

Pentest rapportage

Projectgroep

ICTAISc3

Docent

[Redacted]

School en Opleiding

Windesheim Zwolle HBO-ICT Software Engineering, Business IT Management & Infrastructure Design & Security

Student

Bark, Ivan (s1169347)

[Redacted]

Geen vertrouwelijke behandeling gewenst.

Versiebeheer

Versie	Datum	Omschrijving	Opmerkingen
0.1	29-05-2024	Eerste opzet	-
0.2	29-05-2024	Introductie	-
0.3	29-05-2024	Uitvoering en kwetsbaarheden	-
0.5	30-05-2024	Bevindingen Monitoring	-
0.7	30-05-2024	Bevindingen Penetration Testing	-
0.9	30-05-2024	Laatste aanpassingen en opmaak	-
1.0	30-05-2024	Eerste versie	-

Distributie

Naam	Functie	Versie	Datum toezending	Reden toezending
AIsc4	SOC-team	1.0	30-05-2024	Oplevering
	Docent	1.0	31-05-2024	Oplevering

Inhoudsopgave

1. Introductie.....	3
1.1. Opdracht.....	3
1.2. Scope	3
1.3. Aanpak.....	3
2. Bevindingen.....	4
2.1. Penetration testing	4
2.1.1. Severity Ratings	4
2.1.2. Tijdlijn	5
2.1.3. Uitvoering.....	5
2.1.4. Reverse shell	7
2.2. Monitoring.....	8
Bibliografie	9

1. Introductie

In dit document wordt een rapportage beschreven van een uitgevoerde penetration test op de omgeving van ICTAISc4. In dit document wordt de uitvoering van de opdracht beschreven, daarnaast worden de bevindingen toegelicht. Ook worden de bevindingen beschreven die zijn gemaakt tijdens het monitoren van een penetration test op onze omgeving.

In dit hoofdstuk wordt de opdracht en de scope ervan verder toegelicht. Ook zal de aanpak en taakverdeling worden beschreven.

1.1. Opdracht

De opdracht is om een penetration test uit te voeren op de omgeving van een ander team. In ons geval gaat het hier om ICTAISc4. Dit team zal hun omgeving monitoren op hun SIEM terwijl de penetration test wordt uitgevoerd. Tegelijkertijd zal het andere team onze omgeving testen en zullen wij dit monitoren. De opdracht is bedoeld om kennis te maken met penetration testing en monitoring van een omgeving.

1.2. Scope

Vanuit ICTAISc4 is het verzoek gekomen om ons te richten op de Ubuntu en Windows Metasploitable machines. De Kali en SIEM machines vallen dus buiten de scope. Hetzelfde verzoek hebben wij ingediend bij ICTAISc4.

1.3. Aanpak

Om tegelijkertijd te kunnen testen en monitoren is er gekozen om het team op te splitsen in twee teams:

Team	Verantwoordelijkheid	Leden
Blue team	Monitoring	
Red team	Penetration testing	Ivan &

2. Bevindingen

In dit hoofdstuk wordt de uitvoering van zowel de penetration testing en monitoring toegelicht, daarnaast worden de bevindingen beschreven. Zoals eerder beschreven is de penetration testing uitgevoerd door Red team en was Blue team verantwoordelijk voor monitoring.

2.1. Penetration testing

2.1.1. Severity Ratings

De volgende tabel definieert de ernstniveaus en bijbehorende CVSS-scorebereiken die in dit document worden gebruikt om kwetsbaarheid en risico-impact te beoordelen.

Medium (CVSS V3 Score < 6.0) Lage en informatieve kwetsbaarheden worden niet in dit document gerapporteerd omdat we ons voornamelijk richten op de hoge en kritieke kwetsbaarheden met ernstige implicaties.

Severity	CVSS V3 Score Range	Definitie
Critical	9.0-10.0	Exploitatie is eenvoudig en resulteert meestal in een compromis op systeemniveau. Het wordt aangeraden om onmiddellijk een actieplan te maken en te patchen.
High	7.0-8.9	Exploitatie is moeilijker maar kan leiden tot verhoogde privileges en mogelijk verlies van gegevens of downtime. Het wordt aangeraden om zo snel mogelijk een actieplan te maken en te patchen.
Medium	4.0-6.9	Er bestaan kwetsbaarheden, maar deze zijn niet exploiteerbaar of vereisen extra stappen zoals social engineering. Het wordt aangeraden om een actieplan te maken en te patchen nadat de hoge-prioriteitskwesties zijn opgelost.
Low	0.1-3.9	Kwetsbaarheden zijn niet exploiteerbaar maar zouden het aanvalsoppervlak van een organisatie verkleinen. Het wordt aangeraden om een actieplan te maken en te patchen tijdens het volgende onderhoudsvenster.
Informational	N/A	Er bestaat geen kwetsbaarheid. Aanvullende informatie wordt verstrekt met betrekking tot items die tijdens de test zijn opgemerkt, sterke controles en extra documentatie.

