ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

FAKULTA BIOMEDICÍNSKÉHO INŽENÝRSTVÍ

Katedra biomedicínské informatiky

Demonstrační platforma pro výuku kyberbezpečnosti – ochrana bezdrátových WiFi sítí

Demonstration platform for teaching cybersecurity – protection of wireless WiFi networks

Bakalářská práce

Studijní program:	Biomedicínská a klinická technika
Studijní obor:	Biomedicínská informatika

Autor bakalářské práce:	Kateřina Hanžlíková
Vedoucí bakalářské práce:	doc. Ing. Karel Hána, Ph.D.

Kladno 2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Hanžlíková**	Jméno:	**Kateřina**	Osobní číslo:	**456634**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra informačních a komunikačních technologií v lékařství**				
Studijní program:	**Biomedicínská a klinická technika**				
Studijní obor:	**Informační a komunikační technologie v lékařství**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Demonstrační platforma pro výuku kyberbezpečnosti – ochrana bezdrátových WiFi sítí

Název bakalářské práce anglicky:

Demonstration platform for teaching cybersecurity - protection of wireless WiFi networks

Pokyny pro vypracování:

Proveďte rešerši problematiky ochrany bezdrátových WiFi sítí a souvisejících základů kryptologie z pohledu kyberbezpečnosti. Navrhněte a prakticky realizujte HW a SW platformu umožňující demonstrace základních druhů útoků zneužívajících běžné zranitelnosti WiFi sítí a konkrétní postupy vedoucí ke zvyšování jejich zabezpečení. Problematiku následně rozdělte na samostatnou sadu úloh pro jednotlivá cvičení pro studenty tak, aby bylo možné využít co nejdostupnější HW a SW, na kterém by studenti zvládli realizovat praktická cvičení s ohledem na Covidovou dobu buď zcela samostatně podle návodů nebo na základě on-line pokynů a dohledu vyučujícího.

Seznam doporučené literatury:

[1] Burda, K., Kryptografie okolo nás, ed. 1, CZ.NIC, 2019, ISBN 978-80-88168-52-2
[2] Kolouch, J., Bašt, P. a kol., CyberSecurity, ed. 1, CZ.NIC, 2019, ISBN 978-80-88168-34-8
[3] Buchanan, C., Ramachandran, V., Kali Linux Wireless Penetration Testing Beginner's Guide – Third Edition, ed. 3, Packt>, 2017, ISBN 978-1788831925
[4] R. Jirásek, P., Novák, L., Požár, J., Výkladový slovník kybernetické bezpečnosti: Cyber security glossary, ed. 3, Policejní akademie ČR v Praze, 2015, ISBN 978-80-7251-436-6

Jméno a příjmení vedoucí(ho) bakalářské práce:

doc. Ing. Karel Hána, Ph.D.

Jméno a příjmení konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **15.02.2021**
Platnost zadání bakalářské práce: **18.09.2022**

doc. Ing. Karel Hána, Ph.D.
vedoucí katedry

prof. MUDr. Jozef Rosina, Ph.D., MBA
děkan

PROHLÁŠENÍ

Prohlašuji, že jsem bakalářskou práci s názvem Demonstrační platforma pro výuku kyberbezpečnosti – ochrana bezdrátových WiFi sítí vypracovala samostatně a použila k tomu úplný výčet citací použitých pramenů, které uvádím v seznamu přiloženém k diplomové práci.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně 11. 5. 2022 …..……..……...

Kateřina Hanžlíková

PODĚKOVÁNÍ

Ráda bych poděkovala panu doc. Ing. Karlu Hánovi, Ph.D . za konzultace a cenné rady během vypracovávání práce. Zároveň bych také ráda poděkovala své rodině za trpělivost a psychickou podporu.

ABSTRAKT

Demonstrační platforma pro výuku kyberbezpečnosti – ochrana sítí

Práce se zabývá ochranou bezdrátových sítí a jejímu prolamování. Cílem práce bylo vytvořit sadu úloh pro studenty, v níž bude možné vyzkoušet si různé typy útoků využívajících zranitelnosti WiFi sítí a zamyslet se nad možnou ochranou těchto sítí.

Důraz je kladen na možnost vykonávat tyto úlohy samostatně podle návodu, nebo na základě pokynů a dohledu vyučujícího.

Tato sada úloh je připojena k bakalářské práci a obsahuje osm samostatných úloh.

Klíčová slova

kali, linux, prolamování, wifi, hesla

ABSTRACT

Demonstration platform for teaching cybersecurity – protection of wireless WiFi networks

The thesis addresses the subject of securing wireless networks and the problem of cracking security protocols. The aim of the research was to create a set of tasks for students which will allow for testing various types of attacks attempting to breach the network's security.

