Network Security Profiles
A Collection (hodgepodge) Of Stuff Hackers Know About You

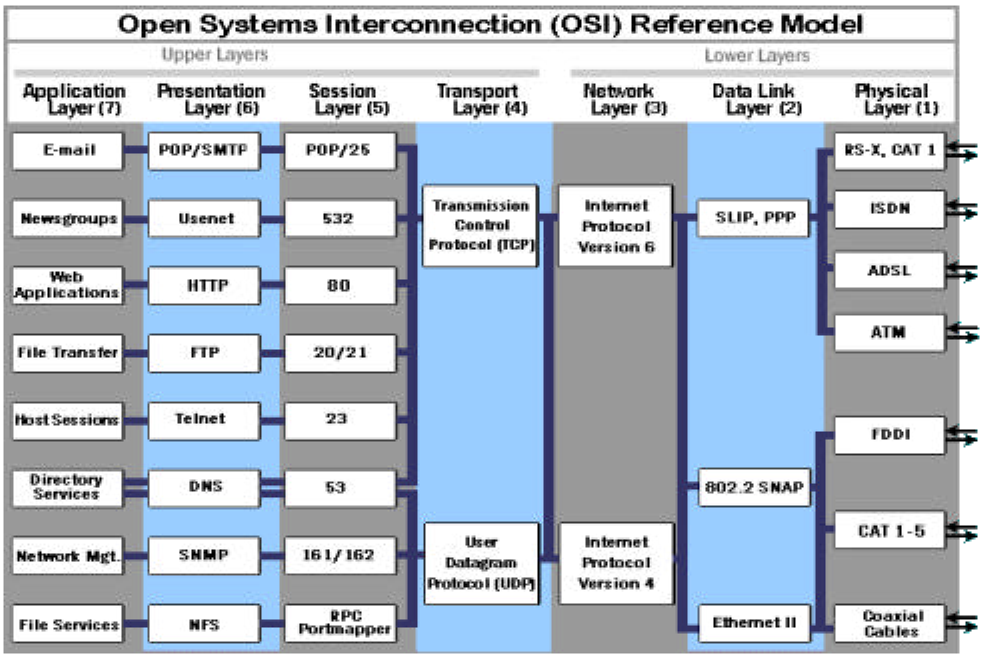
Just checking...

- This is line 1 (28 pt font - TITLES)
    - This would be line 2 (24 pt font - BULLETS)
        - This is clearly line 3 (18-20 pt font - SUB BULLETS)
            - This is definitely line 4 (18 pt font - legal and commentary stuff :-)
- Can you hear me? Check 1…2…3…Check
- **Is it too hot?** **Too cold?**

Reader’s Digest of the Tutorial

- Hacker = Determined Intruder = Diligence
  - learn exactly what components are in place (the profile) to enable focused research (and almost guarantee some level of intrusion success)
  - paying attention to small details in both what you see and don’t see
- The amount of traffic (other than DoS) needed to profile your site is small and the amount of information available to research vulnerabilities to discover exploits is huge
- Sigh…the protocols we depend on are responsible for many of the hard to see, catch, stop, or manage exploit problems

It’s the Protocols



Open Systems Interconnection (OSI) Reference Model

Upper Layers

Lower Layers

Application Layer (7): E-mail, Newsgroups, Web Applications, File Transfer, Host Sessions, Directory Services, Network Mgt., File Services

Presentation Layer (6): POP/SMTP, Usenet, HTTP, FTP, Telnet, DNS, SNMP, NFS

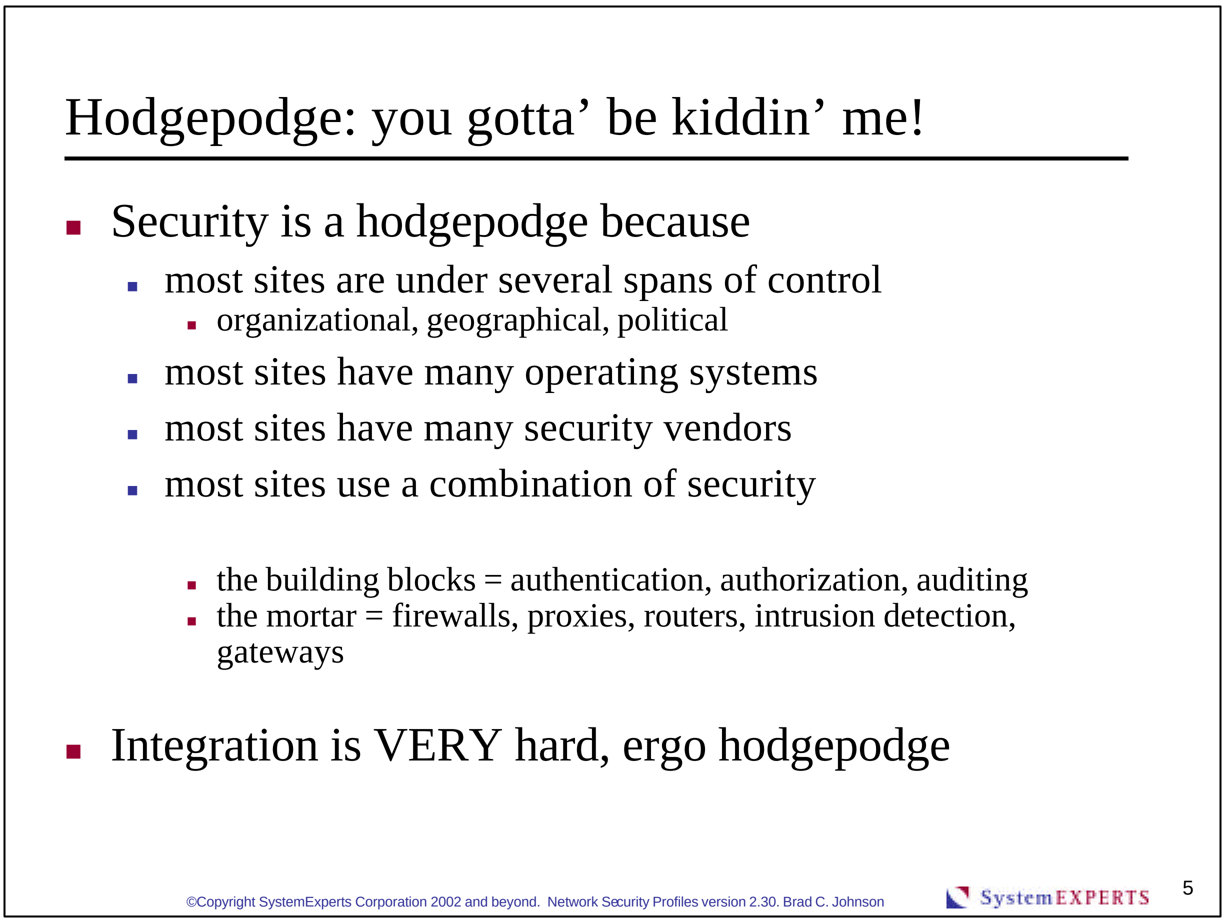
Session Layer (5): POP/25, 532, 80, 20/21, 23, 53, 161/162, RPC Portmapper

Transport Layer (4): Transmission Control Protocol (TCP), User Datagram Protocol (UDP)

Network Layer (3): Internet Protocol Version 6, Internet Protocol Version 4

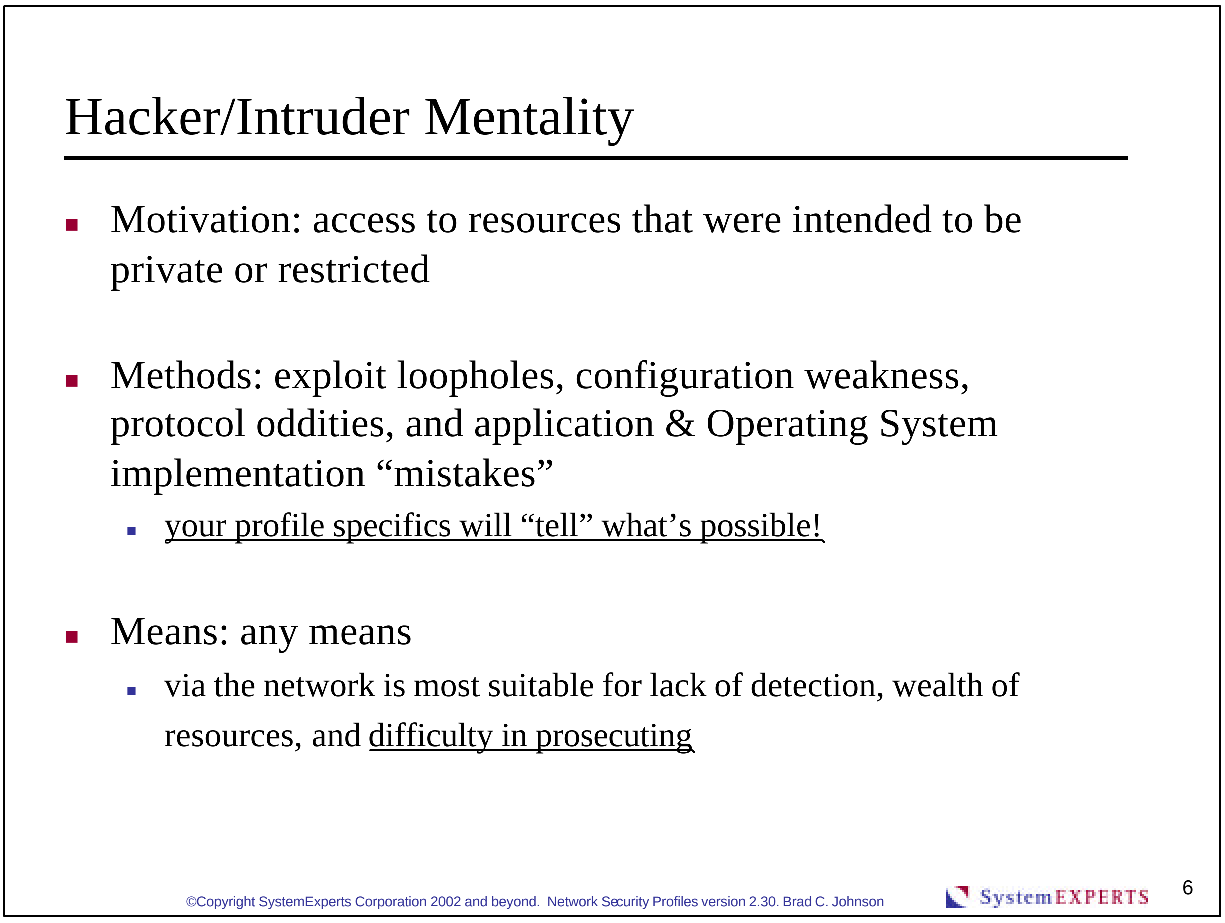
Data Link Layer (2): SLIP, PPP, 802.2 SNAP, Ethernet II

Physical Layer (1): RS-X, CAT 1, ISDN, ADSL, ATM, FDDI, CAT 1-5, Coaxial Cables



Hodgepodge: you gotta’ be kiddin’ me!

- Security is a hodgepodge because
  - most sites are under several spans of control
    - organizational, geographical, political
  - most sites have many operating systems
  - most sites have many security vendors
  - most sites use a combination of security
    - the building blocks = authentication, authorization, auditing
    - the mortar = firewalls, proxies, routers, intrusion detection, gateways
- Integration is VERY hard, ergo hodgepodge



Hacker/Intruder Mentality

- Motivation: access to resources that were intended to be private or restricted
- Methods: exploit loopholes, configuration weakness, protocol oddities, and application & Operating System implementation “mistakes”
  - your profile specifics will “tell” what’s possible!
- Means: any means
  - via the network is most suitable for lack of detection, wealth of resources, and difficulty in prosecuting

What the course is...

- A overview of various ways that people can learn the details of your environment: and how that works to their advantage in “finding” exploits to use against you
- Examples
  - how to profile, what protocols to look “out” for
- Tools, techniques, URLs
  - examples largely public domain (so you can try it)
  - commercial tools also described briefly
- Focus on what’s happening “now”

What the course isn’t...

- Host based or inside jobs
  - escalating privileges
- Buffer overflow or browser (frame) exploits
- Social engineering
- Operating system specific

- THIS COURSE IS…for all TCP/IP environments
  - UNIX
  - Apple
  - Windows, NT
  - Mainframes

What the Hacker KnOwZ… ALREADY!

- Profiling is easy
  - lots of tools →
  - lots of techniques
- Today’s networks are hard to manage
  - integration is hard
  - the 3 A’s are complex
- next…Profiling

- Cron
- cURL
- Dig
- Discover
- Dsniff
- eEye
- ISS
- Jizz
- Land
- Nmap
- Nessus
- Netcat
- Nsat
- Nslookup
- Ping
- Queso
- SAINT
- SARA
- SATAN
- Scotty
- Showmount
- Smurf
- Stacheldraht
- Strobe
- Tcp_scan
- TearDrop
- TFN&TFN2K
- Traceroute
- Trinoo
- Udp_scan
- Whisker
- Whois

Where are We?

- **Profiling**
  - **An example**
  - Intrusions
- Discovery and DoS
  - Discovery
  - Denial of Service
- Protocols
  - SSL
  - DNS
  - SNMP
  - Web
  - Wireless
- Epilog
  - Top 10ish TTD
  - References

An Example

- Workstation flexibility
  - OS running Solaris, Linux, NT, Windows, Trinux, or anything else that runs on Intel

    be compatible with the system you are profiling
    - 200MHz is fine, in fact, 66MHz is plenty fast!
    - 32M memory is fine, in fact, 16M will do
  - Network using ISDN, Ethernet, internal V.90 modem, or external modem
    - except for a special few tasks, 28.8 is fine
  - Storage using SCSI, CD, ZIP, floppy, DVD
    - OK, the DVD is to help when I’m bored!

Rudimentary Data Gathering

- Internet
  - whois -h arin.net
  - whois -h internic.net
  - whois -h icann.net
  - whois -h newregistrars.net
  - whois –h register.com
  - whois -h ???.net
- SCOTTY
  - discover -icmp x.y.z
  - discover -snmp x.y.z
- Network sniffer
  - see what really happens…

    and what doesn’t happen

- *IP space, rate of change, name and mail servers, contact information*
- *Reachable hosts (particularly useful on Internal probe)*
  - *latency: for timeouts*
- *Management, topology, and gateway data*
- *Traffic and protocol flow*

Port, DNS, and SNMP Data Gathering

- For host in list
  strobe and **nmap** $host
- For host in list
  nslookup $host
  nslookup $IP
  dig $host
  traceroute $host
- Attempt DNS zone transfer
  - **dig axfr** @place zone.com
- For host in snmp_list
  Scotty < DONE
  snmp session -address $host
  snmp0 walk x “mib-2” { puts $x }
  DONE

- *Gather list of potential TCP/IP services and well-known exploits*
- *Gather naming information, conventions*
- *Understand routing paths*
- *Understand server relationships (e.g., mail, DNS)*
- *Gather MIB information (neighbors, IP addresses, HW profile)*

Service and Exploit Data Gathering

- For host in ftp_list
  echo QUIT | **nc** -v -w 5 -r $host ftp
- For host in telnet_list
  tcp_scan -b -w 5 $host telnet
- For host in rpc_list
  scotty -c “sunrpc info $host”
- For host in smtp_list
  tcp_scan -b -w 5 $host smtp
- For host in http_list
  scotty -c “http head http://$host”
  curl $host and **whisker** $host
- For host in list
  sscan $host
  nsat $host
  nessus $host

- *Gather service version, platform, and actual exploit data*
- *Notice all the tools just used (in the last few slides)*
  - *NetCat (nc)*
  - *SATAN / SAINT / SARA*
    - *tcp_scan*
  - *SCOTTY*
    - *discover*
  - *cURL*
  - *Whisker*
  - *SScan*
  - *Nsat*
  - *Nessus*
  - *Strobe*
  - *Nmap*
  - *Dig, nslookup, traceroute*

Exploit Research

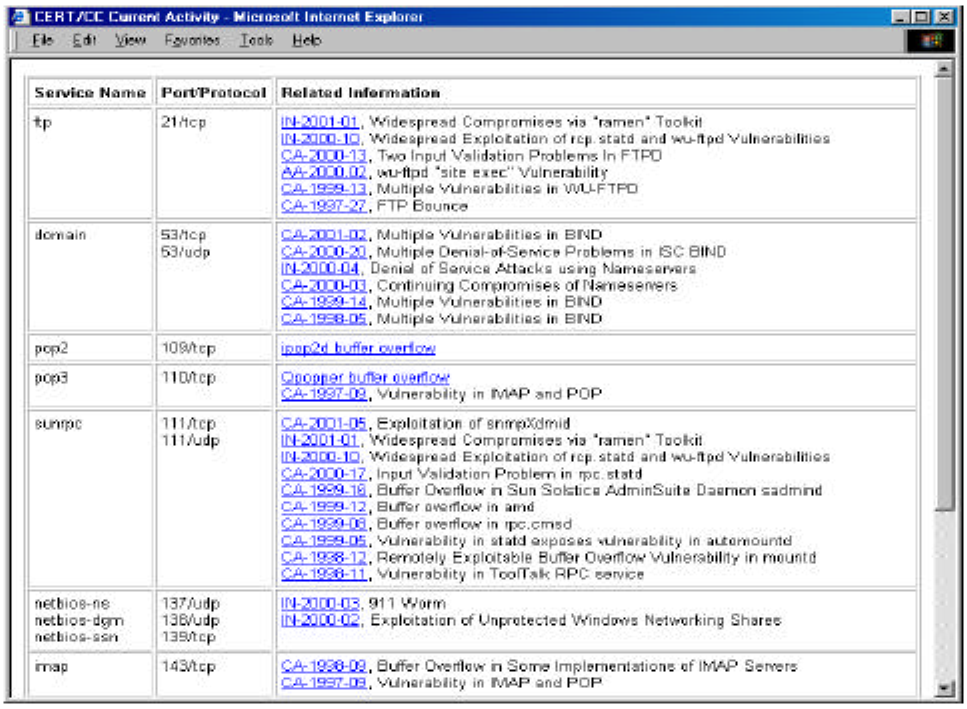
- General Internet security
  - www.cert.org/
  - ciac.llnl.gov/
  - cve.mitre.org/
- Archives
  - www.deja.com/usenet
  - http://packetstorm.decepticons.org/
  - http://xforce.iss.net
  - www.securityfocus.com/ forums->bugtraq->archive
- News
  - www.google.com/
  - www.internetworld.com/
  - www.zdnet.com/

Alcatel Xylan
Omniswitch
<ctrl>d

Exploit Research, cont.

