Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informačních technologií

Využití Metasploit Framework pro penetrační testování

Diplomová práce

Autor: Bc. Vojtěch Jabůrek
Studijní obor: Aplikovaná informatika

Vedoucí práce: doc. Mgr. Josef Horálek Ph.D.

Hradec Králové 8. 2023

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 23.4.2024 Bc. Vojtěch Jabůrek

Poděkování: Rád bych tímto poděkoval svému vedoucímu diplomové práce doc. Mgr. Josefu Horálkovi, Ph.D. za odborné vedení práce, náměty a odborné připomínky. Zároveň děkuji své rodině za podporu po celou dobu studia.

Anotace

Tato diplomová práce je zaměřena na použití Metasploit Frameworku v oblasti penetračního testování. Práce je rozčleněna do tří hlavních bloků. První blok je věnován obecné problematice penetračního testování. Zde jsou uvedeny typy kybernetických útoků. Dále dílčí členění Hackerů do jednotlivých pod skupin podle jejich způsobu provádění kybernetických útoků a nakládaní s útokem zjištěnými zranitelnostmi a daty. Druhý blok práce je věnován operačnímu systému Kali Linux, který se využívá v oblasti penetračního testování včetně výpisu a popisu nástrojů v prostředí Kali Linuxu. Třetí blok je věnován Metasploit Frameworku. Tento třetí blok je dále členěn na popis jednotlivých modulů a programových knihoven, které obsahuje Metasploit Framework. Dále jsou v tomto bloku z míněny možnosti ovládání a práce s tímto nástrojem.

Klíčová slova: Penetrační testování, typy útoků, typy hackerů, Kali Linux, Metasploit Framework

Annotation

Title: Using the Metasploit Framework for penetration testing

This thesis is focused on the use of the Metasploit Framework in the field of penetration testing. The work is divided into three main blocks. The first block is devoted to the general issue of penetration testing. Here are the types of cyber attacks. Furthermore, the partial division of Hackers into individual sub-groups according to their method of carrying out cyber attacks. The second block of work is dedicated to the Kali Linux operating system, which is used in the field of penetration testing, including a list and description of tools in the Kali Linux environment. The third block is dedicated to the Metasploit Framework. This third module is further divided into a description of the individual modules and programming libraries that the Metasploit Framework contains. In addition, this block includes options for controlling and working with this tool.

Keywords: Penetration testing, types of attacks, types of hackers, Kali Linux, Metasploit Framework

Obsah

Seznam Obrázků

Seznam Tabulek

1. Úvod

Diplomová práce se zabývá využitím Metasploit Framework pro penetrační testování.

Důvodem pro penetrační testování je odhalit potenciálně zranitelná místa v počítačové síti firmy, aby bylo možné upravit zabezpečení sítě. Tím pádem následně nedošlo ke zneužití této zranitelnosti v počítačové síti. Obecně v počítačových sítí neexistuje síť připojená do internetu, která by neměla žádné slabé místo. Následně toto slabé místo sítě nešlo využít pro kybernetický útok. Slabinou všech počítačových síti a počítačových systémů je uživatel a případná přílišná benevolence v předpisech pro využívání koncových stanic připojených do firemní sítě. To platí i pokud je daná počítačová sít odpojena fyzicky od internetu. Důvody využití Metasploit Framework je to, že obecně zjednoduší svými nástroji průběh penetrační ho testování.

2. Cíl práce

Prvním cíle práce je v teoretické části uvést obecné postupy penetračního testování.

Druhým cílem je popsat možnosti penetračního testování pomocí Metasploit Framework v Kali Linux

Třetí cílem je vytvořit praktické příklady penetračního testování pomocí Metasploit Framework

3. Metodika zpracování

Diplomová práce se čelní na tři oblasti, které souvisí s problematikou penetračního testování. V první části jsou uvedeny typy kybernetický útoků, a to jak aktivní útoky, tak i pasivní útoky. Dále jsou v této části práce uvedeny čtyři skupin hackerů. V této první části jsou dále uvedeny fáze penetračního testování. Ve druhé část je tato práce věnována operačnímu systému Kali Linux a jeho nástrojům pro penetrační testování. Mezi nástroje instalované v operačním systému Kali Linuxu je i Metasploit Framwork. Třetí část diplomové práce je věnována Metasploit Framework a popsání jeho funkcionalit. Tato třetí část práce se dělí do čtyř dílčích částí. První dílčí část je věnována Modulům, které jsou dostupné v Metasploit Frameworku. Druhá dílčí část se věnuje knihovnám kódu, které se používají v rámci Metasploit Frameworku. Třetí dílčí část je věnována možnostem práce s Metasploit Frameworkem, kdy v této části jsou uvedeny základní příkazy pro práci v msfconsole. Poslední pod část práce je věnována payload modulům a auxiliary modulům. Kdy je uveden popis pro jednotlivé vybrané moduly a zároveň je uvedena praktická ukázka nastavení konkrétních modulů. V závěrečné části práce je věnována praktickému využít Metasploit Frameworku.

4 Penetrační testování a Hackerské útoky

V této kapitole bude postupně zmíněna problematika penetračního testování a možnosti nástrojů pro provádění kybernetických útoků.

4.1 Druhy útoku aktivní, nebo pasivní

Kybernetické útoky jsou děleny na aktivní, nebo pasivní

Mezi aktivní typ útoku jsou například následující druhy útoku Network Maping, Port Scanning a Password Cracking. Do skupiny pasivních útoku řadíme například Listening to network traffic a Monitoring employess. [1]

Port Scanning – Technika skenování portů, při které se zjišťují otevřené porty u jednotlivých zařízeních v síti. Tímto způsobem je zjištěno, na jaké porty se má

u daného zařízení v síti útok zaměřit. [1]

Network Maping – Jedná se o techniku pomocí, které se udělá mapa dané počítačové sítě. [1]

Password Cracking – Jedná se o skupinu nástrojů sloužící k prolomení přihlašovacích údajů napadaného zařízení. Password Cracking má dva typy první typem je slovníkový útok, kdy se jako možná hesla zkouší různá slova a jejich tvary. Druhým typem tohoto útoku je útok takzvaně: „hrubou silou“, kdy se zkouší různé kombinace znaků. [1]

Listening to network traffic – Odposlouchávání provozu v síti je technika, kdy útočník nic přímo v síti nedělá pouze odposlouchává z nějakého místa provoz v síti. Následně z analýzy odposlouchávaného provozu zjistí například, jakou IP adresu má DHCP server, Fille server, nebo DNS server a další důležité prvky dané konkrétní počítačové infrastruktury. [1]

4.2 Typy hackerů

Pod pojme Hacker se skrývají čtyři skupiny IT odborníků. Dělení Hackerů do skupin je popsáno níže. Velmi často má široká veřejnost mimo svět IT označení Hacker spojené s člověkem, který se pohybuje za hranicí zákonnosti a s vím jednáním pouze škodí lidem. Níže je členění do jednotlivých skupin Hackerů.

White hat – Jedná se o skupinu Hackerů, která se věnuje vyhledávaní zranitelností systémů a jejich opravování, tak aby nemohlo dojít v budoucnosti k využití zjištěné zranitelnosti při kybernetickém útku na danou počítačovou infrastrukturu. Jedná se o bezpečnostní experty, kteří pracují zcela legálně a v mezích zákonů. Jejich práce je ochrana proti dalším skupinám Hackerů zejména pak proti skupině Black hat. [44]

Black hat – Jedná se o skupinu Hackerů, která se věnuje nelegálním činnostem

a zneužívání jednotlivých zranitelností systému. Tato skupina se pohybuje za hranicí zákonů. Tato podskupina Hackerů je asi nejvíce spojována s označením Hacker. [45]

Grey hat – Jedná se o skupinu Hackerů, která se pohybuje za hranící zákona, nebo etických pravidel. Tato skupina nekrade data z útokem postižené počítačové sítě

na rozdíl od skupiny Black hat. [46]

Blue hat – Jedná se o skupinu Hackerů, která se podobá výše v této práci popsané skupině White hat. Z pohledu společnosti se na rozdíl od White hat jedná o externí firmu. [47]

Red hat – Jedná se o skupinu Hackerů, která se věnuje lovení Hackerů spadajících

do skupiny Black hat. [48]

4.3 Dělení penetračních tastrů

Penetrační testery lze rozdělit do podskupin podle znalostí a přístupu k testované firemní počítačové infrastruktuře.

black box testing – Tato podskupina penetračních testerů nemá znalosti dané počítačové infrastruktury. Tato skupina má jen ty znalosti firemní počítačové infrastruktury, které lze zjisti z veřejných zdrojů. [68]

grey box testing – Tato podskupina penetračních testerů mám už přístup k firemní počítačové síti jako její uživatel. Penetrační testeři v této skupině jsou něco mezi skupinami black box testing a white box testing. [68]

white box testing – Tato podskupina penetračních testerů mám plný přístup k firemní počítačové infrastruktuře včetně veškeré dostupné IT dokumentace. [68]

4.3 Fáze penetračního testování.

Tato kapitola textově vychází z Hacking: praktický průvodce penetračním testováním. [1]

Na obrázku níže jsou uvedeny body průběhu penetračního testování, kdy vybrané body jsou popsaný v trochu upravené podobě níže v textu práce.

Obrázek1: (zdroj obrázku [50])

Plánování testování

Stanovit cíle penetračního testování, jaké části síťové infrastruktury budou zahrnuty v testování, a naopak, které části sítě budou vyjmuty z testování. Stanovit čas ve kterém bude probíhat testovaní. Dále případně stanovit na jaké části systému a jejich

zranitelnosti bude cílit samotný plánovaný kybernetický útok. Z hlediska zákonnosti je pro penetrační testování nutné uzavřít dohodu s provozovatelem dané počítačové sítě. [1]

Skenování sítě

Jedná se o přípravnou fázi, kdy se zjišťují možná zranitelná místa v počítačové síti. Skenován sítě lze rozdělit do tří typů konkrétně Externí skenování, pasivní odposlech a aktivní odposlech. [1]

Externí skenování – Testuje to, co je běžně dostupné jedná se například o aplikace,

přes které firma komunikuje se zákazníky (webové stránky e-shopu). Tento typ skenování může odhalit například špatně nastavený způsob validace dat, kdy se data ověřují pouze na straně klienta, a nikoliv na straně serveru. Na příklad špatná validace dat byla i v ČR, když se spustila registrace na očkovaní covid 19, tak ověřovaní rodného čísla probíhalo jen na straně klienta. Ve výsledku to způsobilo to, že v době, kdy byla registrace asi od 80 let věku se mohl do systému dostal i člověk, který nespadal do dané věkové kategorie. [1]

Pasivní odpalech – Pouze sleduje probíhajíc komunikaci v dané síti a hledá její slabá místa. Tímto způsob lze například zjistit na jakých IP adresách se nacházejí jaké servery a jaké IP adresy používají počítače, nebo jakou adresu mám pro danou LAN brána do internetu. K pasivnímu skenování sítě se používá například Discover Scriptts Pasivní odposlech sítě lez využít k následnému doppelganger attack. [1]

Aktivní odposlech – Jedná se už o aktivní skenování sítě s cílem vyhledat konkrétní služby a případně konkrétní zranitelnosti dané sítě. [1]

Detekce a analýza

Po fázi skenování sítě následuje ze jištěných údajů detekce zranitelnosti společně s analýzou zjištěných zranitelností a z toho plynujících rizik pro danou počítačovou infrastrukturu. [1]

Post Incident aktivity

Reakce na zjištěné bezpečnostní hrozby jako je úprava nastavení kybernetické bezpečnosti. Úprava podmínek používání firemních koncových zařízeních (PC, telefony). [1]

4.4 Druhy penetračního testování

Penetrační testování lze rozdělit podle toho na jaký typ zranitelnosti se penetrační testování zmařuje.

4.4.1 penetrační testování podle typu služby a typu zařízení

Penetrační testování lze rozdělit podle typu testované služby, nebo podle typu zařízení, které má být při penetračním testování testováno. Jak uvádějí zdroje [50],[51],[52],[53],[54]. Níže v práci jsou tyto postupy penetračního testování popsány.

Penetrační testování mobilních aplikacích

První podskupinou penetračního testování je testování zranitelností v prostředí mobilních aplikací. Tato podskupina penetračních testů v posledních letech nabírá na důležitosti z důvodu velkého rozvoje využívání mobilních aplikací. Metodiky zabezpečení mobilních aplikací vychází z Metodiky zabezpečení aplikací.

- První fáze Discovery – V první fázi se zjišťují veřejné informace o dané mobilní aplikaci.

- Open Source Intelligence – Hledání dostupných informací o konkrétní aplikaci na internetu. Používané knihovny v dané aplikaci, nebo uniklé zdrojové kódy vybrané aplikace.
- Understanding the platform – Při stanovení bezpečnostní rizik je důležití zohlednit konkrétní mobilní platformu.
- Client side vs Server side scenarios – Je nutné rozlišovat nativní aplikaci, která je vytvořena pro danou platformu mobilních operačních systémů, kdy se testují pouze zranitelnosti pro daný operační systém.

Dále rozlišovat hybridní aplikaci, která se musí testovat na zranitelnosti více mobilních operačních systému. V dnešní době se jedná hlavně otestování zranitelností pro Android a Apple. Poslední druhem je webová aplikace, kdy testování webové aplikace je popsáno níže v práci.

- Druhá váze analýza – Analýza zdrojového kódu a používaných knihoven kódu.
- Archive analysis – Kontrola konfigurace používaných balíčku instalovaných pro android, nebo iOS.
- Local file analysis – Kontrola souborů, které využívá daná aplikace.
- Reverse engineering – Převod z kompilovaného zdrojového kódu do člověkem čitelné podoby. Poté následuje analýza daného zdrojového kódu.
- Dynamic analysis – Analýza aplikace za běhu, kdy se analyzuje například komunikace mez severem a daným zařízením.
- Network and web traffic – Přesměrování provozu mezi zařízením a serverem přes proxi. To umožnuje analyzovat síťový provoz na úrovni packetů.
- Třetí fáze Exploitation:
- Attempt to exploit the vulnerability – Pokus o zneužití zjištěných zranitelností s cílem zjisti z napadeného zařízení citlivá data.

- Privilege escalation – Pomocí zjištěných zranitelností získat práva administrátora (superuživatele)
- Čtvrtá fáze Reporting – Ohodnocení zjištěných zranitelností podle stupně nebezpečnosti.
- Final report: - Podrobná zpráva o objevených zranitelnostech jejich hodnocení a bezpečnostních doporučení určených k eliminaci daných zranitelností.

[50]

Penetrační testování webových aplikací

Druhou podskupinou penetračního testování je testování zranitelností webových aplikací. Jedná se o penetrační testování změřené na nastavení prostředí a nastavení webové aplikace. Tyto penetrační testy shromažďují veřejné informace o dané testované webové aplikaci. Dále mapují počítačovou síť, která danou webovou aplikaci hostují. Požívají se zde dva přístupy první přístup je Active Reconnaissance a druhá přístup je Passive Reconnaissance.

Active Reconnaissance – Aktivní skenování cílového systému s využitím skenování dané počítačové sítě. Dále se využívá dopředné a zpětné vyhledávání DNS.

Passive Reconnaissance – Jedná se o shromažďování všech veřejně dostupných informací o dané webové aplikaci bez přímě interakce s danou webovou aplikací. Mezi tyto informace paří na příklad informace subdoménách, které daná webová aplikace využívá.

Penetrační testování webových aplikací se používá v kombinaci s níže popsaným penetračním testováním API rozhraní.

Penetrační testy komunikačních protokolů, se využívá k určení rizika pro danou počítačovou infrastrukturu a komunikaci v rámci dané sítě a internetu. Tyto rizika plynou z používání nezabezpečených protokolů, nebo protokolů s prolomeným

šifrování, nebo používáním nedostatečně dlouhého šifrovacího klíče, nebo špatného šifrovacího algoritmu. Například pro webové stránky společnosti využívat https protokol místo http protokolu. Pro dálkovou správu zařízení používaných v dané počítačové infrastruktury využívat výhradně zabezpečeného SSH protokol a vyhnout se používání nezabezpečeného Telnet protokolu.

[51]

Penetrační testy API rozhraní

Třetí podskupinou penetračního testování je testování zranitelností API rozhraní.

Tyto testy můžou odhalit špatnou validaci, nebo verifikaci v serverové části aplikace (Backend aplikace), nebo špatně napsané API rozhraní ve smyslu autorizace a autentizace. Tyto testy je možné provést bez nutnosti mít celo funkční aplikaci. Lze testovat po napsaní samotné služby, nebo vytvoření serverové části aplikace

bez nutnosti funkční klientské části aplikace (Frontend aplikace). API rozhraní lze testovat na příklad v nástroji Postman, nebo Curl. [52]

Penetrační testování IoT zařízení

Penetrační testování IoT zařízení se dělí do následujících skupin, které jsou popsané níže.

Penetrační testování hardwaru – Testování hardwaru daného IoT zařízení využívá

se zde výpisy paměti, Kryptografická analýza a Reverzní inženýrství.

Penetrační testy firmwaru – Jedná se o techniky zaměření na firmware IoT zařízení. Mezi tyto techniky patří na příklad techniky prolamování hesel, úpravy firmwaru, Přetečení zásobníku. Stejně jako u penetrační testování hardwaru i penetrační testy firmwaru

se využívají techniky Reverzního inženýrství a Kryptografické analýzy.

