GYMNÁZIUM, STŘEDNÍ PEDAGOGICKÁ ŠKOLA, OBCHODNÍ AKADEMIE A JAZYKOVÁ ŠKOLA s právem státní jazykové zkoušky ZNOJMO, příspěvková organizace

ROČNÍKOVÁ PRÁCE

Hacking

Autor: Zdeněk Uttendorfský
Konzultant: Mgr. Jindřich Červinka

Prohlášení

Prohlašuji, že jsem svou ročníkovou práci vypracoval/a samostatně a použil/a jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů.

V Znojmě dne 5.1.2024 ……

Zdeněk Uttendorfský

Poděkování

Chtěl bych v první řadě poděkovat vedoucímu práce panu Červinkovi, který nejen mě, ale všechny pod jeho křídly vedl k cíli dokončení práce. Chtěl bych poděkovat klukům Janu Slanému, Noe Fabianu Bernardovi, Jardovi Schneiderovi a Janu Hamzovi za průběžnou zpětnou vazbu, kontrolu a podporu v této práci. Jardovi také děkuji za poskytnutí Raspberry Pi 3 model B pro vypracování praktické části. A v poslední řadě bych chtěl poděkovat přítelkyni, která mi dělala společnost a poskytovala podporu při psaní práce.

Anotace

Ve své ročníkové práci jsem se zabýval pojmem hacking. Mým cílem bylo vypracovat práci popisující hacking tak, aby byla pochopitelná pro každého bez ohledu na úroveň znalostí v této oblasti. Postupuji od samotných základů, přes nástroje používané až po nejznámější průniky historie. V praktické části vytvořím simulaci vlastního nezabezpečeného webového serveru. Na server je možné se pomocí jednotlivých nástrojů a kroků nabourat. Cílem této práce je vypracovat informativní dokument jednoduše čitelný pro každého.

Klíčová slova

Hacking; Web; Uživatel; Systém; Linux; Windows; Útok

Obsah

1 ÚVOD

Pro svou ročníkovou práci jsem si vybral téma hacking, protože je to téma pro mě velmi zajímavé a důležité. V dnešní době digitalizace, která zasáhla příkladem nemocnice a dopravu, nemluvě o umělé inteligenci, může být a je zabezpečení systémů a hacking velkým předmětem pro všechny z nás.

Hlavním cílem mnou psané teoretické části je, aby kdokoliv, kdo ji přečte jí porozumí. Postupem jednotlivých kapitol se budu dostávat k určitým nástrojům používaných ve světě hackování, které jsem i já osobně používal ke splnění určitých výzev při procvičování a učení se. Společně s nástroji budu jmenovat a popisovat jednotlivé typy útoků a jejich území, ve kterých se mohou využít. Ke konci zmíním pro zajímavost největší hackingové průniky.

V praktické části si vyzkouším provozovat vlastní webový server. Server bude mít za účel simulovat reálné špatně zabezpečené prostředí lehce proniknutelné. Začnu jednoduchým Apache webovým serverem provozovaném na svém Raspberry Pi 3 model B. Na zařízení mám otevřený port 22 neboli Secure Shell port, kde je finále dané aktivity. Předem je potřeba získat přihlašovací údaje k jednomu ze dvou uživatelů s přístupem k SSH. Naštěstí je otevřený i port 80 (HTTP), na kterém je Apache web. Za pomocí nástrojů a trošku přemýšlení se dá dostat k uživateli s přístupem k root právům a získáním trofejního souboru. Simulační hra je inspirována Capture the flag hrám na TryHackMe nebo Hack The Box, kterých jsem udělal spousty. Pro přístup k síti hostující servery používám službu ZeroTier. ZeroTier využívá network id pro připojení k lokální síti bez potřeby veřejné adresy pro přenášení serverů na internet.

2 RECONNAISSANCE

Reconnaissance, česky průzkum, v kontextu hackingu se myslí proces sběru co nejvíce důležitých informací o cílovém systému, firmě, síti nebo aplikaci pro účely napadení. Většina nezkušených a neznalých jednotlivců ihned zkouší bourání do systému bez žádné znalosti a opomíjí tuto fázi. Touto fází se nemůže pohrdat, nelze vykrást dům bez znalosti rozložení domu, kolik lidí v domě bydlí, kdy vychází a dále. Etapa průzkumu se hojně využívá dokonce i v armádě a ve válkách, kde se na rozdíl pokouší zjistit používanou technologii a stroje protivníků nebo čas a místo jejich útoku.

Každá „bezcenná“ informace nemusí být tak k zahození, jak se zdá. Věta k zamyšlení hodna rozboru. Při tomto segmentu je pro úspěšné pozdější proniknutí dbát na maličkosti. Informace se mohou ukrývat ve zdrojovém kódu stránky nebo mohou být pomocí steganografie ukryté soubory v neškodném obrázku. I nesmyslný text si mohl uživatel zadat jako heslo do systému.

2.1 Passive reconnaissance

Ve většině případů je pasivní na prvním místě. Je to průzkum bez přímé interakce s terčem při vyhledávání veřejně dostupných informací. Nalezením údajů zde nám poskytne náležitý náskok, což je velmi cenné a varovné. Bez manipulace s cílem pro něj ještě neexistujeme a jsme neviditelní, přičemž už shromažďujeme a skládáme obrázek o něm.

I jednoduché prozkoumání sociálních sítí firmy se řadí do této kategorie. Tímto příkladem se dostáváme k velkému kousku zaplňujícího pasivního průzkumu, OSINT (Open Source Intelligence), procesu analyzování veřejně dostupných nalezených údajů z otevřených zdrojů. V této práci se OSINT nástrojům a technikám nebudeme tolik věnovat, ale představíme si jiné typy.

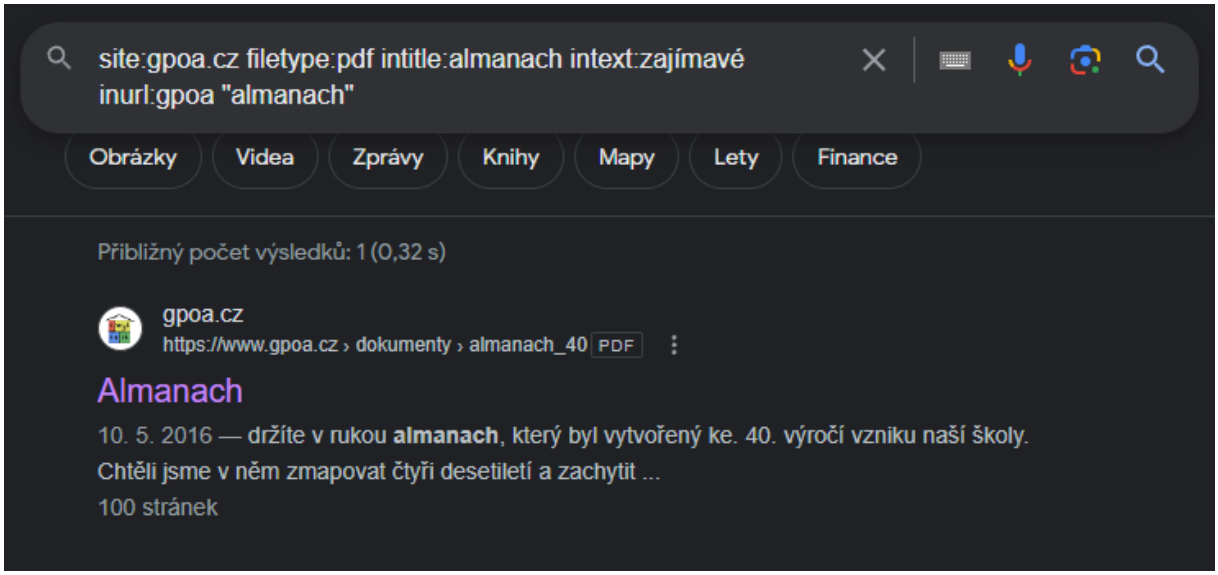
2.1.1 Google Dorking

Jak název napovídá, na použití Google Dorking (Google Hacking) stačí pouhý Google Chrome nebo jiný prohlížeč. Funkcionalitu prohlížečů nelze popsat pomocí pár vět, je to spousta pravidel a postupů, které formují rozhraní mezi uživatelem a serverem hostujícím příslušnou stránku.