- Hackerz
  - www.defcon.org
  - www.l0pht.com/
    - or www.atstake.com/security_news
  - www.antionline.com/
  - www.phreaker.org
  - http://cultdeadcow.com
- NT Specific
  - www.ntsecurity.net/, www.ntbugtraq.com/
- Vendors
  - Microsoft, Sun, HP, IBM, Linux, Netscape, etc.

Exploit Research, cont.
Problem Areas That Won’t Go Away


CERT/CC Current Activity - Microsoft Internet Explorer
File Edit View Favorites Tools Help

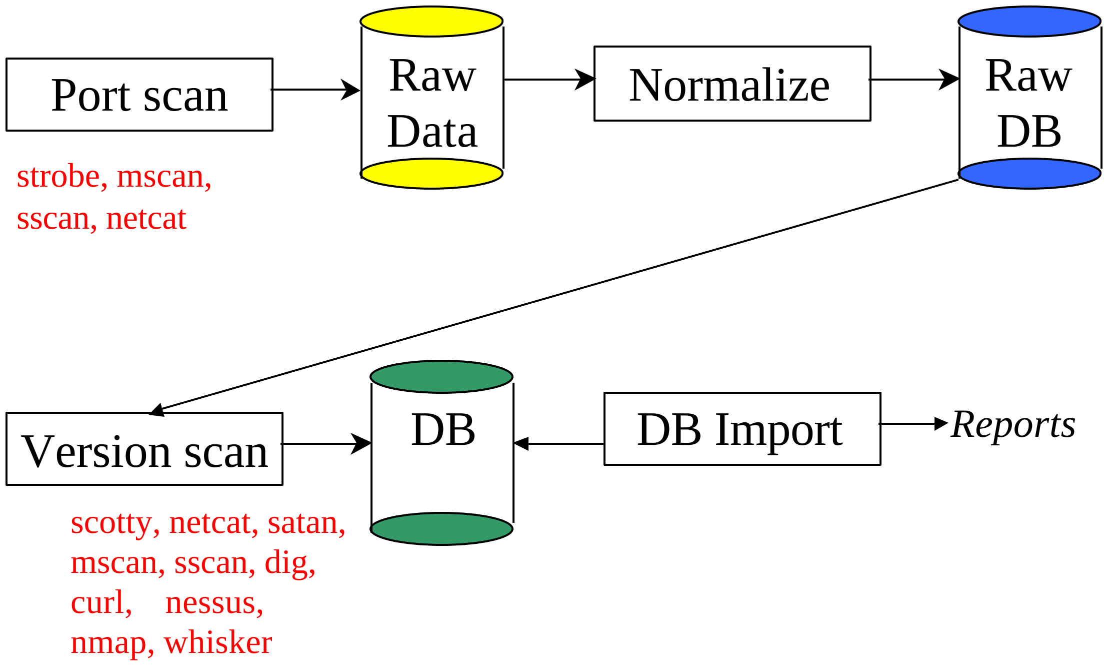
Service Name	Port/Protocol	Related Information
ftp	21/tcp	IN-2001-01, Widespread Compromises via "ramen" Toolkit IN-2000-10, Widespread Exploitation of rpc.statd and wu-ftpd Vulnerabilities CA-2000-13, Two Input Validation Problems In FTPD AA-2000.02, wu-ftpd "site exec" Vulnerability CA-1999-13, Multiple Vulnerabilities in WU-FTPD CA-1997-27, FTP Bounce
domain	53/tcp 53/udp	CA-2001-02, Multiple Vulnerabilities in BIND CA-2000-20, Multiple Denial-of-Service Problems in ISC BIND IN-2000-04, Denial of Service Attacks using Nameservers CA-2000-03, Continuing Compromises of Nameservers CA-1999-14, Multiple Vulnerabilities in BIND CA-1998-05, Multiple Vulnerabilities in BIND
pop2	109/tcp	ipop2d buffer overflow
pop3	110/tcp	Qpopper buffer overflow CA-1997-09, Vulnerability in IMAP and POP
sunrpc	111/tcp 111/udp	CA-2001-05, Exploitation of snmpXdmid IN-2001-01, Widespread Compromises via "ramen" Toolkit IN-2000-10, Widespread Exploitation of rpc.statd and wu-ftpd Vulnerabilities CA-2000-17, Input Validation Problem in rpc.statd CA-1999-16, Buffer Overflow in Sun Solstice AdminSuite Daemon sadmind CA-1999-12, Buffer overflow in amd CA-1999-08, Buffer overflow in rpc.cmsd CA-1999-05, Vulnerability in statd exposes vulnerability in automountd CA-1998-12, Remotely Exploitable Buffer Overflow Vulnerability in mountd CA-1998-11, Vulnerability in ToolTalk RPC service
netbios-ns netbios-dgm netbios-ssn	137/udp 138/udp 139/tcp	IN-2000-03, 911 Worm IN-2000-02, Exploitation of Unprotected Windows Networking Shares
imap	143/tcp	CA-1998-09, Buffer Overflow in Some Implementations of IMAP Servers CA-1997-09, Vulnerability in IMAP and POP

Profiling Results

- Rudimentary
  - Internet registration data
  - all IP addresses
  - SNMP agents
- Expanded data gathering
  - OS types
  - DNS names and conventions
  - ISP routes
  - external services
    - SMTP, POP, DNS
  - TCP & UDP services
  - SNMP MIBs
  - HTTP server exploits

- What we now know
  - known service exposure opportunities
  - OS types and vendors
  - related hacker successes
  - related hacker tools
  - recent exploits
  - detection and prevention tools and techniques
  - relevant articles and techniques to research and understand

Automated Profiling



Port scan

strobe, mscan, sscan, netcat

Raw Data

Normalize

Raw DB

Version scan

scotty, netcat, satan, mscan, sscan, dig, curl, nessus, nmap, whisker

DB

DB Import

Reports

To Net it All Out

- Intrusions are too easy…*why*? and *what to do*?
  - poor detection and escalation
    - write down 10 critical events and create (even if brute force) scripts to review logs and generate events
  - configurations tend to degrade over time
    - make a clone when you upgrade your deployment systems
  - many organizations think in terms of inside and outside
    - be just as concerned about what goes out as what comes in
  - OS/application upgrades are a pain
    - make a clone when you install a new version that works
  - there are no business risk/cost analysis tools
    - quantify your environment, problems
  - integrating disparate layered technologies on multiple OS environments is time consuming
    - consolidate versions to reduce complexities and variables

The SANS Institute: Top 10

- How To Eliminate The Ten Most Critical Internet Security Threats

1. BIND weaknesses: nxt, qinv and in.named allow immediate root compromise
2. Vulnerable CGI programs and application extensions (e.g., ColdFusion) installed on web servers
3. Remote Procedure Call (RPC) weaknesses in rpc.ttdbserverd (ToolTalk), rpc.cmsd (Calendar Manager), and rpc.statd that allow immediate root compromise
4. RDS security hole in the Microsoft Internet Information Server (IIS)
5. Sendmail buffer overflow weaknesses, pipe attacks and MIMEbo, that allow immediate root compromise
6. sadmind and mountd
7. Global file sharing and inappropriate information sharing via NetBIOS and Windows NT ports 135->139 (445 in Windows2000), or UNIX NFS exports on port 2049, or Macintosh Web sharing or AppleShare/IP on ports 80, 427, and 548
8. User IDs, especially root/administrator with no passwords or weak passwords
9. IMAP and POP buffer overflow vulnerabilities or incorrect configuration.
10. Default SNMP community strings set to ‘public’ and ‘private’

- www.sans.org/10threats.doc
- www.sans.org/top20.htm
- SARA is “blessed” to validate these

What the Hacker KnOwZ… about profiling

- You don’t need sophisticated resources
  - almost any UNIX, Windows, or NT machine will do fine
- Simple tools can generate fine-grained information
- Research is easy, will likely reveal lots of good information, and is likely to be compelling

- next…Intrusions

Notes:

Where are We?

- **Profiling**
  - An example
  - **Intrusions**
- Protocols
  - SSL
  - DNS
  - SNMP
  - Web
  - Wireless
- Discovery and DoS
  - Discovery
  - Denial of Service
- Epilog
  - Top 10ish TTD
  - References

Intrusion Awareness

- RootKit - OS centric tools and techniques
  - Windows 2000
  - NT
  - Linux
  - Solaris
  - FreeBSD
  - UNIX* (universal tools)
- Keyghost – record keystrokes
  - www.keyghost.com/pictures.htm
  - KeyGhost II Standard 97K $139
  - KeyGhost II Pro .5 - 2M $250-$350
  - KeyGhost II Keyboard .5 – 2M $300 - $400

Rootkits

- NTrootkit031.zip
  - root_readme.txt

    copy deploy.exe and _root_.sys and run deploy.exe
- rootkitLinux.gz
  - netstat replacement (to hide address, port, socket being used)
- rootkit.zip
  - z2: remove entries from utmp, wtmp, lastlog
  - es: ethernet sniffer
  - fix: fake checksums
  - sl: become root via magic password sent to login
  - netstat and ps replacements

Intrusion Awareness, cont.

- Remote scanners
  - strobe, sscan, netcat, nsat, nessus
  - SATAN, SAINT, SARA
  - COPS, Tiger
  - eEye Retina scan
    - runs on NT
  - Typhoon (was CIS, was Mnemonix NT Info Scan)
    - Web service, SQL, SNMP, SMTP relay
  - Third party applications
    - ISS - Internet Security Scanner – www.iss.net
    - NetRecon – www.axent.com
    - NetRanger - www.cisco.com/warp/public/cc/cisco/mkt/security/nranger/
    - Kane Security Analysis - www.intrusion.com/Products/analystnt.shtml

Intrusion Opportunities

- Large Scale environments
  - scale in number of systems
    - diversity = opportunity ← 12 Different FTP versions
- Hierarchical organizations
  - fiefdoms created disjoint security configurations
    - boundaries = opportunity

Intrusion Opportunities, cont.

- Leading (bleeding) edge companies
  - unexpected side effects of a new language or OS
    - short soak time = opportunity
  - http://www.cert.org/advisories/CA-2000-15.html
    - Netscape allows Java Applets to read protected resources
  - http://www.cert.org/advisories/CA-2000-12.html
    - IE ActiveX HHCtrl allows remote intruders to execute arbitrary code
  - www.cert.org/advisories/CA-2000-02.html
    - dynamically generated pages that are not re-verified at the server
  - www.ntsecurity.net
    - IE ActiveX object reveals clipboard contents
  - http://www.cert.org/advisories/CA-1999-11.html
    - multiple buffer overflow and RPC problems

Intrusion Opportunities, cont.

- IIS (sigh…)
  - Indexing service DLL: remote: arbitrary commands
    - http://www.cert.org/advisories/CA-2001-13.html
  - URL decoding only 1st reference: remote: arbitrary commands
    - http://www.cert.org/advisories/CA-2001-12.html
  - sadmind/IIS worm: remote: arbitrary commands
    - http://www.cert.org/advisories/CA-2001-11.html
  - 5.0 buffer overflow: remote: arbitrary commands
    - http://www.cert.org/advisories/CA-2001-10.html
- Microsoft sites defaced
  - http://www.theregister.co.uk/content/8/19915.html

Intrusion Statistics

- CSI Computer Crime and Security Survey →

  www.gocsi.com/prelea_000321.htm

- Intrusion Detection Market

Cisco	28%
ISS	27%
Axent	19%
Intrusion.com (ODS combined with Kane security)	10%
Network ICE	4%
Others	12%

- 85% detected breaches
- 65% acknowledged financial losses
- 40% detected a penetration from the Internet
- 38% detected a DoS
- 97% of businesses have a web site
  - 47% conduct e-business

Intrusion Statistics, cont.

- CERT Advisories in 2000

Web (HTML, browser, ActiveX/Java):	9
Security infrastructure (Kerberos, PGP):	4
DNS/Bind:	3
Denial of Service:	2
Services (RPC, FTP):	2
Other:	2

Intrusion Statistics, cont.

- CERT incidents thru 2001

1988:	6
1989:	132
1990:	252
1991:	406
1992:	773
1993:	1,334
1994:	2,340
1995:	2,412
1996:	2,573
1997:	2,134
1998:	3,734
1999:	9,859
2000:	21,756
2001:	34,754 Q1-3

- CERT vulnerabilities thru 2001

1995:	171
1996:	345
1997:	311
1998:	262
1999:	417
2000:	1,090
2001:	1,820 Q1-3

- For complete details, see:
  - www.cert.org/stats/cert_stats.html

Intrusion Example #1

- NO detection!
  - main Web server fine…let’s look around
  - staging server not so fine
  - exploit well known Web server bug to initiate interactive login session
  - exploit trust relationship between staging server and main Web server
  - change main Web pages!
- Typical big exploit is a combination of lower level problems

Intrusion Example #1, cont.

- Vulnerabilities to achieve critical access
  - ICMP echo allowed in (low/medium)
  - non default but easily guessed SNMP community string (low/medium)
  - non production quality HTTP server configuration on non production system (low)
  - trust relationship between 2 systems within a close IP address space (low/medium)
  - xterm from DMZ address allowed out through firewall (medium)

Intrusion Example #2

- Hack PC Week
  - PC Week Labs invited people to hack Web site running on Linux
  - result: ability to change any Web pages
    - didn't require interactive session!
  - details highlight how a series of incremental learning on small details revealed HUGE vulnerability
  - in a nutshell
    - Web site running 3rd party AD package
    - intruder acquired and reviewed package source code
    - scrutinized several server-side package scripts
    - minor coding glitch allowed a <7K "image" to be uploaded and OS had a well known SUID exploit
      - image was actually a VERY short program:
        execlp("/tmp/.bs","ls","-c",
        "cp /tmp/xx /home/httpd/html/index.html",0);
  - hispahack.ccc.de/en/mi019en.htm

Intrusion Example #3

- NO detection!
  - DNS poisoning (cache poisoning)
    - populate with bogus entries
      - www.foobar.edu -- w.x.y.z
    - update already populated entries (i.e., add addresses)
      - www.yahoo.com -- w.x.y.z (arbitrary address)
  - original victim www.internic.net: root DNS servers poisoned to point to www.alternic.net

Intrusion Example #4

- NO detection!
  - begin secure session (SSL) with legit login ID
  - download all (possible) pages to review
  - find possible application design flaw
    - modify session ID in (dynamically generated) page
    - modify client side state data (in local file, or registry, or…)
    - modify cookie (on disk OR in memory!)
    - modify data in transit
      - Achilles – proxy server to intercept, change data www.digizen-security.com/
  - begin authorized transactions on any other account
    - server assumed one time authentication and didn’t re-validate

What the Hacker KnOwZ… about intrusions

- Most problems result from a combination of exploiting several low(er) level vulnerabilities
- Monitoring a heterogeneous distributed network is HARD
  - you should detect what you can’t prevent
- Many individuals, groups, and sites, are dedicated to making intrusions possible

- next…Discovery

Notes:

Notes:

____

____

____

____

Where are We?

- Profiling
  - An example
  - Intrusions
- **Discovery and DoS**
  - **Discovery**
  - Denial of Service
- Protocols
  - SSL
  - DNS
  - SNMP
  - Web
  - Wireless
- Epilog
  - Top 10ish TTD
  - References

Discovery - Port Scans

- Direct
  - TCP connect (strobe, SATAN-tcp_scan, netcat, nmap)
  - UDP “connect” (SATAN-udp_scan, netcat, nmap)
  - service protocols (mscan, sscan)
- Indirect
  - tunneling
    - Nmap FTP Bounce
    - telnet through ICMP (sneakin.tgz on PacketStorm)
  - stealth scans

    note: what is “stealthy” changes with time
    - FIN or NULL
    - fragmented packets
    - TCP SYN (half open)

Discovery - strobe

```
usage: strobe [options]
   [-v(erbose)]                [-S services_file]
   [-V(erbose_stats]           [-i hosts_input_file]
   [-m(inimise)]               [-l(inear)] [-f(ast)]
   [-d(elete_dupes)]           [-a abort_port_n]
   [-g(etpeername_disable)]    [host1 [...host_n]]
   [-q(uiet)]
   [-o output_file]
   [-b begin_port_n]
   [-e end_port_n]
   [-t timeout_n]
   [-n num_sockets_n]
```

Strobe Example

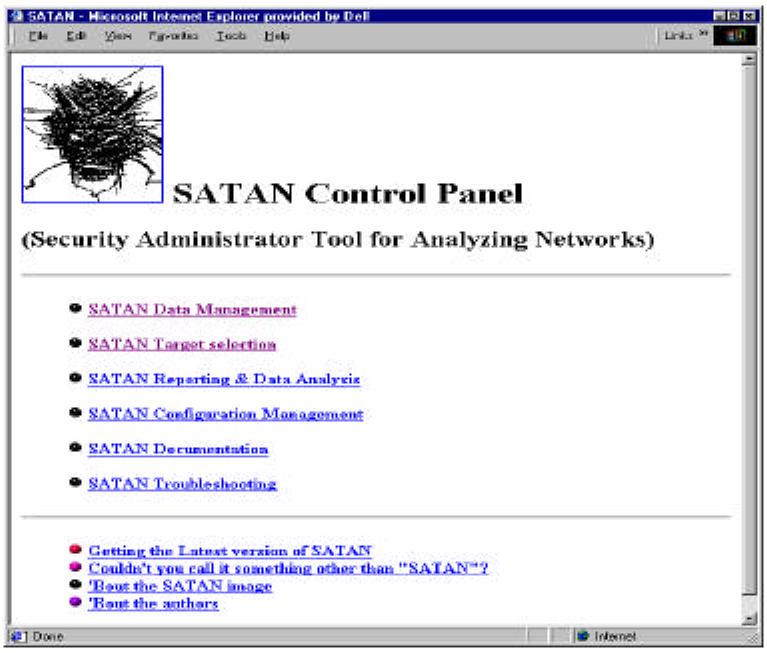
```
strobe 127.0.0.1

strobe 1.03 (c) 1995 Julian Assange
  (proff@suburbia.net).
127.0.0.1    ftp                 21/tcp
127.0.0.1    telnet              23/tcp
127.0.0.1    smtp                25/tcp mail
127.0.0.1    sunrpc              111/tcp rpcbind
127.0.0.1    lockd               4045/tcp
127.0.0.1    unknown             6000/tcp
```

