Pen Testing Windows Active Directory

sid@notsosecure.com

I am sure there are more than one ways of performing a penetration test on windows active directory. In this article, I am listing some of the tricks that I would generally use when I will encounter a windows domain.

The aim of performing a pen test on windows active directory could vary, however, I believe gaining administrative level privileges on the "Domain Controller" is the ultimate challenge for a pen tester. Here are some scenarios you may encounter:-

Case 1: You are allowed to plug your laptop to the internal network and all you have been given is the target range:

This is the most common scenario. I would usually proceed in the following manner:

1. Identify the vulnerabilities:

Use nmap to identify the open ports and then run Nessus. Nessus will give u a very good idea as to how good/bad is the overall security. Hopefully, nessus will come back with certain high risk issues

2. Exploit the vulnerability:

Fire metasploit and verify if the nessus findings are not false positives. If the exploit is successful, you will now have a remote shell on that box.

3. Add a dummy account :

The first thing to do now is to add a localuser with admin privileges to that box:

Net user pentest p3nt3st /add
Net localgroup administrators pentest /add
Sometimes you need to do this too:

net group "domain admins" pentest /add

PS: Make sure that this account is removed after the test is over.

4. Get Hashes from the Box you owned:

Now its time to fire cain. Go to the quick list section, add the ip address of the box you have just owned, and supply the credentials for the account that you have just created.(pentest/pentest). Go to services section → right click, install abel→ disconnect→ connect again with the same credentials.

Now you will see a new section called abel which will have a sub section to dump all users and another subsection to dump the hashes. After you dump the hashes, send them to the inbuilt cain cracker and start cracking. Also it's worth mentioning about 'fgdump' which can be used for similar purposes. It's a modern tool that can evade AV and avoid crashing fully patched systems.

5. Lets focus on the Domain Now

Hopefully at this point in time, you will have the usernames and passwords for all users on the

box which you have just owned. Remember, the entire aim of cracking the hashes is to try if the same passwords work on other boxes as well. If you are lucky, you may be surprised to find the same admin password which you just cracked works for all the local admin accounts.
Now, lets see if the same password works on the domain controller as well.

Question: How do I find out if the box I owned is a part of domain or not?
Answer: the following the command will tell you the domain name as well as the domain controller as well as the groups present on the domain:

Net localgroup /domain

You can also get a list of all the ‘domain users’ with this command’
Net users /doman

6. Owning the Domain Controller

Now then since you know the domain controller, try the same admin password on this box, and it could be game over.

If the same password does not work on the domain controller, things to try are:

- You can obtain the domain users either by issuing a “net users /domain” command on the box you owned or you obtain this information through nessus provided **the null session** [1] settings are enabled on any of the test boxes. As you already have the list of domain users now, identify the domain admin accounts and try to crack the passwords for these accounts against services like smb, rdp etc. If you succeed, you can go home early. Tools to use THCHydra, ntenum3.3, tsgrinder

- It could be possible that the box which you owned in step 2 could have been used by a domain admin to log into some service, so try cache dump and also dumping the LSA secrets to gain all the passwords you could possibly gain. A cached domain admin password will again imply game over. I would quote someone here, "lsadump is a really important thing to try. It gives the clear text passwords for all service accounts. Some of which might be of ‘domain admins’. Not so common on 2k3 networks, but common enough."

- Of course, you will be running nessus against all the boxes including the domain controller and you will have the list of vulnerabilities against every box. Try exploiting the domain controller directly using metasploit modules. One of the things which has a very

[1] Null session can give out a vast amount of information to an attacker. The recommended registry settings to disable a null session and the related security issues in windows 2003 server are :

Hive: HKEY_LOCAL_MACHINE

Key: SYSTEM\CURRENTCONTROLSET\CONTROL\LSA

Name: RestrictAnonymous-1 (set it to 2 on windows 2000)

Name: RestrictAnonymoussam-1

Name: EveryoneIncludesAnonymous-0

high probability to succeed is the ms07-029 issue which exploits a flaw in the MS DNS RPC interface. This service is enabled by default on the 'Domain Controllers'.

7. Get the Domain Users Hashes

Repeat the step 4 to connect to the domain controller as an admin user and get the hash of all the domain users. Should we crack the domain users' hash? Well, not really, but, just do it. ☺

Case2: You are not allowed to plug your laptop to the target network. You have been given access to a workstation and a standard domain account.

Things to try:

- Search milw0rm for local windows exploit against that particular OS and the service pack, and try to gain local 'system' level access on the workstation and repeat the processes 1-6 mentioned above.

- Try to gain access to command prompt. It is a common practise to not **allow access to cmd.exe**. However, in most of the cases it is not very difficult to break this protection. After you have access to cmd.exe run the net users and the net localgroup command to identify the admin domain users and try cracking a domain admin password against services like smb, rdp etc. However, this may/may not work as you will not have admin access to run these tools.

- If the BIOS password is not enabled, you make the workstation book from the CD released by eeye sysrq2 to gain system level privileges on the workstation and then repeat process 1-7.

Hopefully, you know now something about pen testing an active directory.

Tools /References:-

- Nmap –port scanner command line:-
  Nmap –sV –sS –O –oA myreport –vvv -iL targets.txt –p 1-65535 –P0
  www.insecure.org
- Nessus
  Use the GUI
  www.tenablesecurity.com
- Metasploit
  Both command line and web interface available.
  www.metasploit.com
- Nbtenum3.3
  Command line:- nbtenum3.3.exe –s ips.txt mydictionary.txt

- TSgrinder
- THChydra
- Cain (www.oxid.it)
- Cachedump
- Fgdump
- Pwdump
- Nltest

- Lservers
- SYSrq2 (http://research.eeye.com/html/tools/RT20060801-8.html)
- NBtscan