**2) 504.2 - Computer & Network Hacker Exploits, Part 1 quick notes**

2) Computer & Network Hacker Exploits, Part 1 quick notes  
  
First: BE CAREFUL BEFORE RUNNING ANY TOOL!  
ALWAYS review code, and test in a test environment, before running in a live business work environment!  
  
  
ALWAYS get permission before running tools on your network!  
  
Full and documented permission is essential before you run any of these tools on a network! When getting permission it needs to be in writing! Verbal agreement don't hold up too well in court! The documented permission should also state that the giver of permission understand there may be 'adverse' side-effects of the scanning or testing activity! This is also a 'Get Out of Jail Free' document!  
Sample at:  
http://www.counterhack.net/permission\_memo.html  
  
Attack tools are getting easier to use and more easily distributed!  
High-quality, extremely functional attack tools!  
Risk of the antidisclosure movement!  
  
How to make money on malicious code:  
- sell the code for backdoors/bots  
- spam and web-based advertising  
- pump and dump stock schemes  
- phishing: email, phone and targeted (spear) phishing  
- denial of service extortion (not just porn and gambling sites as targets anymore)  
- keystroke loggers stealing financial information  
- rent out armies of infected systems for all of the above  
- RAM scrapers pulling CC numbers of POS terminals  
  
Hack into web and file-sharing sites and alter software to include backdoors.  
Everyone who downloads and uses the tool is impacted!  
More than 60 software packages in total whose Internet updates can be subverted this way!  
  
The marriage of general attack tools and worms, viruses, and bots is resulting in powerful techniques.  
Worms are increasingly being used to carry bots, backdoors, password crackers and scanners.  
Botnets are growing large with self-replicating code.  
Several active botnets with more than 1 million hots.  
Attacks from multiple sources simultaneously.  
Bottom line: it's a good time to be an attacker, or a security practitioner (defender).  
  
Reconnaissance is 'casing the joint'!  
Two types of attackers: script kiddies, and attackers out to get a particular site.  
  
DNS:  
You need to give out postal address, phone numbers, names of points of contacts, authoritative domain name server, in order to register a domain name. This information can be used in social engineering, war dialing, war driving, scanning!  
  
Whois:  
Lookup the registrar at:  
www.internic.net/whois.html  
  
- go to the registrat's whois database to get detailed records:  
www.networksolutions.com/whois/index.jsp  
  
DNS zone Transfer:  
tcpdimp -nn port 53 and host 10.10.10.45  
  
or:  
c:\>nslookup  
server [DNSServer]  
set type=any  
ls -d [domain]  
  
UDP port 53: general queries  
TCP port 53: zone transfers  
  
S = syn packet!  
  
Or use 'dig':  
$ dig @[DNS-server-ip] [target-domain] -t AXFR  
  
DNS Recon Defenses:  
- do not allow zone transfers from just any system  
- use split DNS  
- make sure your DNS servers are hardened  
  
Look for zone transfers (in DNS server logs or data transferred to/from TCP port 53).  
  
Search the target's own websites:  
Press releases, white papers, design documents, sample deliverables, open positions, key people, contacts, search related sites (business partners, ISP, suppliers).  
  
http://www.sec.gov/edgar.html  
https://namechk.com  
www.pipl.com  
https://connect.data.com  
Newspapers, blogs, and magazines.  
Social networking sites (what expertise, which friends/associates), newsgroups with postings from employees.  
Pushpin by Tim Tomes (part of Recon-ng).  
Social-media geolocation (Flicker, Twitter, Picasa). Simply provide a latitude, longtitude, and radius (in kilometers) and pushpin pulls all available social-media posts from that area. Can map targets to behavior patterns (when and where they have lunch, their religious and political leanings), it can even be used to gather internal pictures of secured locations (people love to take pictures of their office and badges).  
  
Look for web spider/crawler activity! Logs show systematic access of entire website, page by page. That could simply be the Google bot or another search engine. Someone just sucked down the entire contents of our site!  
Remember to use Google Dorks to search for information!  
  