SATAN

- Released in April 1995 by Wietse Venema and Dan Farmer to much fanfare (many negative reactions)
- Help administrators assess their network security
- Modular design with (very) easy to use GUI
- Find well known problems
    - NFS file systems exported to arbitrary hosts
    - NFS file systems exported to unprivileged programs
    - NFS file systems exported via the portmapper
    - NIS password file access from arbitrary hosts
    - Old (i.e. before 8.6.10) sendmail versions
    - REXD access from arbitrary hosts
    - X server access control disabled
    - arbitrary files accessible via TFTP
    - remote shell access from arbitrary hosts
    - writable anonymous FTP home directory

SATAN GUI

(SAINT & SARA)



SATAN Control Panel

(Security Administrator Tool for Analyzing Networks)

- SATAN Data Management
- SATAN Target selection
- SATAN Reporting & Data Analysis
- SATAN Configuration Management
- SATAN Documentation
- SATAN Troubleshooting

- Getting the Latest version of SATAN
- Couldn't you call it something other than "SATAN"?
- 'Bout the SATAN image
- 'Bout the authors

SAINT

- Update based on SATAN
- Expanded tests
  - DNS vulnerabilities
  - FTP vulnerabilities
  - SNMP community strings
  - NFS export issues
  - NIS password file access
  - Netscape vulnerabilities
  - POP issues
  - SMTP mail relay
  - SSH vulnerabilities
  - Sendmail vulnerabilities
  - TFTP file access
  - distributed denial of service
  - excessive finger info
  - http server exploits
  - imap version
  - lpd over the internet
  - mountd vulnerabilities
  - netbios over the internet
  - remote login and shell issues
  - r* command issues
  - teardrop
  - NFS and X access
  - FTP issues

Discovery - SAINT (SATAN Derivative)

- Version of 3.4.4 release 11/13/01, recent additions in the last few versions include checks for
  - Nimda
  - SSH
  - Lotus Domino
  - lpd
  - WS_FTP stat
  - Entrust GetAccess

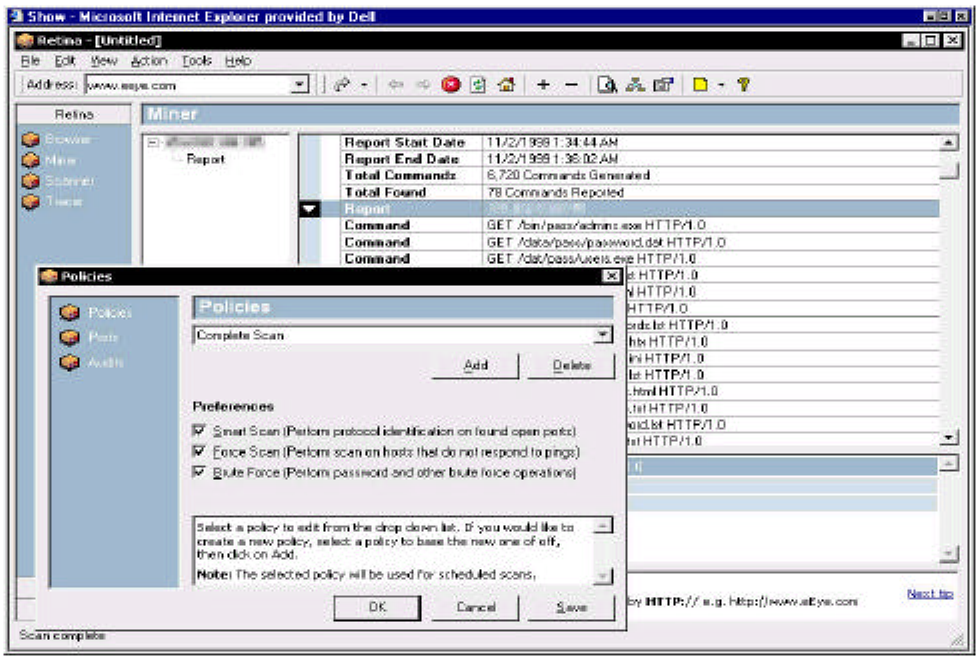
Discovery – SARA (SATAN and SAINT Derivative)

- Two versions (updated v3.4.6 version out June, 2001)
  - generic SARA and SARA PRO
    - newer versions have DDoS, IIS, virus tests
  - author of SAINT is on the team
  - approved by SANS for checking top 10 problems
- Philosophy is to integrate with existing tools
  - use Nmap for OS identification (like SAINT)
  - use SAMBA for SMB analysis
- SARA PRO includes
  - report write
  - gateways to other products
  - monthly updates (much like virus detection programs)

Discovery - eEye Retina Scanner

- NetBIOS
- HTTP, CGI, and WinCGI
- ISAPI and ASP
- FTP
- DNS
- Denial of Service vulnerabilities
- POP, SMTP and LDAP
- Registry Services
  - Users and Accounts
  - Password vulnerabilities
  - Publishing extensions
- SQL Database Servers
- Firewalls and Routers
- Proxy Servers
- www.eeye.com/html/Products/Retina/overview.html

eEye Retina Scanner GUI



Report Start Date	11/2/1999 1:34:44 AM
Report End Date	11/2/1999 1:36:02 AM
Total Commands	6,720 Commands Generated
Total Found	78 Commands Reported
Report	
Command	GET /bin/pass/admins.exe HTTP/1.0
Command	GET /data/pass/password.dat HTTP/1.0
Command	GET /dat/pass/users.exe HTTP/1.0

Policies

Complete Scan

Preferences

☑ Smart Scan (Perform protocol identification on found open ports)

☑ Force Scan (Perform scan on hosts that do not respond to pings)

☑ Brute Force (Perform password and other brute force operations)

Select a policy to edit from the drop down list. If you would like to create a new policy, select a policy to base the new one of off, then click on Add.

Note: The selected policy will be used for scheduled scans.

by **HTTP://** e.g. http://www.eEye.com

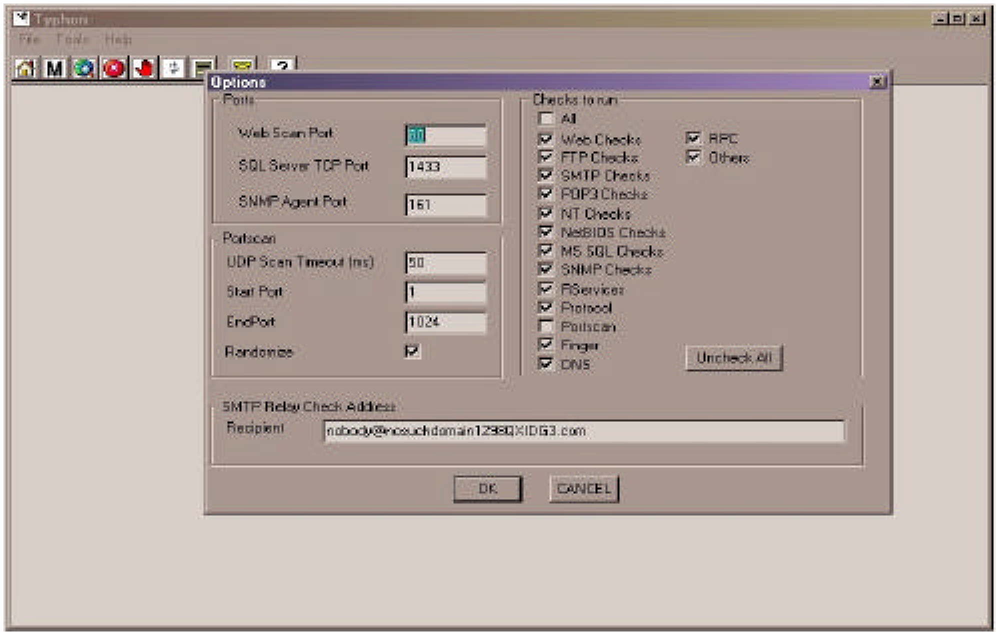
Scan complete

Discovery - Typhoon

- Web
- FTP, SMTP, POP3
- NT/2000 services, registry, and audit
- IE security setttings
- NetBIOS Audit, NT/2000 SAMBA
- SQL
- ICMP
- DNS
- RPC
- UDP

- Coming soon Typhoon II, the commercial version
  - War dialing
  - Oracle
  - SSH and telnet
  - LDAP
  - X, pcAnywhere

eEye Retina Scanner GUI



Ports
Web Scan Port 80
SQL Server TCP Port 1433
SNMP Agent Port 161

Portscan
UDP Scan Timeout (ms) 50
Start Port 1
EndPort 1024
Randomize ☑

Checks to run
☐ All
☑ Web Checks
☑ FTP Checks
☑ SMTP Checks
☑ POP3 Checks
☑ NT Checks
☑ NetBIOS Checks
☑ MS SQL Checks
☑ SNMP Checks
☑ RServices
☑ Protocol
☐ Portscan
☑ Finger
☑ DNS
☑ RPC
☑ Others

SMTP Relay Check Address
Recipient nobody@nosuchdomain12980XIDG3.com

Discovery - Mscan

- Multi-scan
  - focused, application level scanner
  - next generation scanner
  - “current” popular vulnerabilities
    - statd
    - IMAP/POP
    - IRIX lp accounts
    - BIND buffer overflow
    - cgi-bin programs: phf, handler, test-cgi
    - NFS exports
    - X server

From the Author...

- ./mscan -h target -c 125 -at > target.log &

  This command tells mscan that at any given time, it should be checking for vulnerabilities on 125 hosts. A Pentium with 32 megs of ram should support this just fine (**but if an admin is at the console, you can bet he'll notice you RIGHT AWAY !&!@***). If you want to stay discreet, do something like -C 10.

  H4v3 fun k1dd13z *)&!*@*)%&!@%&&@^&(!@4

  - jsbach

Discovery - Sscan

- Mscan derivative
  - another focused, more powerful application level scanner with a scripting language built-in
  - multi part probe
    - TCP ACK check - if any response, do the other checks
      - telnet, smtp, pop3, imap, www
    - vulnerability check
      - telnet, smtp, pop3, imap, www, sunrpc, x11, finger, domain, Back Orifice, lp
    - connection check
      - netbios, ftp, ssh, mSQL, tcpmux
    - OS check
      - telnet banner and “Queso” like check (5 packets vs. 7) – not as robust/successful as nsat or nmap, respectively

From the Author... Jsbach again

- From the ReadMe
  - WE TAKE FULL RESPONSIBILITY FOR EVERYTHING YOU DO ILLEGALLY WITH THIS PROGRAM.
    WE CONDONE ILLEGAL AND MALICIOUS USE OF THIS PROGRAM.

  - You could probably write a whole internet worm in the scripting language..here's a hypothetical example:
    [edited to show just 1 line]

```
send[rm -rf /] # w00h00!!!! dont try this at home kidz ;)
```

Sscan Example

- sscan -o host.com -c ./Sscan.conf -v

```
<[ tcp port: 23 (telnet) ]>                <[ tcp port: 111 (sunrpc) ]>
<[ tcp port: 53 (domain) ]>                <[ tcp port: 25 (smtp) ]>
<[ tcp port: 21 (ftp) ]>                   <[ tcp port: 22 (ssh) ]>
--<[ *OS*: ns1.ispc.org: os detected: solaris 2.x
--<[ *BANNER*: telnet banner: SunOS 5.6
--<[ * rpc servicez? * ]>--
<[ [prog. name -> rpcbind]                 [port -> 111(tcp)] [vers. -> 3]
<[ [prog. name -> status]                  [port -> 32818(udp)] [vers. -> 1]
<[ [prog. name -> status]                  [port -> 32783(tcp)] [vers. -> 1]
<[ [prog. name -> nlockmgr]                [port -> 4045(udp)] [vers. -> 1]
<[ [prog. name -> nlockmgr]                [port -> 4045(tcp)] [vers. -> 1]
<[ [prog. name -> bootparam]               [port -> 32822(udp)] [vers. -> 1]
<[ [prog. name -> bootparam]               [port -> 32784(tcp)] [vers. -> 1]
--<[ * exports ....? * ]>--
--<[ *VULN*: host.com: solaris running nlockmgr.. remote overflow? Y
---------------------------<[ * scan of host.com completed *
```

Discovery - FTP Bounce (Tunneling)

- Normal FTP operation (non-passive)
  - client tells server host/port and server opens “data” connection back to client
    - client need not tell server to come back to itself
  - tell an anonymous ftp server to connect to machines inside its firewall: to map the inside network
- Hard to do something other than chain FTP’s but still of concern
  - can PUSH data to services/ports: e.g., SMTP, HTTP

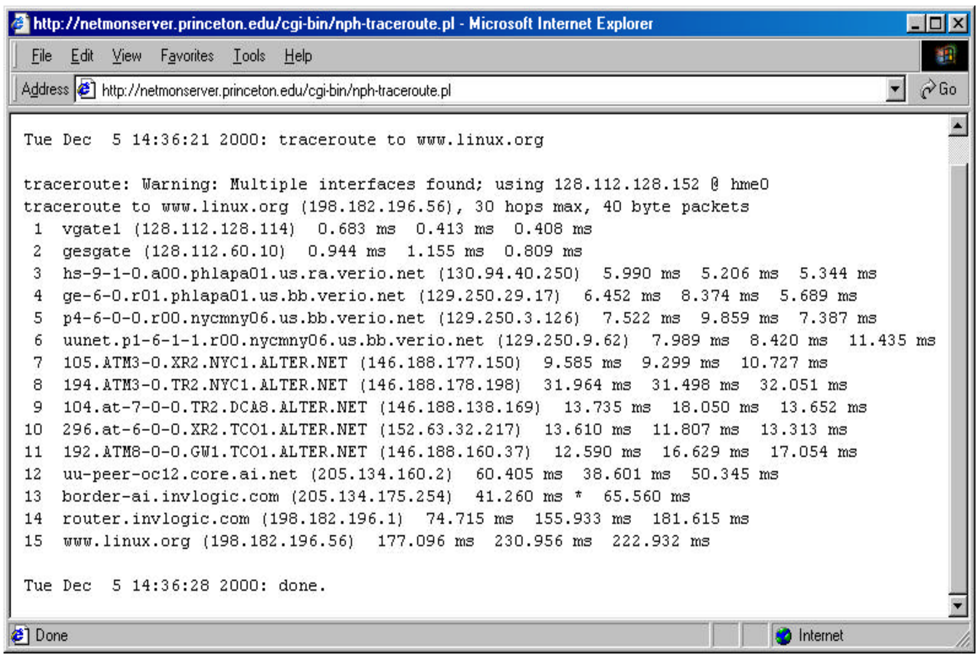
FTP Bounce Example, cont.

```
▪ strobe -b21 -e23 10.0.1.78
  Host Unreachable
▪ strobe -b21 -e21 128.0.254.217
  Port Number  Protocol  Service
  21           tcp        ftp

▪ nmap -ports 20-32 anonymous:foobar@ 128.0.254.217
  10.0.1.78
  Attempting connection to
      ftp://anonymous:foobar@ 128.0.254.217:21
  Initiating TCP ftp bounce scan against 10.0.1.78
  Open ports on 10.0.1.78:
  Port Number  Protocol  Service
  21           tcp        ftp
  22           tcp        ssh
  23           tcp        telnet
```

Discovery - Host and Network Management

- Network management
  - traceroute
    - latency, domains, dynamic/static routes
  - SNMP scans
    - management agents
- Host management
  - ICMP scans
    - reachability (not necessary but speeds discovery)
  - remote OS Identification (fingerprinting)
    - Queso and Mscan
    - Nmap (note: SAINT & SARA use Nmap)

Discovery - traceroute


http://netmonserver.princeton.edu/cgi-bin/nph-traceroute.pl - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://netmonserver.princeton.edu/cgi-bin/nph-traceroute.pl
Go
Done
Internet

```
Tue Dec  5 14:36:21 2000: traceroute to www.linux.org

traceroute: Warning: Multiple interfaces found; using 128.112.128.152 @ hme0
traceroute to www.linux.org (198.182.196.56), 30 hops max, 40 byte packets
 1  vgate1 (128.112.128.114)  0.683 ms  0.413 ms  0.408 ms
 2  gesgate (128.112.60.10)  0.944 ms  1.155 ms  0.809 ms
 3  hs-9-1-0.a00.phlapa01.us.ra.verio.net (130.94.40.250)  5.990 ms  5.206 ms  5.344 ms
 4  ge-6-0.r01.phlapa01.us.bb.verio.net (129.250.29.17)  6.452 ms  8.374 ms  5.689 ms
 5  p4-6-0-0.r00.nycmny06.us.bb.verio.net (129.250.3.126)  7.522 ms  9.859 ms  7.387 ms
 6  uunet.p1-6-1-1.r00.nycmny06.us.bb.verio.net (129.250.9.62)  7.989 ms  8.420 ms  11.435 ms
 7  105.ATM3-0.XR2.NYC1.ALTER.NET (146.188.177.150)  9.585 ms  9.299 ms  10.727 ms
 8  194.ATM3-0.TR2.NYC1.ALTER.NET (146.188.178.198)  31.964 ms  31.498 ms  32.051 ms
 9  104.at-7-0-0.TR2.DCA8.ALTER.NET (146.188.138.169)  13.735 ms  18.050 ms  13.652 ms
10  296.at-6-0-0.XR2.TCO1.ALTER.NET (152.63.32.217)  13.610 ms  11.807 ms  13.313 ms
11  192.ATM8-0-0.GW1.TCO1.ALTER.NET (146.188.160.37)  12.590 ms  16.629 ms  17.054 ms
12  uu-peer-oc12.core.ai.net (205.134.160.2)  60.405 ms  38.601 ms  50.345 ms
13  border-ai.invlogic.com (205.134.175.254)  41.260 ms *  65.560 ms
14  router.invlogic.com (198.182.196.1)  74.715 ms  155.933 ms  181.615 ms
15  www.linux.org (198.182.196.56)  177.096 ms  230.956 ms  222.932 ms

Tue Dec  5 14:36:28 2000: done.
```

traceroute, cont.