Penetrační testová komunikačních protokolů – Tento druh penetračního testování IoT se zaměřuje na technologie umožňující komunikaci IoT zařízení a odesílání dat z daného zařízení (RFID, NFC, ZigBee, Bluetooth, WiFi, SigFox a LoRa). Využívají se například techniky zachycování a analýzy více protokolových rádiových signálů (sniffing). Dále se využívají techniky pro kryptografickou analýzu, nebo techniky DOS útoku.[53]

Sociálním inženýrství

Sociálním inženýrství je samostatnou technikou penetračního testování a do jisté míry odděleným typem penetračního testování od ostatních výše popsaných penetračních technik. U tohoto typu penetračního testování nejsou nutné speciální znalosti jako u ostatních popsaných technik penetračního testování. U Sociálním inženýrství se využívá především znalosti v oblasti psychologie, a nikoliv samotné znalosti IT. Útočník musí s vím jednání zajistit důvěru a strach u napadených lidí. V tomto případě se netestují přímo zranitelnosti systému, ale selhání lidského faktoru. Tato selhání může být způsobenou nedodržování předpisů o používání firemních počítačů a firemní počítačové sítě. Dále se může rovněž jednat o nedostatečné pro školení zaměstnanců o pravidlech využívání firemních počítačů a firemní počítačové sítě. [54]

4.4.2 Dělení dle použité metodologie

V při penetračním testová lze využít tyto následující metodologie.

Open Source Security Testing Methodology Manual (OSSTMM)

OSSTTM metodika obsahuje čtyři fáze, které budou popsány níže v práci.

- Induction Phase – Přípravná fáze pochopení toho, co se má testovat a co má cílem penetračního testování. Dále schválení rozsahu a způsobu provádění

penetračního testování. Tato fáze se dále dělí do tří dílčích částí popsaných níže v práci

- Posture Review – Tato první část se zabývá zkoumáním norem předpisů a legislativy. V této první části je nutné určit rozsah penetračního testování.
- Logistics – Tato část druhá se zabývá omezení interakce jako je vzdálenost a rychlost interakce jako je vzdálenost, rychlost interakce. V této druhé části je nutné určit a znát omezení penetračního testování.
- Active Detection Verification – Tato třetí část se zabývá šířkou detekce, reakce a předvídatelnost reakce. V této třetí části je nutné znát omezení, která jsou kladena pro použití interaktivních testů.

- Interaction Phase – Tato fáze určuje rozsah penetračního testování a dělí se do čtyř částí, které jsou popsány níže v této práci.
  - Visibility Audit – Tato první fáze se zabývá cílem penetračního testování. V téo první části je nutné vědět jaké jsou cíle penetračního testování existují a jak fungují. Dále jaké jsou mrtvé, nebo neexistují cíle, nebo nereagující cíle.
  - Access Verification Audit – Tato druhá fáze se zabývá měření šířky a hloubky interaktivních přístupových bodů a jejich autentizací
  - Trust Verification – Tato třetí fáze se zabývá
  - Control Verification – Tato čtvrtá fáze se zabývá
- Inquest Phase – Inquest Phase fáze se věnuje možnému zneužití špatnému nastavení zabezpečení dat. Tato fáze se dále rozděluje do šesti dílčích částí popsaných níže v práci.
  - Process Verification Tato první část se zabývá určení a existencí záznamů o úrovni zabezpečení a kontrola nastavených pravidel zabezpečení daného počítačového systému. Je nutné znát potřebné používané ovladače a jejich používáné rutiny, kdy procesy mají definované soubory pravidel pro práci

s daným procesem. Pravidla pro procesy je možné předefinovat a tím získat přístup k danému požadovanému procesu.

- Configuration Verification and Training Verification – Tato druhá část se zabývá analýzou běžného provozu v dané počítačové síti. Určuje možné problémy pomocí bezpečnostních a zátěžových testů. Tato část zkoumá, jak cílové zařízení pracuje při běžném provozu v dané počítačové infrastruktuře.
- Property Validation – Tato třetí část se zabývá měřením používání nelegálních, nebo nelicencovaných aplikací. Je nutné znát vlastnická práva a licenční podmínky pro využívání dané aplikace.
- Segregation Review – Tato čtvrtá část se zabývá stanovením úrovní potřebných osobní identifikačních údajů. Je nutné znát požadavky na ochranu osobních údajů jednotlivých států jako je GDPR.
- Exposure Verification – Tato pátá část se zabývá vyhledávání volně dostupných informací, které popisují nepřímo viditelné cíle, nebo aktivity v rámci zvolených kanálů a určeného rozsahu.
- Competitive Intelligence Scouting – Tato šestá část se zabývá vyhledávání volně dostupných informací, které mohou poškodit, nebo ovlivnit napadané zařízení. Informace z procesů napadeného cílové zařízení může mít větší hodnotu než aktivity, kterými jsou informace chráněny.

- Intervention Phase – Intervention Phase fáze, která obsahuje testy zdrojů napadeného zařízení. Tato fáze má za cíl přetížení, nebo vyhladovění zdrojů
- a následně provést průnik do napadeného systému. Jedná se o poslední fází podle OSSTMM. Tato poslední fáze se dělí do čtyř dílčích částí, které jsou popsány níže v práci.
  - Quarantine Verification – Tato první část se zabývá efektivitou využívání takzvané karantény pro přístup do daného systému. Tato část se věnuje účinnosti

autentizace a využívání takzvané černé listiny, nebo bíle listiny pro přístup do daného sytému.

- Privileges Audit – Tato druhá část se zabývá mapování dopadů případného zneužití přihlašovacích údajů, nebo přístupových oprávněních v daném systému. V tato část se zaměřuje na kontrolu nastavení procesu autentizace, nebo autorizace v daném systému. Dále se při této fázi kontroluje správnost nastavení uživatelských rolí v dáném systému.
- Survivability Validation and Service Continuity – Tato třetí část se zabývá měření odolnosti napadeného zařízení z pohledu kontroly integrity a kontinuity daného systému. Dále se ověřuje zamítnutí služby, nebo zamítnutí interaktivity daného systému.
- Alert and Log Review and End Survey – Tato čtvrtá část se zabývá kontrolou provedení penetračního testování, kdy se tato část věnuje popisu použité hloubky penetračních testů. [55]

Open Web Application Security Project (OWASP)

OWASP je organizace, která poskytuje návody, jak vytvářet a udržovat bezpečné a důvěryhodné webové aplikace. OWASP je fórem, kde mohou bezpečnostní experti a odborníci na informační technologie vytvářet volně dostupné metodiky a dokumentaci. OWASP utváří seznam bezpečnostních rizik pro webové aplikace. Níže v práci je popsáno top deset zranitelností podle OWASP.

- Broken Access Control – Ověření uživatelé mají špatně nastavená uživatelská práva, kdy tyto uživatelé mají špatně omezený přístup k funkcím, nebo k datům na daném počítačovém systému. Omezení práv k přístupu do daného počítačového systému pro ověřené uživatele není vynucována.
- Cryptographic Failures – Jedná se o zranitelnosti spojené se selháním šifrování. Tato selhání vedou k odhalení citlivých dat nebo kompromitaci systému. Webové

aplikace a API rozhraní mají zranitelnosti spojené s používaným kódování, které mohou útočníci využít pro odhalení citlivých dat.

- Injection – Injection SQL je útok, který se provádí odesláním chybně formátovaného kódu na databázový server. Tento typ útoku je mezi Hackery populární pro rychlost provedení útoku a jednoduchost daného útoku.
- Cross-site scripting – Cross-site scripting je rizikem v případech, kdy webová aplikace obsahuje nedůvěryhodná data na nové webové stránce bez řádného ověření. Dále se jedná o aktualizaci webové stránky na základě dat dodaných do webové aplikace uživatelem pomocí rozhraní API. Útočník má možnost vložit do aplikace skripty na straně klienta a tímto způsobem může dojí k ukradení uživatelských relací. To může vést k přesměrování uživatelů z napadené webové stránky na škodlivé webové stránky útočníka.
- Insecure Design – Insecure Design je kategorie, která se zaměřuje na rizika související s chybami v návrhu aplikace To znamená použití více modelování hrozeb pro bezpečné návrhové vzory a principy v dřívějších fázích cyklu vývoje aplikací.
- Vulnerable and Outdated Components (formerly referred to as "Using Components with Known Vulnerabilities") - Jedná se o typ zranitelností, které jsou spojeny s používáním zastaralých knihoven a frameworků. Problém těchto zranitelností je to, že vývojáři nemusí vědět jaké open source komponenty, nebo komponenty třetích stran jsou v jejich aplikacích využívány.
  Tato skutečnost má za následek složitou aktualizaci daných komponent využívaných v dané aplikaci. Problém s aktualizacemi používaných komponent je rizikem v případě objevení nových zranitelností pro dané komponenty využívaných v aplikacích.
- Identification and Authentication Failures (formerly referred to as "Broken Authentication") - Jedná se o typ zranitelností spojených se špatnou

implementací jednotlivých funkcí dané aplikaci. Implementační chyby funkcí v aplikaci může vést ke zneužití hesel, klíčů a tokenů relace. Implantační chyby můžou vést k dočasnému, nebo i trvalému převzetí uživatelské účtu.

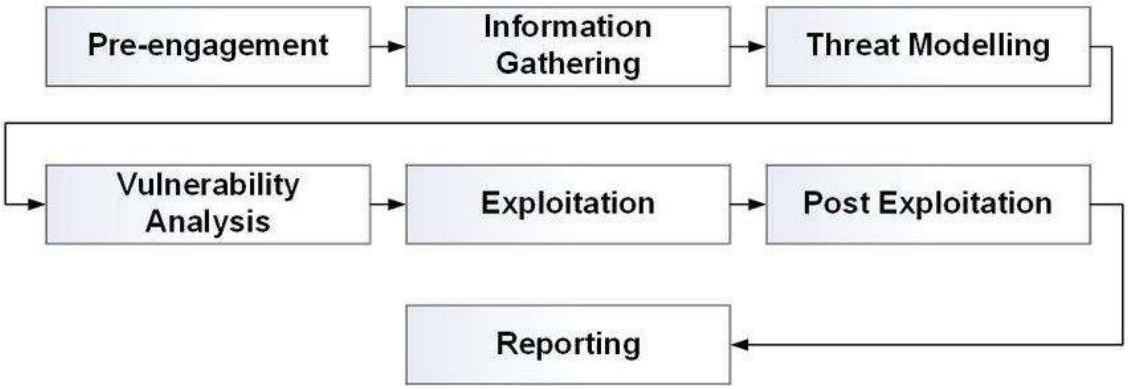
- Software and Data Integrity Failures – Selhání integrity softwaru a dat, se vztahuje na kód a infrastrukturu, které selhávají při ochraně proti narušení integrity. Do tohoto typu zranitelností patří aktualizace softwaru, nebo kritická data. Dále zde patří CI/CD kanály, které nemají žádné ověřování (například: data zakódovaná nebo serializovaná). Dále se jedná o automatické stahování aktualizací aplikací bez dostatečného ověření integrity aplikace, kdy hacker může vydat falešnou aktualizaci důvěryhodné aplikace. Poslední součást této skupiny zranitelností je nezabezpečená deserializace. Nezabezpečená deseralizace může mít za následek vzdálené spuštění kódu. Účelem vzdálené spuštění kódu může být manipulace nebo odstranění serializovaných objektů. Dále může být cíl zvýšení uživatelských oprávnění.
- Security Logging and Monitoring Failures (formerly referred to as “Insufficient Logging and Monitoring”) - Do této skupiny zranitelností patří selhání bezpečnostního protokolování a monitorování spolu s chybějící nebo neúčinnou integrací se systémy reakce na incidenty. Odhalení tohoto typu zranitelností je časově náročné a většinou ho odhalí až externí bezpečnostní audit.
  Mezi typické útoky, které se využívají tento typ zranitelnosti patří například SQL injections, XSS. Hackeři spoléhají na nedostatek v monitorování dané počítačové infrastruktury a s tím spojené jejich neodhalení, nebo pozdní odhalení.
  Tato pozdní detekce útoku má za následek pozdní reakci na daný útok a poskytuje hackerovi čas na provádění cílů daného útoku.
- Server-Side Request Forgery – Jedná se o zranitelnost při, které webová aplikace načte vzdálený zdroj bez ověření uživatelem zadané adresy URL. Hacker může vytvořený požadavek od webové aplikace poslat jinému cíli, než je původní cíl

daného požadavku. Proti tomuto typu zranitelností nepomáhá ani firewallem, VPN nebo jiným typem seznamu řízení přístupu k síti. Jedná se o typ zranitelností, která má za tím malou četnost výskytu, ale četnost výskytu tohoto typu zranitelností pravděpodobně poroste z rozvoje využívání cloudových služeb.

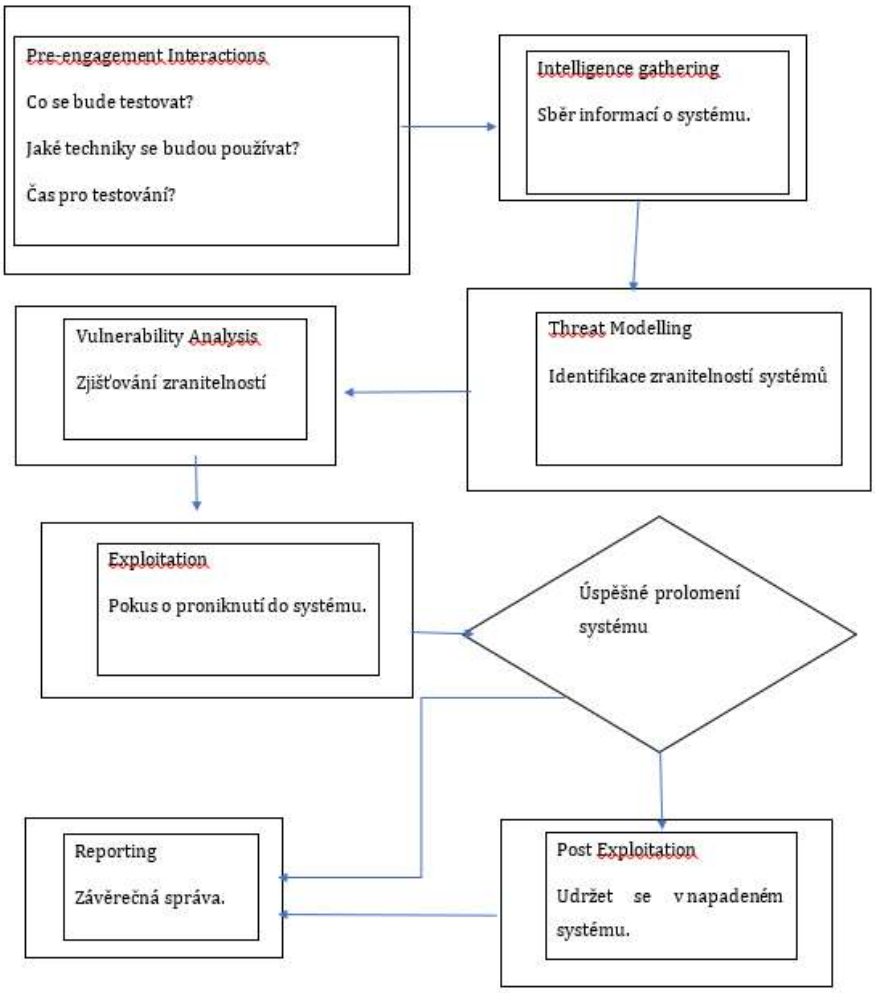
[56]

Penetration Testing Execution Standard (PTES)

PTES je metodika má za cíl řešit potřebu standardu pro penetrační testování. PTES má za cíl informovat klienty pasteračního testování o způsobu provádění penetračních testů. PTES metodika má průběh penetračního testování rozdělen do sedmi částí, které jsou popsány níže v této práci. Na obrázku níže je schéma průběhu penetračního testování s využitím PTES



Obrázek 2 (zdroj: [71])



Obrázek 3 (zdroj: autor)

- Pre-engagement Interactions – V této fázi se plánuje celý průběh penetračního testování včetně používaných nástrojů. Tyto plány se následně písemně schválí.
- Intelligence gathering – V této fázi se provádí sběr informací z externích zdrojů. Tato fáze má za cíl vytvořit co nejlepší pohled na testovanou síť z internetu.

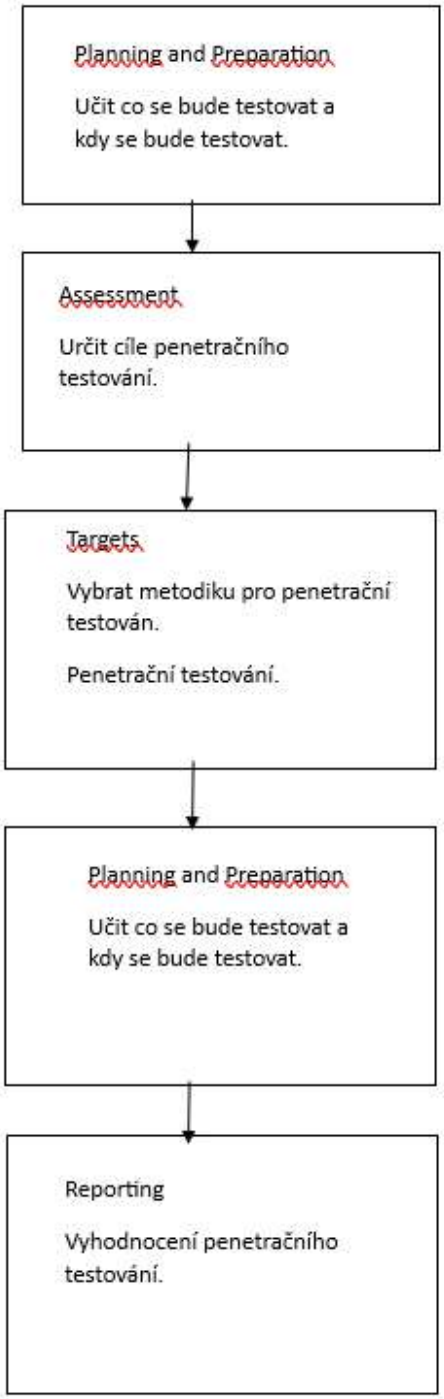
Zjišťuje se, které části firemní počítačové síťové infrastruktury jsou dostupné z internetu.

