Skener siete pre PowerShell

Autor práce: Jan Bachorec
Vedoucí práce: Zdeněk Martinásek

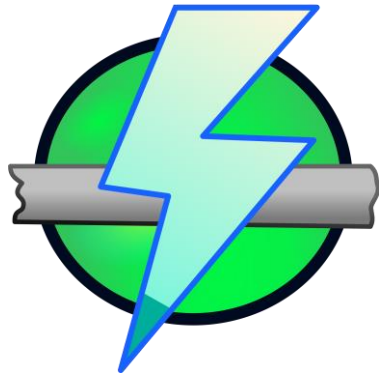
VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Motivácia

- Čo je kyberbezpečnosť a prečo je dôležitá?
  - Ochrana pred útokmi, poškodením, neoprávneným prístupom
  - Závislosť na technológiach => nárast kybernetických hrozieb
  - Krádež identity/údajov/financii, útoky na nemocničné systémy, kybervojna
  - Smernica NIS2
- Ako sa brániť a zlepšiť kyberbezpečnosť?
  - Red-Teaming
  - Penetračné testovanie
  - Bezpečnostný audit

Cieľe práce

- Súčastný stav
  - Nmap, Hping3, Angry IP Scanner, ...
  - Obmedzenia a nedostatky
- Cieľ vyvíjaného nástroja
  - Zefektívnenie kyberbezpečnostných postupov
  - Pokrytie nedostatkov súčastných nástrojov
  - Zvýšenie kyberbezpečnosti v ČR a SR (nemocnice, banky, komerčné firmy, ...)



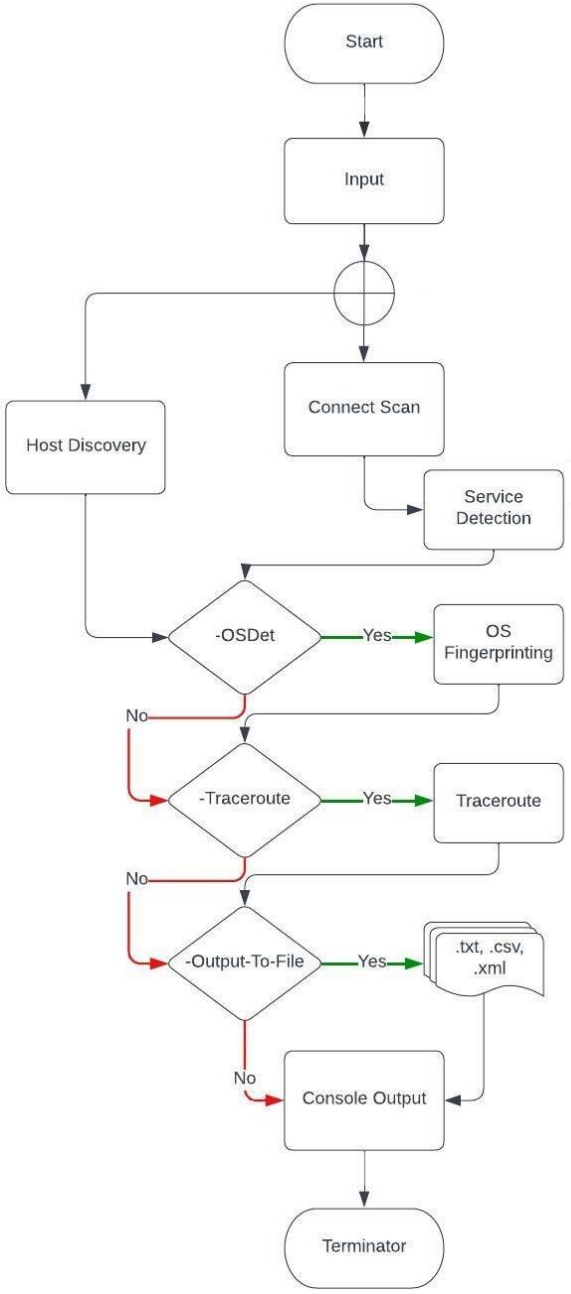
NMAP

Oculus - ligthweight network scanner

- Zadané firmou CYBER RANGERS
  - Najznámejšia kyberbezpečnostná firma v ČR zameraná na Red-Teaming
  - Kontrakty pre nemocnice, energetika, doprava, …
  - ČEZ ,Fakultní Thomayerova nemocnice, Generali Česká Pojišťovna, ...
  - Konzultácie - spoluzakladateľ Ing. Ján Marek