- What did we just learn from traceroute?
  - latency times to plug into other time based (wait period) programs
  - intermediate domains
  - IP addresses
    - small (Class C) or large (Class A or B) address space
  - if polled at various times and days of the week
    - static vs. dynamic routing
    - single point of failure?

Discovery - SCOTTY

- Protocol engine
  - DNS, HTTP, ICMP, NTP, RPC, SNMP, Syslog, UDP
    - UDP {open, connect, send, receive, bind}
    - HTTP {proxy, head, get, put, post, delete}
    - SUNRPC {info, probe, stat, mount, exports, pcnfs}
- Discover
  - TCL subroutine packaged with the program
  - usage: discover [-d delay] [-r retries] [-t timeout] [-w window] [-snmp] [-icmp] networks
  - ICMP
    - discover -icmp w.x.y
  - SNMP
    - discover -snmp w.x.y

SCOTTY SNMP Usage

- `discover -snmp 13.231.244`

```
13.231.244.32     IBM RISC System/6000Machine Type:
0x0100 Processor id: 000001436700The Base Operating
System AIX version: 03.02.0000.0000 TCPIP
Applications version: 03.02.0000.0000

13.231.244.170    RISC System/6000
ArchitectureMachine Type: 0x0400 Processor id:
000047467200Base Operating System Runtime AIX
version: 04.02.0000.0000TCP/IP Client Support
version: 04.02.0000.0000

13.231.244.191    IBM RISC System/6000Machine Type:
0x0400 Processor id: 000038687900The Base Operating
System AIX version: 03.02.0000.0000 TCPIP
Applications version: 03.02.0000.0000
```

SCOTTY ICMP Usage

- `discover -icmp 128.0.182`

```
128.0.182.1      icmp echo 1841 ms
128.0.182.3      icmp echo 1831 ms
128.0.182.9      icmp echo 1825 ms
128.0.182.12     icmp echo 1793 ms
128.0.182.21     icmp echo 1669 ms
128.0.182.23     icmp echo 1646 ms
128.0.182.31     icmp echo 1617 ms
128.0.182.32     icmp echo 1608 ms
```

SCOTTY Discover Performance

- Over 28.8 PPP dial-up line
  - 1 “Class C” address space (256 hosts) in 15 seconds
- Over Ethernet LAN
  - 1 “Class B” address space (65,536 hosts) in 15 minutes

Discovery - Queso

- First tool to focus on OS identification
  - type
    - Solaris, Linux, BSD, NT, Windows, AIX, CISCO, Novell, etc.
  - kernel version
  - about 100 current versions identified
- Current methods are brute-force
  - rpcinfo
  - snmp
  - telnet
  - sendMail version
  - download binaries from the public-ftp
    - (analyzing its format)

QueSO Objective

- Has been leap-frogged by Nmap
  - Nmap is more accurate
  - has more OS fingerprints
- QueSO sends TCP 7 packets
  - 1st packet is legit...the other 6 are bogus
  - the fingerprint of all 7 combined identifies the OS
  - all packets have a random seq_num and a 0x0 ack_num.

QueSO Design

- Packet number and contents are:
  - 0 SYN
    - used to verify LISTEN
  - 1 SYN+ACK
  - 2 FIN
  - 3 FIN+ACK
  - 4 SYN+FIN
  - 5 PSH
  - 6 SYN+XXX+YYY
    - XXX & YYY are unused TCP flags

Discovery - Nmap

- Scanning flexibility
  - striving to be undetected
  - striving to by-pass barriers
    - firewalls
    - intrusion detection
    - DMZs

- Account for network latencies and provide robust port and host designations
  - dynamic delay time calculations
  - retransmission for failed port requests
  - flexible port and target host specification

Nmap Features

- Scanning types
  - TCP connect() (like most other scanners)
  - TCP SYN (half open)
  - TCP FIN (stealth)
  - TCP ftp proxy (bounce attack)
  - SYN/FIN using IP fragments
  - UDP recvfrom()
  - UDP raw ICMP port unreachable
  - ICMP (ping-sweep)
- OS recognition using TCP/IP fingerprinting
  - www.insecure.org/nmap/nmap-fingerprinting-article.html

Nmap Usage

```
-t tcp connect() port scan
-s tcp SYN stealth port scan (must be root)
-u UDP port scan, will use MUCH better version if you are root
-U Uriel Maimon (P49-15) style FIN stealth scan
-l Do the lamer UDP scan even if root.  Less accurate
-P ping \"scan\". Find which hosts on specified network(s) are up
-b <ftp_relay_host> ftp \"bounce attack\" port scan
-f use tiny fragmented packets for SYN or FIN scan
-i Get identd (rfc 1413) info on listening TCP processes
-p <range>
-F fast scan. Only scans ports in /etc/services, a la strobe(1)
-r randomize target port scanning order
-S If you want to specify the source address of SYN or FYN scan
-v Verbose.  Its use is recommended.  Use twice for greater effect
-w <n> delay.  n microsecond delay. Not recommended unless needed
-M <n> maximum number of parallel sockets.
-q quash argv to something benign, currently set to \"%s\"
Optional '/mask' specifies subnet. cert.org/24 or 192.88.209.5/24
scan CERT's
```

Nmap Example

- nmap -p 20-32 -v -e eth0 -sF host.gov

  Starting nmap V. 2.02 by Fyodor

  Host host.gov (233.233.7.7) appears to be up ... good.

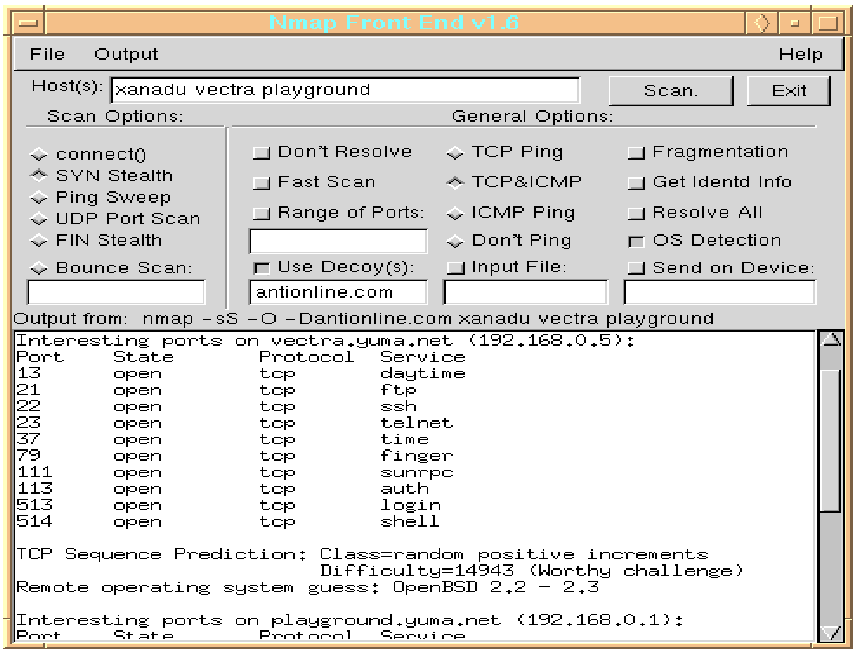
  Initiating FIN, NULL, UDP, or Xmas stealth scan
  against host.gov (233.233.7.7)

  The UDP or stealth FIN/NULL/XMAS scan took
  1 seconds to scan 13 ports.

  Interesting ports on host.gov (233.233.7.7):

```
Port   State    Protocol  Service
21     open     tcp       ftp
22     open     tcp       ssh
23     open     tcp       telnet
25     open     tcp       smtp
```

Nmap GUI



Host(s): xanadu vectra playground

Scan Options:

○ connect()
● SYN Stealth
○ Ping Sweep
○ UDP Port Scan
○ FIN Stealth
○ Bounce Scan:

General Options:

□ Don't Resolve
□ Fast Scan
□ Range of Ports:
☑ Use Decoy(s): antionline.com
○ TCP Ping
● TCP&ICMP
○ ICMP Ping
○ Don't Ping
□ Input File:
□ Fragmentation
□ Get Identd Info
□ Resolve All
☑ OS Detection
□ Send on Device:

Output from: nmap -sS -O -Dantionline.com xanadu vectra playground

```
Interesting ports on vectra.yuma.net (192.168.0.5):
Port     State        Protocol  Service
13       open         tcp       daytime
21       open         tcp       ftp
22       open         tcp       ssh
23       open         tcp       telnet
37       open         tcp       time
79       open         tcp       finger
111      open         tcp       sunrpc
113      open         tcp       auth
513      open         tcp       login
514      open         tcp       shell

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=14943 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Interesting ports on playground.yuma.net (192.168.0.1):
Port     State        Protocol  Service
```

Nmap Concerns

- Scans causes some systems to crash
  - CISCO
    - UDP scans on all 12.0 variants, 11.3AA and 11.3DB : plain old 11.3 is *not* affected
    - TCP scans on high ports on 12.1 variants
      - www.cisco.com/warp/public/707/ios-tcp-scanner-reload-pub.shtml
- On one OS, running Nmap may cause a kernel panic
  - Digital/Compaq UNIX/Alpha
- On another OS, most of the functions don’t work
  - AIX

Nmap Portability

- Working
  - Linux, FreeBSD (2.2.6 - 3.0), OpenBSD (2.2 - 2.4), NetBSD
- Mostly working
  - Solaris (2.4 - 2.6), SunOS (4.1.4 with gcc), IRIX (5.3 - 6.4), HP/UX (10.20), BSDI (2.1 and up)
- Mostly NOT working
  - AIX, Cray UNICOS
- BEWARE (possible kernel panic)
  - Digital/Compaq UNIX/Alpha

Nmap Extensions

- Nmap+V
  - a patch that allows Nmap to capture version numbers for numerous services (much like Nsat already does)
- NDiff
  - compares two Nmap scans and outputs the differences
- Remote Nmap (RNmap)
  - a pair of client and server programs which allow for various clients to run their port scans from a centralized server
- Nlog
  - an Nmap 2.x log management and analyzer toolkit
- Spidermap
  - a coordinated network scanning tool which scans by running many Nmap processes in parallel

Discovery - Whisker

- CGI Scanner
  it does a lot of things in clever ways
  - focused scanning depending on the server type
  - option to try and bypass intrusion detection using URL encoding
    - /cgi-%62in/ph%66 instead of /cgi-bin/phf
  - can query NetCraft to determine server type
    - www.netcraft.com/ - HTTP
    - www.netcraft.com/sslwhats/ - HTTPS
  - latest version will use Nmap to figure out OS type!

Whisker Objective

- Exhaustive, efficient, and “programmable” scanner for server exploits, such as
  - old: test-cgi, phf, count, nph-test-cgi
  - IIS: showcode.asp, /scripts/samples/, /wwwthreads/
  - Domino: pointers to exploit articles
  - Unix: sh, bash, tcsh, ksh, rsh, perl
  - NCSA: archie, calendar, date, uptime, wais.pl
- Over 100 different (potential) tests
  - depends on server type and OS

Whisker Usage

- whisker -s script.file ((-n input.file) | (-h host) | (-H list)) (-l log.file)

```
-s specifies the script database file     **
-n nmap output (machine format, v2.06+)   *
-h scan single host (IP or domain)        *
-H host list to scan (file)             *
-V use virtual hosts when possible
-v verbose.  Print more information
-d debug. Print extra crud++ (to STDERR)
-p proxy off x.x.x.x port y (HTTP proxy)
-l log to file instead of stdout
-u user input; pass XXUser to script
-I IDS-spoof mode--encode URLs to bypass scanners
-E IDS-evasive mode--more IDS obfuscation
-i more info (exploit information and such)
-N query Netcraft for server OS guess
-S force server version (e.g. -S "Apache/1.3.6")
 ** required     * optional; one must exist
```

Nessus

- Robust security scanner
  - plug-in architecture: each test is a unique plug-in
    - you can use their NASL scripting language to build them
  - recognizes services on non-standard ports
  - smart testing: only tests what it can/should
    - e.g., doesn’t test for anonymous FTP if it doesn’t exist
      note: this is a problem area for many other scanners
  - 3 step execution
    - configure nessusd
    - setup the client
    - view the results
  - Version 1.0.9 available August 2001
    - server runs on POSIX UNIX* systems
    - clients on POSIX for UNIX*, Win32, and Java

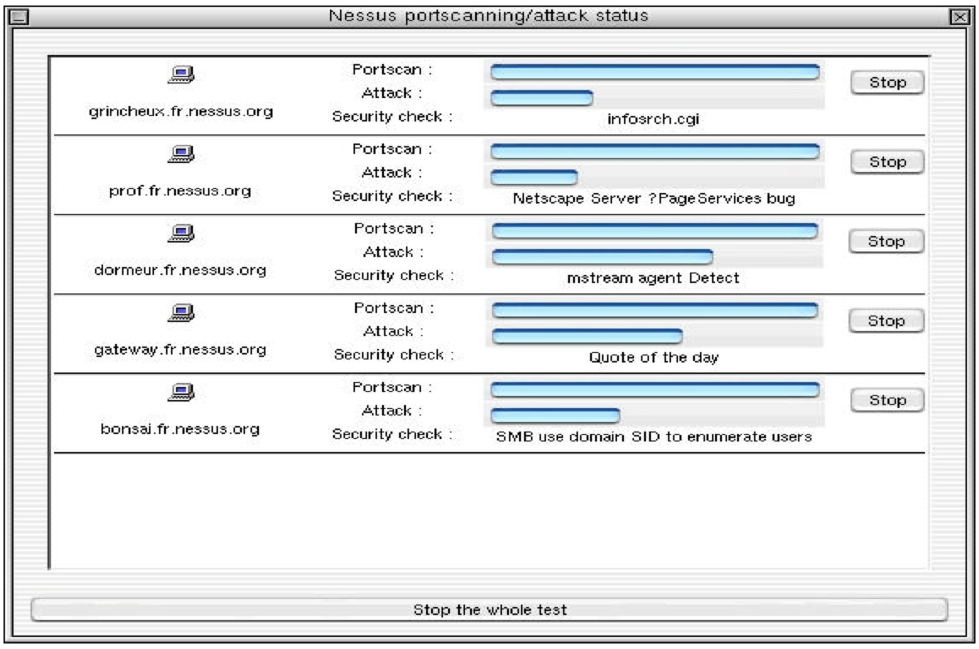
Nessus Plug-in Families

- Backdoors
- CGI abuses
- Denial of Service
- Finger abuses
- Firewalls
- FTP
- Gain a shell remotely
- Gain root remotely
- General
- Miscellaneous
- NIS
- Port scanners
- Remote file access
- RPC
- SMTP problems
- SNMP
- Useless services
- Windows

Nessus Setup

- Client setup
  - plug-ins
    - enable all, enable all but “dangerous”, disable
  - preferences
    - scanning technique (e.g., socket, SYN, FIN), include UDP or RPC, ping host, identify remote OS, get Identd info, etc.
  - scan options
    - port range, maximum threads, do reverse DNS lookup
  - target selection
    - target IP address (range), request a DNS zone transfer

Nessus Status



grincheux.fr.nessus.org
Portscan :
Attack :
Security check : infosrch.cgi

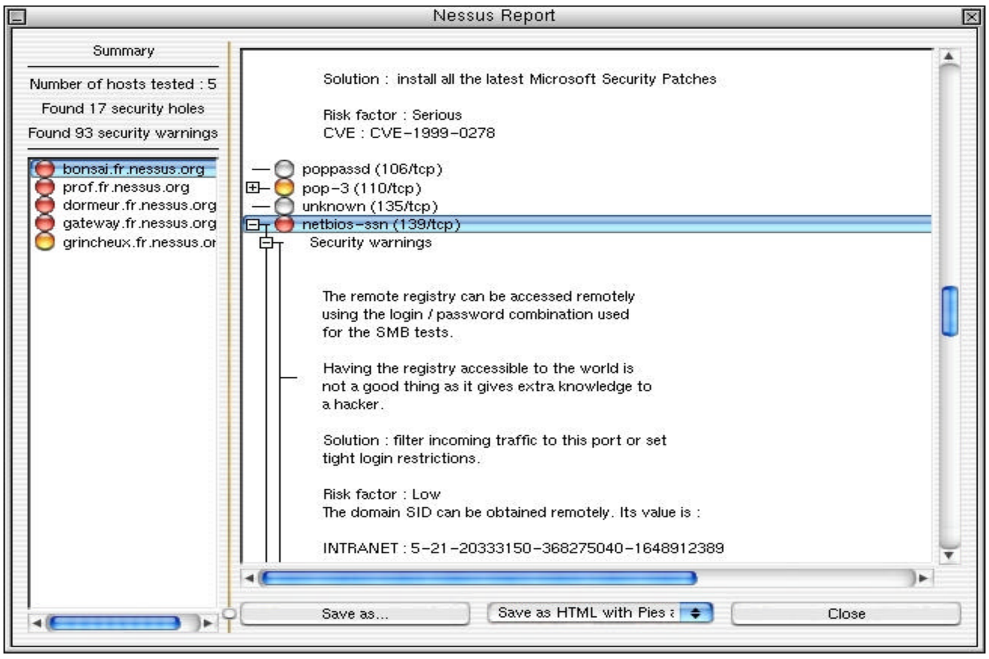
prof.fr.nessus.org
Portscan :
Attack :
Security check : Netscape Server ?PageServices bug

dormeur.fr.nessus.org
Portscan :
Attack :
Security check : mstream agent Detect

gateway.fr.nessus.org
Portscan :
Attack :
Security check : Quote of the day

bonsai.fr.nessus.org
Portscan :
Attack :
Security check : SMB use domain SID to enumerate users

Nessus GUI Report



Number of hosts tested : 5
Found 17 security holes
Found 93 security warnings

bonsai.fr.nessus.org
prof.fr.nessus.org
dormeur.fr.nessus.org
gateway.fr.nessus.org
grincheux.fr.nessus.or

Solution : install all the latest Microsoft Security Patches

Risk factor : Serious
CVE : CVE-1999-0278

poppassd (106/tcp)
pop-3 (110/tcp)
unknown (135/tcp)
netbios-ssn (139/tcp)
Security warnings

The remote registry can be accessed remotely
using the login / password combination used
for the SMB tests.

