

Information Gathering

Sources:

- *Hacking Exposed*, 6th edition, by S. McClure, J. Scambray, and G. Kurtz
- *Hackers Beware* by E. Cole

Through *reconnaissance*, an attacker can gather a large amount of information about a site.

This information can be used to plan an attack.

It can be obtained with freely available tools.

Steps and tools used in gathering information [Cole]:

1. *Obtain initial information:*
 - Open source search
 - Whois
 - Nslookup
2. *Determine address range of network:*
 - ARIN (American registry for internet numbers)
 - Traceroute
3. *Find active machines:*
 - Ping
4. *Find open ports or access points:*
 - Portscanners
 - Nmap
 - Scanport
 - War Dialers
 - THC-Scan
5. *Determine the operating system:*
 - Quesco
 - Nmap

6. *Determine which services are running on each port:*

- Default port and OS
- Telnet
- Vulnerability scanners

7. *Map out the network:*

- Traceroute
- Visual ping
- Cheops

Footprinting

Footprinting is the initial stage of gathering information.

An attacker uses it to develop a profile of an organization's computing resources and security.

Information that can be obtained by footprinting [Scambray *et al*]:

Technology	Identifies
Internet	Domain name Network blocks Specific IP addresses reachable via the Internet TCP and UDP services running on each system Hardware system architecture Access control mechanisms and lists Intrusion detection systems User and group names, routing tables, SNMP information
Intranet	Networking protocols Internal domain names Network blocks IP addresses of reachable systems TCP and UDP services Hardware system architecture Access control mechanisms and lists Intrusion detection systems User and group names, routing tables, SNMP information
Remote access	Analog/digital telephone numbers Remote system type Authentication mechanisms
Extranet	Connection origination and destination Type of connection Access control mechanisms

Open Source Search

Much information useful on an organization is often provided by the organization itself.

Information often provided in organizations' web pages:

- Locations
- Related companies
- Merger or acquisition news
- Phone numbers
- Contact names and email addresses
- Privacy and security policies indicating the security mechanisms in place
- Links to other web servers related to the organization

Information not intended for public viewing may be embedded in HTML source code comments.

Other information about an organization can be obtained by web searches, e.g., news articles and press releases.

For example, there may be news stories about security incidents.

News group postings may contain questions from an organization's staff indicating vulnerabilities.

The Securities and Exchange commission EDGAR database contains information about mergers and acquisitions. See www.sec.gov.

Merging organizations often have problems managing their Internet connections.





















Such information must be made publicly available.

Network Enumeration

Network enumeration is the process of discovering the structure of an organization's network.

The first step of network enumeration is to identify domain names and networks related to the organization.

There are multiple *whois* databases that provide such information about organizations, e.g.,

#1 Domain Names International, Inc.	US		 Contact Information
007 Names, Inc.	US		 Contact Information
1 eNameCo	US		 Contact Information
123 Registration.com	US		 Contact Information
1st Domain.net	US		 Contact Information
A+ Net	US		 Contact Information
A Technology	Canada		 Contact Information
Active ISP ASA	Norway		 Contact Information
Address Creation	US		 Contact Information
AWRegistry	US		 Contact Information

Types of whois queries:

- *Registrar* – Displays registrar information and associated whois servers
- *Organizational* – Displays all information related to a particular organization
- *Domain* – Displays all information related to a particular domain
- *Network* – Displays all information related to a particular network or IP address
- *Point of Contact* – Displays all information related to the administrative contact

Example: Domain query

```
C:\>jwhois case.edu -h whois.educause.net  
[Querying whois.educause.net]  
[whois.educause.net]
```

Domain Name: CASE.EDU

Registrant:

Case Western Reserve University
10900 Euclid Avenue
Cleveland, OH 44106
UNITED STATES

Contacts:

Administrative Contact:

Jeffrey A. Gumpf
Case Western Reserve University
Information Technology Services
Crawford Hall, Room 428 Attn: Jeff Gumpf
Cleveland, OH 44106
UNITED STATES
(216) 368-5893
gumpf@cwru.edu

Technical Contact:

Same as above

Name Servers:

NS.CWRU.EDU 129.22.4.1
NS2.CWRU.EDU 129.22.4.3
NS1.OAR.NET
NS2.OAR.NET

Domain record activated: 25-Jun-1998

Domain record last updated: 30-Oct-2003

Example: Network query

```
C:\>jwhois 129.22.151.35
[Querying whois.arin.net]
[whois.arin.net]
```

```
OrgName:      Case Western Reserve University
OrgID:        CWRU
Address:      10900 Euclid Avenue
City:         Cleveland
StateProv:    OH
PostalCode:   44106
Country:      US
```

```
NetRange:     129.22.0.0 - 129.22.255.255
CIDR:         129.22.0.0/16
NetName:      CWRUNET
NetHandle:    NET-129-22-0-0-1
Parent:       NET-129-0-0-0-0
NetType:      Direct Assignment
NameServer:   NS.CWRU.EDU
NameServer:   NS2.CWRU.EDU
NameServer:   NCNOC.NCREN.NET
Comment:
RegDate:      1988-03-03
Updated:      1999-10-22
```

```
RTechHandle:  JAG3-ARIN
RTechName:     Gumpf, Jeffrey A
RTechPhone:    +1-216-368-2982
RTechEmail:    Gumpf@ins.cwru.edu
```

```
OrgTechHandle: EWC1-ARIN
OrgTechName:   Chan, Eric W
OrgTechPhone:  +1-216-368-1089
OrgTechEmail:  chan@po.cwru.edu
```

```
# ARIN WHOIS database, last updated 2006-01-17 19:10
# Enter ? for additional hints on searching ARIN's WHOIS
database.
```

Network Details from ARIN WHOIS server may contain some of the fields below:

OrgName- OrgID:	<p>The organization (or division within an organization) who manages the network. OrgID is a unique identifier of an organization.</p> <p>If the value of the NetType is not Direct Assignment, this organization could be the network provider for your target organization.</p>
NetRange:	Range of IP Addresses allocated to OrgName.
CIDR:	CIDR stands for Classless Inter-Domain Routing . CIDR is another way to express NetRange, it shows the range of IP Addresses allocated to OrgName.
NetName	The registered network name for the IP addresses.
NetHandle	A unique name that identify the network.
Parent:	<p>Net Handle of the parent network. A parent is an organization that has been allocated address space from RIR or another ISP, with the intention of sub-delegating that space.</p> <p>Type of IP Addresses assignment. It can be one of these types:</p>
NetType:	<p>Direct Assignment: IP addresses are registered to an organization for use within the Internet infrastructure it operates, not for sub-delegation of those addresses.</p> <p>Reallocated: IP addresses are allocated to an organization for use in their internal networks or for further sub-delegation.</p> <p>Reassigned: IP addresses are assigned to an organization from a parent organization for use in their internal networks.</p>
NameServer:	A name server maintains a directory of domain names and their matching IP addresses.
RegDate:	Registration date of this record.

(gadget.stringcodes.com/quis/q-interpret.html)

DNS Interrogation

The *Domain Name System* (*DNS*) is a distributed database used to map IP addresses to hostnames and vice-versa.

If DNS is configured insecurely, it can be used to obtain revealing information about an organization.

One of the worst configuration errors is to allow untrusted Internet users to perform a DNS zone transfer.

A *zone transfer* allows a secondary master server to update its zone database from the primary master.

Many DNS servers are misconfigured to provide a copy of the zone to anyone who asks.

This is a problem if an organization doesn't segregate public and private DNS information.

Then internal hostnames and IP addresses can be revealed to an attacker.

Hardware platforms and operating systems can also be revealed.

Example:

```
C:\Documents and Settings\Andy>nslookup
```

```
Default Server:  home
```

```
Address:  192.168.1.254
```

```
> ns.cwru.edu
```

```
Server:  home
```

```
Address:  192.168.1.254
```

```
Non-authoritative answer:
```

```
Name:      ns.cwru.edu
```

```
Address:  129.22.4.1
```

```
> set type=any
```

```
> ls -d cwru.edu > \tmp\zone_out
```

```
*** Can't list domain cwru.edu: BAD ERROR VALUE
```

```
The DNS server refused to transfer the zone  
cwru.edu to your computer.
```

Network Reconnaissance

The topology of a network can be explored with tools like *traceroute*:

Trace Route from MIT

IMPORTANT: This tool works by sending a series of UDP packets with different port numbers and TTL (Time To Live). If you are running firewall software, your software may interpret the incoming packets as a hostile "port scan" originating from this server (jis.mit.edu). Rest assured, your system is not being attacked.

```
1  W92-RTR-1-W92SRV21.MIT.EDU (18.7.21.1)  0.744 ms  0.327 ms
   0.242 ms
2  EXTERNAL-RTR-2-BACKBONE.MIT.EDU (18.168.0.27)  0.503 ms  0.485 ms
   0.370 ms
3  g3.ba21.b002250-1.bos01.atlas.cogentco.com (38.112.2.213)  1.342 ms
   1.106 ms  0.993 ms
4  g9-2.core01.bos01.atlas.cogentco.com (66.250.14.209)  1.291 ms
   1.326 ms  1.196 ms
5  p5-0.core01.jfk02.atlas.cogentco.com (66.28.4.118)  6.522 ms
   6.586 ms  6.586 ms
6  p5-0.core01.jfk01.atlas.cogentco.com (66.28.4.9)  7.056 ms
   6.608 ms  6.419 ms
7  pl3-0.core01.ewr02.atlas.cogentco.com (154.54.3.146)  6.916 ms
   6.454 ms  6.622 ms
8  151.164.251.17 (151.164.251.17)  11.685 ms  11.721 ms  11.816 ms
9  bb2-p2-0.nycmny.sbcglobal.net (151.164.42.144)  188.097 ms
   140.105 ms  57.481 ms
10 bbl-p6-0.nycmny.sbcglobal.net (151.164.42.160)  11.943 ms
    12.784 ms  11.693 ms
11 core1-p4-0.crnyny.sbcglobal.net (151.164.240.34)  12.006 ms
    14.007 ms  12.112 ms
12 core2-p3-0.crcloh.sbcglobal.net (151.164.188.173)  22.531 ms
    22.433 ms  23.404 ms
13 bbl-p5-1.bcvloh.sbcglobal.net (151.164.241.6)  23.609 ms  22.780 ms
    23.504 ms
14 dist1-g3-1.bcvloh.sbcglobal.net (151.164.43.153)  22.854 ms
    23.634 ms  22.769 ms
15 rback3-g1-0.bcvloh.sbcglobal.net (66.73.20.234)  24.291 ms
    23.858 ms  23.449 ms
16 adsl-68-250-210-210.dsl.bcvloh.ameritech.net (68.250.210.210)
    72.709 ms  79.162 ms  74.207 ms
```


Graphical tools like *VisualRoute* provide additional information:

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		12.88.115.23	-	*			0 528	AT&T ITS
1		199.70.3.58	-	Parsippany, NJ		94		AT&T EasyL
2		199.70.3.49	-	Parsippany, NJ		139		AT&T EasyL
3		12.122.253.24	gbr6-p21.n54ny	New York, NY, U	-5.0	128		AT&T ITS
4		12.122.5.114	gbr3-p90.n54ny	New York, NY, U	-5.0	185		AT&T ITS
5		12.123.1.121	ggr1-p360.n54ny	New York, NY, U	-5.0	157		AT&T ITS
6		192.205.32.17	att-gw.ny.verio.r	New York, NY, U	-5.0	174		AT&T Data C
7		129.250.2.14	p4-1-3-0.r01.ch	Chicago, IL, US	-6.0	203		Verio, Inc.
8		129.250.2.253	p4-6-0.r00.chcg	Chicago, IL, US	-6.0	197		Verio, Inc.
9		129.250.4.89	p4-4-0.r00.dlilst	Dallas, TX, USA		234		Verio, Inc.
10		129.250.3.74	p4-1-0-0.r01.dlilst	Dallas, TX, USA		221		Verio, Inc.
11		129.250.2.41	p1-0-0-0.r01.on	Orem, UT, USA	-7.0	269		Verio, Inc.
12		129.250.29.20	pvu1.wwhpvu1.v	Provo, UT, USA	-7.0	252		Verio, Inc.
13		192.41.43.189	visualroute.com	Highland, UT 8		265		Icon Develo
Roundtrip time to visualroute.com, average = 265ms, min = 195ms, max = 448ms -- 20-Apr-01								

Intrusion detection systems can detect network reconnaissance and generate fake responses.