Návrh a testovacie prostredie

- Návrh štruktúry modulu
- Vytvorenie experimentálneho testovacieho prostredia
- Požiadavky:
  - Compatibilita so staršiou aj aktuálnou verziou Windows
  - Možnosť obchádzať uživateľské obmedzenia privilegií
  - Kompaktnosť
  - Nezávislosť od externých knižníc a programov
  - Obchádzanie Anti-Virus Blocking



Funkcionality a kustomizácia

- **Funkcionality:**
  - Target Enumeration
  - Host Discovery
  - Connection Scan
  - Output .xml, .csv, .txt
  - Multi-Threading

- **Možnosti kustomizácie:**
  - OS detection
  - Service Detection
  - Traceroute
  - Timeout
  - Top1000Ports
  - Threads
  - NoPing

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Ukážka výstupu funkcie “Get-ConnectionScan”:

```
PS C:\Users\domin> Get-ConnectScan -Target "192.168.111.130,150", "scanme.nmap.org"  -Port 21,80, 22, 23, 139, 443 -Threads 10 -Traceroute -OSDet
Starting TCP Connection Scan at 05/03/2023 11:09:37

Scan report for 192.168.111.130:
1 ports are closed or filtered.
OS: Ubuntu
TraceRoute: 192.168.111.130

Port Service
---- -------
  21 FTP Control
  80 HTTP
  22 SSH
  23 Telnet
 139 NetBIOS Session Service



Scan report for 2600:3c01::f03c:91ff:fe18:bb2f:
6 ports are closed or filtered.
OS: Linux/Unix/BSD
TraceRoute: 2a02:8308:a188:7b00:3a43:7dff:fe42:a26c -> 2a02:8300:8::1 -> 2a02:8300::ffff:b9bc:b8fe -> 2a00:11b0:2:100::1 -> 2001:5016:100:4::1 -> 2001:2034:
1:6c::1 -> 2001:2034:1:c1::1 -> 2001:2034:1:73::1 -> 2001:2000:3080:1eeb::2 -> 2600:1488:a180:227::a -> 2600:1488:5fc3:a::a -> 2600:1488:5fc3:28::b -> 2600:
1488:5fc3:d::b -> 2600:1488:a040:228::b -> 2600:1488:a040::21 -> 2600:3c01:3333:4::2 -> 2600:3c01::f03c:91ff:fe18:bb2f


Scan report for 45.33.32.156:
5 ports are closed or filtered.
OS: Unknown
TraceRoute: 192.168.0.1 -> 185.188.184.210 -> 185.188.187.12 -> 0.0.0.0 -> 0.0.0.0 -> 195.2.12.41 -> 195.2.18.250 -> 0.0.0.0 -> 62.115.124.28 -> 62.115.122.
138 -> 62.115.122.159 -> 62.115.123.123 -> 62.115.184.199 -> 23.203.152.40 -> 0.0.0.0 -> 0.0.0.0 -> 23.32.63.27 -> 23.207.232.41 -> 23.203.158.53 -> 0.0.0.0
 -> 0.0.0.0 -> 45.33.32.156

Port Service
---- -------
  22 SSH

 Scanning done: 4 IP addresses scanned.
 1 hosts is/are down.
 End of scanning at 05/03/2023 11:13:03
 Timeout: 1000
```

Záver

- Vývoj a implementácia riešenia
  - Modul
  - One-line script
  - One-line script generátor
- Vyriešenie nedostatkov sučastných nástrojov
  - Zvýšenie kyberbezpečnosti
  - Alternatívne riešenie
  - Jednoduchá rozšíriteľnosť
- Využitie pri Red Teamingu a penetračnom testovaní

Ďakujem za pozornosť!