Having the registry accessible to the world is
not a good thing as it gives extra knowledge to
a hacker.

Solution : filter incoming traffic to this port or set
tight login restrictions.

Risk factor : Low
The domain SID can be obtained remotely. Its value is :

INTRANET : 5-21-20333150-368275040-1648912389

Intrusion Detection Systems

- Many to choose from
  - http://www.networkintrusion.co.uk/ids.htm
  - network (20), host (18), integrity checkers (12)
- Network IDS
  - BlackIce, Centrax, Cisco Secure, LANguard, NFR, Netranger, RealSecure Network Sensor, Shadow, Snort
- Host IDS
  - Entercept, Intruder Alert, Swatch
- Integrity Checkers
  - AIDE, chkrootkit, SecureEXE, Tripwire

Trusting Public Domain Code

- You have to see the code
  - don’t accept binaries
  - review the code for:
    - viruses
    - trojan horses
    - “odd” system calls
- Be careful when you load from unknown sites: if possible...
  - work from a protected network
  - work from a system that can be scrubbed
  - use a network sniffer to watch for strange traffic

What the Hacker KnOwZ…
about discovery

- Well…

  if 50+ slides on discovery tools that reveal a wealth of information about your site hasn’t already generated a lot of concern and a large “To Do” or “To Check-out” list…

  NOTHING WILL!

- next…Denial of Service

Notes:

Where are We?

- Profiling
  - An example
  - Intrusions
- Protocols
  - SSL
  - DNS
  - SNMP
  - Web
  - Wireless
- **Discovery and DoS**
  - Discovery
  - **Denial of Service**
- Epilog
  - Top 10ish TTD
  - References

Denial of Service

- Historically thought of as a brute-force bandwidth issue
  - use up the "pipe"
- More appropriately defined as…
  making a component unavailable
- Many component types
  - host, application, port, process, disk space, kernel resources, file, network bandwidth, modem, ISP, DNS names/addresses, intermediate hop
- Many methods
  - volume, configuration changes, crashing, masquerading, using up available "slots", management (access to interface to control component)
    - logically either a packet level or service level issue

Denial of Service: Packet Level

- Use of a protocol in ways that were unintended by the design
  - http://www.denialinfo.com/
- Packet level
  - SYN flood/attack
  - Smurf
  - TearDrop
    - version 1: overlapping data fragments
    - version 2: pointers outside the bounds of the data
  - Land
  - switch attack

- DDoS
  several major code bases in the "general" public
  - trinoo
  - Tribe Flood Network (TFN)
  - TFN 2000
  - stacheldraht/
    stacheldrahtV4
  - stacheldraht v2.666
  - shaft
  - mstream
  - trinity

Denial Of Service - SYN Attack

- Using up kernel resources
  - 1-to-1 usage relationship
  - www.cert.org/advisories/CA-1996-21.htm
- Normal TCP 3-way handshake
  - c -> s SYN (c-seq-#)
  - s -> c SYN-ACK (c-seq-#, s-seq-#)
  - c->s ACK (c-seq#, s-seq#)
  - doesn’t matter who starts or if both sides start at the same time!

SYN Attack - The Problem

- After the initial SYN
  - server maintains state (the LISTEN-Q)
  - address of client and 2 sequence numbers
  - if there is no response to SYN-ACK, server retransmits
- Attack works by
  - faking client address: must not be a real host or it will send back ICMP error message
  - eventually server’s kernel table fills up: new SYN requests are discarded!
  - **remember: it’s per port, NOT per host**

SYN attack - Tools

- Tuning of servers
  - set SYN relevant timers low and increase queues in the kernel and in apps (listen system call)

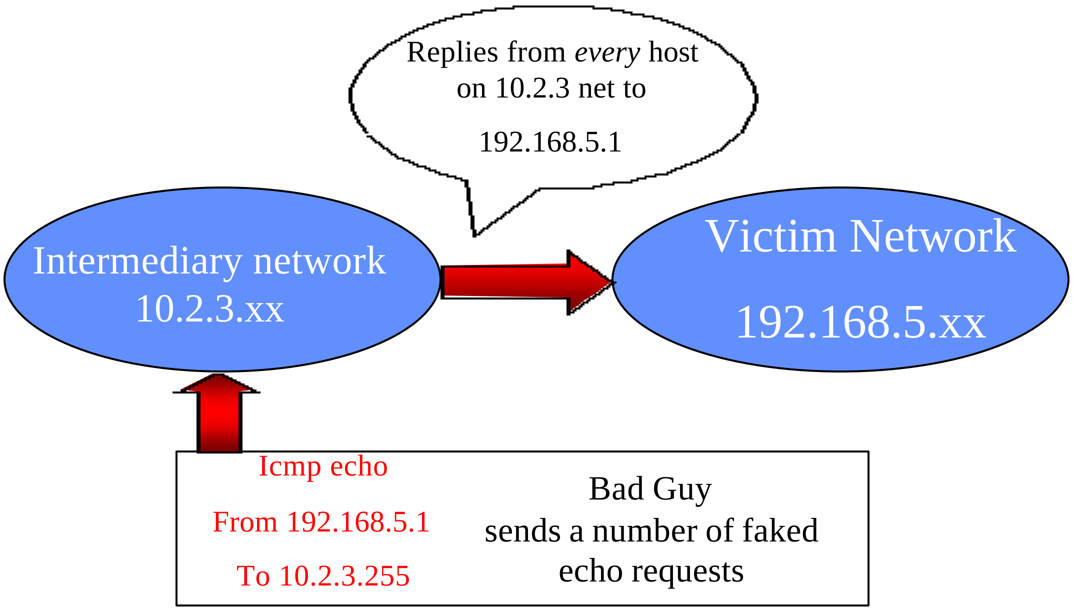
- Network testing
  - ISS’s RealSecure
    - www.iss.net/
  - Cisco (formerly Wheelgroup) NetRanger
    - www.cisco.com/univercd/cc/td/doc/product/iaabu/netrangr/
  - Haystack, consumed by Trusted Information Systems, consumed by Network Associates (which was a merger between McAfee and Network General)…of the Stalker product family

    Whew! Keeping track of this stuff is HARD!

Denial of Service - Smurf

- Smurf
    - ftp://ftp.cert.org/pub/cert_advisories/CA-98.01.smurf
  - ping the broadcast address of remote nets repeatedly (directed broadcasts)
    - 1-to-many usage relationship
  - do it with a forged address
  - can badly mess up both source and destination nets
    - (remember source is faked)
  - the more machines on the destination net the more traffic generated for each echo request

Denial of Service - Smurf, cont.



Replies from *every* host on 10.2.3 net to

192.168.5.1

Intermediary network 10.2.3.xx

Victim Network

192.168.5.xx

Icmp echo

From 192.168.5.1

To 10.2.3.255

Bad Guy sends a number of faked echo requests

Denial of Service - Teardrop/Land

- Teardrop
  - version 1: overlapping IP fragments cause crashes
  - version 2: pointers past the data fragments cause a crash
- Land
  - SYN with source address same as destination can hang targets
    - some Cisco and HP-UX versions vulnerable
- Teardrop and Land reference
  - http://www.cert.org/advisories/CA-1997-28.html

Denial of Service – switch attack

- Switches
  - one use is to prevent network sniffing since routing is based on MAC address
- Several techniques to defeat this benefit

  http://www.sans.org/newlook/resources/IDFAQ/switched_network.htm
  - ARP spoofing
    - send unsolicited fake ARP reply with MAC address of different node (e.g., dsniff)
  - MAC flooding
    - bombard the switch with bogus MAC address data to fill up the available memory for virtual circuits: default to "fail open"
  - MAC duplicating
    - reconfigure your host to have the same MAC address as another host (e.g., ifconfig on Linux)

DDoS: Distributed Denial of Service

- Trinoo
  - staff.washington.edu/dittrich/misc/trinoo.analysis
- TFN & TFN2K
  - staff.washington.edu/dittrich/misc/tfn.analysis
- Stacheldraht
  - staff.washington.edu/dittrich/misc/stacheldraht.analysis
- Mstream
  - staff.washington.edu/dittrich/misc/mstream.analysis.txt

Above analyses by David Dittrich,
University of Washington

DDoS - Trinoo

- Distributed tool used to launch coordinated UDP flood
- A Trinoo network consists of a small number of servers (masters) large number of clients (daemons)
  - intruder --> master; destination port 27665/tcp

    master --> daemons; destination port 27444/udp

    daemons --> UDP flood to target with randomized destination ports

DDoS – TFN and TFN2K

- Distributed tool used to launch coordinated attacks
  - UDP, TCP SYN, ICMP echo, and ICMP directed broadcast (aka Smurf)
- TFN2KModified version of TFN to be more clever, powerful, and stealthy
  - transport TFN2K traffic over multiple transport protocols including UDP, TCP, and ICMP
  - confuse attempts to locate TFN2K nodes in a network by sending "decoy" packets

DDoS - Stacheldraht (German for "barbed wire")

- Combines features of "trinoo" with those of the original TFN
  - adds encryption (Blowfish) of communication between the attacker and stacheldraht masters
  - automated update of the agents

DDoS in CERT News

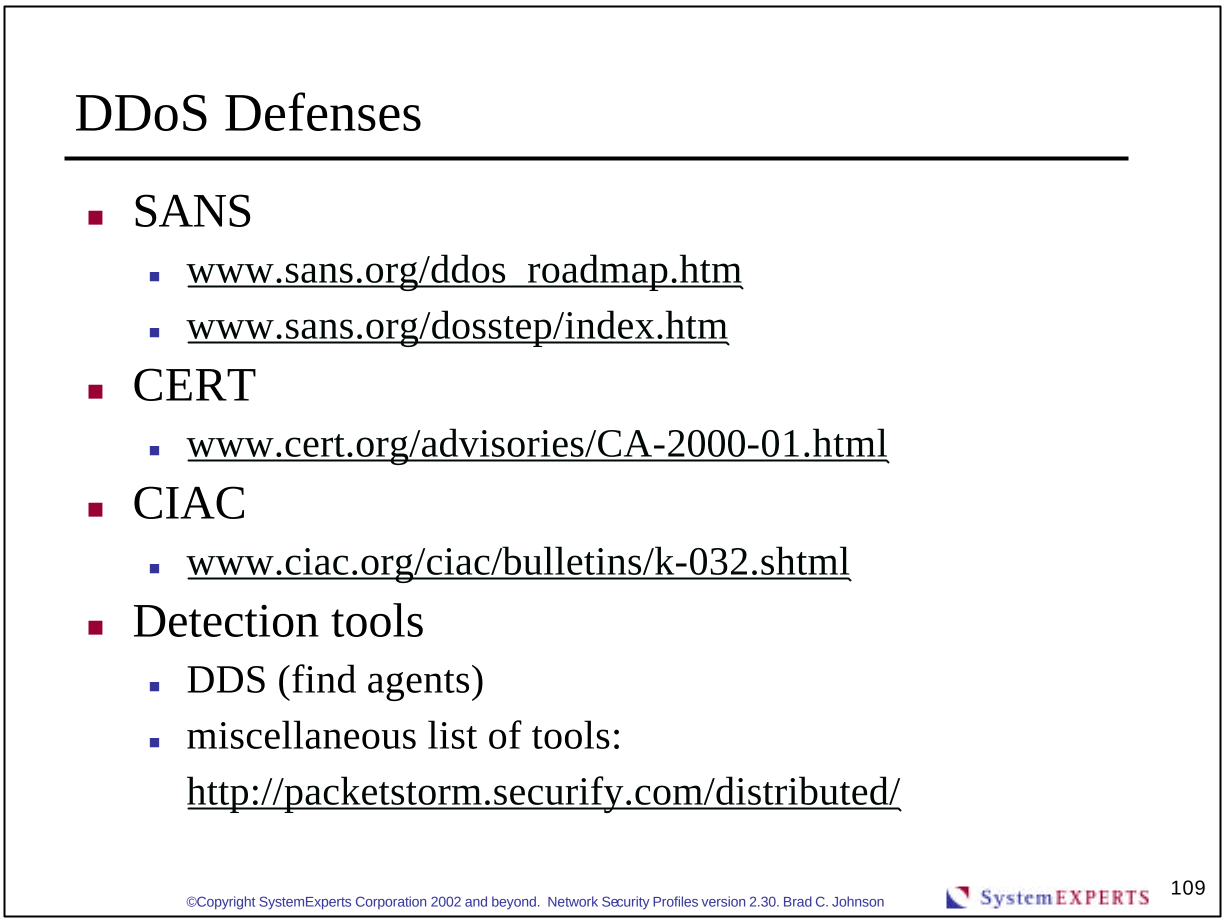
- CERT
  - www.cert.org/tech_tips/denial_of_service.html
  - www.cert.org/advisories/CA-2000-21.html
  - www.cert.org/advisories/CA-1999-17.html
  - www.cert.org/incident_notes/IN-99-07.html
  - www.cert.org/advisories/CA-1998-13.html
  - www.cert.org/advisories/CA-1996-21.html
  - www.cert.org/advisories/CA-1996-01.html

DDOS in the News, cont.

- Consensus Roadmap for Defeating Distributed Denial of Service Attacks
  A Project of the Partnership for Critical Infrastructure Security
  Version 1.10 - February 23, 2000**
  www.sans.org/ddos_roadmap.htm

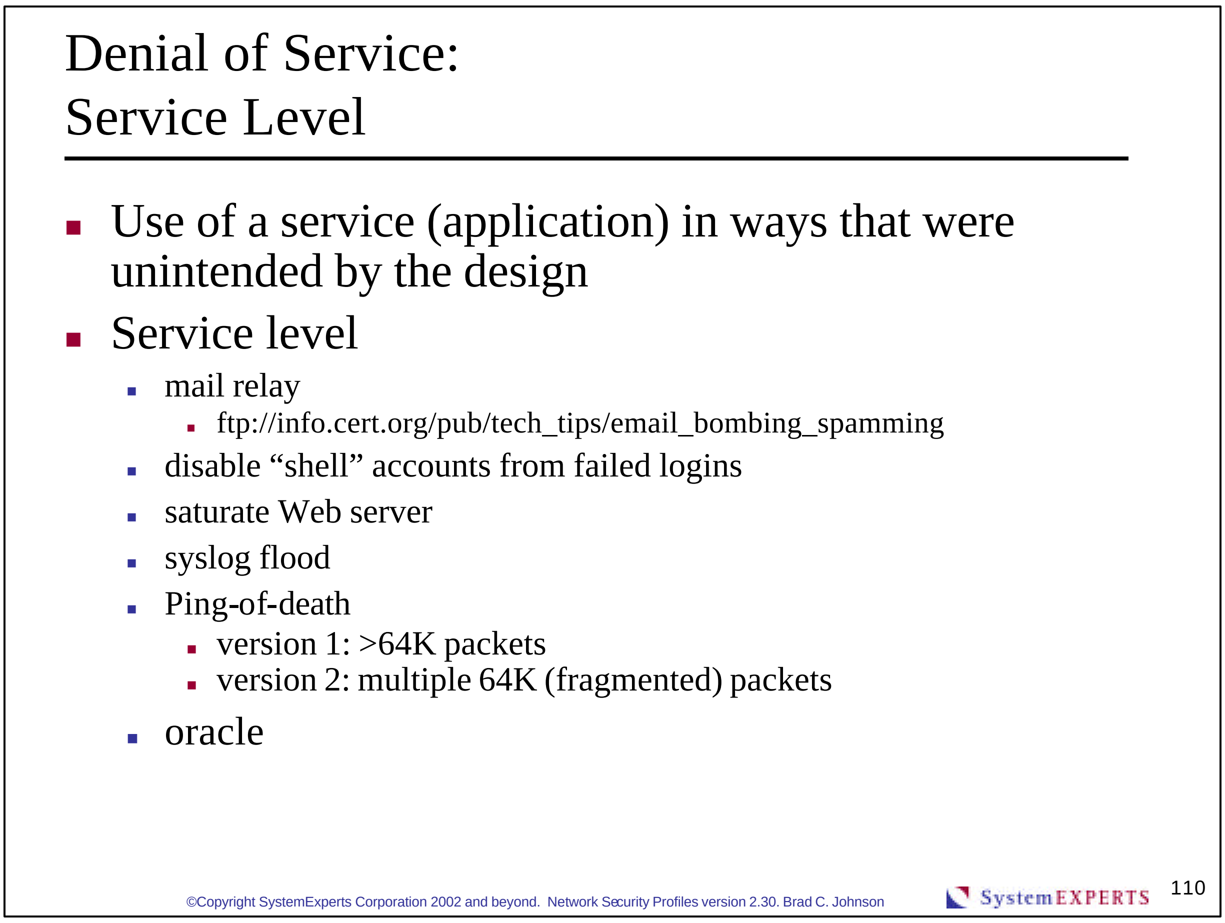
DDOS in the News, cont.