V pozadí všech prohlížečů číhají takzvaní web crawleři nebo spideři (pavouci) a také boti. Jejich úkolem je prohledat stránku za účelem uložení důležitých a častých klíčových slov. Pokud naleznou subdoménu tak se také do ní vydají a zapíšou si do pozadí významné informace použitelné při dalším hledání.

Samozřejmě některé informace si vývojáři stránek nepřejí propouštět web crawlerům. Administrativní stránky, přihlašovací okénka a soubory obsahující hesla byste nechtěli ukazovat nikde. Omezování, kam pavouci mohou zabrouzdat, zajišťuje soubor robots.txt. Působí jako usměrňovač a omezovač těchto funkcí, což závažně omezuje i samotný Google Dorking.

Google Dorking je v principu velmi snadno pochopitelný. Jde o pouhé přidávání operátorů do vyhledávacího řádku Google za účelem zúžení výsledků hledání a pro pokus o nalezení specificky hledaných věcí. Tyto věci mohou být soubory, podstránky, dokumenty nebo i subdomény. Významnost Google Dorking vyvyšuje jeho naprostá legální vlastnost!



Obrázek 1: Ukázka Google Dorking

Zdání o nepoužitelnosti Google Dorkingu vás může napadat. Avšak při správném použití se z něho stává mocná bezmezná zbraň. V reálných situacích místo našeho příkladu by se zadávali klíčová slova typu passwords (hesla), uživatelská jména a další námi hodnotné údaje.

2.1.2 DNS Lookups

DNS protokol překládá dobře čitelná doménová jména na IP adresy a obráceně. DNS Lookups jsou dost nejasné na první pohled, ale jde, jak v celé kapitole reconnaissance, o rozšíření znalostí o oběti. DNS Lookups jsou speciální v tom, že se zaměřují pouze na doménové jména nebo jejich verze v podobě IP adres, ze kterých vyčlení informace.

Na metodu DNS Lookups existuje spousty webových portálů, které mohou, ale nemusí správně fungovat. Používání stránek je pofidérní a pro neprofesionální uživatele. My se zaměříme výhradně na námi oblíbený příkazový řádek a nástroje určené pro tento účel. Jak webů, tak příkazů je mnoho, ale mezi nejčastěji používané příkazy lze zařadit host, nslookup, dig a whois.

K čemu je to dobré? Použitelnost sesbíraných dat se diverzifikuje na základě cíle práce. Nicméně především nám to odhalilo další část obrazu, s čím se potýkáme. Dovolilo nám to možnost identifikovat neaktualizované, zastaralé nebo špatně nastavené servery a potencionálně náchylné služby k průniku. Whois kontaktní údaje nás mohou navést k využití sociálního inženýrství.

2.2 Active reconnaissance

Aktivní reconnaissance už brouzdá jemně do té přímé interakce s nápaditým terčem. Bez žádného působení není možné tento typ provádět. Jasnou konfrontací služeb a systémů získáme více potřebných informací potřebných k dalším krokům. Nevýhoda se vyčlenila hned ze začátku z definice, přímá interakce, tudíž dochází k záznamům a stopám námi zanechanými dostupné pro naše objevení.

Mezi základní kameny aktivního průzkumu se řadí například skenování portů, sítě, zranitelností (vulnerabilities), packet sniffing nebo dokonce netechnické metody sociálního inženýrství. Důležité zmínit, že zde již hraničíme a jsme na pomezí ilegální činnosti bez povolení správce.

Nejzákladnější příkaz zadávaný do příkazového řádku v této kategorii je ping. Úkonem pingu je jednoduše určit, zda je daný systém „naživu“. Nemůžeme zjišťovat informace o něčem, co nefunguje a není aktivní.

Rozsáhlejší verze ping traceroute ukazuje něco navrch. Tracerouting obecně je technika pro zmapování přes jaké routery a stanice putuje paket s daty. To pomůže hackerovi si lépe představit strukturu sítě a lokaci serverů. Traceroute právě zobrazuje počet přeskoků, dobu přeskoku a odkud kam byl přeskok. Na Windows je malá změna v názvu na tracert.

2.2.1 Nmap

Král port skenování. Skenování portů je proces procházení a bádání po otevřených službách a portech na oběti. Opět jak bylo zmíněno u ping, nemůžeme útočit na uzavřené porty a otevřené nám říkají, že zde existuje potencionální vstupní bod. A Nmap (Network Mapper) je výborný pomocník za každé situace. Pojďme si říct, proč.

Funkčnost Nmap závisí na posílání paketů a analýze odpovědí k určení stavu požadované akce. Kromě obyčejného určení stavu portu, jestli je otevřený nebo uzavřený, dokáže Nmap také zaznamenat verzi služby na čísle portu, operační systém v užití a dále se dá rozšířit o uživateli psanými skripty pomocí jeho scripting enginu.

Bez flagů upadá její použitelnost. Mění typ skenu, preferovaný skript pro použití. Flag, říkejme parametr, -sT je prvotní pro zahájení plného TCP připojení k oběti pro skenování. Jeho příbuzným -sU (UDP scan) bez plného připojení TCP. UDP je méně přesný, nedokáže přesně identifikovat, jestli je port otevřený nebo filtrovaný (opened/filtered) v případě žádné odpovědi.

Tohle bylo nevelké vkročení do umění Nmapy, které by mohlo pokračovat do řádu vypracovaných stran. Změn v jeho chování je nespočet a dá se upravovat do ideální podoby pro uspokojení s výsledky. Dále pokračují až nekonečné masy skriptů pro větší oblast smysluplnosti programu příkladem skript na zjišťování chyb a zranitelností. Grafická podoba Nmap, Zenmap, přenáší všechny možnosti do grafického rozhraní.

2.2.2 Wireshark

Dovolím si přeskočit k tématu packet sniffing. Jak Nmap kraluje ve světě port skenů, Wireshark v packet sniffingu a následné analýzy. Packet sniffing zahrnuje zachytávání a analýzu provozu sítě k extrakce informací z odchycené komunikace. I když je spíše packet sniffing pasivní než aktivní, stále dokáže odhalit důležité aspekty zaměřené sítě.

Packet sniffing je užitečný nejen pro hackery a hacking. Analyzováním dat v paketech se dá zjistit, pokud je problém v síti. Také slouží jako přímá ochrana proti hackerům. Monitorováním sítě pomáhá odhalit nežádoucí a podezřelé aktivity vedoucí k rychlejšímu zastavení problému, než nadělá možné škody.