The objective of these tasks is to promote ideas in terms of possible security implementations for these networks.

The tasks provided are emphasised to be completed either individually abiding by instructions or based on the advice of a lecturer. Furthermore, the set of tasks is a part of the bachelor's thesis and consist's of eight individual tasks.

Keywords

kali, linux, cracking, wifi, passwords

Obsah

Seznam symbolů a zkratek

Seznam zkratek

Zkratka	Význam
WiFi	Bezdrátová technologie pro šíření dat
VM	Virtuální počítač
WPA	Chráněný přístup k WiFi
TCP/IP	Primární přenosový protokol/protokol síťové vrstvy
AP	Access point – přístupový bod
MAC	Media Access Control
SSID	Service Set Identifier
KVM	Kernel-based Virtual Machine
GUI	Graphic User Interface

1 Úvod

Žijeme v době, kdy se náš život čím dál víc přesouvá do online prostředí. Takový přesun sebou nese mnoho výhod, například ulehčení práce v mnoha odvětvích, její zefektivnění a dostupnost.

Digitální prostředí nás však může ve velkém ohrožovat. Přese všechnu snahu ochránit uživatele je zde stále velké množství útoků, podvodů a jiných nezákonných jednání, která mohou vést ke ztrátě majetku, domova nebo třeba i života.

Velmi dobrým příkladem za všechny je kyberútok na Benešovskou nemocnici, který se odehrál v noci 11. prosince 2019 a který způsobil škodu přes 59 milionů korun. [1] Životy pacientů naštěstí neohrozil (útok ani nebyl mířený cíleně na nemocnici), a díky včasnému zásahu techniků zůstala data na svém místě, ač zašifrovaná, ale celá tato kauza nám jen ukázala, jakým je kyberbezpečnost stále podceňovaným tématem.

2 Cíle práce

Cílem práce bylo provést rešerši v oblasti ochrany bezdrátových WiFi sítí a souvisejících základů kyberbezpečnosti a na základě těchto získaných vědomostí vytvořit sadu úloh pro studenty, na níž si budou moci vyzkoušet základní útoky zneužívající běžné zranitelnosti WiFi sítí a zamyslet se nad postupy vedoucími ke zvyšování jejich zabezpečení.

Tato cvičení mají být vytvořena tak, aby je bylo možné provádět s ohledem na Covidovou dobu, tudíž samostatně podle návodů nebo na základě online pokynů a dohledu vyučujícího.

3 Přehled současného stavu

Nejprve definujme kybernetický prostor. Podle Českého slovníku kybernetické bezpečnosti je kybernetický prostor digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací. [2]

Kybernetický prostor (dále kyberprostor) je tvořen prvky informačních a komunikačních technologií, které vytvářejí pomocí protokolu TCP/IP celosvětovou, globální počítačovou síť, a jednotlivými počítačovými systémy, které jsou do této sítě připojeny a které v ní interagují. Tvoří tak dynamický, neustále se měnící systém, též těžko definovatelný a prakticky neomezený. Jde vlastně o virtuální realitu bez začátku a konce, závislou na technologiích reálného světa.

Kyberprostor lze definovat také vlastnostmi, kterými disponuje. Popsat ho můžeme jako decentralizovaný, globální, otevřený, bohatý na informace a interaktivní. Jako takový má moc ovlivňovat mínění uživatele.

Z pohledu dostupnosti a dohledatelnosti dat pro běžného uživatele můžeme kyberprostor rozdělit na tři podkategorie: povrchový web, hluboký web a temný web. [3]

Povrchový web je ta část kyberprostoru, která je veřejná a indexovaná. Je to ta část webu, k níž se dostáváme každý den – třeba skrze vyhledávače právě díky indexaci.

Hluboký web je pak část prostoru, která není dohledatelná vyhledávači. Uživatel musí znát příslušné informační zdroje a specifické vyhledávací postupy.

Konečně temný web je pak přístupný pouze za pomocí sofistikovaných nástrojů, které zaručují mimo jiné taky anonymitu uživatele. Často slouží k nelegálním činnostem. [4]

V tomto prostoru (nejčastěji v povrchovém webu či v hlubokém webu) se pohybujeme s různými cíli, z nichž je jeden z nejdůležitějších získávání nebo sdílení informací. Nejsme však sami. Za každou druhou stranou, k níž se připojujeme, může čekat někdo, kdo chce také informace; cenné informace o nás, kterými si nelegálně dopomůže k vlastnímu blahobytu.