Useful Search Directives:  
"site:" directive to search within the given domain  
site:www.counterhack.net  
  
"link:" directive to show all sites linked to a given site  
"intitle:" directive shows whose title matches the search criteria  
"inurl:" directive shows pages whose URL matches the search criteria  
"relative:" directive shows similar pages (sometimes useful, sometimes not)  
"info:" directive finds cached pages, related pages, pages that link to it, pages that containt the term (NOt USEFUL)  
example:  
site:sans.org -www -isc -ics -labs -login -owncloud -survey  
  
  
  
Surround literals with " ", as in "Soc Sec Num"  
Add minus (-) to a search term to maximize effectiveness of resulting hits.  
Search for airline status. Search for VIN for vehicle information. Search for UPC number for product info.  
  
Google's Cache and Wayback machine.   
This can be useful if information was pulled from a website, maybe by an incident response team. Useful for bad guys if IR containment isn't thorough.Browse the Google Cache (HTML is loaded from Google, any images on site are loaded from original site, also, any links browsed take you to the real site, not a good approach for anonymous surfing, still, it's useful for finding recently removed pages).  
  
  
Search for specific file types on a target domain.  
Look for active content:.asp, .jsp, .php, .bak or .cgi.  
Excel spreadsheets: search for .xls and view it as HTML.  
For example, search for:  
site:www.[target].com asp  
Filetype: is also useful, but also just try the suffix.  
  
Search Engine Recon: FOCA  
- many files have metadata (usernames, vulnerable software versions of software, directory paths) that can be useful for attackers.  
- FOCA automates the process of searching for various files, downloading them, and extracting their metadata.  
- in addition to metadata extraction, is has basic Google Hacking Database and basic web-vulnerability scanning.  
  
Example: you can download someone's file from the web server, email it to them in macro's embedded, and tell them to correct gramatical errors and mispells. We could gain remote access with macros on the remote computer!  
  
It inegrates with Shodan and Robtext to identify network ranges and additional targets.  
Can perform subdirectory brute-forcing to identify additional hosts.  
https://www.elevenpaths.com/labstools/foca/index.html  
  
  
  
Available remote desktop systems  
ext: rdp rdp  
(we can use ext: instead of filetype:)  
  
Default web material (Apache, IIS, ColdFusion, and others).  
Web-based FileMaker Pro databases: "Select a database to view"  
(make sure to use quotes)  
Indexable directories: intitle:index.of "parent directory".  
User IDs and passwords (look for "password" and "userid").  
Shell history (look for common shell names and commands).  
Video cameras (example: search for inurl:"ViewerFrame?Mode=").  
  
FOCA has the ability to identify many of these vulnerabilities.  
  
site:blackhillsinfosec.com intitle:index.of  
intitle:index.of  
  
Bishop Fox's SearchDiggity is a fantastic suite that includes Google Diggity, Bing Diggity, and other search capabilities.  
Recon-ng, by Tim Tomes, is another powerfull recon tool.  
Determined attackers use these tools to gain access to target environments without even using an exploit!  
  
Search Engine Recon Defenses:  
Look for information leakage using Google yourself.  
Instructions at http://www.google.com/remove.html  
remove the website using robots.txt file! Monitor all IP addresses that try to access page.  
Remove individual pages ("NOINDEX, NOFOLLOW" meta tag).  
Remove snippets ("NOSNIPPET" meta tag)  
Remove cached pages ("NOARCHIVE" meta tag)  
Remove an image from Google's Image Search.  
Remove unwanted items from Google. URL re-crawl request form (www.google.com/addurl.html)  
See http://www.robotstxt.org for info about non-Google crawlers!  
  
  
Maltego:  
Paterva's Maltego is an intelligence-gathering tool that searches through various public information sources.  
Gathers information about relationships between people, social networks, companies, websites, domains, IP addresses, and more, graphically displays relationships of information.  
http://www.paterva.com/web6/products/maltego.php  
Community Edition: free but with limitations.  
Commercial Edition: around $760 per year.  
  
Some example transforms:  
DomainToPhone\_Whois  
DomainToMXrecord\_DNS  
DomainToPerson\_PGP  
IPAddrToPhone\_Whois  
PersonTOPerson\_PGP  
EmailAddressToEmailAddrSignedPGP  
  
Commercial edition supports specialized transform servers and creating custom transforms!  
  
Check on pastebin.com to see if credentials have been posted for your company.  
Go to https://haveibeenpwned.com  
  
Defenses Against Maltego:  
Preparation:  
Ensure that publicly available information about your organization is accuate.  
Conduct your own recon.  
  