- Threat Modelling – Cílem fáze Threat Modelling je optimalizace zabezpečení počítačové síťové infrastruktury dané společnosti. Účelem této fáze je identifikovat zranitelnosti v dané síti a následně návrh opatření k zamezení zneužití zjištěných zranitelností, nebo minimálně minimalizovat případné škody při zneužití těchto zranitelností.
- Vulnerability Analysis – Fáze při, které se zjišťuje možnost využití zranitelností pro získání autorizovaného přístupu do napadané aplikace, nebo systému.
- Exploitation – Ve fázi Exploitation se Penetrační tester pokouší dostat do testovaného systému pomocí dříve zjištěných zranitelností.
- Post Exploitation – Po úspěšné podniknutí do napadeného systému má tato fáze za cíl udržet se v napadaném sytému a sběr dat z nameteného sytému.
- Reporting – Zpracování závěrečné zprávy informující o průběhu a výsledcích penetračního testování.

[57]

Information Systems Security Assessment Framework (ISSAF)

ISSAF metodika má průběh penetračního testování rozdělen do pěti částí, které jsou popsány níže v této práci. Na obrázku níže je znázorněn průběh penetračního testování podle ISSAF metodiky.



Obrázek 4 (zdroj obrázku: autor)

- Planning and Preparation – Jedná se o fázi výměny informací a smluvní ujednání o tom co se bude testovat a rozsah celého penetračního testování. Musí se identifikovat komunikační kanály mezi společností a týmem pro penetrační testování. Dále je nutné odsouhlasit plán a rozsah penetračního testování včetně eskalací oprávnění.
- Assessment – Popis cílů penetračního testování, a to i s popisem nástrojů penetračního testování, které lze pro ti danému cíli útoku použít.
- Targets – ISSAF poskytuje metodiku pro penetrační testování pro ti různých typů cílových zařízeních. Poskytuje základní informace o typu zařízení a jeho výchozí konfiguraci a typických konfiguracích. V této metodice je obsaženo i druhy nástrojů, které lze využít k útoku na daný typ zařízení. Podle ISSAD se cíle útoku dělí do pěti skupin.
    - První podskupinou je Network Security do této podskupiny patří všechny penetrační testy, které se týkají zabezpečení počítačové sítě. Do této podskupiny patří například Password security testing, Switch security assessment, Router security assessment, Antivirus system security assessment and management stratégy, Storage Area Network (SAN) security, Firewall security assessment a Wireless Local Area Network (WLAN) security assessment.
    - Druhou podskupinou je Host Security do této podskupiny patří všechny penetrační testy, které se týkají zabezpečení operačních systémů počítačů, nebo operačních systémů serverů. Do této podskupiny patří například Unix/Linux system security assessment, Windows systems security assessment, Novell Netware security assessment a web server security assessment.
    - Třetí podskupinou je Application Security, kdy tato podskupina se zabývá zabezpečením aplikací. V této skupině jsou například web application

security assessment (SQL injections), Source code auditing, Binary auditing.

- Čtvrtá podskupina je Database Security, která se zabývá zabezpečením databází. V této čtvrté podskupině se využívají například Remote enumeration of databases, Brute-forcing of databases, Process manipulation attack a End-to-end audit of databases.
- Pátá podskupina je podle ISSAF sociální inženýrství, které bylo popsáno výše v této práci.

- Reporting – Finální zpráva je v písemné podobě a pojednává o výsledcích penetračního testování a o zjištěných zranitelnostech v testované počítačové síti. V naléhavých případech je možné informace z dělit i ústní formou, ale pouze u kritických problémů, které vyžadují okamžité řešení. Speciálním případem je, pokud se během penetračního testování zjistí nějaká nezákonná činnost na síti a v systémech. Ve výsledné protokolu o penetračním testování musí být uvedeno Management summary, který určuje rozsah projektu a použité nástroje Pentest, použité zneužití, datum a čas testu. Všechny výstupy nástrojů a exploitů a seznam zjištěných zranitelností.
- Clean-Up and Destroy Artefacts – Jedná se o fázi úklidu po penetračním testování. Jedná se smazání všech dat a souborů, které byli penetračním testováním vytvořeny.

[58]

5 Kali Linux

Historie

Jedná se speciální distribuci Linuxu pro penetrační testová, která vychází z distribuce Debian Linux. Od roku 2006 do 2011 se používal operační systém BackTrack. ze kterého následně vyšel operační systém Kali Linux. První verze Kali Linux vyšla v roce 2013 a zatím poslední nová veze je z června 2023. [15], [31]

5.1 Nástroje Kali Linux

Operační systém Kali Linux má nainstalováno celkem 13 skupin nástrojů pro oblast kybernetických útoků a penetračního testování.

Database Assessment

Do skupiny těchto nástrojů spadají SQLite database browser a sqlmap

- SQLite database browser – Jedná se o nástroj pro tvorbu a úpravu databáze bez potřeby psaní SQL kódu. [35]
- Sqlmap – Jedná se o open source nástroj pro penetrační testování SQL databáze, který lze použít na všechny známe SQL databáze (například: MySQL, Oracle, PostgreSQL, Microsoft SQL Server). Podpora pro technik SQL injection boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band. Má podporu pro výpis uživatelských účtů včetně všech oprávnění a hash hesla. Tento nástroj obsahuje automatickou detekcí druhů hash použitých pro heslo. Nástroj dále podporuje prolomení hesla za pomocí slovníkového útoku. Dále nástroj podporuje navázání mimo pásmového stavového TCP spojení mezi zařízením útočníka a databázovým serverem, který je základem operačního systému. Tímto kanálem může být interaktivní příkazový řádek, relace Meterpreter nebo relace grafického uživatelského rozhraní (VNC)

podle volby uživatele. Metasploit Meterpreter getsystem pro eskalaci uživatelských práv pro databázové procesy. [36]

Password Attacks

Tato skupina nástrojů se dále dělí do čtyř podskupin podle typy útoků (Offline Atacks, Onlien Attacks, Passing the Hash Tools, Password Profiling & Wordlists) Mezi nástroje na password attacks spadají na příklad tyto níže uvedené nástroje

- Cewl - Custom Word List generátor je aplikace prohledávajíc zadanou URL adresu do určené hloubky a vrací seznam slov, které lze následně využít k prolomení hesla. Cerwl dále umí vytvořit seznam nalezených emailových adres v odkazech mailto. Emailové adresy se použijí jako uživatelské jméno pří útoku hrubou silou (to znamená zkoušení jakékoliv kombinace znaků pro prolomení hesla). [4]

Tabulka níže obsahuje výpis vybraných parametrů pro cewl. Tento výpis se zobrazí

po zadání příkazu: „cewl -h“.

(https://www.hackingarticles.in/a-detailed-guide-on-cewl/)

parametr	Popis parametru
-h	zobrazí nápovědu
-k	stáhne soubor
-w	zapsání výstupu příkazu do souboru
-g	vrací skupinu slov
-e	včetně e-mailové adresy

--meta_file	výstupní soubor pro metadata
--email_file	výstupní soubor pro e-mailovou adresu
-n	nevypisovat seznam slov
-c	počet nalezených slov
-v	podobná slova
--auth_type	typ autentizace
--auth_user	uživatelské jméno
--auth_pass	uživatelské heslo
--proxy_host	proxy host
--proxy_port	nastavení portu proxy
--proxy_username	uživatelské jméno pro proxy
--proxy_password	Heslo pro proxy

Tabulka 1 tato tabulka vznikla překladem ze zdroje [4]

- Crunch - Generátor textových řetězců, které mohou obsahovat všechny použitelné znaky. Tyto řetězce jsou tvořeny kombinací a permutací sady znaků. Lze určit velikost textového řetězce a počet znaků. Příklad generování hesla z minimálně 5 znaky a maximálně 50 znaky Generování znaků se spustí příkazem: „cunch 5 50“

Výpis výsledku generování:

aaaaa

aaaab

aaaac

aaaad

aaaae

aaaaf

aaaag

aawsnz

aawsoa

aawsob

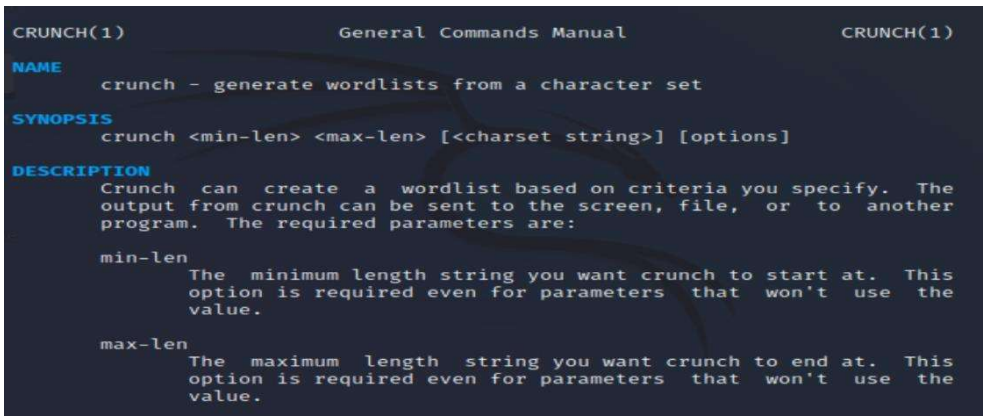
aawsoc

aawsod

aawsoe

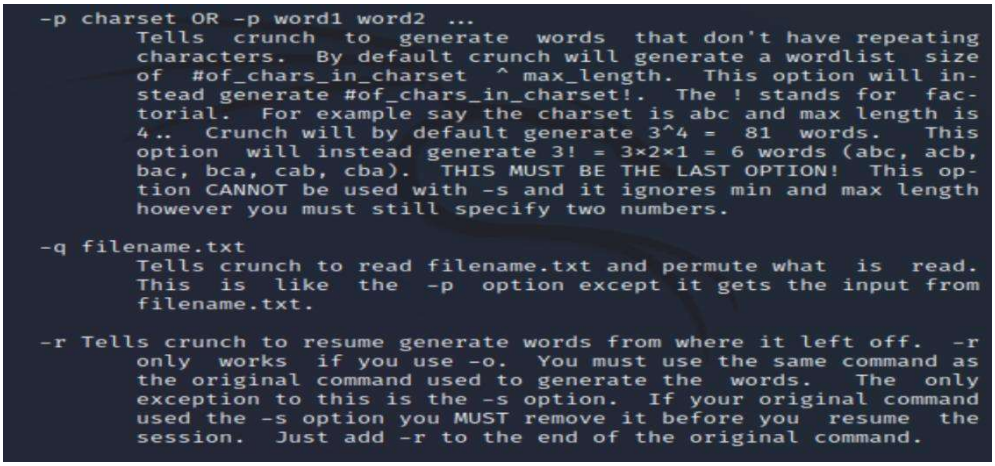
Zvýše uvedeného výpisu z generování je vidět, že tento nástroj generuje různě složitá hesla. Generují se jak hesla, která by odolala slovníkovému útoků (*aawsoe*

), tak i hesla triviální (*aaaaa*), která neposkytují téměř žádnou ochranu. Na obrázcích níže je vidět manuál pro crunch. [5]



```
CRUNCH(1)                General Commands Manual                CRUNCH(1)

NAME
       crunch - generate wordlists from a character set

SYNOPSIS
       crunch <min-len> <max-len> [<charset string>] [options]

DESCRIPTION
       Crunch  can  create  a  wordlist based on criteria you specify.  The
       output from crunch can be sent to the screen, file,  or  to  another
       program.  The required parameters are:

       min-len
              The  minimum length string you want crunch to start at.  This
              option is required even for parameters  that  won't  use  the
              value.

       max-len
              The  maximum  length  string you want crunch to end at.  This
              option is required even for parameters  that  won't  use  the
              value.
```

Obrázek 5 (zdroj: autor)



Obrázek 6 (zdroj: autor)

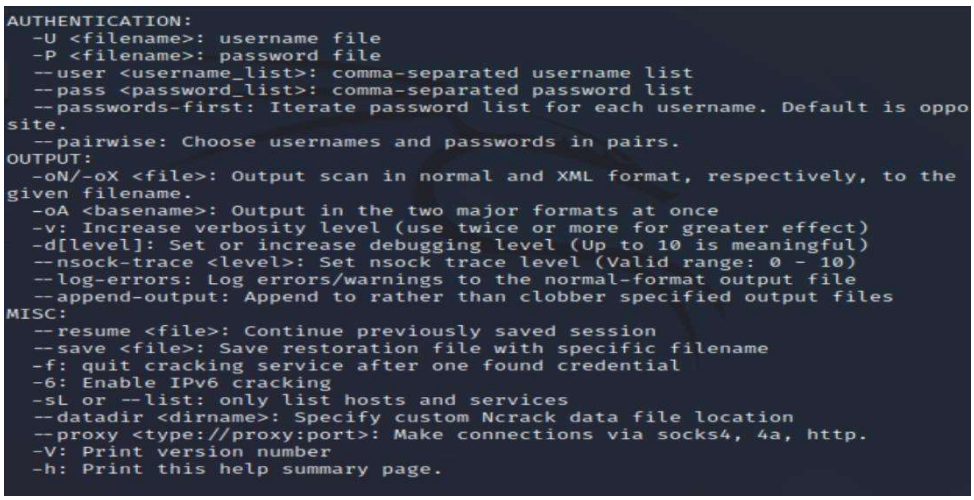
- Hashcat - Podporuje prolomení tři sta hashovacích algoritmů (například: HMAC-MD5, SHA1, HMAC-SHA1, MySQL323, MySQL4.1/MySQL5) Umožnuje několik typů útoku sloužících k prolomení hesla a to Brute-Force attack, Combinator attack, Dictionary attack ,Fingerprint attack , Hybrid attack, Mask attack, Permutation attack, Rule-based attack, Table-Lookup attack, Toggle-Case attack a PRINCE attack. Hashcat podporuje hardwarové akcelerátory na CPU a GPU. Dále umožnuje distribuované prolomení hesla o prolomení hesla se pokouší více zařízení na jednou. [12]
- medusa – Nastroj pro paralelní, modulární, přihlašovaní brute-forcer. Podporuje vzdálenou autentizaci. [20] Tabulka níže obsahuje výpis vybraných parametrů pro medusa. Tento výpis se zobrazí po zadání příkazu: „medusa – h“. [20]

parametr	popis
-n	jiné číslo portu TCP, než je defaultní číslo postu pro TCP
-d	výpis modulů
-t	počet testování přihlášení
-T	počet testování hostitelů
-f	stop skenovaní po první nalezení validního username a password
-F	Stop audit po první nalezení validního username a password
-q	zobrazení informací o použití modulu
-r	uspaní před dalším pokusem
-s	povoleni SSL
-v	zobrazeni verze
-b	potlačí baner po spuštění

Tabulka 2 tato tabulka vznikla překladem ze zdroje [20]

- ncrack - Nástroj pro prolomení vysokorychlostní autentizace sítě. Byl Navržen pro testovaní uživatelských účtů v síti. Podporuje tyto protokoly RDP, SSH,

http(s), SMB, pop3(s), VNC, FTP a Telnet. Na obrázku níže je zobrazen popis jednotlivých parametrů pro ncrack. [42]



Obrázek 7 (zdroj: autor)

- ophcrack – Nástroj na prolomení hesel v operačním systémech Windows. Alfanumerická hesla prolomí řádově během sekund. Využívá se zde kompromisu mezi časem a paměťovou náročností pomocí rainbow tables. [23]
- wordlists – Nástroj na prolamování hesel takzvaně hrubou silou. Slovníky lze pro Kali Linux stáhnout, nebo vytvořit vlastní. Slovník rovná se seznam možných hesel v čistě textové podobě.[43]

Wireless Attacks

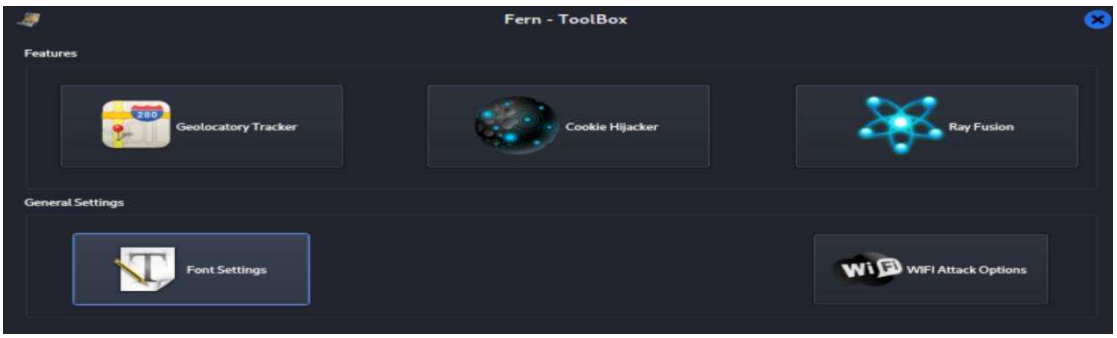
Typy útoků na bezdrátové sítě se dále dělí na útoky proti připojení Bluetooth a útoky proti standartu Wi-Fi (802.11). Mezi nástroje pro Wireless Attacks patří například níže uvedené nástroje.