2.1.2. Tijdlijn

De tijdlijn hieronder beschrijft de belangrijke events en uitgevoerde acties tijdens de penetration test.

Tijd	Actie
12:37	Connecten met pfsense
12:38	Start nmap router
12:44	Start tweede nmap scan router
12:49	AngryIPScanner gerund op het IP range 192.168.1.xxx
12:51	Start nmap metasploitable
13:50	Msfconsole gebruikt voor brute force op glassfish login
13:55	Success login gevonden en successvol ingelogd
14:15	Creëren van reverseshell
14:19	Uploaden en launchen reverseshell

2.1.3. Uitvoering

In deze paragraaf wordt de uitvoering van de penetration test en de genomen stappen beschreven. Bij het uitvoeren van de penetration test is gebruik gemaakt van een laptop Arch linux.

Allereerst is er contact gemaakt met de pfsense router om toegang te krijgen tot de omgeving van ICTAISc4.

```
[sudo] pfsense-00a-119a-vmuser-config \(\)\.open
[sudo] password for tim:
2024-05-29 12:36:58 OpenVPN 2.6.18 [git:makepkg/ba062f0950c56a0+] x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PTINFO] [AEAD] [DCO] built on Mar 28 2024
2024-05-29 12:36:58 library version: OpenSSL 3.3.0 9 Apr 2024, LZO 2.10
2024-05-29 12:36:58 DCO version: N/A
Enter Auth Username: vpmuser
Enter Auth Password: *****
2024-05-29 12:37:17 TCP/UDP: Preserving recently used remote address: [AF_INET]145.44.235.235:1194
2024-05-29 12:37:17 UDPv4 Link local: (not bound)
2024-05-29 12:37:17 UDPv4 Link remote: [AF_INET]145.44.235.235:1194
2024-05-29 12:37:17 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2024-05-29 12:37:17 [InternalError] Peer Connection Initiated with [AF_INET]145.44.235.235:1194
2024-05-29 12:37:18 TUN/TAP device tun0 opened
2024-05-29 12:37:18 net_iface_mtu_set: mtu 1500 for tun0
2024-05-29 12:37:18 net_iface_up: set tun0 up
2024-05-29 12:37:18 net_addr_v4_add: 10.0.0.2/24 dev tun0
2024-05-29 12:37:18 Initialization sequence completed
```

Figuur 2.1: Koppelen met pfsense

Vervolgens zijn er twee 'nmap' scans uitgevoerd op de router.

```
> sudo nmap -sC -sV 192.168.1.1
[sudo] password for tim:
Starting Nmap 7.95 ( https://nmap.org ) at 2024-05-29 12:38 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0082s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  domain       (generic dns response: REFUSED)
80/tcp    open  http         nginx
|_ http-title: Did not follow redirect to https://192.168.1.1/
443/tcp    open  ssl/https    nginx
|_ http-server-header: nginx
|_ ssl-date: TLS randomness does not represent time
|_ http-title: 400 The plain HTTP request was sent to HTTPS port
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.95I=7%D=5/29%Time=665705BA&P=x86_64-pc-linux-gnu%(DNSV
SF:ersionBindReqTCP,E,"\\0\\x0c\\x06\\x81\\x05\\x0\\x0\\x0\\x0\\x0");
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 201.08 seconds
```

Figuur 2.2: nmap scan router

In de omgeving zijn vervolgens meerdere 'nmap' scans uitgevoerd.

