Univerzita Palackého
v Olomouci

BEZIT – 11. cvičení

Skenování portů
Firewall

Karel Panchártek

25. 4. 2024

Univerzita Palackého
v Olomouci

Skenování portů - opakování ze sítí

- Co je to port?
- Co je to otevřený port?
- Jak zjistíme, že je port otevřený?
- Je skenování portů útok?
- Jaký má význam v zabezpečení vlastních systémů?

Univerzita Palackého
v Olomouci

Nástroj Nmap

- Skenování portů -> zjištění „vystavených“ služeb
- Další funkcionality pro nás nyní nedůležité
- Instalace jednoduchá:

```
apt install nmap
```

- Může být rozdíl mezi použitím pod běžným uživatelem a rootem
- Použití z CLI i GUI

Univerzita Palackého
v Olomouci

Nmap základní použití

```
nmap <target>
```

- Např. `nmap 10.0.0.1`
- Výpis vynechává filtrované porty
- Skenuje nejpoužívanějších 1000 portů
- Názvy služeb odvozeny od portu, nemusí odpovídat

Univerzita Palackého
v Olomouci

Nmap použití s některými parametry

- Lze specifikovat porty

```
nmap -p 1-1024, 3755, 65200-65280 <target>
```

- Lze zjistit verzi služeb, které na portech běží

```
nmap -sS <target> -sV
```

- Ignorovat nefunkční ping

```
nmap -sS <target> -Pn
```

Univerzita Palackého
v Olomouci

Firewall

- Co je to firewall?
- Proč je výhodnější drop než reject?
- Jakou roli hraje NAT?
- Kde je vhodné firewall nastavit?
- Jaký je hlavní rozdíl firewalu pro PC a Server?
- Jaký má význam filtrace konkrétních adres?

Univerzita Palackého
v Olomouci

Úkol

1) Zjistěte a vypište, jaké TCP porty jsou na stroji Bezit11 otevřené a jaké služby na nich běží.

2) Nastavte router tak, aby byl bránou (směřoval) mezi sítěmi 10.55.0.0/24 a 10.44.0.0/24 (vnější síť). Síť 10.55.0.0/24 považujeme za vnitřní, zabezpečenou síť. Ve VirtalBoxu vnitřní síť „intnet-inner“. 10.44.0.024 bude vnější síť. Router se do vnější sítě bude hlásit na adrese 10.44.0.1/24. Stroj Bezit11 bude dostupný skrze router. Router bude realizovat firewall. Nastavte router tak, aby byl možný pouze přístup na webový server na stroji Bezit11 z vnější sítě. Stroji Bezit11 nechceme umožnit zahájit spojení do vnější sítě.

Postup popište a pošlete snímky obrazovky Vámi změněných nastavení na routeru. Jsou požadovány snímky celé obrazovky, tak ať je viditelné datum a čas.

Univerzita Palackého
v Olomouci

Úkol

Stroj stroj Bezit11 (název souboru je „Bezit11-studenti“) je ke stažení na tomto odkaze: https://upload.upol.cz/UYVK-FTZM
Síťová karta 1 do vnitřní sítě „intnet-inner“, adresa 10.55.0.200/24
Výchozí brána 10.55.0.1 (router)

RouterOS použijte z předmětu KMI/POS1(2)