V našem světě hackingu to zneužijeme opačným směrem. Pakety mohou ukrývat přenášené citlivé informace jako hesla nebo uživatelská jména, a to nešifrované. A samozřejmě, základ této kapitoly, získat informace o síti a identifikovat potenciální slabiny v ní a vstupní body.

3 COMPROMISING, EXPLOITATION

Po sesbírání dostatku prostředků je na čase nejznámější a nejrozsáhlejší část procesu hackování. Compromising nebo exploitation je proces využití získaných informací z předchozí fáze pro spuštění akcí a technik vedoucí k úspěšnému proniknutí do systémů za účelem přiblížení se k požadovanému výsledku. Způsobů je nespočet a odlišují se na základě používaného operačního systému, jeho verze a konfigurace, zda se jedná o bezdrátové nebo drátové připojení, jestli je to webová aplikace nebo pouhý FTP server atd.

3.1 Kryptografie

Metoda ochránění citlivých informací a komunikace za použití operací a matematických vzorců, aby pouze ten, komu je zpráva určena ji mohl rozluštit, přečíst a vykonal další akce na základě té zprávy. Používala se již před tisíci lety nejen v počítačových sítích, ale i v průběhu války pro bezpečné zaslání poslání. V dnešní době se jednotlivé typy kryptografie v počítačových sítích používají na každém rohu, proto je důležité jim rozumět.

Základní kameny a pokyny, kterými by se měla kryptografie řídit jsou Confidentiality (Důvěrnost), Integrity (Integrita, Neporušenost) a Availability (Dostupnost). Dohromady se pojí do takzvané CIA triády. Prvním prvkem Confidentiality neboli důvěrnost znamená, že jedině oprávněné osoby mají přístup k informaci. Integrita zaručuje neporušení zprávy při přenosu a informace jsou neupravené. A dostupnost se pojí s důvěrností ve způsobu, že oprávněná osoba má přístup k datům kdykoliv je potřeba a neztratí se.

Obrázek 2: The CIA triad

3.1.1 Encryption

Tento typ kryptografie je postaven na změnu čitelného textu do šifry za pomocí jednoho nebo více klíčů a algoritmů. Princip encryption, říkejme šifrování, si nejlépe vysvětlíme na zastaralé Caesarově šifře. V ní jde o posun písmen v abecedě o tolik pozic v abecedě, kolik je předem určeno (klíč). Pokud bychom vzali slovo cipher (anglicky šifra) a prohnaly ho tímto algoritmem s posunem o 2, výsledek by říkal ekrjgt. V této ukázce je cipher nešifrovaný, planý text, ekrjgt je zašifrovaný text, který může být bezpečně přenášen a číslo 2 je sdílený klíč k následnému dešifrování.

3.1.1.1 Symmetric encryption

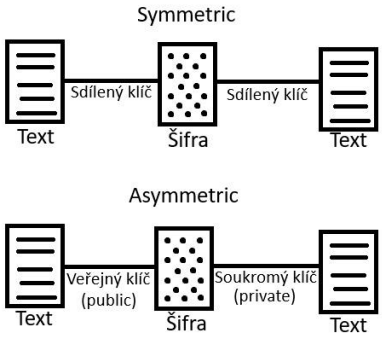
V Caesarově šifře je klíčem 2 od začátku do konce a díky němu byl text, jak zašifrován, tak je díky němu i dále dešifrován, je tedy sdílený. Těmto šifrám se říká symetrické šifry. Současnou hojně používanou šifrou je AES (Advanced Encryption Standard), která nahradila DES.

Přičemž je symetrické šifrování starší, stále se užívá, jelikož je rychlejší a efektivnější než asymetrické šifrování. Kvůli její rychlosti se užívá při šifrování velkého množství dat (databází příkladem) nebo při platebních aplikací. Nevýhodou vyplývá bezpečnost, v případě odchycení nebo odhadnutí sdíleného klíče je jednoduché rozluštit šifru.

3.1.1.2 Asymmetric encryption

Víc klíčů, větší bezpečnost. Na tom staví asymetrické šifrování. Užívají se odlišné klíče pro zašifrování a pro dešifrování. Klíči pro zašifrování se říká public key (veřejný), který je volně distribuovaný a bez problémů se může sdílet a pro dešifrování private key (privátní, soukromý), který se musí držet v tajnosti, jeho zjištění by byl problém.

Asymetrie eliminuje problémy v přenášení klíčů, které není potřeba při existenci dvou, a to výrazně zvyšuje bezpečnost. Víc klíčů je potřeba ukládat a pracovat s nimi, tedy je nezbytné větší množství výpočetního výkonu a s tím souvisí zpomalení. Stále díky bezpečnosti se preferuje při přítomnosti menšího množství dat, příkladem e-mailová komunikace anebo kryptoměny, založené na asymetrickém šifrování.



Obrázek 3: Symmetric vs. Asymmetric encryption

3.1.2 Encoding

Podobný pojem, se kterým se dříve nebo později setkáte při bádání šifrování a obecně změny zpráv je encoding. I když jsou podobné, a mohou se plést a je jednoduché je zaměnit, nejsou stejné. Už v překladu je patrný rozdíl, šifrování (encryption) a kódování (encoding). Nejedná se o podkategorii kryptografie!

Encryption jsme si vysvětlili v předchozí části. Jedná se o způsob užití klíčů pro šifrování zpráv. Encoding na rozdíl je pouhá transformace textu do podoby možné přenosu přes aplikace a systémy. Tedy encoding se nepoužívá pro ochranu dat jako encryption nebo následující hashing, ale pouze pro zacílení jeho integrity.

Base64 kódování je rozšířený typ užívaný pro přenos obrázků, audia nebo videa přes síť nebo pro uložení v databázích. URL kódování panuje v místech webu, převádí speciální charaktery do podoby čitelné URL. Hexadecimální kódování je viděno ve formě hexadecimálních dat a číslic, často používané pro řešení problémů a bugů.

3.1.3 Hashing

Nejsložitější a nejbezpečnější podkategorie kryptografie. Smysl hash funkcí je, že mají být nemožné rozluštit. Hash nemá žádný klíč k dekódování jako u klasického encryption a je tedy nevratný. Jeho reprezentace je v podobě řetězce znaků dané velikosti rozdílné dle hashovací funkce. Důležité poznamenat, že stejný input a typ hashování vrátí vždy stejný set znaků a změna v jediném bitu v inputu výrazně změní výsledný hash.

Kolize nastává v případě, kdy 2 různé vstupy dají stejný výstup. Čím lepší funkce, tím méně často nastává kolize mezi vstupy, ale kvůli designu, podle kterého hashe fungují není možné se tomuto fenoménu vyhnout. Výstupy funkcí nejsou nekonečné, přičemž vstupů je ohromně moc, ne-li nekonečno.

S hashy se nejčastěji pracuje na ověřování hesel a integritu dat. Při přihlášení do samotného počítače nebo i do většiny webových aplikací je vámi zadané heslo přeneseno přes hashovací funkci a uloženo do databáze. Takto uložené heslo, i v případě průlomu a úniku celé databáze, není možné zvrátit, a samotný hash je útočníkovi bezcenný.

Hash funkcí není málo a rozpoznat, jaká funkce byla použita, je nápomocným krokem k jeho dalšímu odhadnutí. Existují nástroje, jako hashid, haiti nebo hash-identifier, k odhadnutí typu, nebo i webové stránky k tomu určené. Samozřejmě výsledky nemusí být přesné, některé funkce mají viditelné rysy, díky kterým se dají rozpoznat pouhým okem.