Scanning

Scanning is used to:

- Determine which machines in a network are active
- Find open ports or access points
- Determine the services running on each port
- Determine the operating system

Network Ping Sweeps

A *ping sweep* of a range of IP addresses and network blocks can be used to determine if individual systems are *alive*.

Ping is traditionally used to send **ICMP ECHO** packets to a target system.

If the target is alive, it will reply with an ICMP **ECHO_REPLY** packet.

Tools like *fping* send out many ping requests at once.

Example:

```
$ gping 192 168 1 1 254 | fping -a
192.168.1.254 is alive
192.168.1.227 is alive
...
192.168.1.3 is alive
192.168.1.2 is alive
192.168.1.1 is alive
...
```

Note that ICMP may be blocked at a border router or firewall; in this case, port scans, etc. can be used.

Ping Sweep Countermeasures

Detecting ping sweeps is crucial to anticipating attacks and identifying the attacker.

They are detected by *network intrusion detection systems* (NIDSs).

The types of ICMP traffic that are allowed should be minimized.

Access control lists can also be used to limit ICMP traffic to specific addresses.

ICMP Queries

ICMP can be used to obtain other valuable information about a system.

For example, the UNIX tool *icmpquery* you can request:

- The time on a system
- The subnet mask of a particular device

(The *subnet mask* is a bit mask for determining what subnet an IP-address belongs to.)

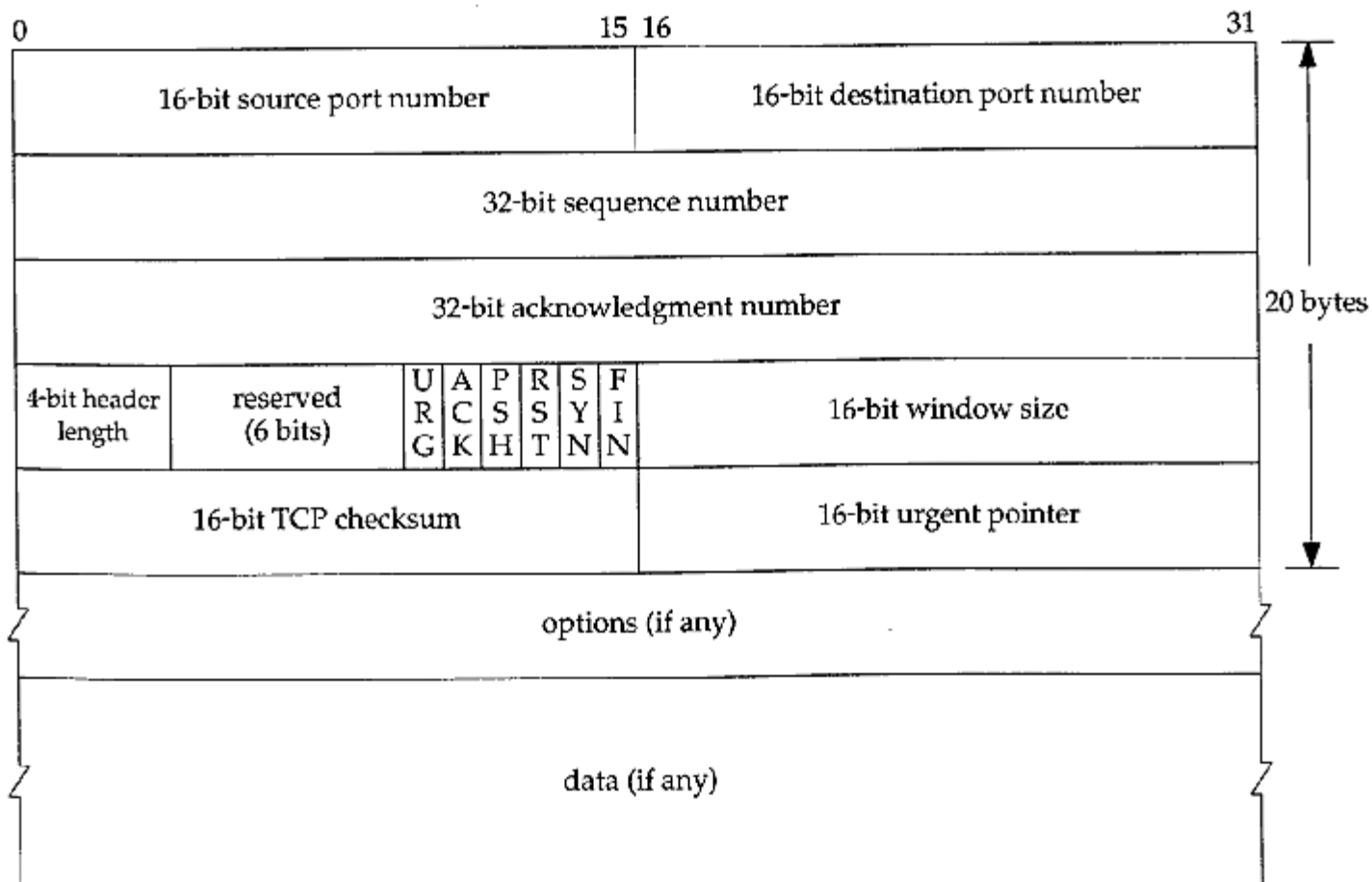
To prevent ICMP queries, you can configure your border routers so they don't respond to them.