Web-based recon and attack tools:  
Many website offer the capability to research or even attack other sites.  
Links to Internet Scanning Web Pages (Traceroute, ping, port scans, Denial of Service tests):  
www.shodanhq.com  
www.dnsstuff.com  
www.tracert.com  
www.traceroute.org  
www.network-tools.com  
www.securityspace.com  
  
https://images.shodan.io/?query=port%3A5900  
  
Do not click on the links or connect to these remote devices, as this is trespassing!   
  
War Dialing and War Driving:  
- war dialers dial a sequence of telephone numbers, attempting to locate modem carriers or a secondary dial tone!  
  
Useful for attacking out of band communications (think remote access to routers).  
  
https://github.com/rapid7/warvox  
(it's a war-dialing tool)  
  
Conducts war dialing using one or more VOIP accounts. No telephony hardware required... just an Internet connection and VOIP account.  
Suppors called ID spoofing.  
  
Conduct war dialing exercises against your own network. Reconcile your findings to the inventory. Utilize a commercial war dialer.  
  
Utilize a commercial war dialer:  
NIKSUN's Phonesweep  
http://www.niksun.com/product.php?id=17  
or utilize WarVOX.  
  
Get list of phone numbers from the phone company based on the bills; they make sure they get paid.  
Train users to use effective PIN passwords for their phones!!!  
  
Defenses:  
Identification:  
Activate scanning-detection function in your PBX, if available.  
Consider PBX firewall/IPS,such as SecureLogix Voice IPS  
  
Containment:  
Shut off modems when they are discovered (if they are not needed).  
Know whom to call in your own telecom group and at the phone company to regionally isolate a modem.  
  
Eradicate, Recover:  
Remote modems from network out-of-band devices (if possible).  
If modem is absolutely required, change phone number and secure it with strong authentication (token, crypto or others).  
  
  
  
War Driving - wireless:  
become a tower:  
www.ettus.com  
  
Stingray cellphone surveillance tool!  
  
Tools for Wireless LAN Discovery:  
NetStumbler by Marius Milner  
InSSIDER by MetaGeek  
  
Both tools above are noisy; they send SSID-less probe requests and look for probe responses! Therefore it cannot detect APs that don't respond to such requests!  
Linux Sniffing with Kismet!  
  
  
You can use a traditional sniffer, gathering wireless packets: tcpdump, wireshark and more.  
Or use a wireless-specific sniffer for better analysis of wireless-specific frame date:  
  
OmniPeek (formerly Airopeek), Commercial:  
www.wildpackets.com  
  
Aircrack-ng for cracking Wep and WPA keys:  
www.aircrack-ng.org  
  
ASLEAP by Josh Wright provides a dictionary attack against LEAP authentication!  
  
CoWPAtty (a dictionary-based cracking tool for pre-shared keys with WPA1 and WPA2). Must sniff four-way handshake. Cryptographically, WPA is a complex protocol. But, WPA folds SSID into its cryptographic exchange. Pre-computed dictionaries are available!  
  
Linux Attack with Easy-Creds:  
Greatly simplifies the process of creating malicious access points!  
  
Karma into Metasploit:  
Metasploit listens on a wireless interface for probe requests. Metasploit serves up a series of exploits for various vulnerable clients when they try to connect.  
  
Wifi Defenses:  
MAC address filtering at an access point isn't secure. We can change MAC addresses!  
  
Set SSID so that it doesn't attact attention. Use WPA2 with a strong password of at least 21 characters! Protect client wireless configs!!!  
  
Use VPN, Layer 3 encryption!  
  
In the lab, try to run Kismet and InSSIDer to find AP with funny names and without security enabled. Do not connect to the access points without security!  
  
  
  
2.5 Scanning Network and Port Scanning with Nmap:  
- an attacker needs to understand the topology of the network he is attacking.  
  
Contents of the IPv4 header:  
Service Type, Identification, Time to Live, Protocol, Flags, Source and Destination IP address, Data, padding.  
Contents of the IPv6 header:  
Payload length, next header, hop limit, source IP address, destination IP address.  
  
A common first component of network mapping is to identify the addresses in use by sweeping through address space.  
By default, Nmap sweeps each target address before port scanning it. This can be configured to use TCP packets or ignored all together (the -PN flag in Nmap, formerly -Po).  
Nmap sends the following 4 packets to each address in the target range: ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, ECMP Timestamp request. Nmap is running with UID 0; when running without UID 0, Nmap sends SYN to port 80 instead of ACK.  
Traceroute sends packets with small TTL values.  
IPV4 TTL and IPv6 Hop Limit is the number of hops the packets should go before being discarded.  
Based on the source address of the TTL-exceeded message, you can determine the router for given hop.  
The scanning system increments TTL for each packet to determine each router hop.  
  