- Pulsing zombie attacks
  - short bursts of traffic
  - service degraded instead of total denial
    - irregular nature makes detection and location harder
  - www.wired.com/news/technology/0,1282,43697,00.html
- Large UDP packets directed at port 80
  - www.nipc.gov/warnings/advisories/2001/01-012.htm
  - fragmented packets
    - intended to bypass detection or blocking
  - outbound packets (from your network) may indicate that you have been infected



DDoS Defenses

- SANS
  - www.sans.org/ddos_roadmap.htm
  - www.sans.org/dosstep/index.htm
- CERT
  - www.cert.org/advisories/CA-2000-01.html
- CIAC
  - www.ciac.org/ciac/bulletins/k-032.shtml
- Detection tools
  - DDS (find agents)
  - miscellaneous list of tools:
    http://packetstorm.securify.com/distributed/



Denial of Service: Service Level

- Use of a service (application) in ways that were unintended by the design
- Service level
  - mail relay
    - ftp://info.cert.org/pub/tech_tips/email_bombing_spamming
  - disable “shell” accounts from failed logins
  - saturate Web server
  - syslog flood
  - Ping-of-death
    - version 1: >64K packets
    - version 2: multiple 64K (fragmented) packets
  - oracle

Denial of Service - Ping of Death

- IP Packets limited to 64k bytes (per RFC791)
- Some implementations allow sending of larger packets
  - some receivers will overflow 16 bit counters and crash
- Despite RFC limit of 64k packets, Windows ping allows arbitrary size

  ping -l 65510 target-host

    - www.cert.org/advisories/CA-1996-26.html
    - www.pp.asu.edu/support/ping-o-death.html

Denial of Service - NT Examples

- NT Exploits continue to be on the rise!
  [note: this is a tautology: it's always true]
  e.g., look at www.netsecurity.net
  - NTFS causes BSOD (Blue Screen of Death) by sending ill formed NT File System requests
    - executable available called crashnt.exe
  - RAS/PPTP causes BSOD by starting a session with an invalid packet length
  - Teardrop 2 causes BSOD with have the data offset in the header point after the data
  - Ping-of-Death 2 causes BSOD with multiple 64K packets
  - Sigh…just using the system causes BSOD

Denial of Service - Oracle

- Running on Windows NT
  - server allocates resources to the request: making repeated requests will use up configured resources
    - i.e., redirect connection requests are sent to a new port and a new thread is allocated: if the connection is NOT made, the thread and memory is lost until the server is restarted
    - once server memory is consumed…BSOD on next login
  - discovered by ISS
    - http://www.theregister.co.uk/content/8/19881.html
  - similar vulnerabilities discovered on Unix
    - http://xforce.iss.net/alerts/advise82.php

Denial of Service - Detection

- See if you are vulnerable...
  - But be very careful as we mentioned…but
    - Cisco (Nmap) UDP scan crashes IOS
      - all 12.0 variants, 11.3AA and 11.3DB
      - plain old 11.3 is *not* affected
    - multiple BSOD issues
      - NTFS, RAS/PPTP, Teardrop, Land, ping-of-death, Oracle
  - Do it! Just be prepared to reboot/recover

Denial Of Service - Packet Level Medicine

- Packet filters
  - stop forged addresses at your border (e.g. Land attack)
    - those coming in…AND
    - those going OUT
  - react to attacks by filtering sender
    - hard to do if the attacker is smart
      - i.e., constantly changing the source address
  - filter directed broadcasts at routers
    - possible functionality issue with LAN style discovery protocols

Medicine, cont.

- ISP Cooperation
  - ISP's could not forward packets with bogus addresses
    - ISP's have lists of valid customer addresses for routing
    - once done you could trace an attack back to its source, currently that is prohibitively expensive
  - but ... almost all do
- Cooperation from all members of the Internet
  - organizations should also not forward packets with bogus addresses…but most don't even look
  - be as concerned about what goes OUT as what comes IN!

What the Hacker KnOwZ… about denial of service

- Most organizations don't like to try denial of service attempts against themselves
- Many organizations have a "You can't stop it, so why test it?" mentality
- Many denial of service attacks are easy to try…and many will be successful

- next…SSL

Notes:

Notes:

____

____

____

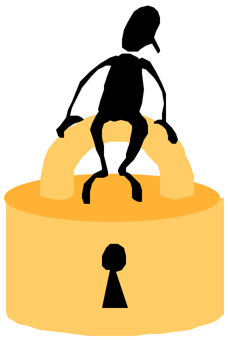
____

Where are We?

- Profiling
  - An example
  - Intrusions
- Discovery and DoS
  - Discovery
  - Denial of Service
- **Protocols**
  - **SSL**
  - DNS
  - SNMP
  - Web
  - Wireless
- Epilog
  - Top 10ish TTD
  - References

SSL Functionality

- Armored pipe between client and server
  - usually WWW (HTTP over SSL - https)
  - both integrity (hashing) and confidentiality (encryption)

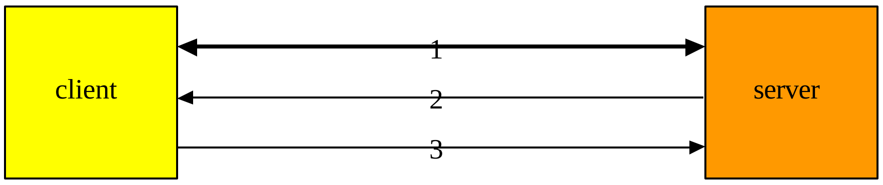


- Commonly:
  - server is authenticated to the client
  - weak or strong algorithms are chosen based on US or International browsers

SSL Functionality, cont.

- Optionally:
  - client can be authenticated via client-side X.509 certificates
    - however, not done by many applications or organizations
      - they have zero foot-print client requirements
    - many different algorithms to chose from (but limited to a just a few by most browsers)

SSL Handshake



1= exchange (pseudo) random numbers
2= server certificate,session ID
3= (pre_master_secret)$\text{PK}_{\text{server}}$

See "**SSL Crunch Time**", *Information Security*, October 1999 for some quantitative performance data on SSL

SSL Exposures: Usage, Technical, & Future

- Certificate problems
  - not signed by a trusted Certificate Authority (CA)
    - "unknown CA, do you want to accept certificates signed by Micros0ft from now on?"
  - Root CA certificates in browsers suspect
    - what mirror did you get your browser from?
      (note: I put this comment here in LATE 1998)
    - **FORGED CERT PGP KEY**
      www.cert.org/contact_cert/PGPwarning.html
    - Unauthentic Microsoft Certificates
      www.cert.org/advisories/CA-2001-04.html
      - **Anyone with the private portions of the certificates can sign code such that it appears to have originated from Microsoft**

SSL Exposures: Technical & Usage

- latent issues not resolved yet
  - (large scale) certificate replacement
  - (large scale) certificate revocation
- improper certificate validation
  - Netscape Navigator: once a valid session (pass SSL checks) is initiated, additional connections to the same IP address are assumed to part of the same session (therefore, subsequent certificate conditions are not checked)

    www.cert.org/advisories/CA-2000-05.html

SSL Exposures: Infrastructure

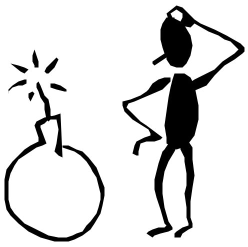
- Only real server authentication is that the DNS name in the URL matches the name in the Certificate
  - DNS lookup is NOT part of the SSL specification
  - you could be fooled into using a wrong name

    (www.delta.com vs. www.delta-air.com)

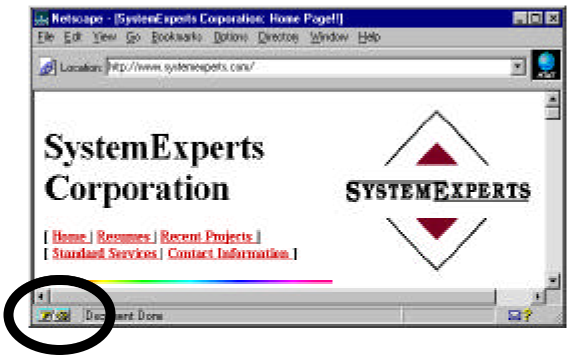
    btw: they are now both for the airline!
    - see “How do you get in the middle?” in Web Spoofing coming up in a “few” slides on how to be fooled
  - SSL doesn’t detect/stop DNS poisoning
    - www.webdevelopersjournal.com/articles/is_ssl_dead.html

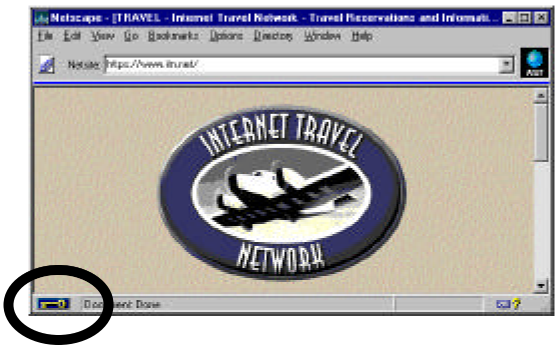
SSL Exposures: Design

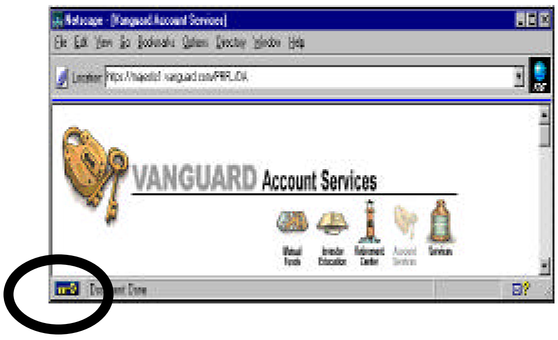
- Only using SSL for forms not all or most of your site
  - no caching of SSL by default therefore performance issues
  - what’s wrong with this picture:
    - https://www.name-changed-to-protect-the-guilty.com/order_form.cgi
    - <FORM ACTION=“http://www.site.com/process_order.cgi” METHOD=POST>



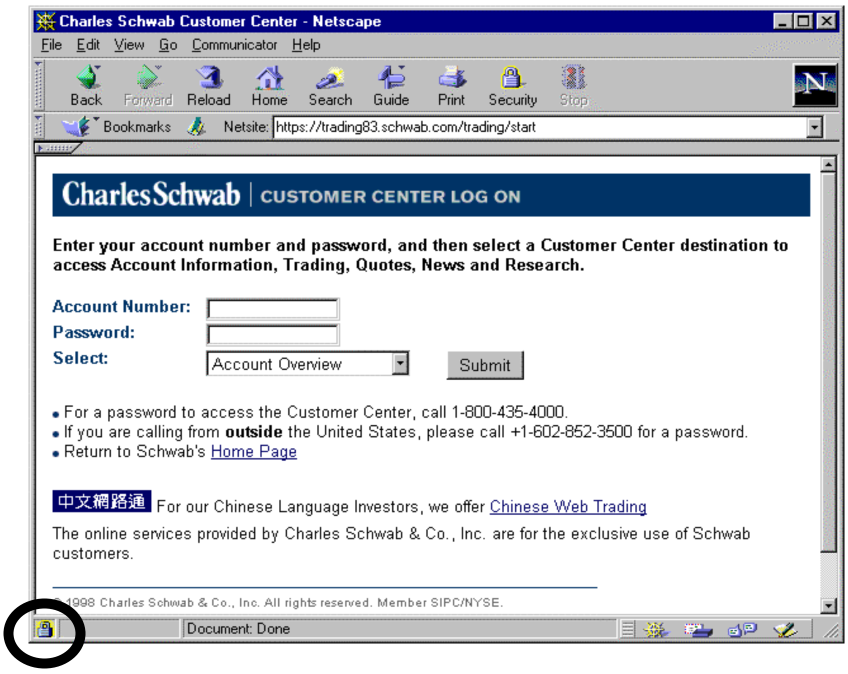
Netscape V3 SSL Strength: How do you tell?


Netscape - [SystemExperts Corporation: Home Page!!]
Location: http://www.systemexperts.com/
SystemExperts Corporation
SYSTEMEXPERTS
[Home | Resumes | Recent Projects]
[Standard Services | Contact Information]
Document Done


Netscape - [TRAVEL - Internet Travel Network - Travel Reservations and Informati...
Netsite: https://www.itn.net/
INTERNET TRAVEL NETWORK
Document Done


Netscape - [Vanguard Account Services]
VANGUARD Account Services
Document Done

Netscape 4*


Charles Schwab Customer Center - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks
Netsite:
Document: Done

https://trading83.schwab.com/trading/start

CharlesSchwab | CUSTOMER CENTER LOG ON

Enter your account number and password, and then select a Customer Center destination to access Account Information, Trading, Quotes, News and Research.

Account Number:

Password:

Select: Account Overview

Submit

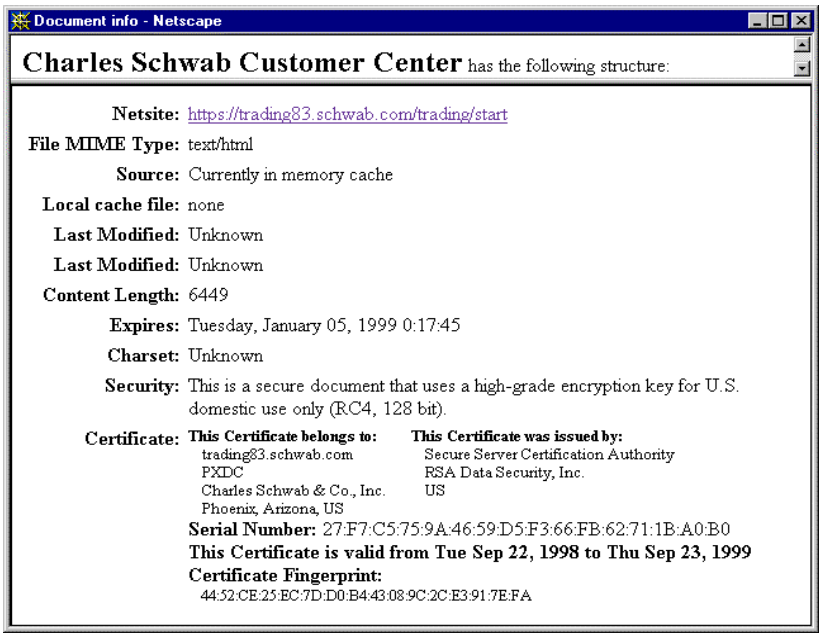
- For a password to access the Customer Center, call 1-800-435-4000.
- If you are calling from **outside** the United States, please call +1-602-852-3500 for a password.
- Return to Schwab's Home Page

中文網路通 For our Chinese Language Investors, we offer Chinese Web Trading

The online services provided by Charles Schwab & Co., Inc. are for the exclusive use of Schwab customers.

© 1998 Charles Schwab & Co., Inc. All rights reserved. Member SIPC/NYSE.

Netscape 4* Additional Info



Charles Schwab Customer Center has the following structure:

Netsite: https://trading83.schwab.com/trading/start

File MIME Type: text/html

Source: Currently in memory cache

Local cache file: none

Last Modified: Unknown

Last Modified: Unknown

Content Length: 6449

Expires: Tuesday, January 05, 1999 0:17:45

Charset: Unknown

Security: This is a secure document that uses a high-grade encryption key for U.S. domestic use only (RC4, 128 bit).

Certificate:

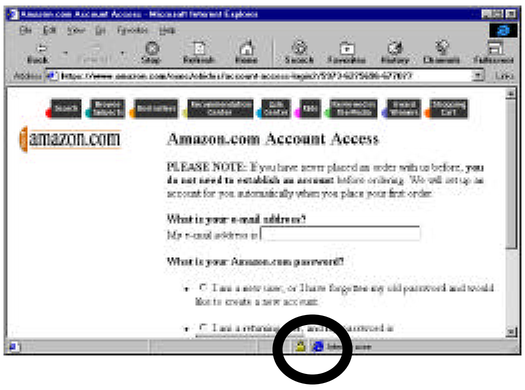
This Certificate belongs to:	**This Certificate was issued by:**
trading83.schwab.com	Secure Server Certification Authority
PXDC	RSA Data Security, Inc.
Charles Schwab & Co., Inc.	US
Phoenix, Arizona, US	

Serial Number: 27:F7:C5:75:9A:46:59:D5:F3:66:FB:62:71:1B:A0:B0

This Certificate is valid from Tue Sep 22, 1998 to Thu Sep 23, 1999

Certificate Fingerprint:
44:52:CE:25:EC:7D:D0:B4:43:08:9C:2C:E3:91:7E:FA

Internet Explorer 4 and 5: How do you tell?


Amazon.com Account Access - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen
Address
Links
Search
Browse Subjects
Bestsellers
Recommendation Center
Gift Center
Kids
Reference Desk
Award Winners
Shopping Cart
amazon.com

Amazon.com Account Access

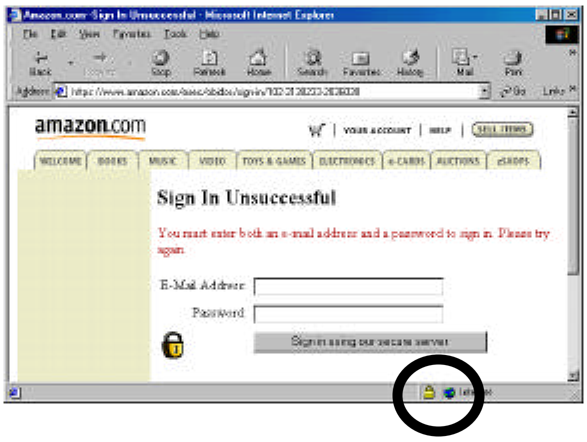
PLEASE NOTE: If you have never placed an order with us before, **you do not need to establish an account** before ordering. We will set up an account for you automatically when you place your first order.

What is your e-mail address?

My e-mail address is

What is your Amazon.com password?

- ○ I am a new user, or I have forgotten my old password and would like to create a new account.
- ○ I am a returning [illegible] and my password is


Amazon.com-Sign In Unsuccessful - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Mail Print
Address
Go
Links
amazon.com
YOUR ACCOUNT
HELP
SELL ITEMS
WELCOME
BOOKS
MUSIC
VIDEO
TOYS & GAMES
ELECTRONICS
e-CARDS
AUCTIONS
zSHOPS

Sign In Unsuccessful

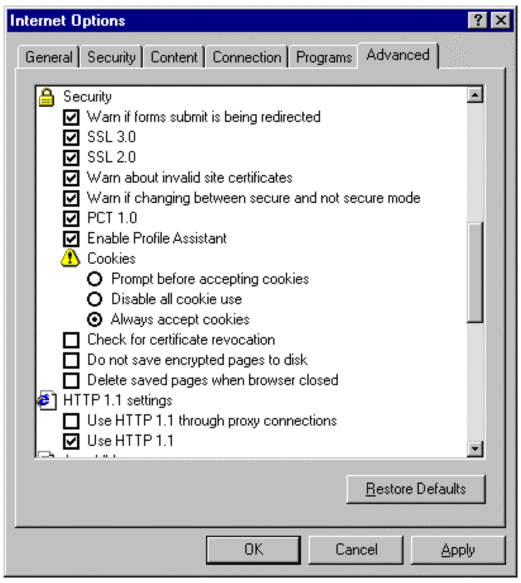
You must enter both an e-mail address and a password to sign in. Please try again.