Port Scanning

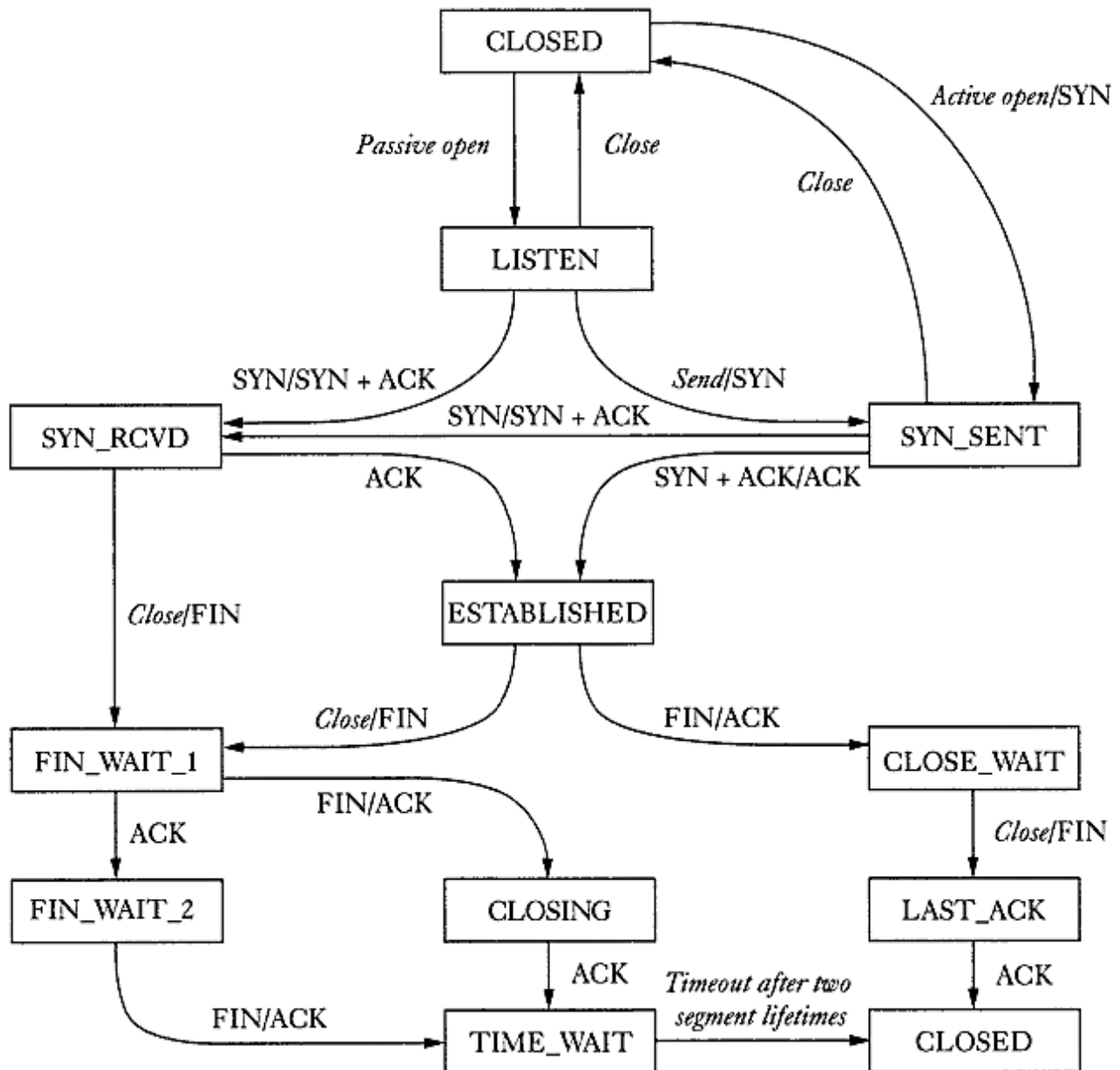
Port scanning is the process of connecting to TCP and UDP ports on a target system to identify:

- The TCP and UDP services running on the target system
- The type of operating system on the target system
- Specific applications or versions of a particular service

TCP Header



TCP State Transition Diagram



TCP Three-Way Handshake

TCP A

TCP B

- | | | |
|----------------|---------------------------------------|------------------|
| 1. CLOSED | | LISTEN |
| 2. SYN-SENT | --> <SEQ=100><CTL=SYN> | --> SYN-RECEIVED |
| 3. ESTABLISHED | <-- <SEQ=300><ACK=101><CTL=SYN,ACK> | <-- SYN-RECEIVED |
| 4. ESTABLISHED | --> <SEQ=101><ACK=301><CTL=ACK> | --> ESTABLISHED |
| 5. ESTABLISHED | --> <SEQ=101><ACK=301><CTL=ACK><DATA> | --> ESTABLISHED |

Scan Types

Scan types implemented by *nmap* tool [Scambray]:

TCP connect scan:

- Connects to target port and completes three-way handshake (SYN, SYN/ACK, ACK).
- Easily detected.

TCP SYN scan (half-open scanning):

- SYN packet sent to target port.
- If SYN/ACK is received, port is in listening state.
- If RST/ACK is received, port is probably not listening.
- RST/ACK is sent by scanner so full connection is not established.
- May not be logged by target system.

TCP FIN scan:

- Sends FIN packet to target port.
- Target system should send back RST if port is closed (RFC 793).
- Some systems send RST regardless of port state.

TCP Null scan:

- Turns off all TCP flags.
- Target system should send back an RST for all closed ports.

TCP ACK scan:

- Used to map out firewall rule sets.
- Can help determine if firewall is simple packet filter allowing only established connections or a stateful firewall performing advanced packet filtering.

TCP Windows scan:

- May detect open as well as filtered/non-filtered ports on some systems.
- Exploits anomaly in how TCP window size is reported.

TCP RPC scan:

- Used to identify remote procedure call (RPC) ports and associated program and version number.
- Specific to UNIX systems.

UDP scan:

- Sends UDP packet to target port
- If target port responds with “ICMP port unreachable”, port is closed
- No response suggests port is open
- Unreliable and slow with device that does packet filtering

Example: *nmap* [Scambray, *et al*]

```
nmap -sS 192.168.1.1
Starting nmap V. 2.53 by fyodor.insecure.org
Interesting ports on (192.168.1.11):
```

(The 1504 ports scanned but not shown below are in state: closed)

Port	State	Protocol	Service
21	open	tcp	ftp
25	open	tcp	smtp
42	open	tcp	nameserver
53	open	tcp	domain
79	open	tcp	finger
80	open	tcp	http
81	open	tcp	hosts2-ns
106	open	tcp	pop3pw
110	open	tcp	pop-3
135	open	tcp	loc-srv
139	open	tcp	netbios-ssn
443	open	tcp	https

Port Scanning Countermeasures

Detecting port scans may indicate when an attack is likely.

The primary method of detecting port scans is to employ *intrusion detection systems*.

Firewalls can also be configured to detect port scans.

When a scan is detected, alerts can be sent via email.

To reduce a system's exposure, unnecessary services should be *disabled*.

Operating System Detection

The operating system running on a target system can be determined in several ways:

- Getting banner information from services like FTP, telnet, SMTP, HTTP, POP, etc.
- Examining the set of active services
- Stack fingerprinting

Stack fingerprinting recognizes nuances in different vendors IP stack implementations.