Tyto informace (a jiné) musíme chránit. O toto pole vědění se zajímá právě kybernetický bezpečnost.

3.1 Kybernetická bezpečnost

Kybernetická bezpečnost se týká každého z nás. Každý jeden uživatel by na ni měl dbát a chránit tak sebe a své informace.

Lze ji definovat jako bezpečnost v kyberprostoru, kdy jde o vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám. Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací. [2]

Kromě jiného se ji snaží definovat také směrnice evropského parlamentu a Rady 2016/1148 ze dne 6 . července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. V čl. 4 odst. 2 uvádí, že „bezpečnost sítí a informačních systémů představuje schopnost těchto sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné.“ [5]

Co se týče přístupu České republiky, ten je podle strategie kybernetické bezpečnosti České republiky na období let 2021–2025 od začátku založen na efektivním modelu spolupráce všech relevantních aktérů na národní a mezinárodní úrovni, v němž má každý subjekt jasně stanovená povinnosti a pravomoci. [6]

Nelze ji podceňovat a už rozhodně ne bagatelizovat. Měla by být řešena dlouhodobě a systematicky. Je nutné si uvědomit, že je realizována jak v kyberprostoru, tak mimo něj.

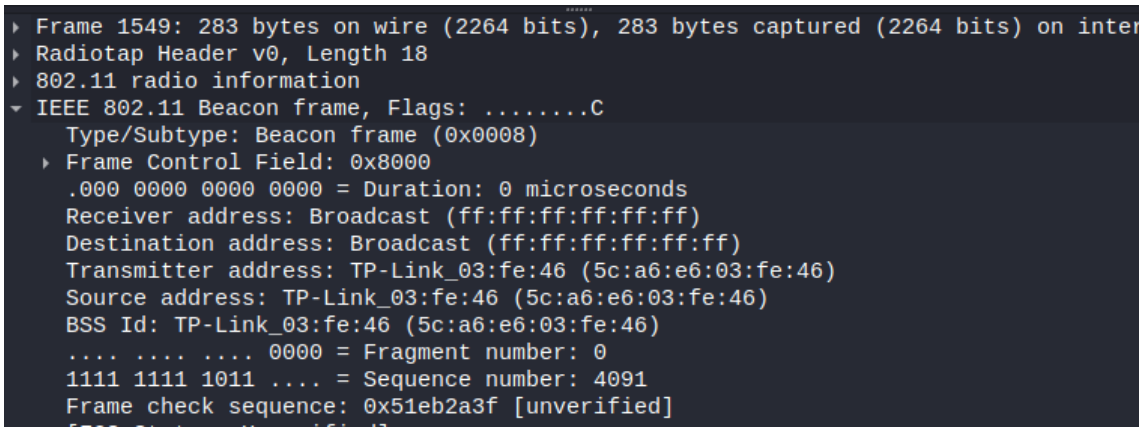
3.2 Bezdrátové sítě

Bezdrátové sítě nám definuje Český slovník kybernetické bezpečnosti jako bezdrátové technologie pro šíření dat („vzduchem“), vhodné pro tvorbu sítových infrastruktur tam, kde je výstavba klasické kabelové sítě nemožná, obtížná nebo nerentabilní (kulturní památky, sportoviště, veletrhy). Pro přenos dat postačí vhodně umístěné navazující přístupové body, lemující cestu od vysílače k příjemci. [2]

Kromě výše zmíněných výhod s sebou WiFi přináší také nezanedbatelná bezpečnostní rizika. Nelze totiž dobře kontrolovat kam a jak se signál šíří. Pro běžného uživatele tak nemusí být viditelný, ale útočník s vhodným vybavením ho zachytí. S tím souvisí také absence ochrany důležité síťové komunikace jako je například rezervace časového pásma nebo připojování k AP, autentizace, deautentizace a další. [3]

Lehce dohledatelný je také Beacon rámec (ten dává ostatním počítačům vědět o existenci AP), který v sobě nese takové informace, jako je například SSID. Ty lze

zachytit určitými programy, jako je například Wireshark, jak můžeme vidět na obrázku č. 3.1.



Obrázek 3.1: Data zobrazená programem Wireshark. Zdroj: snímek obrazovky

Zabezpečení WiFi sítí není bohužel věnována taková pozornost, a ještě stále se traduje, že pro jejich zabezpečení stačí např. filtrace MAC adres nebo skrytí SSID sítě, kdy MAC adresa je identifikátor zařízení přidělený výrobcem a SSID je jedinečný identifikátor každé bezdrátové počítačové sítě. My si však ve cvičeních obsažených v této práci ukážeme, jak snadné je takovými pokusy projít.

