H6 - Upgrade your skills

6.1. Nmap

Network scanning

- Identifying hosts, ports, services in a network
- Part of information gathering: ARP scan, ping sweep, port scan
- Enkel uit te voeren op gekende netwerken
- Nmap is hier het best voor

Aantal actieve live systems op subnet kennen, als nmap niet beschikbaar is:

- Ping: niet ideaal, pings worden soms geblokkeerd
- ARP: beter dan ping, beter en sneller
    - arping (Linux) of arp-ping (Windows)

Nmap

- Network Mapper
- Open source network scanner
- Hosts en services vinden op een netwerk
- Features
    - Host discovery: ontdekken van toestellen op netwerk, TCP/ICMP-requests verstuurd
    - Port scanning: alle poorten overlopen en zien met welke connectie gemaakt kan worden
    - Version detection: voor open poorten bepalen welke applicatie er luistert
    - TCP/IP stack Fingerprinting: achterhalen OS en hardware-eigenschappen
    - Scriptable interaction (with target): LUA programmeertaal
- GUI: Zenmap

Tips & banner grabbing

- `nmap 192.168.1.22`: eerste 1000 gekende poorten scannen
- `nmap -p22 192.168.1.1-100`: enkel poort 22 scannen voor 100 systemen
- `nmap -p- 192.168.1.22`: alle poorten op 1 systeem scannen
- `nmap -sV -p22,80,443 192.168.1.22`: 3 specifieke poorten scannen voor 1 systeem
- `nmap -sn 192.168.1.0/24`: ping scan

6.2. Hack the box & Try hack me

online platformen om cybersecurity-skills bij te schaven

6.3. Metasploit & metasploitable

Metasploit

- Penetration testing framework
- Samenwerking tussen open source community en Rapid7
- Verstrekt info over kwetsbaarheden in computersystemen
- Te gebruiken om exploits te testen
- 2 versies: Metasploit framework en Metasploit pro

Metasploitable

- Virtuele machine om metasploit te testen
- Opzettelijk kwetsbaar gemaakt

Metasploitable 1/2/3

(2010) Metasploitable

- Gebaseerd op Ubuntu 8.04 server
- Runt op VMWare

(2012) Metasploitable 2

- Nog bruikbaar en relevant
- Linux-based, zowel VirtualBox als VMWare

(2016) Metasploitable 3

- Windows Server 2008 R2 (met SP1) of 2012
- Geen virtual disk, script voor automatische deployment

6.4. Automated VM deployments

- Hergebruik van virtual disk of linked/full clone
- Creation en customization van VMs kan geautomatiseerd worden
    - VirtualBox: VBoxManage CLI, VMWare ESXi: vSphere CLI

VBoxManage

- CLI voor Oracle VM VirtualBox
- Alle VMs oplijsten, info specifieke vm, maken/aanpassen/verwijderen VM, starten/stoppen/resetten VM, importeren/exporteren VM, ...