Types of active stack fingerprinting probes [Scambray]:

- *FIN probe*:
 - FIN packet sent to open port.
 - Many implementations (e.g., Windows) respond with FIN/ACK.
- *Bogus flag probe*:
 - Undefined TCP flag is set in header of SYN packet.
 - Some OSs (e.g., Linux) will send response packet with flag set.
- *Initial Sequence Number (ISN) sampling*:
 - Looks for pattern in initial sequence chosen by TCP implementation when responding to connection request.
- *“Don’t fragment bit” monitoring*:
 - Some OSs set this bit to enhance performance.
- *TCP initial window size*:
 - Initial window size on returned packets is tracked.

- Size is unique for some implementations.
- *ACK value*:
 - IP stacks differ in the sequence value they use for the ACK field (some increment the one you sent, some don't).
- *ICMP error message quenching*:
 - OSs may follow RFC 1812 and limit the rate at which error messages are sent.
 - This rate can be checked by sending UDP packets to a random high numbered port.
- *ICMP message quoting*:
 - OSs differ in the amount of information quoted when ICMP errors occur.
- *ICMP error message-echoing integrity*:
 - Some stack implementations may alter the IP headers when sending back ICMP error messages.
- *Type of service (TOS)*:

- For “ICMP port unreachable” messages, the TOS may vary with the implementation.
- *Fragmentation handling:*
 - Different stack implementations handle overlapping packet fragments differently.
 - Some stacks will overwrite the old data with the new data or vice versa during reassembly.
- *TCP options:*
 - Sending a packet with multiple TCP options set (e.g., no operation, maximum segment size, window scale factor, and timestamps) may help identify an OS.

Passive Stack Fingerprinting

Dynamic stack fingerprinting involves sending packets to the target system.

It is relatively easy for network-based IDS system to detect.

In *passive stack fingerprinting*, an attacker passively monitors network traffic to determine the OS in use.

Attributes of TCP/IP session that can be used to identify an OS [Scambray, *et al*]:

- *TTL*: What does the OS set as the *time-to-live* on an outbound packet?
- *Window size*: What does the OS set as its window size?
- *DF*: Does the OS set the *Don't Fragment* bit?
- *TOS*: Does the OS set the *type of service*, and if so, at what?

Tools like *siphon* compare observed attribute values to those in a fingerprint database to identify and OS.

Enumeration

Enumeration involves using active probing to obtain information about:

- Commonly misconfigured network resources and shares
- Users account names
- Older software versions with known vulnerabilities

It involves active connections and directed queries.

Since enumeration is intrusive, it “should” be detected.

Enumeration techniques tend to be OS-specific.

Banner Enumeration

Banner grabbing means connection to a remote application and observing the output.

Banners can provide information that is valuable to attackers.

Many port scanning tools do banner grabbing automatically.

It can be done manually using `telnet` and `netcat`.

Example:

```
telnet www.naiveuniversity.edu 80
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/5.0
Date: Thu, 14 March 2002 00:36:54 GMT
Content-Type: text/html
Content-Length: 87
```

```
<html><head><title>Error</title></head><body>The
parameter is incorrect. </body></html>
```

Windows NT/2000 Enumeration

Windows NT is vulnerable to enumeration due to the *Common Internet File System/Server Message Block* (CFIS/SMB) and *NetBIOS* data transport protocols.

Windows 2000 can run TCP/IP instead of NetBIOS, but uses NetBIOS by default.

The *Windows NT Resource Kit* (NTRK) and the Windows 2000 version (*W2RK*) contain utilities that are valuable to both administrators and to attackers.

Null Sessions

CIFS/SMB and NetBIOS provide APIs that return rich information about a machine via TCP port 139.

This information is available even to unauthenticated users.

These APIs can be accessed remotely by creating an unauthenticated connection to port 139 using the “null session” command:

```
net use \\192.168.202.33\IPC$ "" /u: ""
```

This connects to the hidden interprocess communication “share” (IPC\$) at IP address 192.168.202.33 as the built-in anonymous user (/u: "") with a null (") password.

Null sessions can be prevented by filtering ports 135-139 at perimeter network access devices.

NT Service Pack 3 and Windows 2000 provide mechanisms to prevent enumeration of sensitive information over null sessions.