Pro příklad si zmíníme onu zmiňovanou filtraci MAC adres. Jde o naprosto nevhodný způsob zabezpečení, neboť při něm dochází k přenosu nezašifrovaných dat. Každý průměrně schopný útočník je schopný ji získat a nakládat s ní podle vlastního uvážení. Třeba se vydávat za legitimního uživatele oné MAC. [3]

3.3 Komplex WPA

Komplex WPA („Wi-Fi Protected Access“) je soubor kryptografických protokolů pro zabezpečení Wi-Fi spojů, což jsou rádiové spoje definované standardem IEEE 802.11. [7]

Tento komplex nahradil kryptografický protokol WEP („Wired Equivalent Privacy“), který byl prolomen již v roce 2001 a na routerech už není podporován, ačkoliv na některých se tato možnost ochrany stále nachází, až zšedivělá. [3]

V současné době jsou standardizovány tři verze tohoto komplexu, jež jsou označovány zkratkami WPA, WPA2 a WPA3, z nichž se používají poslední dvě. Náš cvičný AP podporuje druhou zmíněnou verzi.

3.4 WPS

Wireless Protected Setup byl představen roku 2006. Toto zabezpečení mělo pomoci uživatelům bez znalosti bezdrátových sítí je zabezpečit. Toto zabezpečení funguje na základě pinu, který se zadá stisknutím tlačítka WPS na bezdrátovém routeru. Nikdo zvenčí by tak k připojení neměl mít přístup.

V roce 2011 se však zjistilo, že tento pin se dá promocí brute force útoků zjistit. Tento pin se navíc skládá jen z devíti číslic od nuly do devíti, takže útočník má pouze 100 000 000 pokusů ho zjistit. To pro dnešní software není nic složitého. [8]

3.5 Hešovací funkce

Hešovací funkce nebo také hash funkce jednosměrná matematická transformace vstupních dat (textu) do souboru (otisk, hash). Matematicky je prakticky nereálné získat z otisku zpět vstupní data. Tato funkce je využívána v aplikacích zabezpečení dat (například autentizace, digitální podpis, kontrola integrity). Narušení bezpečnosti hash funkce je označováno jako kolize. [2]

Rozeznáváme čtyři útoky na heše: útok hrubou silou, distribuci útoků, slovníkový útok a rainbow tables. V práci jsou použity první dva.

3.5.1 Útok hrubou silou

Při tomto útoku útočník generuje postupně všechna možná hesla, která právě splňují požadavky daného systému na tvorbu hesel. Tento způsob útoku se vyplatí pouze u systémů, které nemají nijak definovanou délku hesla nebo mají na heslo příliš malé nároky. Při dostatečně dlouhém hesle může prolomení hesla trvat i řadu let. [3]

3.5.2 Slovníkový útok

Algoritmy pro slovníkové útoky počítají s tím, že je potřeba vyzkoušet různé kombinace daného slova. Běžné je zkoušet různé kombinace malých a velkých písmen, přidávat do zkoumaného slova čísla a speciální znaky. Heslo „PaSSword1.“ není tedy z tohoto pohledu o nic bezpečnější než „password“. Jeden z velmi známých slovníků, Rockyou (který v práci také využívám), je postupně vytvářen s využitím hesel, která unikla z nejrůznějších systémů. Obsahuje tak veliké množství hesel reálně používaných uživateli.

Vedle již existujících slovníků jsou dostupné nástroje, které umožňují vytvořit slovník na míru dle informací, jež má útočník o své oběti. Nástrojem umožňujícím vytvořit specifický slovník dle obsahu webových stránek je například program cewl. Jiným nástrojem, který lze využít pro generování slovníku na míru, je program cupp. Tento program umí vygenerovat slovník na míru konkrétní osobě, jak můžete vidět na následujícím obrázku. [3]

3.6 Heslo

Heslo je znakový řetězec používaný jako součást autentizační informace. Obecný prostředek k autentizaci uživatele pro přihlášení k počítači, k přístupu k souborům, programům a službám. [2]

Stále jde o nejrozšířenější způsob autentizace uživatelů a jde o velmi dobré zabezpečení dat, pokud jsou dodrženy jisté kroky.

První úskalí hesel nastává už při jeho uložení. Je potřeba, aby se k němu nedostal útočník jak při odesílání, tak při ukládání do databáze. Stejným případem je také situace, kdy se útočník do databáze vloupe. Právě proto se už při odesílání hesla používají výše zmíněné hešovací funkce.

Dalším momentem, kdy lze heslo přečíst, je chvíle, kdy se uživatel přihlašuje do systému. I tehdy zadává své heslo, které je následně porovnáno s heslem uloženým v databázi. Aby tedy došlo k bezpečnému přihlášení, musí se porovnávat právě heše, nikoliv původní řetězce hesel.