E-Mail Address:

Password:

Sign in using our secure server

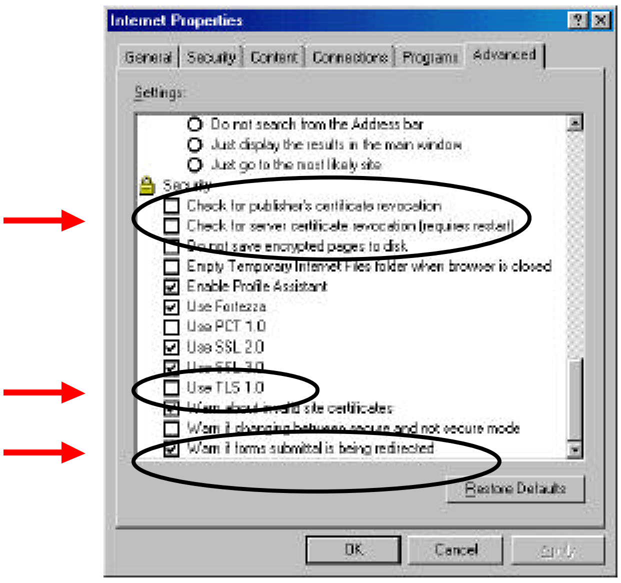
Internet Explorer 4 and 5 Advanced Options



Security
- ☑ Warn if forms submit is being redirected
- ☑ SSL 3.0
- ☑ SSL 2.0
- ☑ Warn about invalid site certificates
- ☑ Warn if changing between secure and not secure mode
- ☑ PCT 1.0
- ☑ Enable Profile Assistant

Cookies
- ○ Prompt before accepting cookies
- ○ Disable all cookie use
- ● Always accept cookies
- □ Check for certificate revocation
- □ Do not save encrypted pages to disk
- □ Delete saved pages when browser closed

HTTP 1.1 settings
- □ Use HTTP 1.1 through proxy connections
- ☑ Use HTTP 1.1



- ○ Do not search from the Address bar
- ○ Just display the results in the main window
- ○ Just go to the most likely site

Security
- □ Check for publisher's certificate revocation
- □ Check for server certificate revocation (requires restart)
- □ Do not save encrypted pages to disk
- □ Empty Temporary Internet Files folder when browser is closed
- ☑ Enable Profile Assistant
- ☑ Use Fortezza
- □ Use PCT 1.0
- ☑ Use SSL 2.0
- ☑ Use SSL 3.0
- □ Use TLS 1.0
- ☑ Warn about invalid site certificates
- □ Warn if changing between secure and not secure mode
- ☑ Warn if forms submittal is being redirected

OpenSSL

- Based on SSLeay - Eric Young's (and Tim J. Hudson) implementation
  - www.psy.uq.oz.au/~ftp/Crypto/
  - Unix and PC native versions
  - Many small certificate and crypto tools
    - s_client & s_server
- V2 & V3 SSL plus TLS (IETF V3 SSL revision)
- www.openssl.org
  - V0.9.6b available since July 9, 2001

SSL Tools - cURL

- Command line URL grabber…and much more! transferring files with URL syntax
  - HTTP and HTTPS (uses SSLeay or OpenSSL)
    - PUT and POST (including FORMS!)
    - HTTPS certificates
  - FTP
    - including upload
  - Gopher, TELNET, DICT, LDAP
  - Miscellaneous support
    - passwords
    - port numbers
    - proxies

SSL Tools cURL, cont.

- curl --help [note: edited output]

```
[Options: (H) means HTTP only (F) means FTP only
 -b/--cookie <string>         Pass the string as cookie (H)
 -c/--continue                Resume a previous transfer where we left it (F)
 -d/--data                    POST data (H)
 -e/--referer                 Referer page (H)
 -E/--cert <cert:passwd>      Specifies certificate file and password (HTTPS)
 -F/--form <name=content> Specify HTTP POST data (H)
 -I/--head                    Fetch the HTTP-header only (HEAD) (H)
 -l/--list-only               List only names of an FTP directory (F)
 -m/--max-time <seconds>      Maximum time allowed for the transfer
 -o/--output <file>           Write output to <file> instead of stdout
 -p/--port <port>             Use port other than default for current protocol
 -P/--ftpport <address>       Use PORT with address instead of PASV when ftping (F)
 -Q/--quote <cmd>             Send QUOTE command to FTP before file transfer (F)
 -r/--range <range>           Retrieve a byte range from a HTTP/1.1 server (H)
 -u/--user <user:password> Specify user and password to use
 -U/--proxy-user <user:password> Specify Proxy authentication
```

SSL Tools cURL, cont.

- A few examples
  - curl -o thatpage.html http://www.netscape.com/
  - curl -d "name=Rafael%20Sagula&phone=3320780" http://www.where.com/guest.cgi
  - curl ftp://name:passwd@machine.domain:port/full/path/to/file
    - http://curl.haxx.se/docs/readme.curl.html for manual
- Comparison to snarf, wget, greed, pavuk, fget, and fetch
  - http://curl.haxx.se/docs/comparison-table.html
- URL
  - http://www.fts.frontec.se/~dast/curl/
  - http://curl.haxx.se
    - “a client that groks URLs”

SSL Update: dsniff

- dsniff 2.3
  - among many other things, exploit flaws in both SSL and SSH

  - arpspoof: hijack IP address
  - dnsspoof: forge DNS replies
  - tcpkill: block TCP by forcing connection to close
  - filesnarf: NFS sniffer
  - mailsnarf: SMTP sniffer
  - msgsnarf: IM sniffer
  - urlsnarf: Web sniffer
- sshmitm: SSH protocol 1 attack
  - “fix”: only use protocol 2
- webmitm: SSL attack
  - “fix”: client-side certs

http://www.monkey.org/~dugsong/dsniff/faq.html

SSL Update: PKI risks

- 10 Risks of PKI: Bruce Schneier & Carl Ellison
  - http://www.counterpane.com/pki-risks.pdf

  - #1 Trusting the CA
  - #2 Who is using “your” key
  - #3 How secure is the verifying computer?
  - #4 Which “John Doe” is it?
  - #5 Is the CA an authority? Let’s look at #5…
- Is the CA an authority?
- Server certificate has 2 parts
  1. DNS name
  2. name of keyholder
- There are DNS server authorities, BUT, none of the SSL CAs in the popular browsers is one!
- There are (business) authorities on corporate names, BUT, again, none of the SSL CAs in the popular browsers is one!

What the Hacker KnOwZ… about SSL

- It isn't mysterious or SOLVE all your problems
- Many organizations think it is mysterious (and therefore secure (security via obscurity) and many think that it solves more than it actually does
- Public domain tools are robust…and getting better
- next…DNS

Notes:

____

____

____

____

Notes:

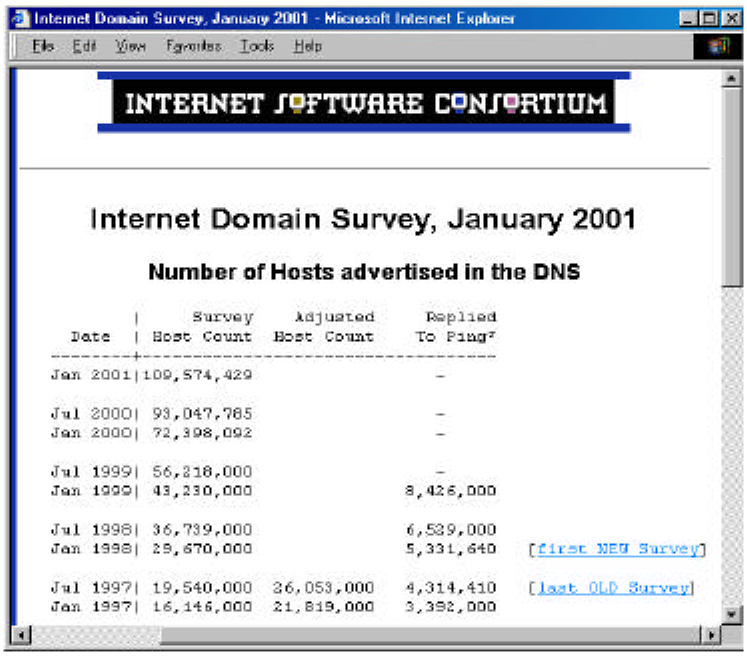
Where are We?

- Profiling
  - An example
  - Intrusions
- **Protocols**
  - SSL
  - **DNS**
  - SNMP
  - Web
  - Wireless
- Discovery and DoS
  - Discovery
  - Denial of Service
- Epilog
  - Top 10ish TTD
  - References

DNS (Domain Name Service) Functionality

- Names instead of addresses
  - hierarchical and distributed for scaling
- Standard record types
  - A - addresses
    - www.systemexperts.com
      - 207.155.248.12, 207.155.252.14, 207.155.252.72, 207.155.252.12
  - CNAME – canonical name
  - HINFO – host information
  - MX - mail exchanger
  - NS - name server
  - PTR - reverse pointer resolution
    - 12.248.155.207.in-addr.arpa
  - SOA – start of authority
  - TXT – text
  - WKS – well-known services

DNS
(An Unbelievable Demonstration of Scale)


Internet Domain Survey, January 2001 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
INTERNET SOFTWARE CONSORTIUM

Internet Domain Survey, January 2001

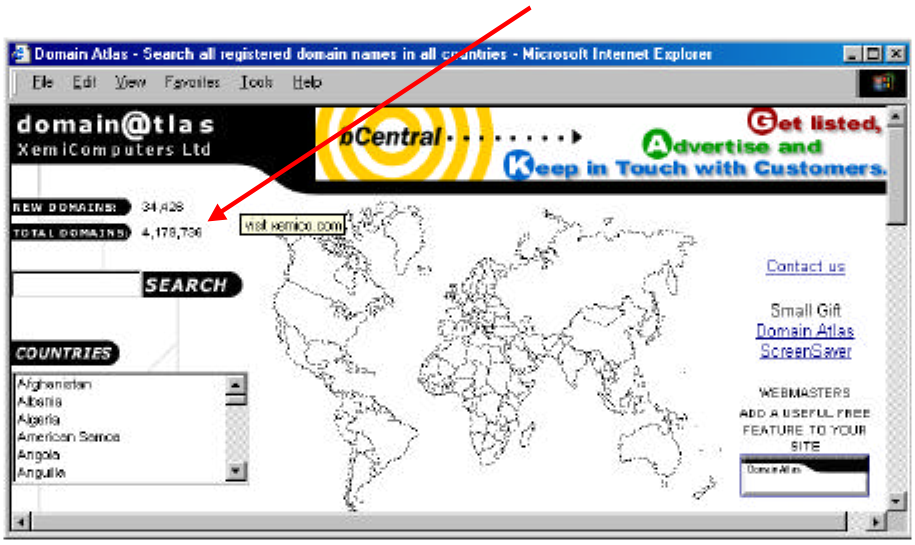
Number of Hosts advertised in the DNS

```
         |     Survey    Adjusted     Replied
  Date   | Host Count  Host Count    To Ping*
---------+-----------------------------------
Jan 2001|109,574,429                      -

Jul 2000| 93,047,785                      -
Jan 2000| 72,398,092                      -

Jul 1999| 56,218,000                      -
Jan 1999| 43,230,000                8,426,000

Jul 1998| 36,739,000                6,529,000
Jan 1998| 29,670,000                5,331,640   [first NEW Survey]

Jul 1997| 19,540,000  26,053,000    4,314,410   [last OLD Survey]
Jan 1997| 16,146,000  21,819,000    3,392,000
```

DNS Domains

www.domainatlas.com
www.domainsondisc.com/stats.html

4+ million Domains



NEW DOMAINS: 34,428
TOTAL DOMAINS: 4,178,736

DNS Exposures

- One common complex implementation
  - BIND (Berkeley internet name daemon)
  - used for **authentication** in FTP, NFS, mail, TELNET, WWW, browser CERT validation, etc.
- Can offer too much information
  - hosts behind firewalls/internal addressing, outside (ISP) services, mail servers, alternate name servers, OS types
- Spoofing
  - poison DNS server and redirect: without breaking in
    - get the target to ask you a question and return bogus unrelated info: this info is believed by older BIND versions

DNS Tools

- Dig and nslookup
- Special and OS specific tools www.dns.net/dnsrd/tools.html
    - debug cached data - DDT
        - ftp://ftp.is.co.za/networking/ip/dns/ddt/
    - find inconsistencies in DNS files - NSLint
        - ftp://ftp.is.co.za/networking/ip/dns/nslint/
- Seminal sites
    - www.isc.org/bind.html
    - www.dns.net/dnsrd/

DNS Tools DIG NS Records

```
dig ns usenix.org
; <<>> DiG 2.1 <<>> ns usenix.org
;; QUESTIONS:
;; usenix.org, type = NS, class = IN

;; ANSWERS:
usenix.org.     164133  NS      NS.UU.NET.
usenix.org.     164133  NS      XINET.COM.
usenix.org.     164133  NS      UUCP-GW-1.PA.DEC.COM.
usenix.org.     164133  NS      UUCP-GW-2.PA.DEC.COM.
usenix.org.     164133  NS      auth00.NS.UU.NET.
usenix.org.     164133  NS      usenix.org.

;; ADDITIONAL RECORDS:
NS.UU.NET.      172772  A       137.39.1.3
```

DNS Zone Transfer

```
Zone transfer usenix.org@usenix.org (131.106.3.1) …
Query for usenix.org type=252 class=1
usenix.org SOA (Zone of Authority) Primary NS:usenix.ORG Responsible
person:jrl@usenix.ORG
        serial:199905114
        refresh:432000s (5 days)
        retry:3600s (60 minutes)
        expire:864000s (10 days)
        minimum-ttl:172800s (2 days)
usenix.org NS (Nameserver) uucp-gw-1.pa.dec.com
usenix.org HINFO (Host Info) Cpu:Sun Sparc 10 Os:SunOS
usenix.org MX (Mail Exchanger) Priority: 10 mail.usenix.ORG
usenix.org MX (Mail Exchanger) Priority: 100 relay1.UU.NET
usenix.org A (Address) 131.106.3.1
```

- What did we learn?
  - Name time-outs/refresh, outside name server, SunOS OS type, primary and second mail server, and (potential) valid username

DNS Zone Transfer, cont.

- What else did we learn?
  - refresh: how often the secondary server should check that their data is up-to-date
  - retry: if the secondary server can’t reach the master site, retry at this interval
  - expire: if the secondary fails to contact the master site for this amount of time, expire (I.e., STOP ANSWERING REQUESTS) the cache data
  - minimum: how long data can live in memory (i.e., cache)
    - note: when you see “non authoritative” when you do a nslookup, that means the data was fetched from the cache (it doesn’t mean the results are questionable!)

DNS Zone Transfer, cont.

- spock.usenix.org A (Address) 131.106.3.24
  quark.usenix.org A (Address) 131.106.3.16
  offquadra.usenix.org A (Address) 131.106.3.19
  picard.usenix.org A (Address) 131.106.3.103
  khan.usenix.org A (Address) 131.106.3.106
  borg.usenix.org A (Address) 131.106.3.104
  guinan.usenix.org A (Address) 131.106.3.17
- What did we learn?
  - “special/fun” names tend to be administrative hosts
    - ask yourself: what are the names of the hosts for your admin folk?

DNS Zone Transfer, cont.

- conference.usenix.org NS (Nameserver) cs.colorado.edu
  usenix-fw.usenix.org A (Address) 131.106.1.253
  mail.usenix.org CNAME (Canonical Name) usenix.ORG
  usenix-gw.usenix.org A (Address) 131.106.1.254
  db.usenix.org A (Address) 131.106.3.253
  mtgusenix.usenix.org HINFO (Host Info) Cpu:Sun 3/80 Os:?
  mtgusenix.usenix.org A (Address) 198.4.88.2
  fw.usenix.org CNAME (Canonical Name) usenix-fw.usenix.org
  gw.usenix.org A (Address) 131.106.3.254
  www.usenix.org CNAME (Canonical Name) db.usenix.ORG
  ftp.usenix.org CNAME (Canonical Name) db.usenix.org
- What did we learn?
  - Another outside name server, hosts that are probably firewall and gateway systems (usually VERY helpful), also systems that are likely database and FTP servers

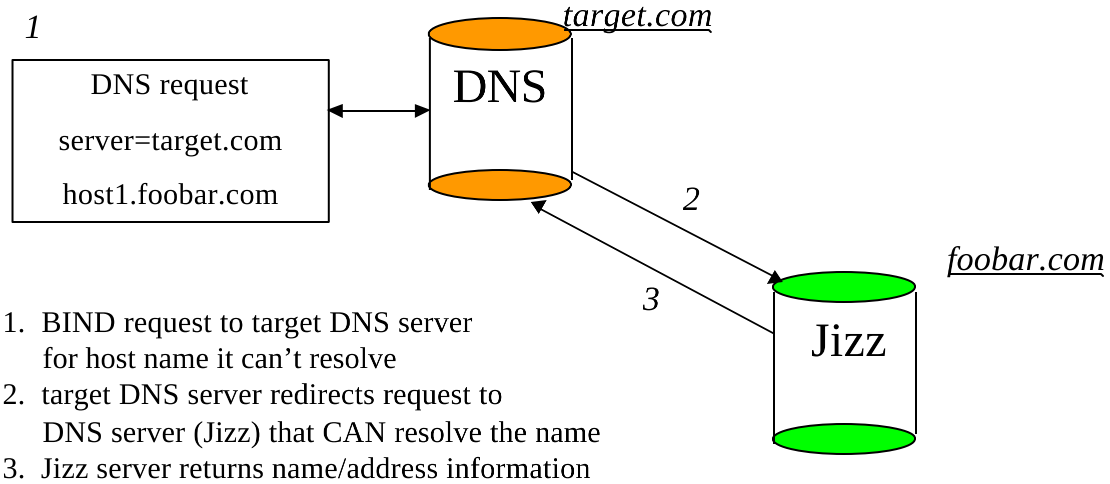
DNS Spoofing

- Jizz
  http://209.100.212.5/cgi-bin/search/search.cgi?searchvalue=jizz
  [PacketStorm]
  - a small DNS server
  - when queried responds with bogus info in additional records
    - we have modified it to support general purpose replies (not the hard coded one that comes with the program)
  - need to get victim DNS server to ask your Jizz server a question

Running Jizz

- Run Jizz on your system
- Register yourself as an authoritative DNS server for some (made up) domain
- Query the target DNS server (the one you want to poison) for a name that only your DNS server (Jizz) would know the answer to
  - dig @target xxx. foobar.com
  - send email to “yyy@xxx.foobar.com” through target
- Jizz responds with an answer to the original host query AND bogus additional records

Jizz Diagram



1. BIND request to target DNS server
   for host name it can’t resolve
2. target DNS server redirects request to
   DNS server (Jizz) that CAN resolve the name
3. Jizz server returns name/address information
   AND “additional information” as well:
   like: new address for microsoft or yahoo or WHATEVER!