Defending Against Network Mapping:  
Preparation:  
You could disable incoming ICMP echo request messages. You could disable outgoing ICMP Time Exceeded messages.  
Identification:  
IDS signatures looking for ping sweep or traceroutes. Many false positives possible.  
  
Containment:  
If you notice a particularly frequent ping sweep, you could temporarily block source address.   
  
TCP/UDP ports:  
- we have 65,536 ports, UDP and TCP.  
- port scanners send packets to various ports to determine what's listening.  
  
Current official port numbers can be found at IANA:  
www.iana.org/assignments/service-names-port-numbers/  
  
TCP header:  
Source Port, Destination Port, Sequence Number, Acknowledgement Number, Cont Bits, Window, Checksum, Urgent Pointer, TCP Options, Padding, Data, etc...  
UDP header:  
Source Port, Destination port, UDP Message Length, UDP checksum, Data.  
  
  
  
Nmap Scan Types:  
Ping Sweeps and ARP scans  
Connect TCP scans - used 3-way handshake.  
SYN scan - half-open scan, harder to detect and much quicker.  
ACK scan - stealthy and bypass some filters.  
FIN scan - steaalthy and bypass some filters.  
FTP Proxy "Bounce" scanning.  
"Idle" Scanning  
UDP scanning - send empty payload to most ports. Send protocol-appropriate payload to about a dozen ports (53, 111, 161, etc).Version Scanning  
IPv6 scanning (-6) now supported for all scan types. Used to be just for ping sweeks (-sP), TCP connect scans (-sT), and version scans (-sV).  
  
  
  
Nmap - ACK Scanning:  
Suppose you want to allow outgoing connection, but not incoming (network diode). You may configure a router to allow in only established connections (for example, connections with ACK control bit set). Allow outgoing SYNs, allow incoming connections only if ACK control bit is set.  
This blocks session initiations from the outside.  
But an attacker can conduct ACK scan to get past some filters.  
ACK scans are useful for mapping, but not for port scanning.  
Great for finding sensitive internal systems port exploitation.  
  
OS Fingerprinting  
Attempts to determine the OS of target by sending various packet types and measuring the response.  
Concept originated with the tool QueSO.  
  
Keeping track of all SYN and SYN/ACKS is hard.  
MassScan and other tools like it separate out the SYNs and the SYN/ACKs. One part sends SYN packets very quickly and the other part waits for SYN/ACKs. By decoupling the two halves the 3-way handshake speed is greatly improved.  
https://github.com/robertdavidgraham/masscan  
  
  
  
Another tool is called EyeWitness!  
It takes screenshots of websites, VNC and RDP servers.  
Effective to sort through hundreds of different websites.  
Attackers and testers look for default pages, out-of-date servers, RDP servers which show domains, index-able directories, etc.  
Many vulnerabilities are not necessary vulnerabilities which have a Metasploit module. Finding backup files and install scripts on web servers can lead to easy access to external systems.  
Developed by Chris Truncer:  
https://github.com/ChrisTruncer/EyeWitness  
  
Proxying Scans: REMUX  
Proof of concept tool to demonstrate scanning through multiple open proxies online.  
Reverse multiplexes connections.  
Browser connectes to remux.py, which federates connections through the proxies.  
The list of proxies are automatically downloaded at runtime. You can also specify your own list of proxies at runtime.  
Makes identifying the scanning system very difficult.  
When remux.py starts, it is very slow and buggy. It slowly learns which proxies are alive and which are not. Gets more stable and faster over time.  
  
  
Remux is faster than the TOR browser!  
  
Port Scanners - Defenses:  
Preparation  
Close all unused ports by shutting off services and applying filters.  
Utilize stateful packet filters and/or proxy firewalls.  
Utilize an intrusion detection system.  
  
Identification:  
Several IDS signatures for port scans.  
Log analysis shows pesky connection attempts.  
  
Locally checking for listening ports on Windows:  
C:\>netstat -na   
shows listening TCP/UDP ports.  
  
netstat -nao    (shows PIDs)  
netstat -nab    (shows EXE and all DLLs used)  
  
As a separate download, Microsoft has the Port Reporter tool.  
It periodically generates logs showing port activity.  
Free at http://support.microsoft.com/kb/837243  
  
For a GUI view of port usage, use TCPView.  
  