Tyto dva případy jsou součástí útoků, které odchycují heslo z provozu na počítačové síti. Dále může být heslo získáno také pomocí malware, sociálním inženýrstvím, jednoduchým uhádnutím nebo lámáním. Poslední zmíněné je však pomalé a pro útočníka nebezpečné, neboť se v logu dané stránky objeví příliš pokusů o přihlášení z jedné IP adresy.

4 Metody

V této kapitole jsou rozebrány použité metody při vypracování práce. Na základě použití těchto metod bylo dosaženo cíle práce.

4.1 Hardware

Tato podkapitola popisuje využité fyzicky existující části cvičné laboratoře nazvané Wireless Lab. Jejich výběr byl uskutečněn na základě rešerše současného stavu kyberprostoru a kybernetické bezpečnosti.

4.1.1 Útočník

Útočník neboli útočící přístroj byl vytvořen jako virtuální počítač (dále VM). Byla mu přiřazena operační paměť 20 085 MB a šest procesorů s přímým přístupem k hardwaru a KVM paravirtualizací. Přidán byl také ovladač Realtek 802.11n NIC.

4.1.2 Oběť

Obětí se mohlo stát jakékoliv zařízení se schopností připojit se k našemu AP. Kvůli požadavkům jedné z pozdějších úloh bylo naznáno, že bude lepší, pokud toto zařízení bude mít přístup k příkazovému řádku.

V úlohách této práce byl jako oběť použit notebook Lenovo ThingPad E450 s nainstalovanými Windows 10.

4.1.3 Bezdrátová síťová karta TP-LINK TL-WN722N

Tato odnímatelná anténa byla jasnou volbou díky jejímu vysokému výkonu a ovladači, který umožňoval přepnout toto rozhraní do monitorovacího módu. Nutno podotknout, že bylo potřeba nainstalovat speciálně upravený ovladač, o němž se zmíním v kapitole 4 .2 .3 Ovladač rtl8188eusr.

4.1.4 Přístupový bod TP-LINK TL-WR841N

Vybrán byl pro jeho spolehlivost, a hlavně místní a cenovou dostupnost. Kromě WPA2 zabezpečení poskytuje také síť pro hosty nebo rodičovskou kontrolu – těch jsem však ve své práci nevyužila. Jeho nastavení je velmi intuitivní a lze jej provést online.

Obrázek 4.1: Přístupový bod v provozu. Foto: autor

4.2 Software

Tato kapitola popisuje programové vybavení cvičné laboratoře nazvané Wireless Lab. Jejich výběr byl uskutečněn na základě rešerše současného stavu kyberprostoru a kybernetické bezpečnosti.

4.2.1 Oracle VM Virtual Box

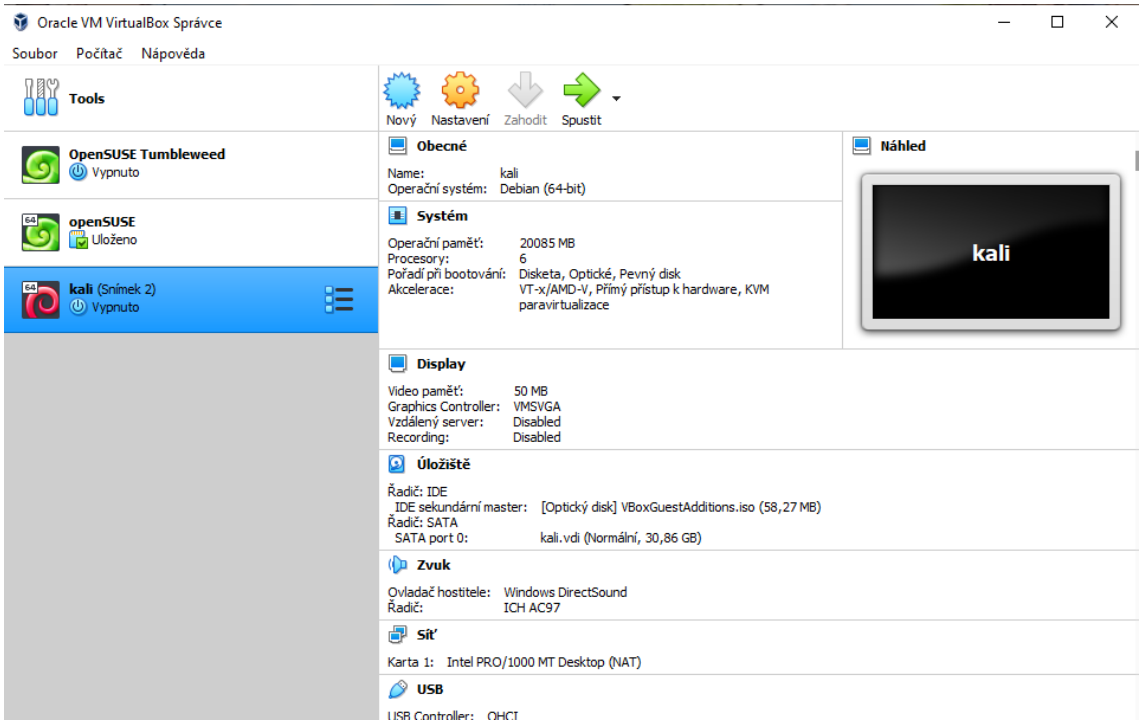
Oracle VM Virtual Box je virtualizační nástroj s distribucí pro Linux/Unix, Windows i Mac OS, který vlastní firma Oracle.

