Information Gathering

Sources:

- *Hacking Exposed*, 2nd edition, by J. Scambray, S. McClure, 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
    - 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 rearchable 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 for 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 HTLM 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.

USENET 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	We Put YOU First.	Contact information
007 Names, Inc.	US	007Names.com	Contact information
1 eNameCo	US	1eNameCo Customer Service 1st	Contact information
123 Registration.com	US	1 2 3 Registration.com	Contact information
1st Domain.net	US	1stDomain.net Domain Registration	Contact information
A+ Net	US	NAMES4EVER	Contact information
A Technology	Canada	identifyourself.com	Contact information
Active ISP ASA	Norway	active isp	Contact information
Address Creation	US	address creation	Contact information
AWRegistry	US	AW Registry	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: Registrar query

```
$ whois "nytimes."

Whois Server Version 1.3

Domain names in the .com, .net, and .org domains
can now be registered
with many different competing registrars. Go to
http://www.internic.net
for detailed information.

Aborting search 50 records found .....
NYTIMESLIPS.COM
NYTIMESLEADER.COM
NYTIMESJOBS.NET
NYTIMESJOBS.COM
NYTIMESINFO.COM
NYTIMESHOMEDELIVERY.COM
NYTIMESGLOBAL.NET
NYTIMESGLOBAL.COM
NYTIMESFCU.ORG
NYTIMESDIGITAL.COM
...
```

Example: Domain query

```
whois -h whois.networksolutions.com nytimeslips.com
...

Registrant:
Esquire Consultant Group, Ltd. (NYTIMESLIPS-DOM)
   80 Bay Street Landing, Suite 4B
   Staten Island, NY 10301
   US

   Domain Name: NYTIMESLIPS.COM

   Administrative Contact, Billing Contact:
     McKenzie, Ari (WDB91) amckenzie@ESQUIRELTD.COM
      Esquire Consultant Group, Ltd.
      80 Bay Street Landing, Suite 4B
      Staten Island, NY 10301
      718-815-3869
   Technical Contact:
      Hostmaster (HO1320-ORG) HOSTMASTER@NJD.XO.COM
      9NETAVE
      110 Meadowlands Pkwy
      Secaucus, NJ 07094
      US
      [No phone]

   Record last updated on 17-Aug-2000.
   Record expires on 17-Aug-2002.
   Record created on 17-Aug-2000.
   Database last updated on 20-Mar-2002 05:30:00EST

   Domain servers in listed order:

   NS2.NJD.XO.COM  216.156.2.2
   NS3.NJD.XO.COM  216.156.2.3
```

Example: Network query

```
03/20/02 16:59:18 IP block 129.22.151.35 @whois.arin.net
Trying 129.22.151.35 at ARIN
Trying 129.22.151 at ARIN
Case Western Reserve University

 (NET-CWRUNET)
   Campus Communications Network - Network Services

   Crawford Hall, Room 426

   Cleveland, OH 44106

   US

   Netname: CWRUNET
   Netblock: 129.22.0.0 - 129.22.255.255

   Coordinator:
      Gumpf, Jeffrey A  (JAG3-ARIN)  Gumpf@INS.CWRU.EDU
      (216) 368-2982

   Domain System inverse mapping provided by:

   NS.CWRU.EDU   129.22.4.1
   NS2.CWRU.EDU   129.22.4.3
   NCNOC.NCREN.NET  192.101.21.1

   Record last updated on 22-Oct-1999.
   Database last updated on  19-Mar-2002 19:58:23 EDT.
```

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.

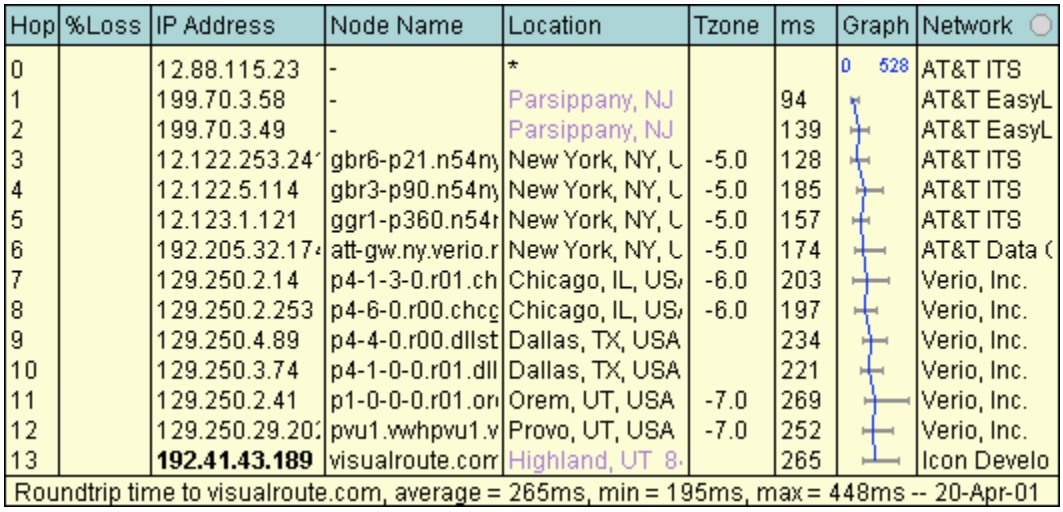
Hardware platforms and operating systems can also be revealed.