Protože hashe se nedají zvrátit, je nemožné tímto způsobem zjistit originální hodnotu. Naopak, stejný výstup pro stejný vstup nabádá k myšlence provedení odhadnuté hodnoty hash fukcí a porovnání výsledku s uloženým výsledkem v databázi. Přeci stejný vstup se musí rovnat výstupu. Na této teorii jsou postaveny crackovací nástroje a aplikace. Nejznámějšími jsou John The Ripper a Hashcat.

3.2 Password attacks

Heslo vedle uživatelského jména je nejrozšířenější způsob k identifikace a autentizace účtu uživatele. Mnoho aplikací a systémů dává na sílu zámku heslem veškerou váhu, nemají žádné dvou faktorové ověření. V takovém scénáři je jednoduché sestavit útok na to heslo a při zjištění se vesele přihlásit za cizí osobu. Jak a co udělat pro největší šanci úspěchu?

Složitost hesla hraje velkou roli. I v případě absence dvou faktorového ověření, pokud heslo je složené z 32 náhodných znaků, tak to žádný člověk ani sebelepší počítač neuhádne. Proč se to tak nedělá? Není jednoduché si zapamatovat 32 náhodných znaků a nemožné v případě používání více hesel u více služeb, jak to dělá dnes téměř každý. Dobře zabezpečené heslo by

mělo mít minimálně 8 znaků, obsahovat velká i malá písmena, znaky, čísla a nemělo by obsahovat slova ze slovníku. To je zlatý základ, který by se měl dodržovat. S technologickým postupem se tyto požadavky posouvají a budou posouvat.

Útoky na hesla jsou možné online i offline. Online útok zahrnuje přímou interakci se systémem posíláním hesla do systému a kontrolování jeho odpovědi. Problém nastává při omezeném počtu pokusů na přihlášení, což dělá takové útoky nepoužitelné. Offline na druhou stranu pracuje na zařízení útočníka, kde z ukořistěného hashe nebo zašifrovaného hesla se snaží vydloubat heslo. Problém tohoto leží v krocích předtím, kde je nutné získat případný hash často pročtením databáze.

3.2.1 Brute-force attack

Staví se na pokus-omyl systému. Hacker zkouší všechny možné kombinace pro získání nejen hesla, ale třeba i objevení skryté webové stránky. Tato postarší metoda je stále oblíbená mezi hackery i přes její nedostatky. V případě složitějšího hesla délka Brute-force útoku se může blížit k několika rokům. Jeho efektivita je závislá na složitosti vstupu, výstupu a na výkonu zařízení provádějící útok.

3.2.2 Dictionary attack

Na rozdíl od kompletní randomizace klasického Brute-force útoku, Dictionary útok vybírá hesla z předurčeného listu. Použitý list si hacker může vytvořit sám předem z určitých souvislostí s uživatelem, jako jeho jméno, nebo si může vybrat z listů hesel uniklých firem. Oblíbeným je známý rockyou.txt. Výhodou oproti Brute-force je jeho systemizace, která se může vymstít v případě listu neobsahující správnou kombinaci.

3.2.3 Rainbow table attack

Zatímco Brute-force a Dictionary útoky se zaměřují hlavně na heslo v podobě klasických znaků, Rainbow table attack staví na hash formách hesel. Samotná duhová tabulka (Rainbow table) je předkalkulovaná a skládá se z kombinací znaků reprezentující možná hesla a jejich formy po projetí hashovací funkcí. Je nutná znalost správné hash formy hesla před použitím tabulek.

3.2.4 Password spraying

Heslo se přiřazuje nejčastěji k uživatelskému jménu a jdou ruku v ruce. Password spraying je rozdílný, jelikož se používá při znalosti hesla, nebo listu známých hesel. Daný seznam se dále „sprejuje“, přiřazuje a zkouší na různých uživatelských jménech, dokud se neshodnou. Zaměřuje se tedy na více uživatelských jmen s jedním heslem.

3.2.5 Keylogging

Keystroke logging, česky zaznamenávání stisku kláves, je forma útoku, kde se zaznamenává každý stisk klávesy na počítači oběti infikovaným keyloggerem, a tedy i heslo do jakéhokoliv systému. Keylogger je software schopný řídit tento útok. Největší problém je dostat keylogger na zařízení bez povšimnutí.

3.2.6 Nástroje

Automatizace je velké téma v dnešní době nejen v hackingu. Existují automatické vysavače, myčky na nádobí umožňující jejich automatické umytí, a dokonce automatická světla, zapínané po soumrak. Je důležitá z dvou důvodů, menší námaha a rychlejší konání činnosti. Takto to platí i v našem tématu.

3.2.6.1 Hydra

Samotný název nic nenapovídá. Jedná se o pouze online password cracking program používající Brute-force. I když neumožňuje offline crackování, její možnosti jsou rozšířené přes spoustu protokolů. Zvládá FTP, SSH, SNMP anebo i webové přihlašovací okénko na všechny způsoby.

3.2.6.2 Hashcat

Populární a silný program, používaný na různé typy Brute-force a Dictionary útoků. Hesla crackuje offline ze sesbíraných hashů. Jeho použití je jednoduché. -a možnost určuje typ útoků pro použití, nejčastější Brute-force, ale je na výběr i přímý nebo hybridní. -m je typ hashe, podle kterého bude předělávat hesla z listu. Bez určení typu Hashcat se pokusí sám rozeznat typ. To byly základní důležité možnosti k použití Hashcat, poslední věci zbývají na konec zadat soubor obsahující hash a seznam hesel, které bude porovnávat.

3.2.6.3 John The Ripper

Přímý rival programu Hashcat. Je velmi verzatilní a užívaný pro stejný účel jako Hashcat. Z mé osobní zkušenosti preferuji John The Ripper nežli Hashcat, ale jejich použití je individuální. Kromě klasického crackování hashů, je schopný prolomit shadow soubor, soubor Linux systémů, obsahující všechny účty a hashe hesel k nim. Zip2john je schopný převést zaheslovaný zip soubor do čitelné podoby programu John The Ripper, který je následně schopný ho prolomit.

3.3 OWASP Top 10 2021

Open Worldwide Application Security Project (OWASP) je nezisková organizace, která pracuje na zlepšení zabezpečení softwaru. Nabízí spousty nástrojů, dokumentů a stránek související s bezpečností programů a webových aplikací. Pracuje na projektech podporující tu myšlenku. Mezi nimi jsou oficiální OWASP nástroje (OWASP ZAP…), návody, vzdělávací materiály, tréninkové kurzy a také OWASP Top 10. OWASP Top 10 je pravidelně aktualizovaný list deseti nejkritičtějších bezpečnostních rizik postihujících webové aplikace.

3.3.1 Broken Access Control

Řízení přístupu určuje meze práv uživatele, které by neměl překročit. Pouze administrátor webu by měl mít práva upravovat vnitřní soubory a manipulovat s nimi. Pokud bez sebemenšího ověření je běžný návštěvník webu schopen vykonávat akce určené administrátorům nebo jiným uživatelům, označuje se to jako Broken Access Control. Příkladem je menší úprava části URL, která způsobí změnu přihlášeného účtu.