Tato aplikace umožňuje vytvoření virtuálního počítače, na kterém je mimo jiné možné testovat různé postupy nebo software, aniž by uživatel tímto jednáním ohrozil vlastní počítač.

Této aplikaci jsem dala přednost před vlastní instalací operačního systému Kali Linux na oddíl reálného pevného disku, stejně jako před vytvořením vzdáleného počítače, k němuž by se dalo připojit přes vzdálenou plochu, a to z toho důvodu, že šlo o nejméně náročný způsob jak časově, tak přístrojově.

Navíc se mezi takto vytvořeným počítačem a vlastní plochou dá jednoduše přepínat a kopírovat obsah.

Bylo však potřeba použít starší verzi, jelikož nová měla s instalací Kali Linux problém.



Obrázek 4.2: Rozhraní aplikace Oracle VM Virtual Box. Zdroj: snímek obrazovky

4.2.2 Kali Linux

Kali Linux je, jak už název napovídá, linuxová distribuce, která je odvozená od Debianu. Používá se pro digitální forenzní analýzu, a co je pro úlohy v této práci důležité, také pro penetrační testy.

Tento operační systém tak obsahuje mnoho užitečných nástrojů právě pro testování zabezpečení WiFi, jako je Aircrack-ng a Wireshark, se kterými se v následující sadě úloh hojně pracuje.

Obrázek 4.3: Rozhraní operačního systému Kali Linux. Zdroj: snímek obrazovky

4.2.3 Ovladač rtl8188eusr

Za zmínku stojí ovladač rtl8188eusr. Jde o upravenou verzi původního ovladače bezdrátové síťové karty TP-LINK TL-WN722N, který nedovoloval kartě přejít do monitorovacího módu, který byl pro mou práci klíčový.

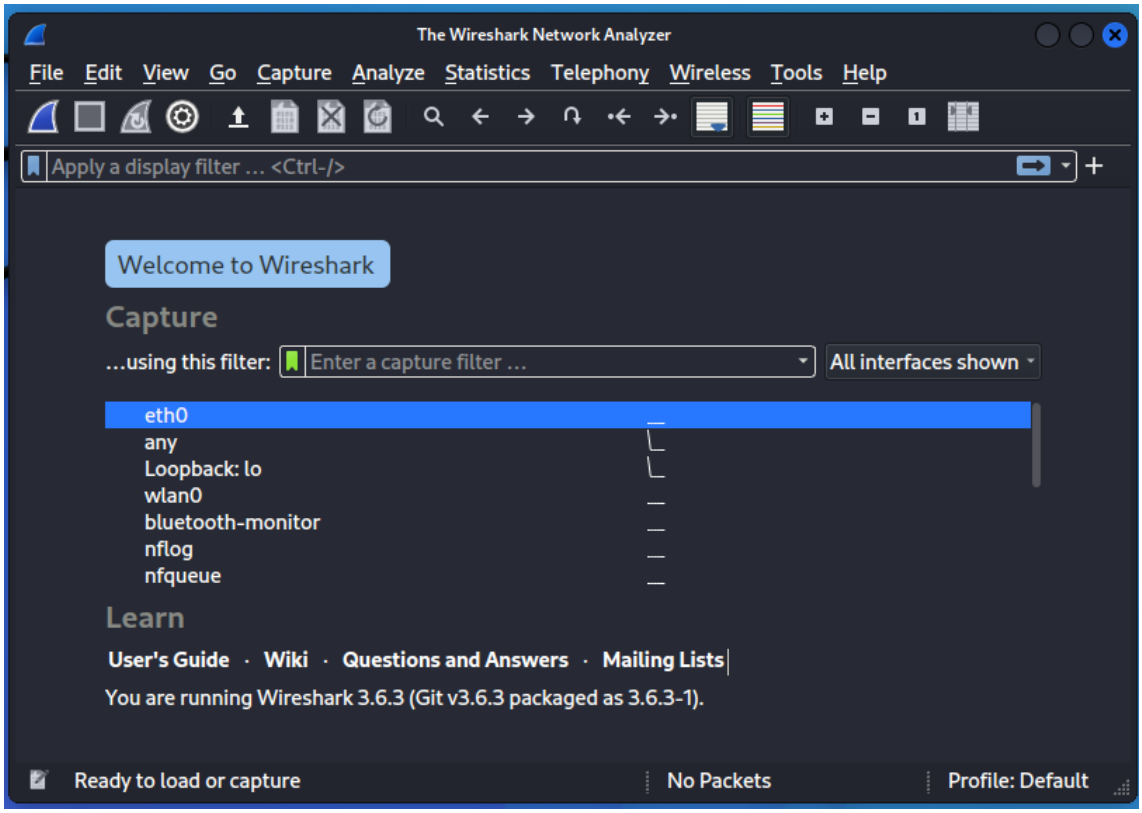
Ve starších verzích ji pravděpodobně podporoval, ale se zvyšujícími se nároky kyberbezpečnosti vývojáři pravděpodobně upustili od podpory takové funkce.

