

Penetration Testing

• En introduction til pentesting

Hvem er jeg?

- Oliver Lind Nordestgaard
- Cyberlandsholdet 2021-2022
- Consult, Cyber Secure @ Implement
- Software Engineering @ SDU

Pentesting – Generalt

- Legalitet
 - Pentesting vs Hacking
- Hvordan gøres det typisk
 - Assume Breach
 - Web-application testing
- Formål
- Forskellen på det vi lære vs pentesting vs red-teaming
- Kun focus på Linux i denne omgang

Advarsel

- Dette er en introduktion til pentesting og ikke redteaming
 - I lære ikke at undgå at lave larm
 - I vil blive opdaget og politiandmeldt hvis I prøver at udføre disse angreb uden tilladelse fra målet.
 - Få styr på hvordan man laver et juridisk gældende aftale inden du laver en pentest for nogen
 - Husk hvad er in-scope og hvad er out-of-scope
 - Kunder kan tage fejl – hosting, MS SSO, etc
 - Angreb på andre, uden aftale er ulovligt
 - Ingen andre en myndigheder eller egentlige ejere kan give tilladelse

Metodik

- [illegible]

Metodik – HackTheBox-style servere

- Enumeration
- Exploitation
- Foothold
- Enumeration
- Privesc
- (Enumeration)
- (Privesc)
- Done?

Enumeration – IP Enumeration

- Hvis du ikke får udleveret en IP-adresse
- `nmap -sP [din-ip]/24`
 - `-sP` pinger alle ip adresserne
 - Du kan bruge `-p [port]` hvis du kender en specifik port der er åben
 - Ellers `-p-` hvis du vil scanne alle porte på alle ip adresserne
- Hvis din IP er 172.17.0.1 så scanner den 172.17.0.0 - 172.17.0.255
 - Scan højst /24 (som udgangspunkt – enkelte gange op til /16)
 - Evt to forskellige /24 så fx 172.17.0.1/24 og 172.17.1.1/24
 - Hvis ikke det giver noget har du nok misset noget

Enumeration – Port Scanning

- Når du har fundet en IP-adresse
- `nmap [options] [ip-adresse]`
 - `-p-` for at scanne alle porte
 - `-sC` for at køre nogle default nmap scripts der giver lidt info
 - `-sV` for at få nmap til at prøve at finde versionen af den software der kører
- Kan godt tage lidt tid så kørs evt i baggrunden

Enumeration – Web

- Hvilket software og versioner bruges
 - Wappalyzer
 - Kig i HTML, JS og CSS efter spor
- Find mapper og paths
 - Dirbuster (eller gobuster eller ...)
- Find Virtual Hosts (DNS enumeration)
 - Wfuzz eller ...
- Dette gennemgås i “GRUNDLÆGGENDE WEB-SIKKERHED”

Enumeration – Hands-on

- <https://github.com/olnor18/DDC-Pentest-Course>
- Øvelse 01 og 02
- 20 min.
- Follow-up
- 10 min. pause

Exploitation - Find exploits

- Når du kender software og version
 - Check på Exploit-DB og github
 - Exploit-DB viser også Metasploit scripts, ellers kan man søge i metasploit
 - CVE
- Når du har creds
 - Nogle systemer tillader code execution som admin, uden at der er en exploit, såsom wordpress plugins og lignende.
 - Står der brugbar information i systemet, såsom en note eller lignende?
 - Genbrug credentials. Brugernavn og password til en hjemmeside kan evt. bruges til SSH.

Exploitation – Reverse shells

- Bindshell vs revshells
- Revshells.com
- Netcat
 - `nc -lvnp 4444`
 - `python3 -c 'import pty; pty.spawn("/bin/bash")'`
- Meterpreter

Exploitation - Metasploit

- Search [term]
- Use [exploit-name or index]
- Options
 - Show options
 - Set LHOST [IP]
- Payload
 - Show payloads
 - Set payload [payload-name]
- Run

Exploitation – Extra

- Alternative veje
 - .ssh/authorized_keys
 - Chmod!
 - .ssh/id_rsa
- Information
 - <https://book.hacktricks.xyz/>
 - <https://github.com/swisskyrepo/PayloadsAllTheThings>

Exploitation – Hands-on

- <https://github.com/olnor18/DDC-Pentest-Course>
- Øvelse 03
- 30 min.
- Follow-up
- 1 times pause

Privilege Escalation – Enumeration

- Auto-scripts
 - LinPEAS, Linenum
- Permissions
 - Setuid
 - PATH variable
 - sudo -l
 - gtfobins
 - Groups (docker, sudo)
- Files
 - Config-files with credentials, database information
 - Scripts with credentials, run as privileged users, but highjackable
 - Cron
 - Databases

Privilege Escalation – Enumeration 2

- Running internal services
 - Check ports in use
 - Processes: `ps aux`, `pspy`
 - `lsof` (`lsof -i -P -n | grep LISTEN`), `netstat` (`netstat -tulpn | grep LISTEN`)
- Vulnerabilities
 - Software vulnerabilities (`pkexec`, `sudo`, `mysql`)

Privilege Escalation – Utilities

- Kopier filer til og fra host
 - SCP
 - Base64
 - Curl/wget + python3 -m http.server
- find
 - Setuid: -perm /4000
 - Brugernavn: -user [username]

Privilege Escalation – Hands-on

- <https://github.com/olnor18/DDC-Pentest-Course>
- Øvelse 04
- 30 min.
- Follow-up