- Aircrack-ng - Aircrack-ng je balíček nástrojů pro útoky proti Wi-Fi, který obsahuje tyto nástroje. Sniffer, WEP a WPA/WPA2 Cracker, analyzující nástroj a

nástroj pro zachycení hash. Využívá se k monitorování sítě a zachytávání soubory CAP, paket nebo hash. Typy útoků jsou dvojího typu. Prvním typem útoku je vytváření falešných přístupových bodů. Druhým typem útoku je deauthentication útok, který se podobá s vím principem DOS útoku. Tento druhý typ útoku má za cíl znepřístupnit připojení uživatelských zařízení přes útokem zasažený přístupový bod. [16]

- Fern wifi cracker (root) - Program umožnuje prolomovat a obnovovat klíče WEP, WPA a WPS Dále může spuštět další útoky na síť. Na rozdíl od většiny zde uvedených nástrojů se Fern wifi cracker neovládá pomocí příkazové řádky, ale ovládá se pomocí GUI. Níže na obrázku je GUI tohoto nástroje. [10]

obrázek číslo 8 (zdroj: autor)



Obrázek číslo 9 (zdroj autor)

- Kismet – Jedná se o nástroj na detekci zařízení v bezdrátové komunikaci. Kismet umí detekci spojení Wi-Fi, Bluetooth, nebo RTLSDR. [18]
- Pixiewps – Jedná se o nástroj, který používá vynucení pinu WPS offline. Tímto způsobem využívá nízkou entropii daného zařízení, nebo zařízení bez entropie. Pixiewps je psán v jazyce C. [26]

Reaver – Pro útok hrubou silou proti zabezpečenému přístupovému bodu sítě. Jakmile nalezne WPS pin může rekonfigurovat napadené bezdrátové zařízení, nebo obnovit WPA PSK. [30]

Wifite – Auditní nástroj pro WEP a WPA šifrování. Je ho výhodou jeto, že může být používán automatizovaně. [38]

Reverse Engineering

První podskupinou nástrojů je skupina OS Backdoors do které patří následující programy.

- dbd – Šifrovací nástroj, který by měl poskytovat silné šifrování pomocí AES-CBC-128 + HMAC-SHA1.[6]
- powersploit – Obsahuje skripty pro PowerShell, které lze využít pro post-exploitation při autorizovaných penetračních testech. [27]
- sbd – Použití sbd je podobné jako u výše popsaného dbd. Podporuje pouze komunikaci TCP/IP. [32]

Druhá pod skupina nástrojů pro Reverse Engineering je podskupina Tunnelin & Exfiltation do které spadají následující programy.

- dns2tcpc – Sada nástrojů pro zabalení TCP relace do DNS packetů. Výhodou je menší velkost výsledných packetu oproti IP-over-DNS. [8]
- exe2hexbat – Skript, který provádí překlad spustitelného souboru Windows PE na datový soubor a obráceně. Jedná se o skript vytvořený v jazyce Python. [9]
- iodine – Nástroj umožňující obejití zabezpečení firewall pomocí poveleného dotazování na DNS serve v dané síti. Kdy se pomocí DNS severu vytvoří tunel pro přenos dat. [14]
- miredo – Pomocí miredo lze obejít NAT a dostat se z internetu do soukromé sítě, která využívá NAT. Zapouzdřuje IPv6 packety do UDP/IPv4 datagramů. [21]
- libproxychains4 – Nástroj na přesměrování připojení přes proxy SOCKS4a/5 nebo HTTP. Jedná se o Unixový nástroj využívající knihovnu DLL (dlsym(), LD_PRELOAD). [27]
- proxytunnel - Vytváří tunel http, nebo https proxi. Využívá se pro protokoly založené na základě protokolu TCP. Původně se jednalo o rozšíření SSH protokolu. [28]

Forensics

První pod skupina je Forencis Carving Tools. Tato podskupina obsahuje tyto popsané programy.

- magicrescue – Nástroj pro obnovu smazaných dat, nebo poškozeného paměťového média (například pevného disku). Prohledává jednotlivé boky disku. Lze použít například pro tyto soubory JPG, PNG, GIM, sqlite a zip. Lze využít buď předefinované obnovovací soubory, nebo vytvořit vlastní obnovovací soubory. [19]
- scalpel – Nástroj pro obnovu dat a forenzní vyšetřování. Čte databázi definic záhlaví, zápatí a extrahuje odpovídající soubory ze sady obrazových souborů nebo souborů raw uložených v paměťovém zařízení. Není závislí na používaném

souborovém systému. Umí pracovat například s těmito souborovými systémy FAT16, FAT32, exFAT, NTFS, Ext2, Ext3, Ext4, JFS, XFS, ReiserFS a raw oddíly. [32]

- scrounge-ntfs – S tejne jako výše popsaný scalpel je i scrounge-ntfs využitelný při forenzním vyšetřování. Používá se k obnovení dat na discích využívajících souborový sytém NTFS. Čte bloky disku a zkouší obnovit původní adresářovou strukturu daného disku. [33]

Druhá podskupina je Forensic Imaging Tolls, která má pouze jednoho zástupce.

- guymager(root) - Guymager, byl navržen tak, aby podporoval různé formáty obrazových souborů. [11]

Třetí podskupina je PDF Forensics Tools s následujícími programy

- Pdfid – Nástroj pro nalezení klíčových slov v souborech formátu PDF. [24]
- pdf-parser – Analyzuje soubory formátu PDF. [25]

Čtvrtá podskupina je Sleuth Kit Suite, která má následující zástupce nástrojů.

- autopsy(root) - Program zjišťující to, co se nadaném zařízení stalo. Jedná se o GUI k nástrojům The Sleuth Kit. Pro hashovaní, analýzu a obnovu souborů. [7]

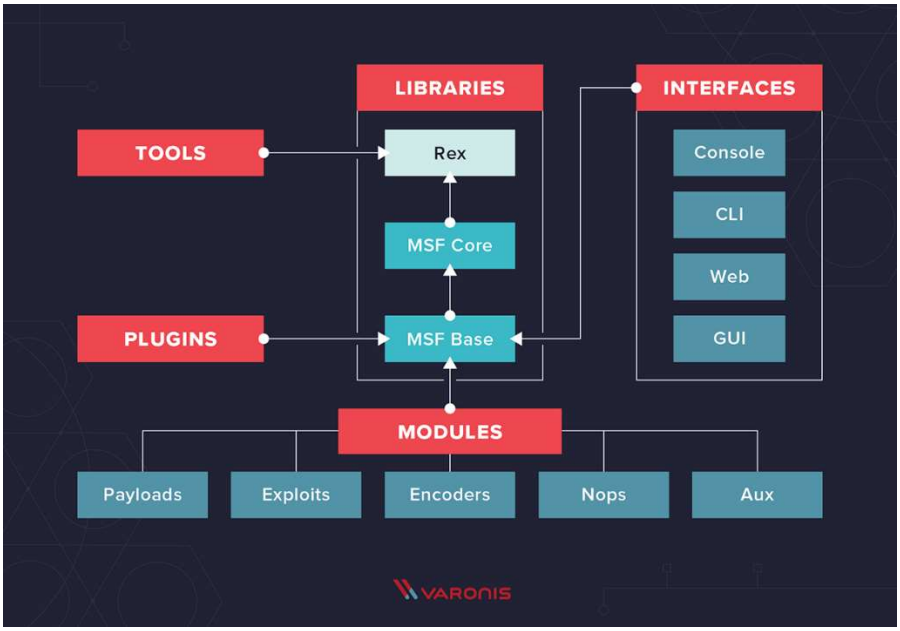
- Binwalk - Nástroj na prohledávání binární souborů. Tento nástroj byl navržen pro identifikaci kódu vložených do firmwaru. Používá knihovnu libmagic, která umožnuje využívat magic signatures vytvořené v sytému Unix, nebo vytvářet vlastní magic signatures. [2]

- bulk_extractor – Sleduje obrazy disku a extrahuje důležitá data, a to bez analýzy systému souborů, nebo struktur souborového systému. Výsledky je možné dále automatizovaně zpracovávat. [3]

4 Metasploit Framework

Metasploit Framework je nástroj pro penetrační testování, který se používá ke skenování počítačové sítě a k odhalování zranitelností v dané počítačové infrastruktuře. Metasploit Framework je součástí programů instalovaných v operačním systému Kali Linux. Tento nástroj se ovládá pomocí msfconsole. Msfconsole vychází v základu z ovládání příkazové řádky v systémech založených na Linuxu (například: tabulátor = dokončování příkazů). [22]

Na obrázku je znázorněno schéma architektury Metasploit Framework.



Obrázek číslo 10 (zdroj obrázku [51])

4.2 Historie Metasploit Framework

Historicky první verze Metasploit Framework je z roku 2003. Tuto první verzi vyvinul H. D. Moore. První verze byla vytvořena v jazyce Perl, ale v roce 2007 byl Metasploit Framework přepsán do programovacího jazyka Ruby. Metasploit Framework začal být

populární v roce 2007, kdy tento projekt získala společnost Rapid7. Zatím nejnověji verze je Metasploit Framework 6.3, kdy tato verze vyšla v roce 2023.

[59],[60]

4.2 Moduly Metasploit Framework

Tato část práce vychází textově ze zdrojů označených: [22], [37].

Metasploit Framework má 5 hlavních modulů

Auxiliary

Modul skládající se z následujících nástrojů fuzzers, skener a SQL injection. Tento modul je v Metasploit podporován od verze Metasploit 3.0. Auxiliary se využívá k provádění jednorázových útoků jako je port scanning, denial of service, a even fuzzing.

Encoders

Maskuje šifruje payloads a exploits, tak aby nebyl útok odhalen antivirovým programem, který používá metody signature-based.

Exploit

Moduly pro využívání zranitelností počítačového systému pomocí datové zátěže. Nastavení cíle útoku v Exploit se nastavuje pomocí příkazu set a jeho parametrů. Pro nastavení IP adresy cílového zařízení se používá parametr RHOST. Pro nastavení cílového portu se používá parametry RPORT. Zobrazení možných úniků DS a IPS se požívá příkaz show advanced. Pro ověření zranitelnosti lze využít příkaz check, kterým se vyzkouší, jestli je daný cíl útoku zranitelný proti aktivnímu exploit modulu. Používá se k ověření nastavení útoku. Check příkaz by neměl vést ke zhroucení napadeného systému, nebo jeho z nezpřístupnění. Příkaz Check, ale nelze použít u všech exploit modulů. Dále ne všechny zranitelnosti lze zjisti tímto příkaz bez dalšího přímého útku na napadené zařízení. Ke spuštění útoku slouží příkaz exploit, když spuštění proběhne daný

exploit se spustí, nebo nabídne možnost interakce s příkazovým řádkem útokem postiženého zařízení.

Payload

Využívá se k jako moduly pro podporu útoku, přes který se zjišťují zranitelnosti. Tyto moduly otvírají takzvaná: „zadní vrátka“, do napadeného zřízení. Poté následují další fáze útoku jako například instalací nějakého škodlivého systému. Pyload moduly jsou podporovány od verze Metasploit 3.0. -Generují instrukce bez provádění operací tento způsob se využívá k padding out buffers.

Post

Používá se ke zjištění dalších informací o napadeném zařízení. Zjištění uživatelských jmen, hash hesel. Následně je možné měnit uživatelská práva napadeného systému.

[22]

Nop Modules

Nop modulu umožnuje generování takzvaných: „NOP sled“, které můžou mít různou velikost. Pro zobrazení v daném formátu se využívá generování komunikace. [41]

(https://www.infosecmatter.com/metasploit-module-library/?mm=nop/cmd/generic)

The Meterpreter

Jedná se o pokročilo část Metasploit, kde je funkce „multi-function payload„. Kdy zátěž na cílovém zařízení může být dynamicky prodlužována. Tento modul poskytuje shell

pro pásaní funkcí a přidávaní funkcí za běhu modulu. [41]

PassiveX Payloads

Tento modul Metasploit se využívá ke zneužití procesu v napadeném zařízení. Z neužitý proces spustí Internet Explorer s URL odkazující zpět na rámec. Framework spouští jednoduchý web server, který přijme požadavek a odešle zpět webovou stránku s pokynem k načtení součásti ActiveX. Napadený systém pak stáhne, zaregistruje a spustí ActiveX. Součást tohoto modulu PasiveX se používá k provádění příkazu v shellu. PasiveX se používá pro načtení Meterpreter, nebo služby VNC. PassiveX emuluje připojení k serveru pomocí TCP a dále se zde využívá protokol http s požadavky GET a POST. [41]

Chainable Proxies

Chainable Proxies modul obsahuje podporu TCP proxy a obslužné rutiny pro servery HTTP CONNECT a SOCKSv4. Exploit je nutné nastavit proměnnou v prostředí proxy. Hodnotou této proměnné je seznam proxy, kdy jednotlivé proxy jsou odděleny čárkami. Zápis jednotlivých proxy v seznamu je v tomto formátu: „type:host:port“. U SOCKS v4. Proxy je možné mít libovolnou délku řetězce. [41]

Win32 UploadExec Payloads

Využívá zranitelnosti operačního systému Windows, který nemá výkonný příkazová řádek (powerful command line). Tato funkce umožnuje útočníkovi nahrávat a spouštět nástroje v napadeném zařízení pomocí: „payload socket connection“. Tato funkce je použitelná s jazykem Perl a podobnými skriptovacím jazyky, Dále lze tato funkce využít spolu se samo rozbalovacím nástrojem rootkit. [41]

Win32 DLL Injection Payloads

Modul obsahující fázovanou užitečnou zátěž. Pomocí této zátěže je možné vložit vlastní DDL, které se bude využívat společně z dalšími Win32 exploity. Toto užitečné zatížení nebude mít za následek zápis všech souborů na disk, ale dojde k načtení DDL přímo

do paměti. Následně se dané DDL spustí v exploited procesu. Tvorba daného DDL se provádí pomocí knihovny standardní Win32 DLL. [41]

VNC Server DLL Injection

Funkce zajišťující přístup k ploše napadeného systému pomocí win32. Do procesu napadeného systému se vkládá DDL, které se následně spustí požadovaného VNC klienta. Získané informace jsou následně z napadeného zařízení odeslány útočníkovi prostřednictvím VNC klienta. Následně se útočník pokouší získat plný přístup k ploše napadeného počítače. [41]

4.2 Metasploit Framework Knihovny

REX

Knihovna REX je základní knihovna Metasploit Frameworku. Tato knihovna v sobě obsahuje funkce pro provádění HTTP požadavků. Tyto http požadavky se vytvoří pomocí „#request_cgi“, nebo „#request_raw“. Request_cgi zajištuje kompatibilitu s CGI

a request_raw nezajištuje plnou kompatibilitu s CGI. Níže v tabulce jsou uvedeny argumenty příkazu pro inicializaci „Rex::Proto::Http::Client“, kdy je povinný pouze argument z názvem „host“. [40]

Název argumentu	Datový typ	Popis
host	String	IP adresa cílového zařízení.
port	Fixnum	Cílový port.
contex	Hash	Určuje, které zařízení je z odpovědné

		za vytvoření soketu.
ssl	Boolean	Povolení, nebo zakázaní používaní ssl.
ssl_version	String	SSL2, SSL3, or TLS1
proxies	String	Natavení proxi.
username	String	Uživatelské jméno pro automatickou autentizaci.
password	String	Heslo pro automatickou autentizaci.

Tabulka 3 tato tabulka obsahuje vybrané parametry ze zdroje [40]

Níže jsou popsány názvy klíčových slov pro nastavení určitých parametrů pro příkaz: „#request_cgi“.

Název klíče	Datový typ	Popis
pad_get_params	Boolean	Povoluje vycpávku pro GET parametrů.
pad_get_params_count	Fixnum	Počet náhodných parametrů typu GET
vars_get	Hash	Hash z GET prameturů.
encode_params	Boolean	Povolení kodovaní URI pro GET, nebo POST parmetry
pad_post_params	Boolean	Povoluje vycpávku pro POST parametrů.
pad_post_params_count	Fixnum	Počet náhodných parametrů typu POST

Tabulka 4 tato tabulka obsahuje vybrané parametry ze zdroje [40]

Request raw obsahuje oproti „request cgi“ mnohem více parametrů, které je možné nastavit. Níže v tabulce jsou popsány názvy klíčů pro nastavení určitých parametrů.

Název klíče	Datový typ	Popis
query	String	Nezpracovaný řetězec dotazu GET.
data	String	Nepracovaný řetězec dat metody POST.
uri	String	Nezpracovaná URI.
ssl	Boolean	Výběr protokolů http (False) a https (True)
agent	String	
method	String	HTTP methoda
proto	String	protokol
version	String	version
vhost	String	Host header
port	Fixnum	Port for the host header
authorization	String	The authorization header
cookie	String	The cookie header
connection	String	The connection header
headers	Hash	A hash of custom headers. Safer than raw_headers

raw_headers	String	A string of raw headers
ctype	String	Typ obsahu

Tabulka 5 tato tabulka obsahuje vybrané parametry ze zdroje [40]

4.3 Ovládání Metasploit Framework

Jak už zde bylo zmíněno výše tato sada nástrojů se ovládá v prostředí Kali Linux pomocí msfconsole. Metasploit Framework lze používat jak v systémech založených na Linuxu, tak i v systémech Windows a MacOs. U systému Windows se požívá msfgui.