Za zpřístupnění verze umožňující monitorovací mód poděkujme vývojářům nástroje Aircrack-ng, kteří ji uveřejnili na svém GitHubu.

4.2.4 Wireshark

Wireshark je světově nejpoužívanější analyzátor protokolu sítí. Zpřístupňuje jeho uživateli informace takřka na mikroskopické úrovni a poskytuje mnohé funkčnosti jako například filtrování informací, zachytávání zazipovaných souborů, a co je pro tuto práci důležité, dokáže dekódovat WPA/WPA2 protokol. [9]

Tyto všechny informace (a mnohem více) jsou pak uživateli poskytnuty v jednoduchém a přehledném GUI.



Obrázek 4.4: Rozhraní programu Wireshark. Zdroj: snímek obrazovky

4.3 Balíčky

Tato kapitola popisuje dodatkové balíčky použité k realizaci cvičné laboratoře nazvané Wireless Lab. Jejich výběr byl uskutečněn na základě rešerše současného stavu kyberprostoru a kybernetické bezpečnosti.

4.3.1 Aircrack-ng

Aircrack-ng je kompletní balíček nástrojů pro akce týkající se zabezpečení WiFi. Zahrnuje funkce jako monitorování, testování, útočení a prolamování. Všechny příkazy se používají v příkazovém řádku a jsou vyvinuty primárně právě pro Kali Linux.

4.3.2 Slovníky

Slovníky jsou soubory s uniklými hesly, které slouží k porovnávání se zjištěnými hesly systému, který se snažíme prolomit. Nejsou však porovnávána přímo hesla, nýbrž jejich heše a to z toho důvodu, že s heše nejde zpětně získat původní řetězec.

Na tomto principu funguje Aircrack-ng nebo třeba Hashcat. První ze zmíněných byl použit při tvorbě úloh.

5 Výsledky

Výsledkem práce je sada úloh, v níž se jednotlivá cvičení zabývají problematikou zabezpečení WiFi a simulacemi různých útoků, které studenta inspirují v zamyšlení se nad možnou ochranou před kybernetickým nebezpečím.

5.1 Příprava laboratoře

Tato úloha je prerekvizitou k úlohám následujících. Obsahuje podrobný návod instalace VM a Kali Linux, dále pak nastavení AP a síťové karty.

5.2 Čmuchání paketů

Druhé cvičení provede studenty základním nastavením rozhraní *wlan0*, které odpovídá užité síťové kartě, a seznámení se s programem Wireshark. Kromě základního odchytávání paketů se student naučí používat také filtry Wiresharku a vyzkouší si i paketovou injekci.

5.3 Obcházíme WLAN autentifikaci

Třetí cvičení studentům ukáže, jak se vydávat za jiné zařízení a obejít tak filtry MAC adres, které lze nastavit na každém AP.

5.4 Prolamování hesla

Ve čtvrtém cvičení studenti zachytí tzv. handshake, neboli pakety obsahující heš hesla k AP. Vzhledem k nastavení slabého hesla stačí provést obyčejný slovníkový útok.

5.5 Útok na WLAN infrastrukturu

Student si vyzkouší brute force útok na nezabezpečený AP v podobě masové deautentifikace a následnému připojení oběti k vytvořenému falešnému AP.