Disabling Windows Services Listening on ports:  
Kill running process using Taskmgr (be careful).  
Or use  
wmic process [pid] delete  
  
Disable services with services.msc in the Control panel.  
  
Use the 'sc' command:  
For a list of services, type c:\>sc query  
To shut off a service, type C:\> sc stop [service]  
To disable a service type:  
sc config [service] start = disabled  
(don't forget the space after "start="  
Be careful!  
  
  
Locally checking for listening ports on Linux/UNIX:  
  
#netstat -nap  
  
(it shows listening ports, PID and program name)  
  
#lsof -i  
  
  
Disabling Linux/UNIX services listening on Ports:  
To kill a process, run kill or killall  
  
Disable service by reconfiguring inetd or xinetd:  
in inetd: comment out lines in /etc/inetd.conf  
/etc/xinetd.d - delete files or make sure it contains "disable=yes"  
  
Disable service by altering /etc/rc.d files or running systemd (which alters rc.d automatically).  
#systemctl list-units --type service  
#systemctl disable <service>  
  
Be careful not to kill critical processes!  
  
  
Lab TIME:  
Logon to the slingshot Linux machine, with sec504/sec504 and perform nmap scans!  
  
nmap 127.0.0.1  
su -  
tcpdump -i lo  
  
nmap --reason 127.0.0.1  
su -   
nmap 127.0.0.1  
  
get more information with nmap:  
nmap -A 127.0.0.1  
  
################  
2.6 Scanning Evading IDSIPS and Web Vulnerability Scanning:  
  
many IDS/IPS systems do not validate the TCP checksum, because of too much overhead.  
An attacker can insert a TCP Reset with an invalid checksum to clear the IDS/IPS buffer.  
Target systems drop any packet with an invalid TCP checksum.  
  
Example:  
Packet 1:  
get /etc/shadow  
Packet 2:  
Badsum Reset  
Packet 3:  
Dow...  
  
Network Intrusion Detection by Judy Novak book!  
Packetstand.com  
  
Blending In:  
Many attackers today abuse services and protocols your environment uses every day, such as SSH, RDP, Citrix, OWA.  
The goal is to use a protocol which is normal, many times with a valid user ID and password for the target environment.  
Makes detection far more difficult.  
Many attacks will use and exploit/payload combination on the initial attack, but will quickly switch to stolen valid user credentials as soon as possible.  
  
  
IDS/IPS Evasion - Defense:  
Preparation:  
Keep your IDS and IPS up to date.  
Supply IDS and IPS with recommended resources (network performance, processor, RAM and hard drive).  
For sensitive systems, use host-based IDS in addition to network-based IDS and IPS.  
Implement User Behavioral Analytics.  
Utilize Host Based IDS/IPS systems.  
  
Identification:  
IDS signatures indicate heavy fragmentation or overlapping TCP Segments.  
IPS can block odd packets fragments.  
  
Vulnerability Scanners:  
- can help map a network, scan for open ports, and find various vulnerabilities  
- test against a list of known exploits  
- we need to use security in-dept  
- multi-layered, sound architecture needed  
  
Generate pretty reports:  
Information overload.  
What do you do with a 2,000-page report.  
  
  
Many commercial scanners are available:  
Rapid7 Nexpose (rapid7.com)  
SAINT (saintcorporation.com)  
BeyondTrust Retina Network Security Scanner (www.eeye.com)  
Nessus, by Tenable Network Security (tenablesecurity.com)  
OpenVAS, a fork of the previous free, open-source version of Nessus 2.  
  
Some commercial services offer these features (as web-based application service providers), such as:  
Qualsys and McAfee FoundScan.  
  
Nessus is great!  
Is has plug-ins that are characterized as 'dangerous' and they may impact targets with crashes, locked-out accounts, 'Safe Checks' is the GUI option that turns off dangerous plug-ins, these dangerous plug-ins are disabled by default.  
  
  
Nessus uses the NASL (Nessus Attack Scripting Language).  
Make sure it updates, as it does every 24 hours or invoke the manual update by running 'nessus-update-plugins' script.  
  
Defenses:  
Close ports, shut off unneeded services, apply all system patches (run Win updates), run creds scans of your environment, review results sorts by plugin ID!!! Not by IP address!  
  