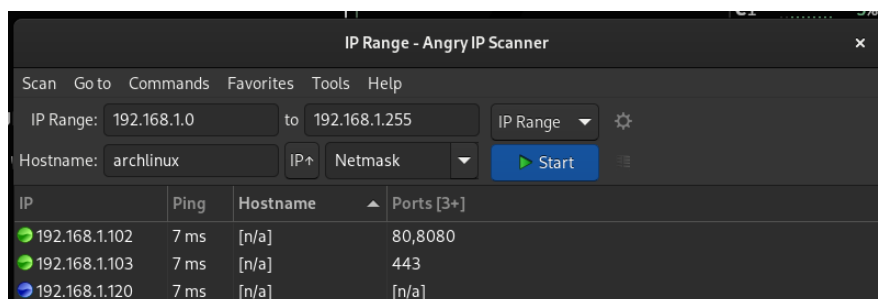
```
> sudo nmap -sC -sV 192.168.1.121
Starting Nmap 7.95 ( https://nmap.org ) at 2024-05-29 12:49 CEST
Nmap scan report for 192.168.1.121
Host is up (0.036s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7 ((Ubuntu))
445/tcp   open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
|_ http-robots.txt: 1 disallowed entry
|_ /
|_ http-methods:
|_ Potentially risky methods: PUT
3000/tcp   closed ppp
3306/tcp   open  mysql        MySQL (unauthorized)
8080/tcp   open  http         Jetty 8.1.7.v20120910
|_ http-title: Error 404 - Not Found
8181/tcp   closed intermapper
Service Info: Host: MS-UBUNTU1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_ smb-security-mode:
|_   account_used: guest
|_   authentication_level: user
|_   challenge_response: supported
|_   message_signing: disabled (dangerous, but default)
|_ smb-os-discovery:
|_   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|_   Computer name: \x00
|_   NetBIOS computer name: MS-UBUNTU1\x00
|_   Workgroup: WORKGROUP\x00
|_   System time: 2024-05-29T10:51:37+00:00
|_ clock-skew: mean: 2m02s, deviation: 3s, median: 2m00s
|_ smb2-security-mode:
|_   3.1:1:
|_     Message signing enabled but not required
|_ smb2-time:
|_   date: 2024-05-29T10:51:34
|_   start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 210.31 seconds
```

Figuur 2.3: nmap scan

Er is vervolgens een scan uitgevoerd doormiddel van AngryIPScanner op het IP-range 192.168.1.xxx.



Figuur 2.4: AngryIPScanner op het IP-range 192.168.1.xxx

Met de informatie uit AngryIPScanner en de 'nmap' scans kunnen wij kunnen concluderen dat er een GlassFisch admin paneel op het 120:4848 IP/port zat.

```
[-] 192.168.1.102:4848 - Failed: 'admin:22222'
[-] 192.168.1.102:4848 - Failed: 'admin:88888888'
[-] 192.168.1.102:4848 - Failed: 'admin:anthony'
[-] 192.168.1.102:4848 - Failed: 'admin:justin'
[-] 192.168.1.102:4848 - Failed: 'admin:test'
[-] 192.168.1.102:4848 - Failed: 'admin:bailey'
[-] 192.168.1.102:4848 - Failed: 'admin:q1w2e3r4t5'
[+] 192.168.1.102:4848 - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_login) > |
```

Figuur 2.5: Password burte force attack metasploit

Nadat er met succes een login gevonden was op een GlassFish service, die draaide op 192.168.1.102:4848, is hierin verder gekeken om hogere rechten te verkrijgen. Zoekend naar mogelijke exploits zagen we dat een reverse shell mogelijk was. (Seven Layers LLC, n.d.)

Met de metasploit package kon een reverse shell gemaakt worden en naar worden geluisterd op de lokale machine. Hierdoor krijg je toegang tot de shell op de machine. De shell zelf moet dan via Applications in Glassfish deployed en gelaunched worden om zo de shell aan te maken.

2.1.4. Reverse shell

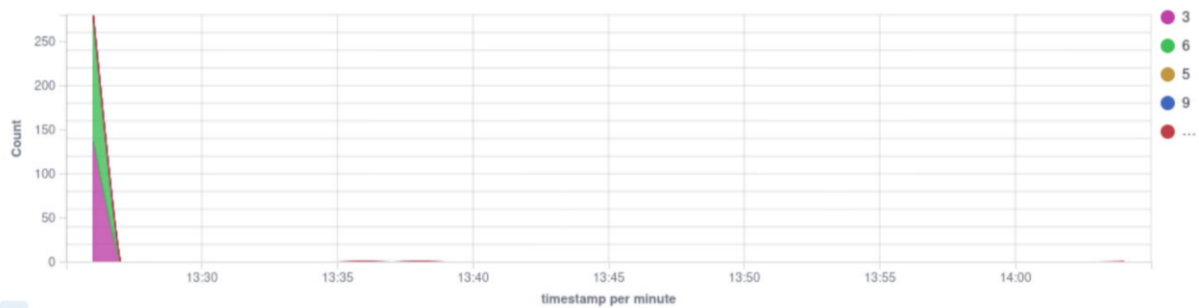
Een reverse shell is een soort shell sessie welke geïnitieerd wordt op de doelwit machine. Deze sessie maakt verbinding vanuit het doelwit machine naar de aanvallers machine. De aanvallers machine heeft een 'listener' aan staan welke luistert op een bepaalde poort en wacht om de verbinding van de reverse shell.