Windows Network Resource Enumeration

The *net view* command is a built-in enumeration tool in Windows:

```
$net view /domain
```

```
Domain
```

```
-----
```

```
ADSTEST
```

```
ARRG
```

```
ATEUCLID
```

```
COLECOVISION
```

```
COMPBIO
```

```
CSE_DEAN
```

```
DATABASE
```

```
EECS
```

```
ESCI 602
```

```
ESCI 710
```

```
KUSCH
```

```
MAE
```

```
MUDSLUT
```

```
OPTIMIZER
```

```
ROHAN
```

```
SCSI-NET
```

```
SOFTLAB
```

```
SOFTWARELAB
```

```
UTI
```

```
WORKGROUP
```

```
The command completed successfully.
```

net view can also list computers in a particular domain:

```
net view /domain:softlab
```

Server Name	Remark
-------------	--------

\\SOFTENG4-2	
--------------	--

The command completed successfully.

The *nbtstat* command gets the NetBios *Name Table* from a remote system:

```
nbtstat -A 251.45.151.62
Local Area Connection:
Node IpAddress: [251.45.151.62] Scope Id: []
```

NetBIOS Remote Machine Name Table

Name	Type	Status

KARUNA	<00> UNIQUE	Registered
SOFTWARELAB	<00> GROUP	Registered
KARUNA	<20> UNIQUE	Registered
SOFTWARELAB	<1E> GROUP	Registered
SOFTWARELAB	<1D> UNIQUE	Registered
..__MSBROWSE__.	<01> GROUP	Registered
MAC Address = 00-B4-D0-C3-E2-7E		

nbtstat extracts the system name, its domain, logged-on users, services running, and the MAC address.

The *nltest* tool identifies the Primary and Backup Domain controllers, which hold NT network authentication credentials:

```
nltest /dclist:elves
List of DCs in Domain elves
  \\SLEEPY (PDC)
  \\GRUMPY
  \\DOPEY
```

With a null session established, *net view* can enumerate shares on remote systems:

```
C:\net view \\sleepy
```

```
Shared resources at \\134.234.8.33
```

```
SLEEPY
```

Share name	Type	Used as	Comment
NETLOGON	Disk		Logon server share
Pub	Disk		Public access

The command completed successfully.

Windows SNMP Enumeration

Windows NT/2000 systems may provide sensitive information to unauthorized users via the *Simple Network Managment Protocol* (SNMP).

The SNMP service permits remote management of network components.

The default configuration of the NT SNMP Service answers to the SNMP *community name* “public”.

This is given read-write permissions.

The default configuration of the Windows 2000 SNMP Service allows any user to access SNMP parameters in the Registry.

These can be used to monitor or reconfigure machines in a community.

SNMP can be used to obtain information about:

- Running services
- Share names
- Share paths
- Comments on shares
- User names
- Domain name

To avoid this, the SNMP Service can be turned off, or it can be configured more securely.

Access to TCP and UDP ports 161 (SNMP GET/SET) should be disabled at all perimeter network access devices.

Windows User and Group Enumeration

Scambray, *et al*: 50% of the effort in cracking and account is done once the username is obtained.

Given usernames, an attacker can use password cracking programs to gain access.

Several user enumeration techniques require a null session.

Some exploit NetBIOS.

Others employ SNMP and Windows 2000 Active Directory.

Example: Enumerating users with *enum* (bindview.com):

```
server: 133.44.171.49
setting up session... success.
password policy:
  min length: none
  min age: none
  max age: 42 days
  lockout threshold: none
  lockout duration: 30 mins
  lockout reset: 30 mins
opening lsa policy... success.
server role: 3 [primary (unknown)]
names:
  netbios: MOE
  domain: STOOGES
quota:
  paged pool limit: 33554432
  non paged pool limit: 1048576
  min work set size: 65536
  max work set size: 251658240
  pagefile limit: 0
  time limit: 0
trusted domains:
  indeterminate
netlogon done by a PDC server
getting user list (pass 1, index 0)... success, got 3.
Administrator (Built-in account for administering the computer/domain)
attributes:
  groucho attributes:
  harpo attributes:
  zeppo attributes:
Guest (Built-in account for guest access to the computer/domain)
attributes: disabled no_passwd
```