Níže v tabulce jsou uvedeny základní příkazy pro práci s Metasploit Framework, které vycházejí z příkazů pro ovládání systému založených na jádře Linuxu.

příkaz	popis
cd	přepínání adresářů
ls	výpis adresáře
?	nápověda
search	vyhledávání Metasploit databázi
use	výběr konkrétního modulu se sady modulů
info	informace o aktuálním modulu
show	zobrazí jméno a možné využití aktuálního modulu
check	zjištění zranitelnosti napadeného zařízení

set	nastavení volitelných částí aktuálního modulu
unset	opak příkazu set
run	spuštění daného modulu
show payloads	zobrazení všech užitečných zařízení
show options	možnosti užitečného zatížení
edit	editovat aktuální modul
get	získá hodnotu kontextově specifické proměnné
getq	získá hodnotu globální proměné
quit	exit console
jobs	zobrazení a spravovat procesu
kill	ukončení procesu
option	zobrazí globální možnosti pro jeden, nebo více modulů
irb	přepnutí do irb sktiptu
load	načtení pluginů pro Metasploit Framework

Tabulka 6 vybraných základních příkazů pro Metasploit Framework

Níže v tabulce jsou uvedeny používané zkratky a jejich popis.

kód	popis

S	souhrn
O	možnosti
A	pokročilé použití
I	únik IDS
P	užitečné zatížení
T	cíle
AC	pomocné
C	zkouška zranitelnosti
E	využití zranitelnosti

Tabulka 7 tabulka používaných zkratek

Metasploit Framework je možné kromě klasického lokální instalace na počítači využívat i na serveru, kdy se k tomto nástroji přistupuje pomocí webového prohlížeče. Pro sever se používá nástroj „msfweb“, který se spustí. Poté je možné nástroj využívat pomocí webového prohlížeče, kdy se do URL zadána příslušná IP adresa daného serveru a port na kterém je v daném serveru spuštěn tento nástroj.

[41]

show payloads

Po zadání toto příkazu dojde ke zobrazení dostupných možností pro užitečné zatížení, kdy v tomuto výpisu je uvedena cesta k danému skriptu. Dále je zde uveden popis k čemu leze daný skript použít a datum zveřejnění daného skriptu. Poslední informace zobrazená tímto příkazem je hodnota s názvem: „Rank“, která kategorizuje jednotlivé exploity do skupin, podle potenciálních dopadů na napadené zařízení. Níže v tabulce

jsou uvedeny hodnoty pro Rank a jejich popis.

název	popis
ExcellentRanking	Nikdy nevede k pádu služby na cílové zařízení. Například SQL Injection, CMD provádění, RFI a LFI
GreatRanking	Exploit má výchozí cíl a může automaticky detekovat tento cíl, nebo používá návratovou adresu specifickou pro aplikaci po kontrole verze.
GoodRanking	Exloit má zadaný výchozí cil a exloit sám neumí cíl detekovat.
NormalRanking	Exploit závislý na konkrétní verzi typu softwaru.
AverageRanking	Exploit, který má úspěšnost použití 50 % a více procent pro běžně používané platformy.
LowRanking	Exploit, který má úspěšnost použití pod 50 % a méně procent pro běžně používané platformy.
ManualRanking	Pro nestabilní, nebo obtížné exploity, kdy má úspěšnost použití 15 % a méně procent (například DDOS útok)

Tabulka 8 tabulka popisu hodnot parametru „RANK“

Show auxiliary

Má stejný formát výpisu jako výše popsaný příkaz: „show payloads“. Dále lze pro práci s tím to nástrojem využít msfcli u této možnosti se jako první zadává název modulu. Poslední parametr je kód pro danou operaci, která se má použít.

4.4 Vybrané payload moduly

- Inline – Jedná se o payload, který obsahuje exploit a úplný kód v shellu pro danou úlohu. Inline payload je stabilnější než jiné payload moduly, ale ne vždy je velikost výsledného užitečných zatížení podporována exploity.
- IPv6 – Moduly pro využití užitečného zatížení v počítačových sítích, které využívají IPv6 adresy.
- Meterpreter – Tento payload funguje pomocí dll injection, kdy celý Meterpreter se ukládá do paměti napadaného zařízení. Umožňuje dynamické načítání a uvolňovaní jednotlivých pluginů podle aktuální potřeby. Největší výhodou tohoto modulu je to, že je obtížně detekovatelný konvenčními forenzními technikami, protože nezanechává stopy na pevném disku napadeného zařízení. [41]
- PassiveX – Využívá se k obcházení firrewall pro odchozí komunikaci. Pomocí ActiveX dojde vytvoření skryté instalaci Internet Exploer. Následná komunikace mezi útočníkem a napadeným zařízením probíhá pomocí http požadavků. [42]
- NoNX – Payload pro obcházení Bit NX (No eXecute) funkce, která zabraňuje spuštění kódu v určitých částech operační paměti. Bit NX obsahují CPU. Ve Windows je NX implementován jako Data Execution Prevention (DEP). NoNX payload je navržen právě k obcházení DEP. Pro zpřístupnění NoNX se použíje následující příkaz:
  „use payload/cmd/windows/powershell/custom/bind_nonx_tcp“.

V dalším kroku se nastaví cíl útoku v tomto příkladu je cílem útoku serve s názvem: „Server-PT DNS“, kdy jeho IP adresa je uveden v kapitole „Praktická část“. Dále byla nastavena cesta k souboru pomocí atributu: „SHELLCODE_FILE“. Nastavení parametru: „LPORT“ bylo necháno na výchozím číslu portu, a to na portu číslo 4444. Na obrázku níže jsou vidět použité příkazy pro výše uvedené nastavení.

```
msf6 payload(cmd/windows/powershell/custom/bind_nonx_tcp) > set RHOST 192.168.0.3
RHOST ⇒ 192.168.0.3
msf6 payload(cmd/windows/powershell/custom/bind_nonx_tcp) > set SHELLCODE_FILE /home/kali/Docum
ents/1.txt
SHELLCODE_FILE ⇒ /home/kali/Documents/1.txt
```

Obrázek 11 (zdroj: autor)

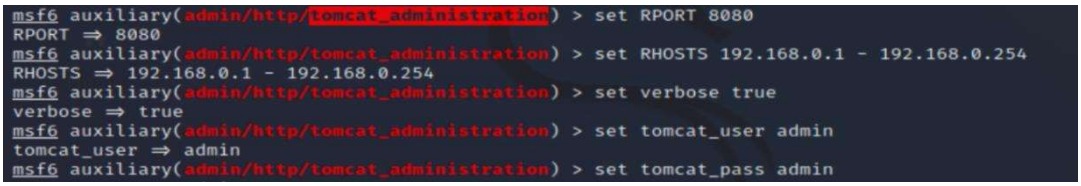
- Ord (Ordinal payloads) - Payload využívající se na útok proti systémům Windows, kdy tento payload lze využít na všech variantách operačního systému Windows od verze Windows 9x. Jedná se o malý payload. Musí mít načten ws2_32.dll v procesu, který je využíván před zneužitím. Oproti odstáním payloads modulům má nižší stabilitu.

4.5 Vybrané auxiliary moduly

Tato podkapitole textově vychází z jedno zdroje dat [39].

Axuiliary moduly se dají rozdělit do tří skupin Admin, Scanner a Server. Níže jsou popsaný vybrané auxiliary moduly.

- tomcat_administration module – Modul, který se používá k nalezení serveru Tomacat a jeho verze. Hledání severu probíhá na základě prohledávání IP adres. Příklad nastavení tohoto modulu pro cílovou síť 192.168.0.0/24. Po zadaní příkazu: „use auxiliary/admin/http/tomcat_administration“, se zpřístupní tento požadovaný modul a postupně se nastaví požadované hodnoty, jak je vidět na obrázku níže.



Obrázek 12 (zdroj obrázku: autor)

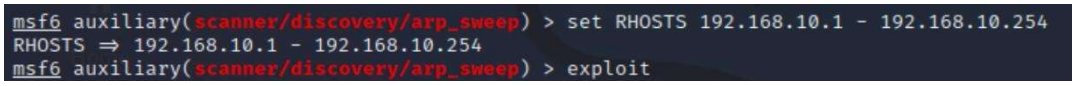
Po nastavení parametrů na obrázku následuje příkaz: „run“, který daný modlu spustí.

- mssql_enum – Modul, který přijímá sadu pověření a provádí dotazovaní na konfiguraci MSSQL. Pro použití tohoto modulu se použije výchozí uživatelské jméno a nastaví se tyto proměnné „PASSWORD“ a „RHOST“.
- mysql_enum – Modul pro připojení ke vzdálenému MySQL databázovému serveru a provede jeho základní výčet informací u zadaného databázového serveru. Pro použití tohoto modulu je nutné nastavit proměnné a to „PASSWORD“, „RHOST“ a „USERNAME“. Přes tento modul je možné provést připojení na databázový server a provádět příkazy SQL na napadeném databázovém serveru.
- poweron_vm – Modul sloužící pro přihlášení se do VMware, kdy po úspěšném přihlášení se tento modul pokouší zapnout určený virtuální počítač, nebo virtuální server.
- arp_sweep – Modul sloužící pro skenování zařízení ve stejné síti jako je útočníkův počítač. Pro použití tohoto modulu je nutné nastavit zdrojovou IP adresu a zdrojovou MAC adresu toto nastavení se provádí pomocí proměnné „SHOST“ a proměnné „SMAC“. Tento modul se používá ke skenování v počítačových sítích, které využívá IP adresy, pokud se v dané síti používají IPv6 adresy tak se využívá pro toto výše pospané skenování sítě modul s názvem: „ipv6_neighbor“, který funguje podobně jako zde popsaný „arp_sweep“ modul. Po zadaní příkazu: „use auxiliary/scanner/discovery/arp_sweep“, se zpřístupní tento požadovaný modul a postupně se nastaví požadované hodnoty, jak je vidět na obrázku níže.

První příklad je nastavení tohoto modulu pro sever: „Server-PT FTP“ viz tabulka v kapitole 7 Praktická část.

Obrázek 13 (zdroj obrázku: autor)

Druhý příklad je nastavení tohoto modulu pro útok na sít „VLAN10“ viz tabulka v kapitole 7 Praktická část



Obrázek 14 (zdroj obrázku: autor)

Kromě výše na obrazcích uvedených nastaveních. Lze nastavit IP adresy pomocí souboru s příponou .txt, kde je uveden seznam IP adres, kdy za „RHOST“ se dá cesta k danému souboru, který se má použít (set RHOSTS file:/tmp/ip_list.txt).

- ftp/Anonymous – Modul, který hledá FTP server, který umožnuje anonymní přístup a zjišťuje, jestli jaká jsou na nalezeném FTP serveru oprávnění (čtení, zápis) k uloženým souborům. Vyhledávání modul se provádí na základě zadaného rozsahu IP adres.

msf > use auxiliary/scanner/ftp/Anonymous

msf auxiliary(anonymous) > set RHOSTS 192.168.0.1-254

RHOSTS => 192.168.1.0-254

msf auxiliary(anonymous) > set THREADS 55

THREADS => 55

msf auxiliary(anonymous) > run

- ftp_login – Modul, který se pokouší přihlásit k FTP severu pomocí seznamu slov, nebo uživatelský pověření. Příklad nastavení pro útok proti „Server-PT FTP“.

msf > use auxiliary/scanner/ftp/ftp_login

msf auxiliary(ftp_login) > set RHOSTS 192.168.0.5

RHOSTS => 192.168.0.5

msf auxiliary(ftp_login) > set THREADS 205

THREADS => 205

msf auxiliary(ftp_login) > set USERNAME admin2022

USERNAME => admin2022

msf auxiliary(ftp_login) > set PASSWORD admin2022

PASSWORD => admin2022

msf auxiliary(ftp_login) > set VERBOSE false

VERBOSE => false

msf auxiliary(ftp_login) > run

- ftp_version – Tento modul na základě zadaného rozsahu IP adres vyhledá všechny běžící FTP servery a vrátí jejich verzi. Pro použití tohoto modulu je nutné nastavit následující proměnné „RHOSTS“ a „THREADS“. Příklad nastavení pro útok proti „Server-PT FTP“.

msf > use auxiliary/scanner/ftp/ftp_version

msf auxiliary(ftp_version) > set RHOSTS 192.168.0.5

RHOSTS => 192.168.0.5

msf auxiliary(ftp_version) > set THREADS 55

THREADS => 55

msf auxiliary(ftp_version) > run

- Cert – Modu, který pomocí skenování sítě zjišťuje platnost certifikátů serverů v dané síti. Pro použití modulu je nutné nastavit tyto proměnné „RHOSTS“ a „THREADS“. Příklad nastavení pro síť 192.168.0.0, kde se nacházejí servery.

msf > use auxiliary/scanner/http/cert

msf auxiliary(cert) > set RHOSTS 192.168.0.0/24

RHOSTS => 192.168.0.0/24

msf auxiliary(cert) > set THREADS 254

THREADS => 254

msf auxiliary(cert) > run

- dir_listing – Modul, který zjistí, jestli je na zadaných severech povolen výpis jejich adresářů. Tento výpis může poskytnout přístup k informacím uložených na daném severu. Příklad nastavení pro síť 192.168.0.0, kde se nacházejí servery.

msf > use auxiliary/scanner/http/dir_listing

msf auxiliary(dir_listing) > set RHOSTS 192.168.0.1-254

RHOSTS => 192.168.0.1-254

msf auxiliary(dir_listing) > set THREADS 55

THREADS => 55

msf auxiliary(dir_listing) > run

- dir_scanner – Tento modul se využívá k nalezení zajímavých adresářů na jednom webovém serveru, nebo na více webových serverech současně. Vyhledávání je prováděno na základě nastavení cíle útoku a slovníku, který je součástí Metasploitu.

msf > use auxiliary/scanner/http/dir_scanner

msf auxiliary(dir_scanner) > set RHOSTS 192.168.0.1-254

RHOSTS => 192.168.0.1-254

msf auxiliary(dir_scanner) > run

- imap_version – Modul pro zachytávání „banner“ určených pro IMAP servery. Pro použití tohoto module se nastavují tyto proměnné „RHOSTS“ a „THREADS“.

msf > use auxiliary/scanner/imap/imap_version

msf auxiliary(imap_version) > set RHOSTS 192.168.0.1-254

RHOSTS => 192.168.0.1-254

msf auxiliary(imap_version) > set THREADS 20

THREADS => 20

msf auxiliary(imap_version) > run

- nbname – Modul prohledává seznam zařízení a určuje jejich jména pomocí NetBIOS. Pro požití tohoto modulu je nutné nastavit tyto proměnné „RHOSTS“ and „THREADS“.

msf > use auxiliary/scanner/netbios/nbname

msf auxiliary(nbname) > set RHOSTS 192.168.0.1-254

RHOSTS => 192.168.0.1-254

msf auxiliary(nbname) > set THREADS 11

THREADS => 11

msf auxiliary(nbname) > run

- nbname_probe – Modul, který k určení názvů NetBIOS vzdálených zařízení používá sekvenční testy NetBIOS. Pro požití tohoto modulu je nutné nastavit tyto proměnné „RHOSTS“ a „THREADS“. Příklad nastavení pro síť VLAN 30, která je uvedena v kapitole Praktická část.

msf > use auxiliary/scanner/netbios/nbname_probe

msf auxiliary(nbname_probe) > set RHOSTS 192.168.30.1 – 192.168.30.254

RHOSTS => RHOSTS 192.168.30.1 – 192.168.30.254

msf auxiliary(nbname_probe) > set THREADS 11

THREADS => 11

msf auxiliary(nbname_probe) > run

- pop3_version – Modul pro vyhledávání emailových serverů, které využívají POP3 protokol. Pro požití tohoto modulu je nutné nastavit tyto proměnné „RHOSTS“ and „THREADS“.

msf > use auxiliary/scanner/pop3/pop3_version

msf auxiliary(pop3_version) > set RHOSTS 192.168.0.1-254

RHOSTS => 192.168.0.1-254

msf auxiliary(pop3_version) > set THREADS 20

THREADS => 20

msf auxiliary(pop3_version) > run

- ssh_login – Modul pro otestování sady přihlašovacích údajů. Tyto údaj jsou uveden v souboru, kdy uživatelská jména a hesla jsou mezi sebou odděleny mezerou. Dále je možné provádět pokusy o přihlášení takzvaně: „hrubou silou“. Pro využití tohoto module je nutné do proměnné „USERPASS_FILE“ nastavit cestu k souboru s přihlašovacími údaji.

msf > use auxiliary/scanner/ssh/ssh_login

- ssh_login_pubkey – Modul, který se využívá k pokusu přihlášení pomocí SSH klíčů. Pro požití tohoto modul je nutné získat přístup k soukromému SSH klíči.
- telnet_login – Modul, který se na základě zadaného rozsahu IP adres a souboru uživatelských jmen a hesel pokouší o přihlášení k serverům které využívají Telnet.

msf > use auxiliary/scanner/telnet/telnet_login

msf auxiliary(telnet_login) > set BLANK_PASSWORDS false

BLANK_PASSWORDS => false

msf auxiliary(telnet_login) > set PASS_FILE passwords.txt

PASS_FILE => passwords.txt

msf auxiliary(telnet_login) > set RHOSTS 192.168.1.0/24

RHOSTS => 192.168.1.0/24

msf auxiliary(telnet_login) > set THREADS 254

THREADS => 254

msf auxiliary(telnet_login) > set USER_FILE users.txt

USER_FILE => users.txt

msf auxiliary(telnet_login) > set VERBOSE false

VERBOSE => false

msf auxiliary(telnet_login) > run

- telnet_version – Modul, který zjistí jednotlivé verze protokolu Telnet, které se používají na severech v zadám rozsahu IP adres. Pro využití tohoto modulu je nutné nastavit tyto proměnné „RHOSTS“ a „THREADS“.

msf > use auxiliary/scanner/telnet/telnet_version

msf auxiliary(telnet_version) > set RHOSTS 192.168.0.1/24

RHOSTS => 192.168.0.1/24

msf auxiliary(telnet_version) > set THREADS 254

THREADS => 254

msf auxiliary(telnet_version) > run

- vnc_login – Modul skenující zadanou IP adresu, nebo rozsah IP adres a na základě zadaného seznamu slov se pokouší přihlásit k zařízení pomocí VNC. Pro využití tohoto modulu je nutné nastavit tyto proměnné „RHOSTS“, „THREADS“ a „BRUTEFORCE_SPEED“.

msf > use auxiliary/scanner/vnc/vnc_login

msf auxiliary(vnc_login) > set RHOSTS 192.168.0.1-254

RHOSTS => 192.168.0.1-254

msf auxiliary(vnc_login) > set THREADS 11

THREADS => 11

msf auxiliary(vnc_login) > set BRUTEFORCE_SPEED 1

BRUTEFORCE_SPEED => 1

msf auxiliary(vnc_login) > run

- vnc_none_auth – Modul, který na základě zadaného rozsahu IP adres hledá VNC bez nastavené autentizace. Pro využití tohoto modulu je nutné nastavit tyto proměnné „RHOSTS“

a „THREADS“.

msf auxiliary(vnc_none_auth) > use auxiliary/scanner/vnc/vnc_none_auth

msf auxiliary(vnc_none_auth) > set RHOSTS 192.168.0.1/24

RHOSTS => 192.168.0.1/24

msf auxiliary(vnc_none_auth) > set THREADS 50

THREADS => 50

msf auxiliary(vnc_none_auth) > run

- John the Ripper – Modul sloužící k rychlému odhalování slabých hesel. Pokud se bude jednat o prolamování složitých hesel tak by měl být tento nástroj používán zvlášť mimo Metasploit.