Om de reverse shell aan te zetten op het doelwit machine moet daar een mogelijkheid zijn om zulke shell sessies aan te maken of te uploaden. Dit wordt dan een 'payload' genoemd. In de payload staat dan aangegeven met welke IP en poort de shell sessie moet verbinden. De 'listener' wacht dan dus op het signaal van de 'payload'. Wanneer deze verbinding is gemaakt, kan de aanvaller via zijn eigen machine commando's uitvoeren op de doelwit machine.

Omdat deze commando's dan eigenlijk vanuit de doelwit computer uitgevoerd worden, worden deze commando's niet tegengehouden door een firewall. Firewalls staan meestal ingesteld om verkeer van buitenaf te blokkeren, en niet andersom. Ook worden deze commando's niet gezien als kwaadaardig, omdat het doelwit machine ze zelf uitvoert, welke al over de nodige rechten beschikt. (Cuncis, 2023)

De bijbehorende CVE is de CVE-2011-0807 met een CVSS 2.0 score van 10.0. (NVD, 2011)

2.2. Monitoring



Figuur 2.6: Tijdlijn alle events tijdens pentest event (... = 10)

Alle geconstateerde events die plaatsvonden tijdens de afgesproken periode zijn hierboven gevisualiseerd. Alle waargenomen events vielen in de periode van 13:25 en 14:05.

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
May 28, 2024 @ 14:04:02.686	001	Windows-Agent			CVE-2022-37966 affects Windows Server 2008 R2	10	23505
May 28, 2024 @ 13:38:40.805	001	Windows-Agent			Windows application error event.	9	60602
May 28, 2024 @ 13:36:20.278	001	Windows-Agent			Windows application error event.	9	60602
May 28, 2024 @ 13:26:37.581	001	Windows-Agent	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
May 28, 2024 @ 13:26:37.565	001	Windows-Agent	T1078 T1531	Defense Evasion, Persistence, Privilege Escalation, Initial Access, Impact	Logon failure - Unknown user or bad password.	5	60122
May 28, 2024 @ 13:26:37.550	001	Windows-Agent			Windows User Logoff.	3	60137
May 28, 2024 @ 13:26:37.534	001	Windows-Agent	T1550.002 T1078.002 T1021.001	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Successful Remote Logon Detected - User:ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that nmap is allowed to perform RDP connections	6	92657
May 28, 2024 @ 13:26:37.519	001	Windows-Agent			Windows User Logoff.	3	60137
May 28, 2024 @ 13:26:37.502	001	Windows-Agent	T1550.002 T1078.002 T1021.001	Defense Evasion, Lateral Movement, Persistence, Privilege Escalation, Initial Access	Successful Remote Logon Detected - User:ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that nmap is allowed to perform RDP connections	6	92657
May 28, 2024 @ 13:26:37.487	001	Windows-Agent			Windows User Logoff.	3	60137

Figuur 2.7, Laatste 10 waargenomen events

De laatste paar events waren degene met de hoogste level. De level 10 is een resultaat van de vulnerability detector welke een nieuwe CVE exploit gevonden had, namelijk CVE-2022-37966. Deze CVE is al langer bekend, maar had op 29-mei-2024 een nieuwe update erbij gekregen. Het is dus onduidelijk of de pentesters deze CVE veroorzaakte, of doordat de CVE geüpdatet is de vulnerability detector het op dat moment wel detecteerde.

Rule ID	Description	Level	Count
60137	Windows User Logoff.	3	137
92657	Successful Remote Logon Detected - User:ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that KALI is allowed to perform RDP connections	6	133
60122	Logon failure - Unknown user or bad password.	5	5
92657	Successful Remote Logon Detected - User:ANONYMOUS LOGON - NTLM authentication, possible pass-the-hash attack - Possible RDP connection. Verify that KALI is allowed to perform RDP connections	6	4
60602	Windows application error event.	9	2
23505	CVE-2022-37966 affects Windows Server 2008 R2	10	1

Figuur 2.8, Samenvatting alle events

Dit waren alle gedetecteerde events. De meeste hiervan waren Windows Logon en Logoff events. Ons vermoeden is dus dat er geprobeerd is om in te loggen met een brute-force aanval.

Bibliografie

Cuncis. (2023, februari 24). *Reverse Shell Cheat Sheet: Creating and Using Reverse Shells for Penetration Testing and Security Research*. Retrieved from Medium:
<https://medium.com/@cuncis/reverse-shell-cheat-sheet-creating-and-using-reverse-shells-for-penetration-testing-and-security-d25a6923362e>

NVD. (2011, september 21). *CVE-2011-0807 Detail*. Retrieved from NIST:
<https://nvd.nist.gov/vuln/detail/CVE-2011-0807>

Seven Layers LLC. (n.d.). *EXPLOITING GLASSFISH*. Retrieved from SEVENLAYERS:
<https://sevenlayers.com/index.php/173-exploiting-glassfish>