3.3.2 Cryptographic Failures

Kryptografii a její nutnost v počítačových sítích jsme si již představili. V případě absence šifrování nebo při nejlepším hashování, tak se to považuje za riziko nazývané Cryptographic Failures. Mezi tuto chybu se řadí i používaní nechráněných protokolů jako HTTP, FTP nebo SMTP, používaní slabých algoritmů kryptografie nebo užití obecných klíčů opakovaně používaných. Daná chyba se dá zneužít například pomocí On-Path útoků, dříve nazývaných Man In the Middle útoky.

3.3.3 Injection

Injection útoky se mohou objevit v případě uživateli zadávaných vstupů, které nejsou čištěné ani žádným jiným způsobem kontrolované. Základní dva typy jsou SQL Injection a Command Injection dle použitých technologií. SQL Injection nastává, když vstup je posílán do SQL databáze, pomocí toho je útočník schopen manipulovat výstup pro odhalení sensitivních informací. Command Injection nastává při posílání vstupu do příkazového řádku. Tímto je možné spouštět nepovolené příkazy všeho druhu bez zabezpečení.

3.3.4 Insecure Design

Tento problém nastává už v samé myšlence sestavení aplikace. I v případě nejbezpečnějších implementací bezpečnostních prvků, špatný design aplikace to může pokazit. Nečastým příkladem může být vyžadování pouze uživatelského jména bez hesla. Nejčastěji se chyba objevuje hned na začátku při vytváření aplikace s nápadem, který se přenese až do samotného vydání. Redukce těchto problémů není změnou nefunkčního kódu, ale systematického rozložení principu fungování aplikace a jeho analýzy.

3.3.5 Security Misconfiguration

Většina služeb má pro první přihlášení nastavené veřejně dostupné výchozí přihlašovací údaje. Jejich změna je fundamentální věc, kterou by měl každý udělat. Ale pokud se tak neučiní, nastává problém zvaný Security Misconfiguration. Není to pouze zapomnění na změnu přihlášení, je to také odhalování příliš mnoho nezbytných informací v zprávách o chybě, zakomponované pro lidi dostupné stránky se zneužitelným obsahem, zapnuté zanedbatelné služby, práva a dále. Prevence je vypnutí a odstranění přebytečných zdrojů.

3.3.6 Vulnerable and Outdated Components

Žádný programy ani služby nejsou po vydání perfektní. Časem užíváním lidí se běžně objevují chyby a bezpečnostní díry, které opravují aktualizace. Aktualizace nejsou většinou povinné, a tak se na ně zapomíná nebo se tím správci neobtěžují a tím si budují na problémy. Problémy s určitou verzí systému se vyskytují globálně na internetu a jejich nalezení a zneužití potom není problém pro útočníka.

3.3.7 Identification and Authentication Failures

Po přihlášení do webové aplikace je nejčastější systém kontrolování práv pomocí cookies. Po přihlášení je uživatelskému počítači s prohlížečem přiřazen session cookies (relační), autorizující daný prohlížeč. Získáním cizího session cookies je změna identity bez problémů. Tato chyba je nejčastěji objevena pomocí Brute-force útoků, slabých přihlašovacích údajů nebo slabého session cookie s předvídatelnými hodnotami.

3.3.8 Software and Data Integrity Failures

Integrita je, jak jsme poznali důležitá. Je to ověření, že nedošlo ke změně dat v průběhu přenosu a jsou shodná jak ze startu, tak v cíli. Pokud neprobíhá žádná kontrola integrity dat, je to chyba povolující útočníkovi změnu dat přidáním škodlivého kódu nebo jakékoliv úpravy dle svých představ. Předcházení této chyby se dělá pomocí kontrolního součtu každého kousku dat.

3.3.9 Security Logging and Monitoring Failures

Zaznamenávání a monitorování akcí je důležité ze dvou faktorů. Monitorování umožňuje časné odhalení pokusů o průnik a nastolit kroky k jeho omezení a zaznamenávání v případě povedeného průniku zabránit podobným katastrofám. Záznamy by měli obsahovat čas provedené změny, následek změny a kdo změnu udělal. Chybějící monitorovací a záznamové systémy jsou pomocné, avšak nejsou fatální.

3.3.10 Server-Side Request Forgery (SSRF)

Nastává v případě uživatelovi schopnosti zneužití serveru pro úpravu prostředků. Útok zahrnuje manipulaci s URL řádkem, který následně přečte a zpracuje server. Pomocí zpracování serveru je možné zneužít do podoby zobrazování citlivých dat, útržky z databází a dalším věcem neurčeným k odhalení. Manipulace může dojít až ke čtení z jiných serverů pomocí URL adresy.

3.3.11 Nástroje

Pro zjednodušení nalezení a využití chyb zmiňovaných v OWASP Top 10 byla vytvořena řada nástrojů kompletující daný úkol. Nejznámější z nich si tady představíme a letmo vysvětlíme. Jejich funkčnost samozřejmě záleží na dovednostech člověka užívající služby. Zdaleka tu nebudou zmíněny všechny, ale mně nejvíce blízké.

3.3.11.1 Burp Suite

Jeden z nejlepších softwarů pro testování bezpečnosti webů používaný profesionály, etickými i neetickými hackery pro identifikaci chyb a jejich opravě. Je vhodný pro začátečníky i pokročilé díky jeho přívětivému prostředí a rozšířenosti nápomocných nástrojů vhodné pro všechny způsoby testování. Má placenou i neplacenou verzi, kde placená odemyká hranice všech možností, ale komunitní verze zdarma sama o sobě nabízí to nutné.

Základní první funkcí je jeho schopnost odchytu requestů pro analýzu a otevřenou úpravu, a i odpovědí ke kontrole. Přívětivě a přehledně rozepsané jsou všechny headery a cookies vystavené také k modifikaci. Request se dá dále poslat do jiné funkce programu jako intruder nebo repeater, popřípadě poslat dále nebo ho zahodit.

3.3.11.2 Gobuster/DirBuster

Oba nástroje jsou užívány pro zjišťování složek, souborů a stránek na webu. Zjištěné skryté stránky a soubory mohou obsahovat citlivé informace, chybu anebo něco cenného pro naši hacking cestu. Výběr mezi Gobuster a DirBuster je čistě individuální, oba mají silnější a slabší stránky i přestože jsou na stejný účel. Gobuster je jednodušší, pouze v příkazovém řádku a hlavně rychlejší. DirBuster má grafické prostředí s více možnostmi, které ho zároveň zpomalují oproti Gobusteru.

3.3.11.3 SQLMap

Neplacený program určený k identifikaci a využití chyb v SQL databázích, nejčastěji SQL Injection. Automatizace nesmí chybět a není jedinou výhodou. Má rozšířenou knihovnu systémů na každý případ obsahující MySQL, PostgreSQL, Microsoft SQL Server a další. Důležité zmínit užití většiny zmiňovaných programů a aplikací bez povolení hraničí se zákonem.

3.4 Další útoky

Ani zdaleka jsme nepokryli všechny možné způsoby a typy útoků. Každý je unikátní svým provedením, použitými nástroji, kroky a cílem. Časem a technologickým vývojem zanikají a objevují se nové průniky, viry, systémy a nebezpečí. Pojďme si představit ještě pár zajímavých útoků.

3.4.1 On-Path Attack

Dříve nazývaný Man In the Middle attack (MITM). Jeho kouzlo stojí doslova uprostřed dvou zařízení. Útočník zmanipuluje jednu část komunikace k přeposílání dat přes jeho počítač. Odchycená komunikace je následně pročtena a je možné ji upravit před zasláním druhé straně. Je nebezpečný v případě nešifrované a nechráněné komunikace, přes kterou se zasílají citlivé informace. Nejznámější nástroj nadesignovaný pro On-Path attack je Ettercap podporující více protokolů.