5.6 Útok na klienta

Student si vyzkouší několik dalších útoků na klienta, jako je honeypot útok (vytvoříme návnadu), deautentifikace klienta s WPA/WPA2 zabezpečením a prolamování WPA/WPA2 bez fyzického AP.

5.7 Pokročilé WLAN útoky

Student se pokusí o pokročilé útoky na strukturu WLAN. Provede útoky jako je man-in-the-middle (vytvoří si prostředníka), bezdrátové odposlouchání (odposlechne heš hesla) a unese připojení.

5.8 Útok na WPS

Ačkoliv již ochrana WPS není aktuální, AP použitý pro práci ji stále využívá, a tak jsem ji pro zajímavost zahrnula také. Studen se přesvědčí, jak jednoduché je prolomit WPS pin.

6 Diskuse

Z informacích uvedených v současném stavu lze vyčíst, že zabezpečení bezdrátových sítí není tak komplexní jako u sítí jiných. S pomocí přiložené sady úloh je možné vyzkoušet různé typy útoků na různé typy zabezpečení, které momentálně bezdrátové routery nabízí.

Je poměrně bezpečné říci, že pomocí Kali Linux a jeho balíčků je relativně jednoduché získat heš zadaného hesla, který pak lze porovnat s dostupnými slovníky.

Nám, jakožto uživatelům, tedy nezbývá mnoho. Jako první taková zásada se jeví nepřipojovat se k nezabezpečeným sítím. Za všemi volně dostupnými sítěmi, kterých si všímáme v obchodních domech nebo například ve fastfoodech, se může skrývat útočník, který čeká na připojení své oběti. Pokud se už k takové síti potřebuje uživatel připojit, je dobré neprovádět žádné důležité úkony a nikam se nepřihlašovat.

Jakožto majitelé routerů bychom pak měli volit bezpečná silná hesla a nešířit informace, která by mohly vést k jejich vyzrazení. Ideálním heslem je heslo náhodně generované. Takové heslo se nedá najít v žádných slovnících a sociálním inženýrstvím je nikdo nezjistí.

7 Závěr

Zabezpečení bezdrátových sítí se na první pohled vskutku může jevit jako bezpečné a neprostupné. Běžný uživatel internetu se může pokusit maximálně o uhádnutí hesla a více, než připojení zdarma nedostane.

Problém nastává, pokud se objeví útočník s vhodnými nástroji, jako je například Kali Linux použitý v této práci.

Tato práce měla za cíl vytvořit sadu úloh pro studenty, kteří si na jejich základě budou moci vyzkoušet různé útoky na bezdrátové sítě a zamyslet se nad jejich ochranou.

Sada úloh obsahuje dohromady osm cvičení, v nichž si studenti postupně osvojí základní dovednosti Kali Linux a přiložených balíčků. Vyzkouší si tak v praxi, jak se dá zabezpečení prolomit a jak ho vylepšit.

Seznam použité literatury

[1] Kyberútok na nemocnici v Benešově způsobil škodu přes 59 milionů. Pachatele se vypátrat nepodařilo. In: IRozhlas.cz [online]. 18. 8 . 2020 [cit. 2022-05-05]. Dostupné z : https://www.irozhlas.cz/zpravy-domov/kyberutok-kyberneticky-utok-nemocnice-v -benesove-skoda-pachatel-hacker_2008180912_ako

[2] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0 .

[3] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z .s .p .o ., 2019. CZ.NIC. ISBN 978-80-88168-34-8 .

[4] ČERNÝ, Jan. Tři druhy webu. In: Informační gramotnost [online]. [cit. 2022-05-05]. Dostupné z : https://www.informacnigramotnost.cz/tri-druhy-webu/

[5] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 ze dne 6 . července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. In: . Dostupné také z : https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

[6] Národní strategie kybernetické bezpečnosti České republiky na období let 2021 - 2025 [online]. [cit. 2022-05-05]. Dostupné z : https://nukib.cz/cs/infoservis/dokumenty-a -publikace/strategie-akcni-plan/

[7] BURDA, Karel. Kryptografie okolo nás. Praha: CZ.NIC, z .s .p .o ., 2019. CZ.NIC. ISBN 978-80-88168-52-2 .

[8] BUCHANAN, C ., Ramachandran, V ., Kali Linux Wireless Penetration Testing Beginner’s Guide – Third Edition, ed. 3 , Packt>, 2017, ISBN 978-1 -78328-041-4

[9] Wireshark.org [online]. [cit. 2022-05-05]. Dostupné z : https://www.wireshark.org