Identification:   
Utilize intrusion detection system signatures.  
Most vulnerability scanners tip hundreds of signatures.  
  
Nessus Lab:  
$ sudo systemctl start nessusd  
$ firefox https://localhost:8834 &  
# systemctl stop nessusd  
  
  
The user/pass for Nessud in Slingshot is root/!nessuspw!  
  
Run Nessus and export the results to HTML, based on Plugins.  
  
The smartest way to secure a network, after scanning with Nessus, is to export based on the vulnerability found and then fixing the vulnerability itself on all the machines, instead of taking a vulnerable machine at a time.  
  
  
2.7 SMB Sessions:  
  
SMB is a Layer 7 protocol that implements file and printer sharing, domain auth, remote admin, and other features.  
Used in Windows environments; client tools include File Explorer, net use command, reg command, sc command, Sysinternals psexec tool, and more.  
Supported in Linux and UNIX via SAMBA client tools (smbclient, smbmount, rpcclient, and more) and smb daemon.  
Heavily used in post exploitation to avoid detection.  
Accessed via TCP port 445 on modern systems.  
In older systems (WinNT, Win2K) systems, SMB is carried over NetBIOS, which uses TCP and UDP ports 135-139.  
  
Establishing an SMB Session from Windows:  
  
On Windows machines, the net use command establishes a session:  
  
net use \\[targetIP]  
  
  
The currently logged-on user's credentials are sent via pass-through authentication.  
The default administrative share is selected (typically ipc$, but other shares such as admin$, c$ or others may be connected.  
  
To Connect to another user or to a specific share, use:  
  
net use \\[targetIP]\[ShareName] [password] /u:[UserName]  
  
  
  
That user does not need to be in the admin group to connect to ipcs$ or other open shares (although c$ and admin$ require admin privs).  
If you leave off the [password], Windows prompts for it.  
  
To connect as no user (or anonymous or NULL SMB session), use  
net use \\[targetIP] "" /u:""  
- a NULL SMB session has a blank username and password.  
  
  
Interrogating targets via SMB Sessions:  
- to view accessible shares, establish SMB session as a given user via "net use" and run:  
net view \\[TargetIP]  
  
- we can see more if we use a tool that enumerates other information across an SMB session:  
enum -U     (pulls list of users)  
enum -G        (pulls groups and membership)  
enum -P        (pulls password policy information)  
  
Enum uses a NULL SMB Session:  
- use -u [UserName] -p [password] for an authenticated session in Enum.  
  
  
First three commands:  
net view  
  
users:  
net user /domain   
Put users from above into users.txt  
  
Now, we crack passwords:  
@FOR /F %n in (users.txt) DO @FOR /F %p in (pass.txt) DO @net use  
\\DomainController\IPC$ /user:DOMAIN\%n %p 1>NUL 2>&1 &&echo [\*] %n:%p && @net use /delete  
 \\DomainController\IPC$ > NUL  
  
Choose a very good password and spray it throughout an environment. One password at a time!  
This can help avoid domain account lockout for user accounts!  
Service accounts are different than user accounts. User accounts will most likely lock out, but service account, should never be setup to lockout. This can become an IT management overhead to always unlock an account!  
  
  
  
PowerShell Empire:  
Backdoor built in PowerShell.  
Fantastic post-exploitation scanning abilities!  
Family of modules under Situational Awareness:  
- situational\_awareness/network/sharefinder: find accessible shares  
- situational\_awareness/network/arpscan: ARP scan the local IPv4 systems  
  
Also has the ability to map domain trusts, group membership, portscan and conduct reverse DNS lookups.  
Uses built in Microsoft Protocols like SMB.  
www.powershellempire.com  
  
Bloodhound:  
A tool which graphs the quickest way to get domain admin.  
For example:  
1. Gain Access to a Domain user.  
2. Find all systems (sometime out of 1000's) where DOmain Users (or your group) is in the Local Administrators group.  
3. Find one of those systems where a Domain Admin is logged on.  
4. Steal the Domain Admin's access.  
  
Free at:  
https://github.com/adaptivethreat/BloodHound.  
  
  
Establishing SMB Sessions from Linux to Windows via smbclient  
- use the smbclient tool to establish an SMB session from Linux to Windows.  
- to list available shares  
  
smbclient -L [WinIPaddr] -U [username] -p 445  
Enter the password when prompted.  
  