3.4.2 DoS and DDoS Attack

Nejčastěji viděné na větších firmách a korporátech. Cílem útoku je narušení sítě, služby nebo webové stránky. Toho dosáhnou pomocí přetížení terče a zaplavením provozu. DoS (Denial of Service) využívá jeden systém provozující přetížení, je pomalejší, jednoduše vyhledatelný a zlikvidovatelný. DDoS (Distributed Denial of Service) je častější verzí, která využívá systémů více. Více systémů pracují rychleji a je složitější zablokovat veškerá zařízení zahlcující provoz.

3.4.3 Pass-the-Hash Attack

Veškeré Windows systémy ukládají hesla a jejich hashe v SAM souboru (Security Accounts Manager). Pro účel autentizace byl vytvořen protokol NTLM komunikující se SAM souborem a hodnotami v něm. Jelikož hashe nemohou být zvráceny, tak místo přihlášení pomocí hesla následně přeměněného do hashe použijeme samotný hash. Nevýhodou útoku je čas jeho možného užití, který je až po získaném přístupu do systému a sesbírání hashů. Pro nejen tento útok se využívá mocný program Mimikatz.

3.4.4 DNS Poisoning

DNS cache poisoning nebo DNS spoofing je útok zneužívající protokolu DNS. Pro rychlejší vyhledávání IP adres ukládá do cache paměti DNS domény s danými IP adresy zasílanými uživateli do prohlížeče. Při manipulaci cache paměti a změně IP adresy na námi vhodnou je následně zaslána chybná i uživateli. Taková IP adresa může být našeho serveru s virem nebo čímkoliv jiným.

3.4.5 Evil Twin Attack

Jednoduchý princip útoku, kde útočník započne vlastní přístupový bod (Access Point nebo AP) a donutí oběť k připojení. Před zahájením je třeba konfigurace AP do podoby stejné jako AP, které napodobujeme. Je běžný na veřejných a nechráněných Wi-Fi sítích, kde po připojení na zlé dvojče hacker sbírá prováděnou komunikaci s potencionálními citlivými daty.

4 POST EXPLOITATION, PRIVILEGE ESCALATION

Získali jsme přístup a nabourali jsme se do systému. Co teď? O tom se zabývá tato kapitola, jelikož je to důležitá součást celého procesu hackování. Co dělat po dosáhnutí moci nad systémem se dělí podle motivace a cíle celého procesu. Chcete získat určitá data, co nejvíce poškodit systém, být na systému co nejdéle a sbírat informace nebo mít pod rukou celou síť?

4.1 Privilege Escalation

Pokud již máte root, respektive práva administrátora, tak tuto podkapitolu a celou problematiku není třeba řešit. Privilege escalation je proces zvýšení vlastních práv, při nejlepším získání všech práv. Pokud máte uživatele, který nemůže ani vytvořit textový soubor, tak je to jako kdybyste se do systému ani nedostali. Při privilege escalation už velmi záleží na nabouraném systému, techniky použité na systému Linux nefungují na systému Windows ani macOS. Všechna práva vám dovolí měnit hesla ostatních účtů zapsaných v systému, a dokonce měnit všechny konfigurace systému.

4.1.1 Linux PrivEsc

Nejsilnější stránka a největší slabina Linuxů je jejich otevřenost a určitá hladina jednoduchosti. Ale nemyslete si, že pokud máte přístup k Linuxovému systému, tak jeho privilege escalation bude bez problémů. Většina způsobů a chyb se dá ošetřit správnými opatřeními, každopádně správci mohou udělat krok vedle a chyba se vyskytne, pak ji pouze objevit a využít.

4.1.1.1 Kernel Exploits

Tyto chyby jsou zakomponované v samotné verzi kernelu (jádra) systému, a ne na chybě nastavení správce. Kernel je fundamentální součástí všech Linux systémů, propojující paměť, systém a veškeré aplikace. Po zjištění verze kernelu stačí prohledat veřejně dostupné databáze exploitů a možná vaše verze se objeví v seznamu.

4.1.1.2 Sudo

Příkaz sudo je mocný sám o sobě. Sudo říká ať se příkaz nebo program spustí s root právy neboli nejvyššími právy. Je to užitečná funkce umožňující správci dát nejvyšší práva uživatelům pouze na nutné programy jimi používanými. Jak a na co máte práva zjistíte příkazem sudo -l. GTFOBins pak je knihovna obsahující všechny příkazy a jak se dají zneužít se sudo příkazem.

4.1.1.3 SUID a SGID

Soubory mají tři hlavní kontrolovatelné permise. Právo číst soubor, upravovat soubor a spustit soubor. Toto rozšiřují SUID a SGID funkce. SUID (Set-user Identification) způsobí, že soubor se spustí s právy vlastníka souboru a SGID (Set-group Identification) s právy vlastníka skupiny. Dané soubory se dají vyhledat jednoduše pomocí příkazu find a mají také sekci na GTFOBins.

4.1.1.4 Cron Jobs

Automatizace je zmiňována mnohokrát v celé práci a zde to nebude výjimkou. Cron Jobs jsou skripty nebo programy, které se spouští pravidelně v nějaký čas nebo po nějakém čase. V základu se spouští s právy vlastníka práce, a ne přihlášeného uživatele. Všechny jsou uložené v /etc/crontab. Tento problém je velmi jednoduše řešitelný, ale je to další cesta k právům.

4.1.1.5 PATH

Jedna z environmentálních proměnných ukazující cestu, ve které systém hledá spustitelné soubory. Obecně environmentální proměnné ukazují prostředí, ve kterém má daný proces běžet. Pokud je modifikace PATH proměnné povolena, můžeme vytvořit vlastní cestu ke spustitelnému programu nebo skriptu a navést ji kam potřebujeme.

Je třeba myslet na následky způsobené těmito a dalšími způsoby. Pokud se nepovedou a pokazí se, mohou způsobit pád systému nebo vám uzamknout přístup. Průzkumu byla vystavená kapitola sama o sobě. Zde je prováděna menši fáze vnitřního průzkumu odhalující informace o systému a možnosti, jak s nimi nakládat. Pro vnitřní průzkum bylo vytvořeno několik automatizovaných skriptů urychlující proces, mezi nejznámější, se kterými mám zkušenosti jsem použil LinPEAS nebo LinEnum.

4.1.2 Windows PrivEsc

Operační systém Windows za ty roky ušel dlouhou cestu a stal se velmi zabezpečenou a možnostmi omezenou jednotkou, ale ne neproniknutelnou. Má dva základní druhy uživatelů, obyčejné standardní uživatele s omezenými právy a administrátory s nejvíce právy. Administrátoři a všechny účty s administrátorskými právy se nachází ve skupině administrátorů a zbytek ve skupině uživatelů.

4.1.2.1 Scheduled Tasks

Podobná funkce funkci cron jobs v Linux systémech. Scheduled tasks automatizuje spouštění programů a skriptů ve specifický čas nebo jako odpověď na specifickou událost. Je to užitečná funkce ulehčující čas strávený opakováním kroků a manuálním zapínání aplikací. Každopádně podobně jako u cron jobs, každou položku v scheduled tasks vlastní uživatel, pod kterým se spouští. Pokud máme štěstí a některý z nich je vlastněn administrátorem, přičemž máme přístup k jeho přepisu, můžeme spustit cokoliv si přejeme s jeho právy.