4.6 Metasploit Framework 5.0 a Metasploit Framework 6.3

Tato kapitola se věnuje porovnání Metasploit Framework 5.0 a Metasploit Framework 6.3. Verze 5.0 byla vydána v roce 2019 a verze 6.3 byl vydána v roce 2023

Nové funkce Metasploit Framework 5.0

Metasploit Framework 5.0 rozšiřuje možnost použití exploit modulů, kdy je od této verze Metasploit Frameworku možné použít exploit modul proti více cílovým zařízením, kdy se do proměnné „RHOSTS“ zadá konkrétní IP adresa sítě, nebo rozsah IP adres. V předchozích verzích bylo možné exploit modul použít pouze proti jednomu cílovému zařízení. Přenastavení cílového zařízení je možné použít proměnou „RHOSTS“, nebo „RHOST“. V rámci této verze Metasploit Frameworku byla přidána možnost psaní modulů pomocí programovacích jazyků Go a Python, kdy v předchozí verzích Metasploit Frameworku bylo možné používat pouze programovací jazyk Ruby.

Výhody této verze Metasploit Frameworku:

- Možnost pouštět databázi PostgreSQL jako RESTful službu – Tato funkcionalita umožňuje spolupráci více Metasploit konzolí a externími nástroji.
- Hromadné operace jsou přepracovány do podoby databázové služby

- JSON-RPC API – Tato funkcionalita umožňuje integrovaní Metasploit společně s dalšími nástroji a programovacími jazyky.
- Web service framework – Tato funkcionalita se využívá pro odhalení databáze i automatizačních API Web service framework podporuje pokročilé ověřování a souběžné operace.
- Došlo k přidání evasion modulů, knihoven a možnosti generování vlastních evasive payloads modulů bez dalších externích nástrojů.
- Metashell funkce – Funkce umožňující spouštět relace na pozadí a komunikovat s relacemi prostředí.

[61]

Nové funkce Metasploit Framework 6.3

Novou funkcionalitou u Metasploit Framework 6.3 je zefektivnění útoků Kerberos a Active Directory, kdy je možné provést autentizaci pro více služeb a tím to způsobem řetězit útok s jinými moduly Metasploit Framework 6.3.

Výhody této verze Metasploit Frameworku:

- Nativní Kerberos autentizace pomocí protokolů HTTP, LDAP, MSSQL, SMB, nebo WinRM
- Možnost vytvoření požadavku na Ticket-Granting Tickets (TGT) a Ticket-Granting Server (TGS) z Key Distribution Center (KDC)
- Pokud se získat heslo, hash NT, nebo šifrovací klíč je možné požadovat tickets PKINIT s certifikáty vydanými AD CS.
- Karberos využívá pro ladění ticketů následující moduly.
    - auxiliary/admin/kerberos/inspect_ticket
    - auxiliary/admin/kerberos/keytab:

Tento modul se využívá pro dešifrování souborů Kerberos v programu Wireshark. Dešifrování se provádí pomocí generování souborů Keytab.

- Plně automatizovaná eskalace oprávněních pomocí Certifried

V nové moduly Metasploit Framework 6.3, které se využívají při útocích proti Active Directory a Domain Service. Níže v práci jsou stručně popsány tyto nové moduly

Moduly používané proti službám Active Directory a Domain Service:

- auxiliary/admin/dcerpc/samr_computer – Tento modul se používá pro vyhledávání, vytváření, nebo mazání počítačových účtů z domény spravované pomocí nástroje Active Directory.
- auxiliary/admin/ldap/rbcd – Tento modul se používá pro konfiguraci objektů v rámci Active Directory, kdy tato nastavení umožnuje útočníkovi vydávat se za jakýkoliv jiný účet v rámci dané domény spravované pomocí Active Directory.
- auxiliary/gather/ldap_query – Tento modul umožnuje tvorbu jednotlivých dotazů, nebo tvorbu skupiny dotazů na LDAP server.

Moduly používané proti službě Active Directory Certificate Services:

- auxiliary/admin/dcerpc/icpr_cert – Modul pro podporu vydávání certifikátu prostřednictvím Active Directory Certificate Services.

- auxiliary/gather/ldap_esc_vulnerable_cert_finder – Modul podporující vyhledávání zranitelností v certifikátech ESC1, ESC 2 a ESC 3 na napadeném serveru Active Directory Certificate Services s využitím LDAP.
- auxiliary/admin/kerberos/get_ticket – Modul požadující tiket TGT/TGS od KDC pomocí certifikátů prostřednictvím PKINIT.

[62]

6 Shrnutí výsledků

Metasploit framework nabízí řadu modulů pro penetrační testování, kdy některé vybrané moduly byly zmíněny a popsány výše v práci v kapitolách podle toho, jestli se jedná o modul ze skupiny Payloads moduly, nebo ze skupiny Auxiliary moduly. Základní ovládání a nastavení parametrů pro jednotlivé výše uvedené moduly bylo poměrně snadné a u každého vybraného modulu se pozadí příkazu: „show „options“ zobrazil přehledná nápověda. Tato nápověda přehledně zobrazoval názvy atributů společné se stručným popisem daného atributu a informací, jestli je daný atribut pro daný modul povinný, nebo volitelný. U Metasploit framework není pro základní použití nutná nějaká speciální znalost v oblasti kybernetický útoků stačí pouze vědět to co chce daný člověk udělat a na internetu má poměrně pěkné bezplatné návody pro Metasploit framework. V práci před hlavní kapitolu o Metasploit framework byla kapitola o Kali Linuxu a o jeho dalších nástrojích spadající do oblasti penetračního testování. Platí pro všechny tyto nástroje poměrně přehledná nápověda v příkazovém řádku daného konkrétního nástroje. Vzhledem k výše popsaný skutečnostem je jasné, že dnes může nějaký útok

na počítačovou sít provést na prosto kdokoliv kdo si dá práci s hledáním toho, jak daný útok provést a jaké je nutné nadstavit parametry v daném modulu Metasploit frameworku, nebo jiném nástroji v Kali Linuxu. Zde v práci není uvedeno maskování útoku a zařízení přes, které se daný útok na počítačovou síť provádí. Vzhledem dostupnosti nástrojů pro penetrační testování je v dnešní době je složitější maskovat zdrojové zařízení útočníka než provést nějaký samotný útok na počítačovou síť.

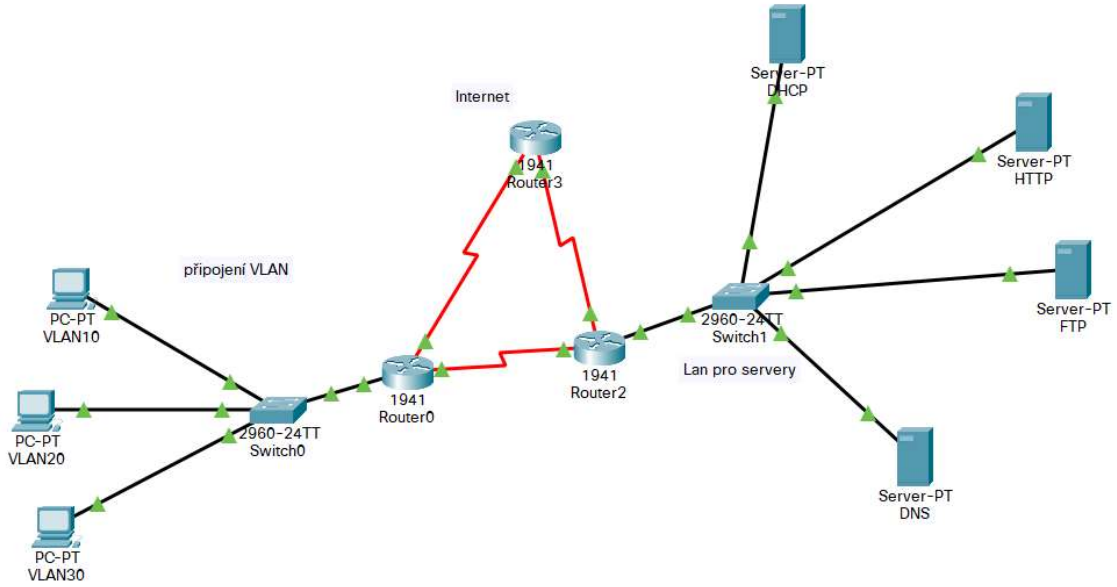
7 Závěry a doporučen

Platí zde obecná doporučení o nastavení zabezpečení sítě. Na Switche deaktivovat nepoužívané porty nastavit port security s limitem povolených MAC adres. Port security by mělo být nataveno buď restrict, nebo shutdown. Režim protect sice splní účel blokování zařízení s neznámou MAC adresou, ale na rozdíl od výše uvedených módů ne vytváří se záznam o narušení bezpečnosti na nadaném portu. Režim shutdown. Mám jednu nevýhodu, a to nutnost resetovat daný interface na switche. Nejvhodnější se mi jeví řežím restrict, ale záleží na požadavcích na danou síťovou infrastrukturu. Dalším obecným pravidlem by mělo být využívání ACL na routerech. V ideálním případě extended ACL, který umožnuje filtrovat povolené služby (http, fttp) podle zdrojové IP adresy, pokud v daném místě sítě stačí filtrovat provoz jen na základě zdrojové IP adresy tak by se měl použít standard ACL. Dále je nutné rozdělit sít do jednotlivých VLAN, podle skupin uživatelů vdané počítačoví síti. Minimálně rozdělit na VLAN pro zaměstnance a VLAN pro administrátory dané počítačové sítě. Poslední doporučením je pravidelná aktualizace všech systémů (operační systémy PC) v dané počítačové síti. Ideálně nasadit nějaký monitoring sítě, který pomohl při odhalování kybernetického útoku na danou síťovou infrastrukturu. Nejdůležitějším bodem je dělaní pravidelných záloh dat a případně i záloh aktuálních konfigurací síťových prvků. Měl by být nastaven systém pro monitorování systémů, tak aby bylo možné detekovat anomální spouštění souborů a procesů v daném operačním systému. Dále na základě monitorování sítě je nutné provádět analýzu síťového provozu, aby bylo možné detekovat anomální provoz v dané počítačové síti, nebo v dílčí části počítačové sítě. Při v časné detekci anomálního provozu v dané části sítě je možné tuto část sítě v čas odpojit od zbytku síťové infrastruktury a tím zamezit případnému šíření škodlivého sw do dalších částí počítačové sítě. Dále při analýze síťového parovozu je vhodné sledovat porty na kterých má běžet konkrétní služba. Jestli se používají obvykle používaná čísla portů pro danou webovou službu.

Pokud je povoleno používání externích paměťových médií. Je nutné monitorovat abnormální přístupy k souborům na daném vyměnitelné médium. V případě využívání sdílených složek a souborů, nebo využívání cloudových úložišť je nutné monitorovat i přístupy do těchto sdílených složek a souborů stejně jako v případě využívání externích paměťových medií. Dále by se měla monitorovat tvorba nových uživatelských účtů, aby bylo možné identifikovat nově vytvořené podezřelé uživatelské účty, nebo účty vytvořené během kybernetického útoku na počítačovou síť. [49]

8 Praktická část

V této kapitole diplomové práce se nachází jednoduché schéma zapojení sítě a tabulka, ve které jsou uvedeny IP adresy koncových zařízeních (PC a Servery). Údaje uvedené v této kapitole jsou použity pro příklady nastavení v kapitolách 4.5.4 Vybrané payload moduly a 4.5.5 Vybrané auxiliary moduly a Servery).



Obrázek 15 (zdroj autor)

Název	IP adresa	Subnet Mask	Default Gateway
PC-PT VLAN10	DHCP (192.168.10.3 192.168.10.254)	255.255.255.0	192.168.10.1
PC-PT VLAN20	DHCP (192.168.20.2 192.168.20.254)	255.255.255.0	192.168.20.1
PC-PT VLAN30	DHCP (192.168.30.2 192.168.30.254)	255.255.255.0	192.168.30.1
Server-PT DHCP	192.168.1.2	255.255.255.0	192.168.0.1
Server-PT DNS	192.168.1.3	255.255.255.0	192.168.0.1
Server-PT FTP	192.168.1.5	255.255.255.0	192.168.0.1
Server-PT HTTP	192.168.1.4	255.255.255.0	192.168.0.1

Tabulka 9 seznam zařízení vytvořeno pro tento text

8.1 Skenování sítě

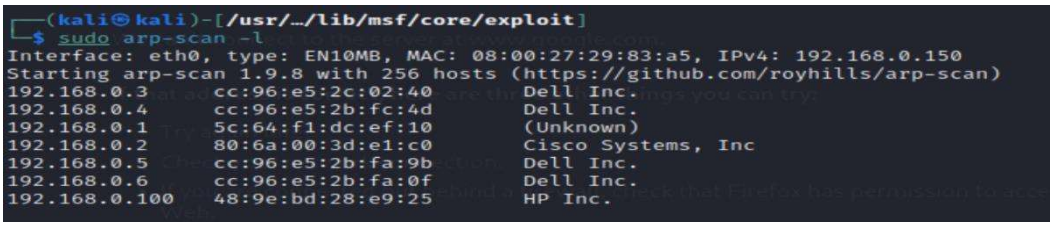
V první podkapitola praktické části práce bude věnování skenování a zjišťováním informací o daní podsíti pomocí arp_sweep. Tato část bude níže rozdělena do dvou příkladů.

8.1.1 Skenování LAN sítě

Pro skenování sítě byl využit příkaz: „arp-scan -l“

Použití bez VLAN

Níže na obrázku je vidět skenování sítě bez používaní VLAN.



Obrázek 16 příkaz arp-scan (zdroj obrázku: autor)

Na obrázku výše je vidět u jednotlivých připojených zařízeních je vidět názve výrobce daného zařízení. Dále je z výpisu vidět IP adresa a MAC adresa daného zařízení.

IP adresu 192.168.0.2 má nastavenou switche a IP adresu 192.168.0.1 má interface routeru (Default Gateway). Zařízení Dell Inc. jsou legální stanice dané sítě a zařízení HP Inc. Je zařízení útočníka.

Použití při rozdělení sítě do VLAN

Rozdělení sítě do tří VLAN sítí, a to do VLAN10, VLAN20 a VLAN30.

VLAN10:

Jedná se o VLAN pro správu, kdy síťová IP adresa je 192.168.10.0/24.

Níže v tabulce je výstup pro použití příkazu: „sudo arp-scan -l“.

IP adresa	MAC adresa	Výrobce zařízení
192.168.10.3	cc:96:e5:2c:02:40	Dell Inc.
192.168.10.2	80:6a:00:3d:e1:c0	Cisco Systems, Inc
192.168.10.1	5c:64:f1:dc:ef:10	(Unknown)
192.168.10.100	48:9e:bd:28:e9:25	HP Inc

Tabulka 10 arp-scan pro VLAN10 (zdroj autor)

Z výše v tabulce uvedených údajů je vidět, že na IP adrese 192.168.10.2 je umístěn switche a IP adresu 192.168.10.1 má interface routeru (Default Gateway). Na adrese 192.168.10.3 je legální stanice dané VLAN. Dále je vidět, že zařízení útočníka je na IP adrese 192.168.10.100.

VLAN20:

Jedná se o VLAN pro správu, kdy síťová IP adresa je 192.168.20.0/24.

Níže v tabulce je výstup pro použití příkazu: „sudo arp-scan -l“.

IP adresa	MAC adresa	Výrobce zařízení
192.168.20.4	cc:96:e5:2b:fc:4d	Dell Inc.
192.168.20.5	cc:96:e5:2b:fa:9b	Dell Inc.
192.168.20.1	5c:64:f1:dc:ef:10	(Unknown)
192.168.20.100	48:9e:bd:28:e9:25	HP Inc

Tabulka 11 arp-scan pro VLAN20 (zdroj: autor)

Na IP adrese 192.168.20.4 a IP adrese 192.168.20.5, jsou legální stanice dané VLAN. Dále na IP adrese 192.168.20.1 je interface routeru (Default Gateway). Dále je vidět, že zařízení útočníka je na IP adrese 192.168.20.100.