To connect to an SMB share and pull files interactively (behaving like an FTP client)  
$ smbclient //[WinIP addr]/test -U [username] -p 445  
  
Enter the password when prompted.   
You will get an "smb:\>" prompt  
Use "ls" for directory listing, "cd" to change directories, and "get" to get files.  
  
Use Linux rpcclient tool can pull even more information.  
Establish a session with:  
$rpcclient -U [username] [WinIPaddr]  
  
Enter the password when prompted.  
  
You have an rpcclient prompt with many commands available:  
enumdomusers: list users  
  
enumalsgroups [domain]|[builtin]: list groups  
lsaenumsid: show all users SIDs defined on the box  
lookupnames [name]: show SID associated with user- or group name  
lookupsids [sid]: show username associated with SID  
srvinfo: show OS type and version.  
  
  
The rpcclient man page lists hundreds of other commands.  
- those listed here are the most useful and a lab covers them shortly!  
  
  
Seeing and Dropping SMB Sessions:  
On Windows, to see where you have established outbound SMB sessions run:  
> net use  
  
- to drop an outbound SMB session, run:  
> net use \\[IPaddr] /del  
  
- on Windows, to see who has established inbound SMB sessions (you are acting as an SMB server), run:  
> net session  
  
- to drop an inbound SMB session, run:  
> net session \\[IP addr] /del  
  
  
Preparation: Defenses Against Evil SMB sessions:  
Modify registry for   
RestrictAnonymous  
RestrictAnonymousSAM  
EveryoneIncludesAnonymous  
  
These only block information for NULL SMB Sessions.  
Good idea, but even with these settings, an attacker can enumerate all info with one valid username and password.  
  
DON'T set these registry up on a DOMAIN Controller or Exchange Server!!!!  
  
Preparation (cont.):  
Block access to the following ports across network boundaries and local firewalls where SMB sessions are not required for admin or file share usage.TCP/UDP 445: MS Server Message Block  
TCP 135: RPC/DCE Endpoint mapper  
  
TCP 137: NetBIOS Name Service  
  
TCP 138: NetBIOS Session Service  
  
TCP 139: NetBIOS Session Service  
  
  
Of course, block all ports except those required!  
  
Alternatively, allows access to these ports only from systems or networks that absolutely require SMB access to a given destination (such as file servers and domain controllers).  
  
Private VLAN (PVLANs) are a switch feature that can help implement this.  
  
Identification:  
Check for access to the ports listed above in logs and IDS alerts.  
  
  
Workstations should never communicate with each other; only workstations should communicate with servers!  
  
  
LAB Time:  
SMB Sessions with net use, smbclient and rpcclient!  
  
Lab goals:  
- Open and list SMB Sessions with "net use" and "net session"  
  
  
- enumerate various settings with enum on Windows  
- make smbclient and rpcclient connections from Linux to Windows  
- enumerate the target with rpcclient on Linux  
- drop SMB sessions  
  
Make sure that your Windows machine is ready.  
- we return to some common defaults.  
  
  
net use  
net session  
  
net use \* /del  
  
net use  
net session  
  
Make sure that your Linux machine can ping Windows  
C:\> ping 10.10.75.1  
  
#ping 10.10.0.1  
  
  
If you can't ping, double-check that you disabled your firewall (from an elevated command prompt on Windows)  
  
c:\> netsh firewall set opmode disable   
  
or  
  
c:\> netsh advfirewall set allprofiles state off   
(for Windows 8+ systems)  
  
$sudo ifconfig eth0 10.10.75.1 netmask 255.255.0.0  
  
$sudo iptables -F  
  
  
$ smbclient -L 192.168.2.203 -U win7user  
(type password at prompt)  
  
$ rpcclient 192.168.2.203 -U administrator  
(type password at prompt)  
  
enum  
enumdomusers  
help  
getusername  
srvinfo  
enumdomains  
querydominfo  
enumalsgroups domain  
enumalsgroups builtin  
lookupname administrator  
lookupname administrators  
queryaliasmem builtin 544  
queryuser 500  
  
In the lab, we covered how to  
- create Windows accounts at the command line  
- Make SMB Sessions with the Windows 'net use' command  
- analyze and drop SMB sessions with 'net use' and 'net session'  
- use Linux rpcclient to enumerate users, groups, group membership, and other detailed account information  
- these are immensely useful capabilities for attackers...and incident handlers.  
  
################# End Part 1 ####################