4.1.2.2 Windows Services

Úlohy kontroluje Service Control Manager (SCM). Každá úloha má přivlastněný vlastní spustitelný soubor na zařízení a také uživatelský účet pod kterým úloha bude držena. Pokud do úlohy servisního účtu máme práva psát a upravovat cestu, jsme schopni jednoduše získat jeho práva její přeměnou.

Další lehce přehlédnutelnou chybkou ve správci úloh bývá špatně zapsaná cesta k souboru. Mezery mezi názvy složek a samotných programů jsou počítači špatně převáděné. V případě cesty zapsané například ve tvaru C:\Windows\Muj program\program.exe je mezera mezi slovy Muj a program převedena na rozdělení příkazu a část program\program.exe následně je

rozpoznána jako argument. Využití se dá pomocí vytvoření programu nazvaném Muj.exe po kterém sáhne operační systém v první řadě.

4.1.2.3 Windows Privileges

Práva mohou být individuálně u každého uživatele modifikována, udělována a ubírána. Práva umožňují uživateli vykonávat nutné akce pro jeho práci s počítačem bez komplikací nebo pomoci cizího účtu. Ale některá práva povolují příliš, a to se dá využít pro přístup k většímu množství ne-li ke všem právům.

SeBackup a SeRestore práva povolují přečtení a přepsání jakéhokoliv souboru v systému ignorující omezení. Myšlenka práv je zpočátku zcela nevinná, povolit některým uživatelům zálohovat soubory bez administrátorských práv. Samozřejmě psaním a čtením všech souborů je náš cíl získání kontroly nad systémem přímo triviální. Dostačující je jeden příklad zneužití, zkopírování SAM a SYSTEM registru k extrahování hashe administrátorského účtu.

Náchylné verze softwarů na systému nebo samotného operačního systému se také objevují a je to cesta k cíli. Jako na Linux systémech pro automatizaci existuje řada skriptů a Windows systémy nejsou výjimkou. Mezi nejběžnější zmíním obdobu LinPEAS WinPEAS nebo PrivescCheck kontrolující běžné způsoby privilege escalation.

4.2 Co dále?

Kromě běžných privilege escalation technik jsou zde další překážky a problémy, které nemůžete jen tak vypustit z hlavy. Systémy, hlavně větších firem, jsou průběžně kontrolovány právě kvůli podezřelým aktivitám. Pokud budete odhaleni, správci se vás pokusí ze sítě vyhnat a zablokovat jakýkoliv další pokus o přístup. Je to hra s časem a se schopnostmi obou stran, strany hackera a strany obránce. Mezi legální sférou hackingu se takovému dělení říká Red Team a Blue Team.

První nápad, co vás musí narovinu trknout ještě před samým privilege escalation je maintaining access (udržení přístupu). Jde o sadu postupů, které zkomplikují druhé straně vás vymazat ze sítě. Nejčastěji se pokládají na systému backdoory. Backdoor, se dá říct, je typ malwaru otevírající jednoduchý přístup útočníkovi bez nutnosti provádění celého procesu útoku od samotné začátku v případě ztráty přístupu. Mohou to být samostatné aplikace, nebo být součástí existující aplikace, kterou nakazí. S maintaining access souvisí persistence, která je potřeba ošetřit, abychom byli přítomni na nabouraném systému i po jeho rebootu (restartu).

Po získání veškerých práv můžeme manipulovat, upravovat, mazat nebo vytvářet jakýkoliv soubor si umíníme. Data Exfiltration je jeden z posledních kroků celého hacking dobrodružství. Jedná o převedení dat, které požadujeme a chceme je na námi vlastněný systém. Po sesbírání vzácného ovoce z jedniček a nul stačí pouhé zahalení stop pro naše zpětné vyhledání.

5 BIGGEST BREACHES IN HISTORY

Poslední kapitola odlehčující technicky náročné přemýšlení nad vesmírem plný zařízení, útoků a hacking technik nám představí největší průniky v historii. I největší firmy nejsou nedobytné a stačí pouhá jedna objevená chyba, některá skupina zkušených hackerů nebo jedinec a je problém.

5.1 Yahoo

Yahoo je světově známý americký internetový portál z roku 1994. Není to pouhá vyhledávací služba, větví se dále na e-maily Yahoo Mail, Yahoo skupiny, Yahoo odpovědi, a dokonce i Yahoo finance. Tato firma zažila hack katastrofu v srpnu roku 2013, kde více jak 1 miliarda účtů bylo nabouráno. Součástí účtů byly jména, telefonní čísla, data narození a zašifrovaná hesla. Ve výsledku bylo ovlivněno více jak 3 miliardy uživatelů.

5.2 LinkedIn

Neobvyklá sociální síť používaná profesionály, zaměstnavateli i zaměstnanci nabízející a diskutující o pracovních příležitostech. Už v březnu 2011 překonala hranici 100 milionů registrovaných uživatelů a dodnes je největší profesní sítí na světě. Nehoda na tuto ohromnou firmu nastala v červnu 2012. Afektováno bylo před 117 milionů účtů, ze kterých bylo přes 100 milionů hesel ukradeno. Hesla byla prodávána na černém trhu.

5.3 eBay

Největší americký internetový obchod charakteristický svými aukcemi rozšířený po celém světě. Útok se nadál na přelomu února a března roku 2014. Útočníkům se povedlo získat přístup ke všem 145 milionům zákaznickým účtům a později získali přístup k celé databázi všech uživatelských jmen a šifrovaných hesel.

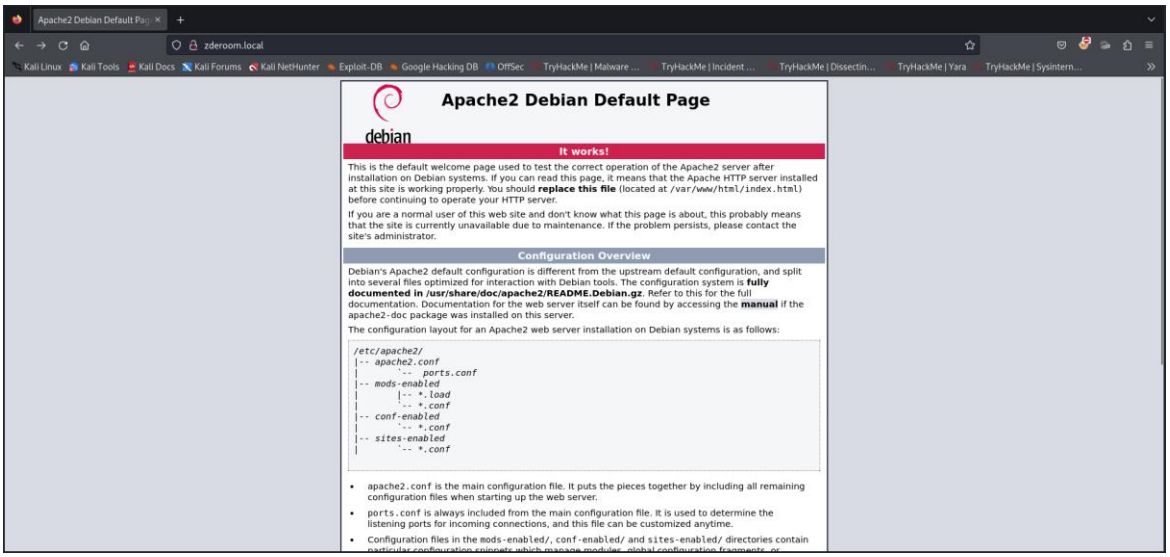
6 PRAKTICKÁ ČÁST

Mou praktickou částí bylo vytvoření simulace serveru, do kterého se pomocí zmíněných technik dá dostat a získat formou hry vítězný soubor.