VLAN30:

Jedná se o VLAN pro správu, kdy síťová IP adresa je 192.168.30.0/24.

Níže v tabulce je výstup pro použití příkazu: „sudo arp-scan -l“.

IP adresa	MAC adresa	Výrobce zařízení
192.168.30.6	cc:96:e5:2b:fa:0f	Dell Inc.
192.168.30.1	5c:64:f1:dc:ef:10	(Unknown)
192.168.30.100	48:9e:bd:28:e9:25	HP Inc

Tabulka 12 arp-scan pro VLAN30 (zdroj: autor)

Na IP adrese 192.168.30.6 je legální stanice dané VLAN. Dále na IP adrese 192.168.30.1 je interface routeru (Default Gateway). Dále je vidět, že zařízení útočníka je na IP adrese 192.168.20.100.

ft8.2.3 ftp/Anonymous“

Vstupní údaje

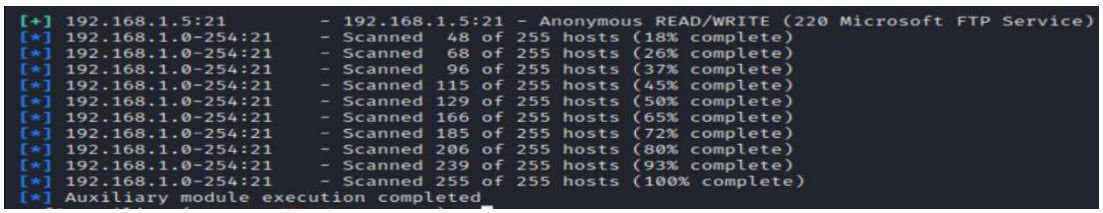
Parametr RHOST nastaven na hodnotu: „192.168.1.0/24“

To znamená, že se bude prohledávat celý adresní rozsah a to celkem 254 IP adres.

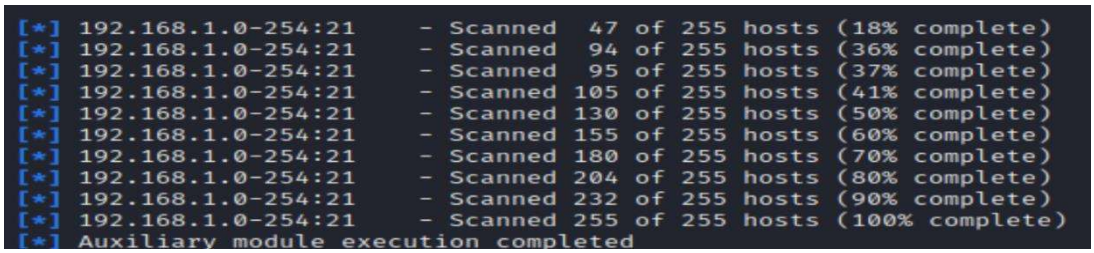
Parametr THREADS nastaven na hodnotu 51

Výstupní údaje

Na obrázcích níže jsou vidět výsledky, a to prvním případě pro nalezení serveru a v druhém případě pro nenalezení serveru.



Obrázek 17 výstup ftp/Anonymous modulu (zdroj obrázku: autor)



Obrázek 18 výstup ftp/Anonymous modulu (zdroj obrázku: autor)

Jak je vidět z obrázků výše v případě nalezení serveru se zobrazí IP adresa daného serveru oprávnění u serveru v ukázkovém případě je na serveru oprávnění pro čtení i zápis.

Prevence útoku

V první řade je nutné zvážit, jestli je vůbec potřeba anonymní přístup k souborům na FTP serveru. Pokud je anonymní přístup potřeba měl by být povolen pouze pro čtení, a

nikoliv jako v tom to konkrétním případě pročtení i zápis. Pokud není anonymní přístup vyžadován měl by být na daném serveru zakázán. Příkladem důvodu, kdy povolit anonymní přístup je možnost, aby uživatelé daných webových stránek si mohli stáhnou nějakou šablonu konkrétního dokumentu, nebo nějaký dokument určený pro veřejnost.

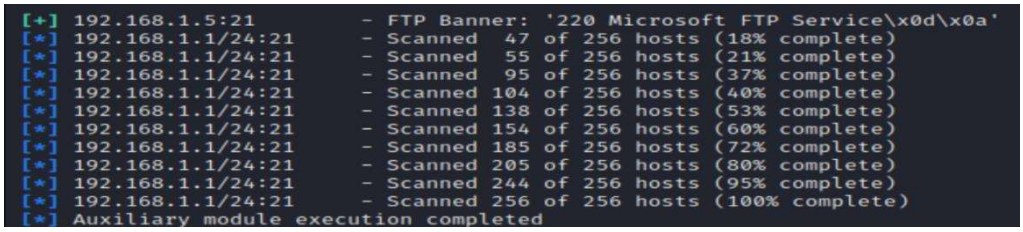
8.2.3 ftp/ftp_version

Vstupní údaje

Parametr RHOST nastaven na hodnotu: „192.168.1.0/24“.

Výstupní údaje

Na obrázku níže je vidět, že byl nalezen server na IP adrese 192.168.1.5 a portu 21 server s operačním systémem od Microsoftu.



Obrázek 19 výstup ftp/ftp_version modulu (zdroj obrázku: autor)

8.2.4 ftp/ftp_login

Vstupní údaje

Parametr RHOST nastaven na stejně jakoo u předešlých výše popsaných příkladů na konkrétního hosta to na IP adrese 192.168.1.5, vzhledem k tomu, že v předešlé podkapitole výše bylo zjištěno, že na IP adrese se nachází server, který umožnuje Anonymní přístup, proto už se v této části udává už konkrétní IP adresa daného FTP serveru. Pro demonstrativní účely v této práci bylo zvoleno nastavení následujících parametrů. Kdy parametr username byl nastaven na hodnotu „Administrator“ a

parametr password nastaven na hodnotu „KalliLinux2024“. Níže na obrázku je vidět výše popsané nastavení.

Obrázek 20 nastavení ftp/ftp_login (zdroj obrázku: autor)

Při reálném útoku by se místo parametru username a password použily tři níže popsané varianty nastavení. V první variantě by se nastavovaly opět dva parametry a to USER_FILE, kde se v tomto parametru se nastaví cesta k souboru s potenciálními uživatelskými jmény. Následně se nastaví parametr PASS_FILE, kde se nastaví cesta k souboru s potenciálními hesly U těchto parametrů se každá hodnota nachází na novém řádku v daném souboru.

Příklad pro USER_FILE:

Admin

Administrator

Admin2024

Příklad pro PASS_FILE:

Administrators

Admin2024

KalliLinux2024

Ve druhé variantě se využívá parametr USERPASS_FILE, kdy je formát uživatelské jméno mezera heslo, kdy další varianta přihlašovacích údajů je na novém řádku v daném souboru.

Příklad pro USERPASS_FILE:

Admin DiplomkaUHK2024

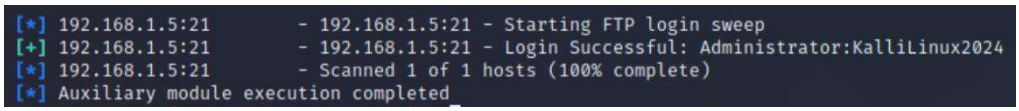
Administrator Admninistrator2024Diplomka

Administrator KalliLinux2024

Ve třetí variantě se využívá parametr USER_AS_PASS, kde se jako heslo využívá uživatelské jméno.

Výstupní údaje

V případě úspěšného nalezení uživatelských údajů se ve výstupní výpisu objeví IP adresa konkrétního FTP serveru společně s číslem portu pře, který daný server komunikuje. Dále se ve výpisu se objeví uživatelské jméno a heslo, kdy tyto dva údaje jsou vzájemně odděleny dvojtečkou. U příklad použitém v této práci to bude IP adres 192.168.1.5 číslo portu 21 a přihlašovací údaje jsou Administrator:KalliLinux2024 Níže na obrázku je vidět daný výše popsaný výpis.



Obrázek 21 výstup příkazu ftp/ftp_login modulu (zdroj obrázku: autor)

Prevence útoku

Jediné účinné doporučení je používat dostatečně dlouhá hesla, která v sobě kombinují písmena, číslice a speciální znaky. Obecně se uvádí minimálně 12 znaků pro heslo běžného uživatele a minimálně 15 znaků pro administrátora.

8.2.5 FTP login

V předchozí kapitoly byly zjištěny přihlašovací údaje pro FTP server, které se v této kapitole je využijí pro přihlášení k danému serveru. Přehlášení se provede zadáním příkazu „ftp 192.168.1.5, dy se následně zadá uživatelské jméno a heslo. Po úspešeném přihlášení se zobrazí v příkazovém řádku „ftp>“, následně lze využívat příkazy linuxu jako například: „ls“ pro vypsání daného adresáře. Pro vytvoření adresáře je možné použít příkaz „mkdir“. Příkaz „rename“, pro přejmenování souborů. Na obrazcích níže je znázorněn výše popsaný postup.

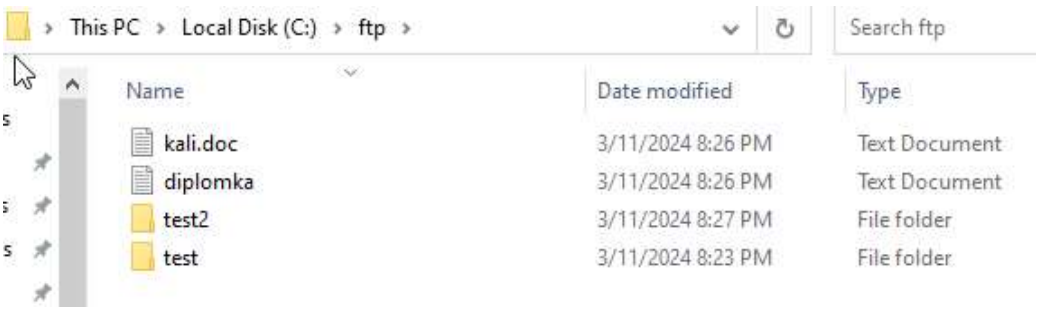
```
ftp> ls
229 Entering Extended Passive Mode (|||56727|)
150 Opening ASCII mode data connection.
02-15-24  08:37PM                  182 kali.rtf
226 Transfer complete.
ftp> mkdir test
257 "test" directory created.
ftp> ls
229 Entering Extended Passive Mode (|||56728|)
150 Opening ASCII mode data connection.
02-15-24  08:37PM                  182 kali.rtf
03-11-24  08:22PM       <DIR>          test
226 Transfer complete.
```

Obrázek 22 vytvoření složky na napadeném FTP serveru (zdroj obrázku: autor)

```
ftp> ls
229 Entering Extended Passive Mode (|||56732|)
150 Opening ASCII mode data connection.
03-11-24  08:26PM                    0 kali.doc.txt
03-11-24  08:26PM                    6 kali.txt
03-11-24  08:23PM       <DIR>          test
03-11-24  08:27PM       <DIR>          test2
226 Transfer complete.
ftp> rename kali.txt diplomka.txt
350 Requested file action pending further information.
250 RNTO command successful.
```

Obrázek 23 změna názvu souboru na napadeném serveru (zdroj obrázku: autor)

Na obrázku níže je vidět daný adresář na FTP serveru po provedení výše uvedených příkazů.



Obrázek 24 změny v adresáři pro provedení útoku (zdroj obrázku: autor)

Prevence útoku

Nastavení přístupu ke služby FTP na daném serveru pomocí ACL.

Příklad nastavení ACL:

ip access-list extended ftpPermit

permit tcp 192.168.10.0 0.0.0.255 host 192.168.1.5 eq ftp

permit tcp 192.168.20.0 0.0.0.255 host 192.168.1.5 eq ftp

deny tcp any host 192.168.1.5 eq ftp

permit tcp any any

8.3 Útok serverům

V této podkapitole se budou využívat ty to dva moduly dir_scanner a dir_listing.

8.3.1 dir_listing

Použití modulu s názvem dir_listing.

Vstupní údaje

Parametr RHOST nastaven na hodnotu: „192.168.1.0/24“

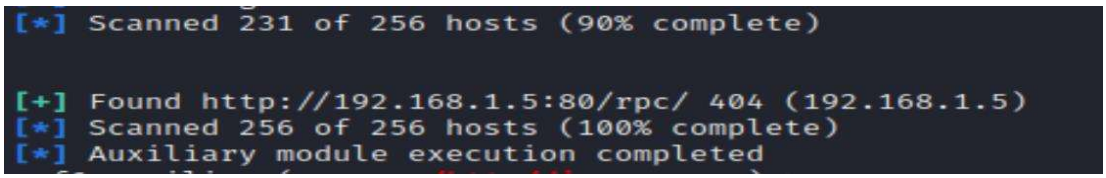
To znamená, že se bude prohledávat celý adresní rozsah a to celkem 254 IP adres.

Parametr THREADS nastaven na hodnotu 51

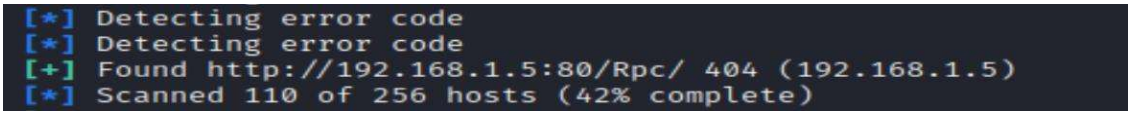
Parametr PATH nastaven na: „/“.

Výstupní data

Na obrázcích níže jsou uvedeny nalezené servery, kdy oba servery hlásí 404.



Obrázek 25 výstup z dir_listing modulu (zdroj obrázku: autor)

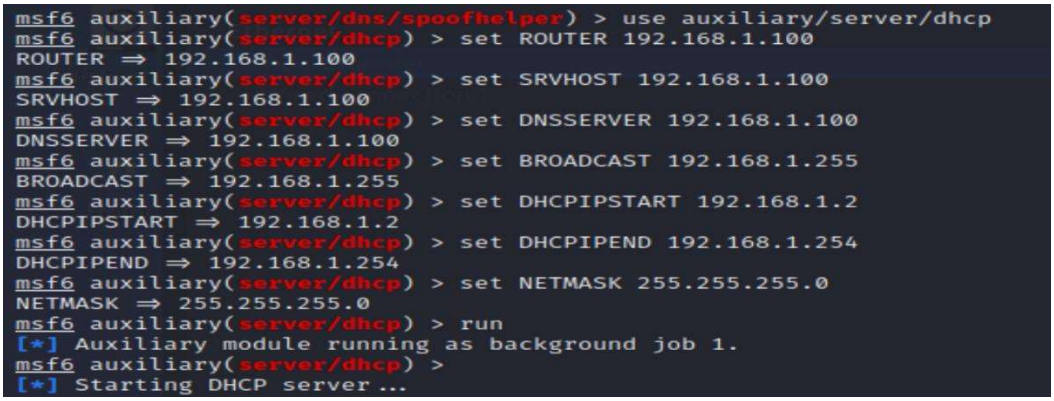


Obrázek 26 výstup z dir_listing modulu (zdroj obrázku: autor)

8.4. DHCP server

Vstupní údaje

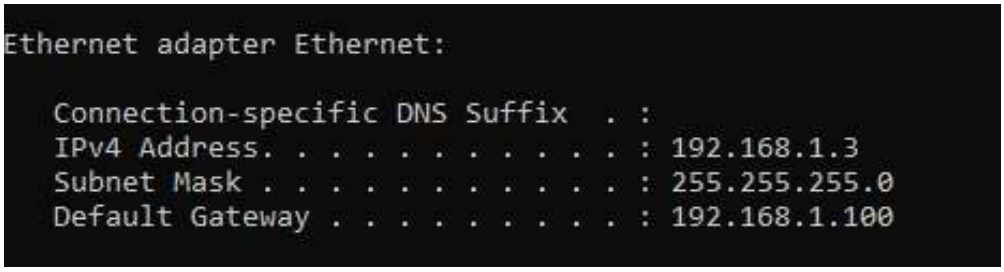
Pro nastavení falešného DHCP serveru se vyžívá: „auxiliary/server/dhcp“, kde se nstaví postupně 7 parametrů. První parametr je: „ROUTER“, kde se nastaví falešná výchozí brána na IP adresu útočníka. Druhý parametr je: „DNSSERVER“, kde se nastaví falešná adresa DNS serveru na IP adresu útočníka. Třetí parametr je „BROADCAST“ skutečná broadcast pro danou síť. Čtvrtým a pátý parametry jsou „DHCPIPSTART“ a „DHCPIPEND“ pro nastavení rozsahu IP adres použitelných pro hosty dané sítě. Šestý parametr je „NETMASK“ pro nastavení masky dané sítě. Na obrázku níže je vidět nastavení falešného DHCP serveru.



Obrázek 27 nastavení z použití server/dchp modulu (zdroj obrázku: autor)

Výstupní data

Počítač by měl mít nastavenou výchozí bránu na IP adrese 192.168.1.2 a DNS server na IP adrese 192.168.1.3, kdy místo těchto hodnot dostane falešné IP adresy z falešného DHCP serveru. Níže na obrázku je vidět nastavení údajů, které počítač získal z falešného DHCP serveru.



