Dokumentace k projektu Vizualizace architektury sítě

Obsah

[Cíl projektu 1](#_Toc151892631)

[Skenování sítě 1](#_Toc151892632)

[Topologie sítě 3](#_Toc151892633)

[Popis naší aplikace - Vizualizer sítě 3](#_Toc151892634)

[Seznam literatury 6](#_Toc151892635)

[Seznam obrázků 6](#_Toc151892636)

# Cíl projektu

Naším tématem semestrálního projektu je vizualizace architektury sítě. Mezi hlavní cíle tohoto projektu patří skenování celé sítě a následně síťovou topologii zobrazit.

## Skenování sítě

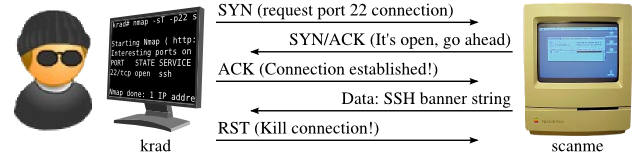
Cíl našeho skenování je získání co nejvíce informací, které by útočníkovi mohli sloužit pro vektory útoku. Je důležité znát otevřené porty a dostupné služby, pro ověření, zda se nedají zneužít nebo disponují verzí systému, jenž obsahuje velké zranitelnosti. Na skenování využíváme aplikaci NMAP, která zajišťuje získání dostupných informací jako jsou například IP adresy, MAC adresy, používané služby a otevřené porty apod [1].

NMAP provádí skenování pomocí různých technik a přepínačů. My v aplikaci využíváme příkaz ve tvaru ***nmap -T4 -A -O -oX <výstup souboru> <adresa sítě/prefix>***, kde přepínače označují tyto parametry:

1. -T4 označuje rychlost skenu, zvolili jsme vyváženou možnost mezi poměrem rychlost/stability.
2. -A označuje agresivní styl skenu, který se snaží získat co nejvíce informací. Na rozdíl od jiných je velmi lehce detekovatelný, ale pro naše účely, kdy se snažíme zjistit co nejvíce zranitelností je dobrou volbou.
3. -O slouží pro detekci systému a jeho bližší identifikaci.
4. -oX tvoří výstup skenu do souboru ve formátu XML.

NMAP využívá různé techniky skenování

* TCP Connect Scan
  + NMAP navazuje TCP spojení s cílovým zařízením na všech definovaných portech. Naváže spojení pomocí TCP protokolu a pomocí Three-Way HandShake postupu ověřuje dostupnost všech portů [1] Obr. 1.



Obr. 1 - Dokončené TCP spojení

* SYN/Stealth Scan
  + Podobný průběh jako u TCP skenu, ale po obdržení zprávy od zařízení s příznakem SYN/ACK spojení ukončí [1] Obr.2.

Obsah obrázku text, snímek obrazovky, Elektronické zařízení, multimédia

Popis byl vytvořen automaticky

Obr.2 TCP spojení bez dokončení (Stealth režim)

* UDP Scan
  + NMAP posílá UDP packety na všechny porty, kdy některé porty dostávají UDP packet s nějakým payloadem a jiné nesou prázdný payload. NMAP zpracuje odpovědi na tyto packety a po následné analýze vyhodnotí jaké služby běží na jakém portu [1].
* OS Detection
  + Nmap odesílá sérii TCP a UDP paketů na cílového hosta a pečlivě zkoumá prakticky každý bit v odpovědích. Po provedení desítek testů, jako je vzorkování TCP ISN, podpora a pořadí TCP opcí, vzorkování IP ID a kontrola velikosti počátečního okna, Nmap porovnává výsledky s databází otisků operačních systémů nmap-os-db, katerá obsahuje více než 2 600 známých otisků operačních systémů, a vypíše podrobnosti o OS, pokud dojde k shodě [1].
* Service Version Detection
  + Určuje verze služeb, které běží na otevřených portech [1].
* Ping Scan
  + Kontroluje dostupnost zařízení pomocí ping (ICMP) nebo jiných protokolů [1].
* Script Scanning
  + Nabízí využití, kde je možnost vybrat jiná kritéria pro skenování například použití „script vuln“ zjistíme, zda vybrané porty disponují známou zranitelností [1].
* Agressive Scan
  + Poskytuje agresivní typ skenu, kdy je kombinováno více technik dohromady [1].