Obrázek 4: Raspberry Pi 3 model B v zavřený krabičce

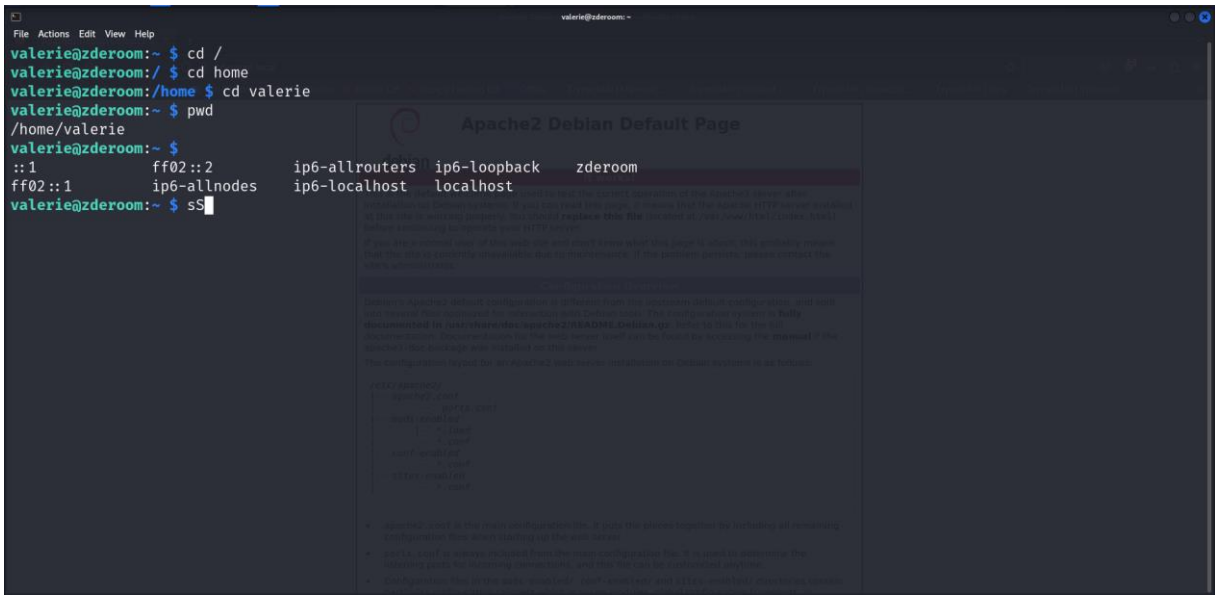
Obrázek 5: Raspberry Pi 3 model B v otevřené krabičce

Server je hostován na zařízení Raspberry Pi 3 model B.



Obrázek 6: Hlavní stránka webu

Jedná o Apache2 webový server. Později jednotlivými kroky a postupy se dostanete na samotný příkazový řádek serveru přes protokol SSH.



Obrázek 7: SSH příkazový řádek

Výherní soubor je umístěn v jedné ze složek. Pro připojení do hry je potřeba softwaru ZeroTier a ID sítě. Veškeré informace najdete na webu https://zderoom.wz.cz/.

7 ZÁVĚR

Díky této jsem mohl předat svoje znalosti a zkušenosti s okruhem hackingu ve formě word dokumentu. Pověděli jsme si od samotných základů a fundamentálních termínů po jednotlivé útoky a jakým způsobem jim předejít, pokud se s touto problematikou setkáme v budoucnosti.

V teoretické části mou snahou bylo pro každého srozumitelně popsat každou sekci bez zmatení nebo nepochopí z textu. Zaměřoval jsem se na ty nejzajímavější a největší části oboru a ty vysvětlit. Zakomponoval jsem také do své práce dodatečné kapitoly pro úplnost a vzájemně příjemnou kombinaci s hlavní problematikou.

V praktické části jsem místo textu do dokumentu nebo prezentace vytvořil vlastní webový server na vlastním počítači. Pro spojitost s tímto tématem jsem se inspiroval simulačními hrami, a tedy server je určený výhradně jako test vědomostí mých i ostatních.

V ročníkové práci by bylo možné pokračovat rozšířením a prohloubením jednotlivých kapitol přidáním dalších příkladů nebo všeobecně nových typů a stylů. Také by bylo možné přidat oddíl historie a porovnání historie zabezpečení se současností.

8 POUŽITÁ LITERATURA

1. Tryhackme, Google Dorking, Dostupné na: https://tryhackme.com/room/googledorking
2. Nude Systems, Passive Reconnaissance Explained [Methods & Tools], Dostupné na: https://nudesystems.com/passive-reconnaissance-explained-methods-tools/
3. DevX, Active Reconnaissance, Dostupné na: https://www.devx.com/terms/active-reconnaissance/
4. APTIEN.COM, Co je CIA triáda informační bezpečnosti, Dostupné na: https://aptien.com/cs/kb/articles/what-is-cia-triad
5. TechTarget, asymmetric cryptography (public key cryptography), Dostupné na: https://www.techtarget.com/searchsecurity/definition/asymmetric-cryptography
6. Tryhackme, Hydra, Dostupné na: https://tryhackme.com/room/hydra
7. OWASP, About the OWASP Foundation, Dostupné na: https://owasp.org/about/
8. Pentest People Ltd, OWASP Top Ten: Cryptographic Failures, Dostupné na: https://www.pentestpeople.com/blog-posts/owasp-top-ten-cryptographic-failures
9. OWASP, OWASP Top Ten, Dostupné na: https://owasp.org/www-project-top-ten/
10. GeeksforGeeks, Difference between DOS and DDOS attack, Dostupné na: https://www.geeksforgeeks.org/difference-between-dos-and-ddos-attack/
11. Tryhackme, Linux Privilege Escalation, Dostupné na: https://tryhackme.com/room/linprivesc
12. Tryhackme, Windows Privilege Escalation, Dostupné na: https://tryhackme.com/room/windowsprivesc20
13. Black Hat Ethical Hacking, Post-Exploitation Techniques: Maintaining Access, Escalating Privileges, Gathering Credentials, Covering Tracks, Dostupné na: https://www.blackhatethicalhacking.com/articles/post-exploitation-techniques-maintaining-access-escalating-privileges-gathering-credentials-covering-tracks/
14. CardConnect, The 10 biggest data breaches of all time, Dostupné na: https://www.cardconnect.com/launchpointe/payment-security/10-biggest-data-breaches/
15. Wikipedie, eBay, Dostupné na: https://cs.wikipedia.org/wiki/EBay
16. Wikipedie, LinkedIn, Dostupné na: https://cs.wikipedia.org/wiki/LinkedIn
17. Wikipedie, Yahoo!, Dostupné na: https://cs.wikipedia.org/wiki/Yahoo!
18. Cisco, Ethical Hacker, Dostupné na: https://skillsforall.com/course/ethical-hacker?courseLang=en-US&instance_id=80c156bc-84a4-47c9-a233-5eafe7bdde82

9 SEZNAM OBRÁZKŮ