Obrázek 28 výstup z použití server/dchp modulu (zdroj obrázku: autor)

Využití falešného DHCP serveru

Pomocí falešného DHCP je možné podvrhnou adresu DNS server a Default Gateway. Pokud dojde k podvržení Default Gateway, tak provoz, který by měl jít mimo danou síť, tak místo toho, aby se to posílalo na Router, tak se to nejdříve pošle útočníkovi o něho až

na Router. Tímto způsobem může útočník sledovat komunikaci, která jde z dané sítě mimo danou síť. V případě, že dojde k podvržení adresy DNS severu, tak útočník může přesměrovat dotaz na vlastní servery a vlastní aplikace, které se jeví jako legitimní aplikace. Kdy přes stejnou URL, kterou používá legitimní aplikace se zobrazí falešná aplikace.

Prevence útoku

V rámci ACL povolit službu DHCP pouze pro konkrétní cílové IP adresy na kterých jsou umístěny skutečné DHCP servery pro danou síť. Pro všechny ostatní cílové IP adresy zakázat pro službu DHCP.

Příjlad nastavení ACL:

ip access-list extended DHCP

permit icmp any host 192.168.1.3

permit tcp any host 192.168.1.2 eq bootps

permit tcp any host 192.168.1.2 eq bootpc

deny tcp any any eq bootps

deny tcp any any eq bootpc

permit tcp any an

8.5 Nbname

Vstupní údaje

Pa Parametr RHOST nastaven na hodnotu: „192.168.1.2 - 254

To znamená, že se bude prohledávat adresní prosto od IP adresy 192.168.1.2 do IP adresy 192.168.1.254. Parametr THREADS nastaven na hodnotu 100.

msf > use auxiliary/scanner/netbios/nbname

msf auxiliary(nbname) > set RHOSTS 192.168.1.2 – 192.168.30.254

RHOSTS => RHOSTS 192.168.30.2 – 192.168.30.254

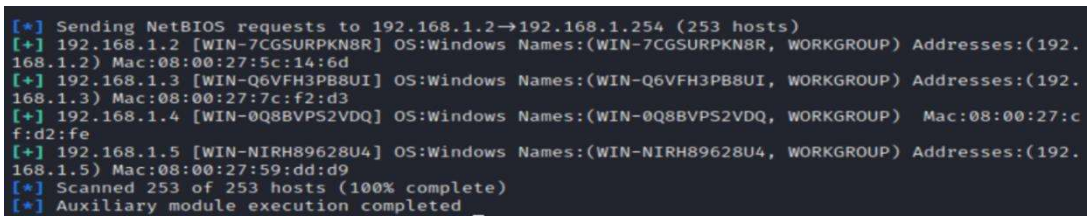
msf auxiliary(nbname) > set THREADS 100

THREADS => 100

msf auxiliary(nbname) > run

Výstupní údaje

Na obrázku níže je vidět, že na zadaném rozsahu IP adres se nachází celkem čtyři zařízení.



Obrázek 29 výstup z nbname modulu (zdroj obrázku: autor)

Tabulka nalezených hostů, která vychází z obrázku výše.

Název zařízení	Typ operačního systému	IP adresa	MAC adresa
WIN-7CGSURPKN8R	Windows	192.168.1.2	08:00:27:5c:14:6d
WIN-Q6VFH3PB8UI	Windows	192.168.1.3	08:00:27:7c:f2:d3
WIN-0Q8BVPS2VDQ	Windows	192.168.1.4	08:00:27:cf:d2:fe
WIN-NIRH89628U4	Windows	192.168.1.5	08:00:27:59:dd:d9

Tabulka 13 nalezených hostů pomocí Nbname (zdroj: autor)

Níže je příklad změny MAC adresy a názvu zařízení. Útočník se tímto způsobem může maskovat jako legitimní zařízení sítě.

sudo hostnamectl set-hostname WIN-7CGSURPKN8R

ifconfig eth0 down

macchanger -m 08:00:27:5c:14:6d eth0

ifconfig eth0 up

macchanger -s eth0

8.6 Závěr praktické části práce

V praktické části byly nastíněny možnosti praktického využít Metasploit Frameworku v prostředí KaliLinuxu. V prakticky zde v této práci byl ukázán jen zlomek funkcionalit Metasploit Frameworku. Největší část praktické části práce byla věnována útokům proti FTP serverům.

9 Závěr

V práci byla vysvětlena problematika penetračního testování. Práce byla rozdělena do čtyř hlavních částí, kdy první tři části jsou teoretické a čtvrtá část je praktická. První část je věnována obecnému úvodu do problematiky penetračního testování. Jsou zde popsány metodiky postupů využívaných při penetračním testované v četně stručného schématu postupu při využití konkrétní dané metodiky. Dále jsou popsány typy penetračních testů a skupiny hackerů podle jejich zaměření a cíle. Druhá část práce se věnuje operačnímu systému KaliLinux, který se využívá pro penetrační testování. Byl zde uveden úvod do KaliLinuxu v čteně stručné historie jeho vývoje. Dále zde byly popsány nástroje pro penetrační testování, které jsou v prostředí tohoto operačního systému na instalovány. U každého uvedeného nástroje byla popsána jeho funkce a využití pro penetrační testování. Třetí část je věnována Metasploit Frameworku v této části byla uvedena stručná historie vývoje Metasploit Frameworku. Dále byly v této čísti popsané vybrané funkcionality využívané v Metasploit Frameworku. Kdy každá funkcionality byla popsána k čemu se využívá a co je pro její využití potřeba nastavit jako vstupní hodnoty. Byla zde zmíněno porovná mezi Metasploit Framework 5.0

a Metasploit Framework 6.3. Co, která verze přinesla nového a výhody dané verze Metasploit Frameworku. Poslední praktické části byla použita nástroj KaliLinuxu pro skenování dané LAN sítě, nebo VLAN sítě. Velká pod část této čtvrté části je věnována nástrojům využívaných proti FTP serveru. Balo zde ukázáno vytvoření falešného DHCP serveru. Dále je zde ukázány funkce dir_listing a nbname. U každé části jsou popsány vstupní parametry a jejich nastavení. Následně je zde uveden výstup po použití dané funkce a popsání jejího výstupních hodnot. V praktické části této práce byly zmíněny jen velmi malá část z možných funkcionalit Metasploit Frameworku. Metasploit Framework je velmi robustní nástroj z pohledu možného použití v oblasti penetračního testování.

10 Seznam použité literatury

10.1 Knižní zdroje

[1] Kim, Peter, a Jan Pokorný. Hacking: praktický průvodce penetračním testováním. Vydání první, Zoner Press, 2015.

10.2 Webové zdroje

[2] „Binwalk | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/binwalk/. Viděno 13. únor 2023.

[3] „Bulk-Extractor | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/bulk-extractor/. Viděno 13. únor 2023.

[4] „Cewl | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/cewl/. Viděno 13. únor 2023.

[5] „Crunch | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/crunch/. Viděno 13. únor 2023.

[6] „Dbd | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/dbd/. Viděno 13. únor 2023.

[7] „Digital Forensics Investigation Using Autopsy In Kali Linux". Ehacking, 17. březen 2020,

https://www.ehacking.net/2020/03/digital-forensics-investigation-using-autopsy-in-kali-linux.html.

[8] „Dns2tcp | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/dns2tcp/. Viděno 13. únor 2023.

[9] „Exe2hexbat | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/exe2hexbat/. Viděno 13. únor 2023.

[10] „Fern-Wifi-Cracker | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/fern-wifi-cracker/. Viděno 13. únor 2023.

[11] „Guymager | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/guymager/. Viděno 13. únor 2023.

[12] „Hashcat | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/hashcat/. Viděno 13. únor 2023.

[13] „Home". Metasploit Documentation Penetration Testing Software, Pen Testing Security, https://rapid7.github.io/metasploit-framework/. Viděno 13. únor 2023.

[14] „Iodine | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/iodine/. Viděno 13. únor 2023.

[15] „Kali linux". blog.hackerlab.cz, 18. červen 2016, https://blog.hackerlab.cz/kali-linux/.

[16] „Kali Linux-Aircrack-Ng". GeeksforGeeks, 26. červenec 2020, https://www.geeksforgeeks.org/kali-linux-aircrack-ng/.

[17] „Kali Linux Wordlist - What You Need to Know | FOSS Linux". Https://Www.Fosslinux.Com, https://www.fosslinux.com/48115/kali-linux-wordlist-what-you-need-to-know.htm. Viděno 13. únor 2023.

[18] „Kismet | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/kismet/. Viděno 13. únor 2023.

[19] „Magicrescue | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/magicrescue/. Viděno 13. únor 2023.

[20] „Medusa | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/medusa/. Viděno 13. únor 2023.

[21] „Miredo | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/miredo/. Viděno 13. únor 2023.

[22] Niazi, Rumaisa. „A Beginner's Guide to Metasploit in Kali Linux (With Practical Examples)". MUO, 11. únor 2022, https://www.makeuseof.com/beginners-guide-metasploit-kali-linux/.

[23] „Ophcrack | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/ophcrack/. Viděno 13. únor 2023.

[24] „Pdfid | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/pdfid/. Viděno 13. únor 2023.

[25] „Pdf-Parser | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/pdf-parser/. Viděno 13. únor 2023.

[26] „Pixiewps | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/pixiewps/. Viděno 13. únor 2023.

[27] „Powersploit | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/powersploit/. Viděno 13. únor 2023.

[28] „Proxychains-Ng | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/proxychains-ng/. Viděno 13. únor 2023.

[29] „Proxytunnel | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/proxytunnel/. Viděno 13. únor 2023.

[30] „Reaver | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/reaver/. Viděno 13. únor 2023.

[31] „Releases History". Kali Linux, https://www.kali.org/releases/. Viděno 13. únor 2023.

[32] „Sbd | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/sbd/. Viděno 13. únor 2023.

[33] „Scalpel | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/scalpel/. Viděno 13. únor 2023.

[34] „Scrounge-Ntfs | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/scrounge-ntfs/. Viděno 13. únor 2023.

[35] „Sqlitebrowser | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/sqlitebrowser/. Viděno 13. únor 2023.

[36] sqlmap: automatic SQL injection and database takeover tool. https://sqlmap.org/. Viděno 13. únor 2023.

[37] What Is Metasploit? The Beginner's Guide. https://www.varonis.com/blog/what-is-metasploit. Viděno 13. únor 2023.

[38] „Wifite | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/wifite/. Viděno 13. únor 2023.

[39] „Auxiliary Module Reference - Metasploit Unleashed". OffSec, https://www.offsec.com/metasploit-unleashed/auxiliary-module-reference/. Viděno 25. duben 2023.

[40] How to Send an HTTP Request Using Rex Proto Http Client". Metasploit Documentation Penetration Testing Software, Pen Testing Security, Viděno 18. červenec 2023.

[41] *Metasploit Framework User Guide* , Version 3.1. 2006, http://cs.uccs.edu/~cs591/metasploit/users_guide3_1.pdf, Viděno 25. července 2023

[42] Ncrack | Kali Linux Tools". *Kali Linux*, https://www.kali.org/tools/ncrack/. Viděno 25. červenec 2023.

[43] Wordlists | Kali Linux Tools". Kali Linux, https://www.kali.org/tools/wordlists/. Viděno 25. červenec 2023.

[44] Co znamená White Hat? - IT Slovník. https://it-slovnik.cz/pojem/white-hat. Viděno 26. červenec 2023.

[45] Co znamená Black Hat? - IT Slovník. https://it-slovnik.cz/pojem/black-hat. Viděno 26. červenec 2023.

[46] „Grey Hat". Wikipedia, 1. červenec 2023. Wikipedia, https://en.wikipedia.org/w/index.php?title=Grey_hat&oldid=116287082

[47] Blue Hat Hacker Definition - Glossary | NordVPN. 9. listopad 2022, https://nordvpn.com/cybersecurity/glossary/blue-hat-hacker/.

[48] techslang. „What Is a Red Hat Hacker? — Definition by Techslang". Techslang — Tech Explained in Simple Terms, 12. srpen 2021, https://www.techslang.com/definition/what-is-a-red-hat-hacker/.

[49] MITRE ATT&CK®. https://attack.mitre.org/. Viděno 7. srpen 2023.

[50] Mobile Application Penetration Testing. https://subscription.packtpub.com/book/security/9781785883378/1/ch01lvl1sec12/the-mobile-application-penetration-testing-methodology. Viděno 12. prosinec 2023.

[51] ECSA, Strahinja Stankovic. „Web Application Penetration Testing: Steps, Methods, & Tools". PurpleSec, 10. listopad 2019, https://purplesec.us/web-application-penetration-testing/

[52] How To Prepare For An API Pentest - Curl | White Oak Security. 10. listopad 2020, https://www.whiteoaksecurity.com/blog/how-to-prepare-for-an-api-pentest-curl/

[53] IoT pentest – Connected objects penetration test. https://www.vaadata.com/en/iot-connected-objects-pentest/. Viděno 12. prosinec 2023.

[54] Testy sociálního inženýrství. https://www.systemonline.cz/it-security/socialni-inzenyrstvi-1.htm. Viděno 12. prosinec 2023.

[55] Herzog, Pete. OSSTMM 3 – The Open Source Security Testing Methodology Manua. ISECOM, 210n. l.

[56] What is the Open Web Application Security Project (OWASP) | Radware. https://www.radware.com/cyberpedia/application-security/what-is-owasp/. Viděno 12. prosinec 2023.

[57] „Penetration Testing Execution Standard (PTES)". GeeksforGeeks, 25. říjen 2019, https://www.geeksforgeeks.org/penetration-testing-execution-standard-ptes/.

[58] „Information System Security Assessment Framework (ISSAF)". FutureLearn, https://www.futurelearn.com/info/blog. Viděno 12. prosinec 2023.

[59] „What Is Metasploit: Overview, Framework, and How Is It Used | Simplilearn". Simplilearn.Com, 25. listopad 2021, https://www.simplilearn.com/what-is-metaspoilt-article. Viděno 12. prosinec 2023.

[60] „Metasploit Framework 6.3 Released | Rapid7 Blog". Rapid7, 30. leden 2023, https://www.rapid7.com/blog/post/2023/01/30/metasploit-framework-6-3-released/. Viděno 12. prosinec 2023.

[61] Sahay, Priyanshu. Metasploit Framework 5.0 Has Released With New Features. Hackers Online Club, 2019, https://hackersonlineclub.com/metasploit-framework-5-has-released/. Viděno 12. prosinec 2023.

[62] „Metasploit Framework 5.0 Released | Rapid7 Blog". Rapid7, 10. leden 2019, https://www.rapid7.com/blog/post/2019/01/10/metasploit-framework-5-0-released/. Viděno 12. prosinec 2023.

[63] „Metasploit Unleashed | Scanner FTP Auxiliary Modules". OffSec, https://www.offsec.com/metasploit-unleashed/scanner-ftp-auxiliary-modules/. Viděno 21. duben 2024.

[64] Administrator. „Attacking the FTP Service". Penetration Testing Lab, 1. březen 2012, https://pentestlab.blog/2012/03/01/attacking-the-ftp-service/.

[65] „Metasploit Unleashed | Scanner HTTP Auxiliary Modules". OffSec, https://www.offsec.com/metasploit-unleashed/scanner-http-auxiliary-modules/. Viděno 21. duben 2024.

[66] Chandel, Raj. „DHCP Penetration Testing". Hacking Articles, 29. prosinec 2017, https://www.hackingarticles.in/dhcp-penetration-testing/.

[66] „Metasploit Unleashed | Scanner NetBIOS Auxiliary Modules". OffSec, https://www.offsec.com/metasploit-unleashed/scanner-netbios-auxiliary-modules/. Viděno 21. duben 2024.

[67] „How to Change the Mac Address in Kali Linux Using Macchanger?" GeeksforGeeks, 28. květen 2020, https://www.geeksforgeeks.org/how-to-change-the-mac-address-in-kali-linux-using-macchanger/.

[68] Exploring the Colorful World of Pentesting: Red, Blue, Purple Teams & More | Infosec. https://www.infosecinstitute.com/resources/penetration-testing/what-are-black-box-grey-box-and-white-box-penetration-testing/. Viděno 22. duben 2024.

10.3 Zdroje obrázků

[69] Cousra; Penetration Tetsting incident; IBM; week 2; Incident Respons Demo Part1

[70] What Is Metasploit? The Beginner's Guide. https://www.varonis.com/blog/what-is-metasploit. Viděno 13. únor 2023.

[71] Ahmed , Mohiuddin, et al. *ECU-IoFT: A Dataset for Analysing Cyber-Attacks on Internetof Flying Things*. 2022. Viděno 22. dubna 2024

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor: **Bc. Vojtěch Jabůrek**

Studium: I2100062

Studijní program: N1802 Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Název diplomové práce: **Využití Metasploit Framework pro penetrační testování**

Název diplomové práce AJ: Using the Metasploit Framework for Penetration Testing

Cíl, metody, literatura, předpoklady:

Cílem práce je podrobně popsat možnosti využití Metasploit Framework v rámci Kali Linux pro penetrační testování a vybrané metody a postupy realizovat. V teoretické části práce autor provede analýzu možnosti využití Metasploit Framework v rámci Kali Linux pro penetrační testování. V praktické části pak autor zpracuje sadu nejméně pěti podrobných ukázkových řešených úloh.

Penetrační testy a exploitace

Matúš Selecký;

Hacking : praktický průvodce penetračním testováním

Peter Kim; Jan Pokorný

Brno : Zoner Press ; 2015;

online zdroje - Cousera

Zadávající pracoviště: Katedra informačních technologií,
Fakulta informatiky a managementu

Vedoucí práce: doc. Mgr. Josef Horálek, Ph.D.

Oponent: Ing. Lubomír Almer, Ph.D.

Datum zadání závěrečné práce: 15.10.2021