## Topologie sítě

Náš projekt provádí načrtnutí toplogie na základě dané metodiky – host spustí naši aplikaci, kde spustí NMAP sken, ten si zkontroluje default-gateway a ta tvoří střed sítě. Velmi jsme se této problematice věnovali, a došli jsme k závěru, že takovýto sken nelze vytvořit bez „invazivního přístupu“. Tento přístup by spočíval v úspěšném napadení uzlu, kde by potom následně pomocí různých protokolů například ARP nebo CDP bylo zjištěno, jak přesně je topologie tvořena.

## Popis naší aplikace - Vizualizer sítě

Naše aplikace umožňuje uživateli bez žádných znalostí problematiky spustit skenování podsítě ve které se nachází. Uživatel tedy nepotřebuje nic víc než nainstalovaný NMAP, python a spuštění skriptu na potřebné knihovny k naší aplikaci.

Po spuštění aplikace se zobrazí okno Obr. 3.

Obsah obrázku text, snímek obrazovky

Popis byl vytvořen automaticky

Obr. 3 Spuštění aplikace (základní okno)

Obsah obrázku text, snímek obrazovky, displej, software

Popis byl vytvořen automatickyUživatel vybere nmap sken na základě operačního systému, na kterém pracuje, pokud používá windows tak spustí nmap sken. Poté se provedený sken uloží do složky, kde je uložena aplikace. NMAP sken ukládá ve formátu XML, ale udělali jsme vlastní konvertor na formát JSON, jenž se považuje za vyšší standard strojově čitelného formátu (Obr. 4). Po stisknutí tlačítka „Konvert XML souboru“ si vybereme soubor který chceme změnit ten se bude jmenovat (napevno nastaven pro zjednodušení práce) „nejnovejsiSken.xml“ a ten se překonvertuje na JSON, kde souboru nastavíme jméno (Obr. 5). Poté tlačítkem „Vyberte JSON soubor“ vybereme JSON, který chceme vizualizovat (Obr. 6). Následně se nám zobrazí vizualizované okno.

Obr. 4 - Otevření provedeného skenu pro následné překonvertování

Obsah obrázku text, snímek obrazovky, displej, software

Popis byl vytvořen automaticky

Obr. 5 - Vybraný xml soubor bude překonvertován na zadané jméno ve formátu JSON

Obsah obrázku text, snímek obrazovky, software, displej

Popis byl vytvořen automaticky

Obr. 6 - Výběr JSON souboru pro vizualizaci

Po otevření JSON skenu se zobrazí okno s vizualizací. Tato vizualizace je dělaná pomocí knihoven networkX. Následně se zobrazí hostova default-gateway, která tvoří topologický vrchol a další připojené zařízení ve stejné podsíti. Po kliknutí na každé zařízení se nám zobrazí dostupné zjištěné informace o daném zařízením. Na naší skenované síti je rozkliknuté zařízení s IP adresou 10.0.1.17, podle zobrazených zjištěných informací a po následné analýze na internetu uživatel zjistí, že se jedná o access point zařízení Obr. 7.

Obsah obrázku text, snímek obrazovky, diagram, řada/pruh

Popis byl vytvořen automaticky

Obr. 7 - Vizualizace topologie sítě

## Seznam literatury

1. Nmap. *Nmap* [online]. [cit. 2023-11-26]. Dostupné z: <https://nmap.org/>

## Seznam obrázků

1. Nmap. *Nmap* [online]. [cit. 2023-11-26]. Dostupné z: <https://nmap.org/book/scan-methods-connect-scan.html>
2. Nmap. *Nmap* [online]. [cit. 2023-11-26]. Dostupné z: https://nmap.org/book/synscan.html