Network Reconnaissance

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

```
03/20/02 18:32:34 Fast traceroute NS1.WORLDWIDEDNS.NET
Trace NS1.WORLDWIDEDNS.NET (63.126.69.125) ...
 1 129.22.150.1      0ms    0ms    0ms  TTL:  0  (No rDNS)
 2 10.0.70.1         0ms    0ms    0ms  TTL:  0  (No rDNS)
 3 129.22.1.1        0ms    0ms    0ms  TTL:  0  (CWRU-GW.CWRU.Edu ok)
 4 192.5.110.18      0ms    0ms    0ms  TTL:  0  (No rDNS)
 5 199.18.114.109    0ms   47ms    0ms  TTL:  0  (clv2-atm2-0s2.cleveland.oar.net ok)
 6 199.18.202.2      0ms    0ms    0ms  TTL:  0  (oebc2-atm1-0-0.columbus.oar.net ok)
 7 199.18.199.16     0ms    0ms    0ms  TTL:  0  (oeb6-gigeth1-0.columbus.oar.net ok)
 8 160.81.15.21     16ms   16ms   16ms  TTL:  0  (sl-gw4-roa-0-3.sprintlink.net ok)
 9 144.232.17.205   15ms   15ms   16ms  TTL:  0  (sl-bb22-roa-2-1.sprintlink.net ok)
10 144.232.8.81     16ms   16ms   15ms  TTL:  0  (sl-bb22-chi-6-1.sprintlink.net ok)
11 144.232.26.109   16ms   16ms   16ms  TTL:  0  (sl-bb24-chi-8-0.sprintlink.net ok)
12 204.255.168.241  15ms   15ms   15ms  TTL:  0  (51.ATM1-0.BR1.CHI2.ALTER.NET ok)
13 152.63.64.118    16ms   16ms   16ms  TTL:  0  (0.so-5-0-0.XL2.CHI2.ALTER.NET ok)
14 152.63.67.109    15ms   16ms   16ms  TTL:  0  (0.so-2-0-0.TL2.CHI2.ALTER.NET ok)
15 152.63.19.170    31ms   31ms   31ms  TTL:  0  (0.so-3-0-0.TL2.DCA6.ALTER.NET ok)
16 152.63.38.74     32ms   31ms   31ms  TTL:  0  (0.so-6-0-0.XL2.DCA6.ALTER.NET ok)
17 152.63.35.117    31ms   31ms   32ms  TTL:  0  (0.so-0-0-0.XR2.DCA6.ALTER.NET ok)
18 152.63.42.46     31ms   31ms   31ms  TTL:  0  (184.at-4-0-0.XR2.PHL1.ALTER.NET ok)
19 152.63.37.21     32ms   32ms   31ms  TTL:  0  (POS7-0.GW4.PHL1.ALTER.NET ok)
20 63.111.123.198   47ms   47ms   46ms  TTL:  0  (gw3.customer.alter.net ok)
21 63.126.69.125    47ms   47ms   31ms  TTL:107  (No rDNS)
```

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.n54n	New York, NY, U	-5.0	128		AT&T ITS
4		12.122.5.114	gbr3-p90.n54n	New York, NY, U	-5.0	185		AT&T ITS
5		12.123.1.121	ggr1-p360.n54r	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 (
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.dllst	Dallas, TX, USA		234		Verio, Inc.
10		129.250.3.74	p4-1-0-0.r01.dll	Dallas, TX, USA		221		Verio, Inc.
11		129.250.2.41	p1-0-0-0.r01.or	Orem, UT, USA	-7.0	269		Verio, Inc.
12		129.250.29.20	pvu1.vwhpvu1.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 (IDSs).

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 of a network card allows you to determine all of the subnets being used.

To prevent such 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

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 sent 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 programs.

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 NT) 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 amound 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* use compare observed attribute values to those in a fingerprint database to identify and OS.

Enumeration

Enumeration involves using active probing to obtain information about:

- Network resources and shares
- Users and groups
- Applications and banners

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

Enumeration techniques tend to be OS-specific.

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.

NT/2000 Network Resource Enumeration

The *net view* command is a built-in enumeration tool in Windows NT/2000:

```
$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 NT/2000 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 NT/2000 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
```

Banner Enumeration

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

Banners can provide information that is valuable to attackers.

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>
```