všeobecnými informáciami
    - `lab_smerovace` ..... fotografia laboratória so smerovačmi
    - `smerovace_info` ..... informácie o nastaveniach smerovačov
  - `test_http` ..... adresár s výsledkami útoku na HTTP
    - `skript` ..... adresár so skriptom použitým pri útočení na HTTP
  - `test_ssh` ..... adresár s výsledkami útoku na SSH
  - `test_telnet` ..... adresár s výsledkami útoku na Telnet
  - `test_upnp` ..... adresár s výsledkami útoku na UPnP
  - `test_wpa2` ..... adresár s výsledkami útoku na WPA2
- `text` ..... text práce
  - `Bakalárska práca.pdf` ..... text práce vo formáte PDF
- `src`
  - `Bakalárska práca` ..... zdrojová forma práce vo formáte LaTeX
    - `images` ..... adresár s obrázkami použitými v práci