Jizz Process Flow

```
▪ 1    Jizz host1. foobar.com
       www.bradcj.gov IN A 5.6.7.8

  3    DNS Poison Server – BIND cache vulnerability
       Poison Data: www.bradcj.gov IN A 5.6.7.8
       Packet from target : Port 53 host1. foobar.com.


▪ 2    dig @target host1.foobar.com
  ; <<>> DiG 2.1 <<>> @target host1. foobar.com
  ;; QUESTIONS:
  ;; test. foobar.com, type=A, class=IN


  4    ;; ANSWERS:
       host1. foobar.com. 600 A 127.0.0.1
       ;; ADDITIONAL RECORDS:
       www.bradcj.gov. 600 A 5.6.7.8
```

More DNS Exposures

- Really, this is big stuff:
  www.cert.org/incident_notes/IN-2001-03.html
  www.cert.org/advisories/CA-2000-20.html
  www.cert.org/advisories/CA-2000-03.html
  www.cert.org/summaries/CS-2000-02.html

  - NXT RR exploit (improper validation)
    - in BIND 8.2, execute arbitrary code
  - SIG RR (improper validation)
    - crash named
  - SO LINGER (violate protocol rules)
    - pause named up to 120 seconds
  - FDMAX (consume file descriptors)
    - crash named

More DNS Exposures, cont.

- Domain Name Registration process in flux
  - used to be 1 registration entity Network Solutions (USA) for .com, .net, .org., .edu
  - several "testbed" registrars chosen to create more competitive registration market
    - Network Solutions, CORE NIC, registrar.com, Internet Names (Australia), and France Telecom/Oleane
  - currently over 60 active registrars
    - www.newregistrars.com/activeregs.html
  - 7 other top-level domains being considered
    - .firm, .store, .web, .arts, .rec, .info, .nom
      - www.gtld-mou.org

More DNS Exposures, cont.

- Domain registration problem
  - fake mail to Internic (or registry.com or whomever) to change DNS registration!

    (note: I put this comment here in 1999)
    - April 2000, over 50 domains "hacked" by forging email to Network Solutions for sites using email registration which allowed the "owner" to be changed to a Hotmail email address
    - June 2000, www.2600.com had their domain transferred to register.com using the same technique
- ISC DHCP client with root exploit
  - versions prior to 2.0 patch level 3 and 3.0b patch level 7

Even More DNS Exposures, cont.

- More CERT announcements
  - http://www.cert.org/advisories/CA-2001-02.html

    prior to 4.9.8/8.2.3
    - TSIG error handling
      - BIND8, execute arbitrary code
    - 2 different nslookupComplain()
      - BIND4, execute arbitrary code
    - expose program and environment variables
      - BIND4 and BIND8
  - http://www.cert.org/incident_notes/IN-2001-11.html
    - cache corruption (on glue records: e.g., top-level domain servers) on Microsoft DNS servers (NT 4.0 and 2000)

DNS Medicine

- DNSSec (IETF RFC 2535)
  - features
    - data is signed (using SIG and KEY records)
    - transfers are signed (TSIG)
  - related works
    - RFC 2536 : storage of DSA keys, 2537 : storage of RSA keys, 2538 : defines CERT RR, 2539 : storage of Diffie Hellman keys, 2541 : operational concerns
  - issues
    - lots of operational concerns (e.g., compatibility, scalability, policies)
      - gaps in the key-signing chaining
  - reference material
    - www.nic-se.se/dnssec/

DNS Medicine, cont.

- BIND version 9.1.2 available (May 4, 2001)
  - DNS Security
    - DNSSEC (signed zones)
    - TSIG (signed DNS requests)
  - IP version 6
    - Answers DNS queries on IPv6 sockets
    - IPv6 resource records (A6, DNAME)
  - Rewritten code base
    - smaller, less complex, attention to coding practices (e.g., buffer overflow problems)
- Run “as current” BIND version as you can
  - Push your ISP to run current BIND if they handle your DNS
    - how many ISPs do you have?
- Disallow, control, or wrap DNS queries
  - many sites use external/internal (split) DNS servers

DNS Medicine, cont.

- Foiling DNS attacks – Jay Beale
  Configuration decisions
        - define appropriate allow-transfer and allow-query values
        - chroot the server
    - HINFO and TXT record decision
        - remove from zone data file or use split DNS
    - Header decision
        - obscure or change version – to make it hard for script kiddies
- Other DNS help
    - www.acmebw.com/resources/papers/securing.pdf

What the Hacker KnOwZ…
about DNS

- DNS exploits are another BIG/HUGE opportunity
    - affect many important services (e.g., HTTP, FTP, TELNET, mail, NFS, Login*, etc.)
    - source of many "hacking" efforts
- In all likelihood, you have to depend on servers that you don't manage/own or can assume you should trust!

- next…SNMP

Notes:

Where are We?

- Profiling
  - An example
  - Intrusions
- **Protocols**
  - SSL
  - DNS
  - **SNMP**
  - Web
  - Wireless
- Discovery and DoS
  - Discovery
  - Denial of Service
- Epilog
  - Top 10ish TTD
  - References

SNMP

- Simple Network Management Protocol
  - agents
    - collect data (MIB), provide data to managers, and respond to commands
  - managers
    - interface for controlling and observing agent data
- Four functions
  - get (read data)
  - set (change data)
  - trap (agent send an alert to a manager)
  - inform (manager send an alert to another manager)

Default MIB Overview MIB-II (Management Information Block)

- System Group
- Interfaces Group
  - quantity, type, characteristics
- AT Group
  - interface address mappings
- IP Group
  - metrics, mappings
- ICMP Group
  - metrics
- TCP Group
  - metrics, connections
- UDP Group
  - metrics, connections
- EGP Group
  - metrics, neighbors
- SNMP Group
  - metrics

MIB Group Example

```
▪ tcpConnTable OBJECT-TYPE
          SYNTAX SEQUENCE OF TcpConnEntry
          ACCESS not-accessible {read-only, write-only, read-write}
          STATUS mandatory {optional, obsolete}
          DESCRIPTION
                         "A table containing TCP connection-specific information."
  ::= { tcp 13 }
▪ tcpConnEntry OBJECT-TYPE
          SYNTAX TcpConnEntry
          ACCESS not-accessible
          STATUS mandatory
          DESCRIPTION
                         "Information about a particular current TCP connection."
          INDEX {              tcpConnLocalAddress, tcpConnLocalPort,
                               tcpConnRemAddress, tcpConnRemPort }
  ::= { tcpConnTable 1 }
```

SNMP Exposures

- Data Gathering
  - hardware and software profiles
    - data is dynamic real-time information
  - network topology
    - data is dynamic real-time information
  - administrative environment characteristics
    - data is static and manually defined
- Network management behavior
  - modify administrative parameters

Network Management Behavior
27 Default Parameters that can Change

- System contact, name, and location
- Interface state (up, down)
- Media physical address
- Network (IP) address
- IP state (gateway forwarding or not)
- IP TTL value
- IP next HOP address
- IP route age and mask
- TCP state (terminate connection)
- Neighbor state (start and stop communication)
- Enable SNMP traps

Default SNMP community string management:
How about your wireless Access Points?

SNMP Detection

- SNMP request failures
  - snmpInBadVersions
  - snmpInBadCommunityNames
  - snmpInBadCommunityValues
  - snmpInNoSuchNames
  - snmpInASNParseErrs

Good fields to check for generating events or alarms

SCOTTY SNMP Overview

- SNMP session -address w.x.y.z -community 2ez2ez
  -port, -version, -writecommunity, -user, -password, etc.

  - snmp0 get sysDescr.0
  - snmp0 get “sysDescr.0 sysName.0 sysContact.0”
  - snmp0 walk x “tcpConnTable” { puts $x }
  - snmp0 set [list ipDefaultTTL.0 “254”]

SCOTTY SNMP Source

-
```
proc SnmpDiscover
{net delay window retries timeout}
{for {set i 1} {$i < 255} {incr i}
        {set s [snmp session -address $net.$i
        -delay $delay -window $window -retries $retries
        -community $password -timeout $timeout]
        $s get sysDescr.0
        {if {"%E" == "noError"}
                {set d [lindex [lindex {%V} 0] 2]
                regsub -all "\[\n\r\]" $d "" d
                puts "[%S cget -address]\t$d”}
        %S destroy}
update}
snmp wait}
```

- I wrap this with a routine to check all historically valid SNMP community strings from previous projects

SNMP Medicine

- Community string naming strategy
  - should be similar to username/password policies
- Use router (DMZ) IP address filtering
- Disable SNMP agents on systems not being probed by network management software

Medicine, cont.

- SNMPv3 (RFC 2570) - used in conjunction with SNMPv2 (preferred) or SNMPv1
  - security features
    - encryption and authentication
  - issues
    - difficulty in agreeing on a common approach, two approaches (V2u and V2*) being researched that will blend into an Advisory Team to create a single common approach
  - reference material
    - www.snmp.com/snmpv3/index.html
    - www.ietf.org/html.charters/snmpv3-charter.html
    - Sys Admin, Network Security, May 2000, Vol. 9 #5, Eric Davis p. 43, “SNMPv3 — User Security Model”
    - www.networkcomputing.com (use search engine)
      - vendors have products “in the wings” and a survey indicates that most users (~70%) will not deploy for at least 1 year

What the Hacker KnOwZ… about SNMP

- Incredibly rich, accurate, and relevant information
- Many organizations either forget about managing SNMP, or manage it quite loosely

- next…Web

Notes:

____

____

____

____

Notes:

Where are We?

- Profiling
  - An example
  - Intrusions
- **Protocols**
  - SSL
  - DNS
  - SNMP
  - **Web**
  - Wireless
- Discovery and DoS
  - Discovery
  - Denial of Service
- Epilog
  - Top 10ish TTD
  - References

Web Exposures

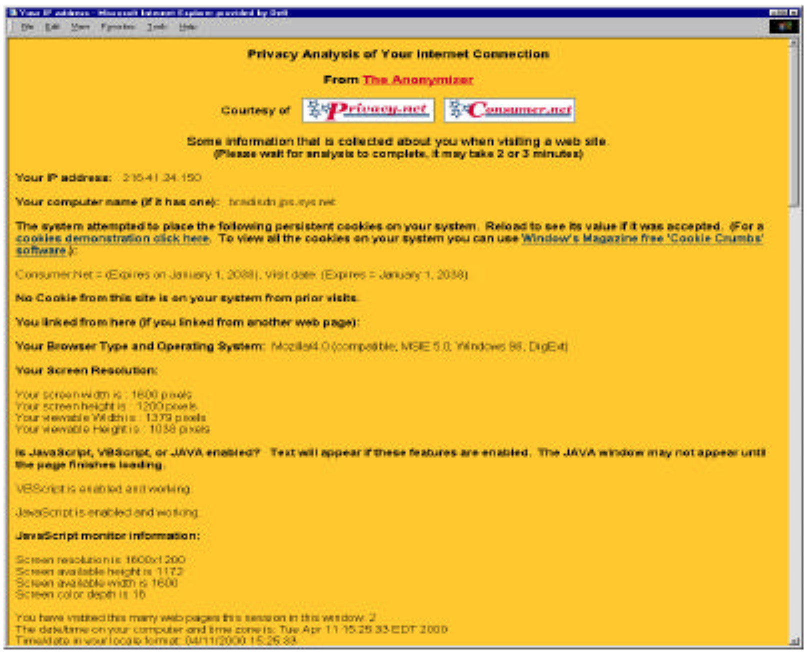
- Protocol
  - HTTP, HTTPS
  - SSL
    - Certificates (granting, revoking)
    - (DNS) Name lookup
- Web Application Source
  - FORMS and page input rewriting
  - HTML, ActiveX, Java*, other client-side code
  - cookie modification
    - on-disk for HTTP
    - in memory for HTTPS
- HTTP server
  - server configuration exploits
  - distribution examples exploits

Web Protocol - Web Spoofing

- Used to "take over" an entire site
  - you might ask for that!
    - www.anonymizer.com/ (Anonymous surfing)
      - e.g., anon.free.anonymizer.com/http://www.systemexperts.com
    - www.shodouka.com/ (View Web in Japanese)
      - e.g., www.lfw.org/shodouka/http://www.netscape.com/ja/
- Allows traffic to be intercepted and changed
- Requires some vigilance by user to detect
  - detection not likely in mass market situations

    does your mother, uncle, mechanic, or neighbor know… What a URL is? What a valid CERT looks like? What a fingerprint is for? How to look at the HTML source?

Anonymizer


Your IP address - Microsoft Internet Explorer provided by Dell
File Edit View Favorites Tools Help

Privacy Analysis of Your Internet Connection

From The Anonymizer

Courtesy of Privacy.net Consumer.net

Some information that is collected about you when visiting a web site.
(Please wait for analysis to complete, it may take 2 or 3 minutes)

Your IP address: 216.41.24.150

Your computer name (if it has one): bradjohn.gis.sys.net

The system attempted to place the following persistent cookies on your system. Reload to see its value if it was accepted. (For a cookies demonstration click here. To view all the cookies on your system you can use Window's Magazine free 'Cookie Crumbs' software.):

ConsumerNet = (Expires on January 1, 2038), Visit date: (Expires = January 1, 2038)

No Cookie from this site is on your system from prior visits.

You linked from here (if you linked from another web page):

Your Browser Type and Operating System: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98; DigExt)

Your Screen Resolution:

Your screen width is : 1600 pixels
Your screen height is : 1200 pixels
Your viewable Width is : 1379 pixels
Your viewable Height is : 1038 pixels

Is JavaScript, VBScript, or JAVA enabled? Text will appear if these features are enabled. The JAVA window may not appear until the page finishes loading.

VBScript is enabled and working.

JavaScript is enabled and working.

JavaScript monitor information:

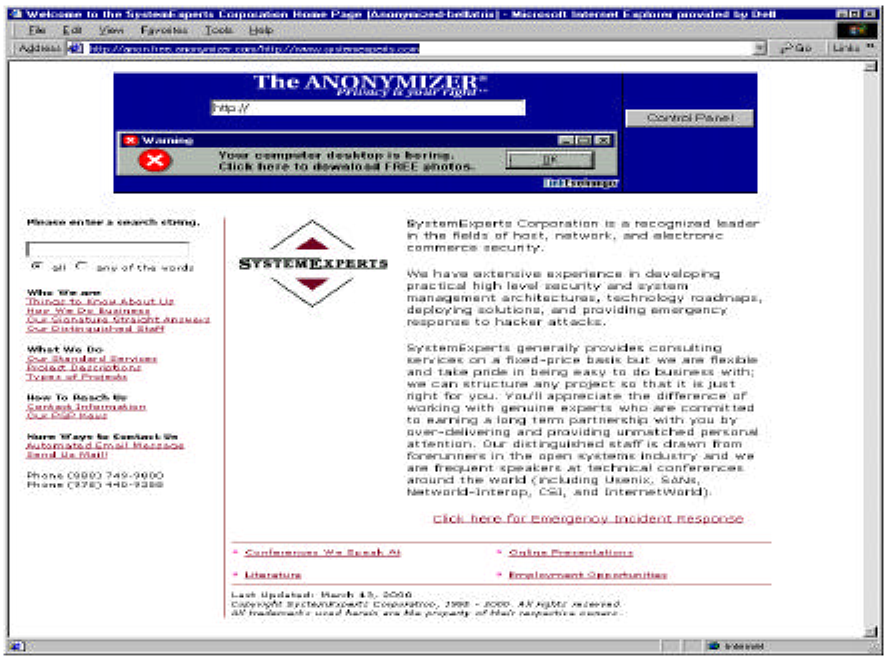
Screen resolution is: 1600x1200
Screen available height is: 1172
Screen available width is: 1600
Screen color depth is: 16

You have visited this many web pages this session in this window: 2
The date/time on your computer and time zone is: Tue Apr 11 15:25:33 EDT 2000
Time/date in your locale format: 04/11/2000 15:25:33

Understanding URL Deconstruction

- Protocol://host:port/pathname#hash?search
  - protocol is up to and including the first colon (client: e.g., browser)
  - host is the host and domain name/IP (DNS)
  - the port that the server uses for communications (socket connect)
  - pathname is the URL-path (file) portion of the URL (file system)
  - hash is an anchor name fragment in the URL, including the hash mark (#) -- this applies to HTTP URLs only (HTTP server)
  - search is any query information in the URL, including the question mark -- this applies to HTTP URLs only: the search string contains variable and value pairs; each pair is separated by an ampersand (server application)
- Examples
  - http://www.systemexperts.com
  - http://www.systemexperts.com:80/index.htm
  - http://www.intruder.com:8080/http://www.systemexperts.com

Web Spoofing Example



Welcome to the SystemExperts Corporation Home Page [Anonymized-bellatrix] - Microsoft Internet Explorer provided by Dell

Address: http://anon.free.anonymizer.com/http://www.systemexperts.com/

Warning

Your computer desktop is boring.
Click here to download FREE photos.

Please enter a search string.

○ all ○ any of the words

Who We are
Things to Know About Us
How We Do Business
Our Signature Straight Answers
Our Distinguished Staff

What We Do
Our Standard Services
Project Descriptions
Types of Projects

How To Reach Us
Contact Information
Our PGP Keys

More Ways to Contact Us
Automated Email Message
Send Us Mail!

Phone (888) 749-9800
Phone (978) 440-9388

SystemExperts Corporation is a recognized leader in the fields of host, network, and electronic commerce security.

We have extensive experience in developing practical high level security and system management architectures, technology roadmaps, deploying solutions, and providing emergency response to hacker attacks.

SystemExperts generally provides consulting services on a fixed-price basis but we are flexible and take pride in being easy to do business with; we can structure any project so that it is just right for you. You'll appreciate the difference of working with genuine experts who are committed to earning a long term partnership with you by over-delivering and providing unmatched personal attention. Our distinguished staff is drawn from forerunners in the open systems industry and we are frequent speakers at technical conferences around the world (including Usenix, SANS, Networld-Interop, CSI, and InternetWorld).

Click here for Emergency Incident Response

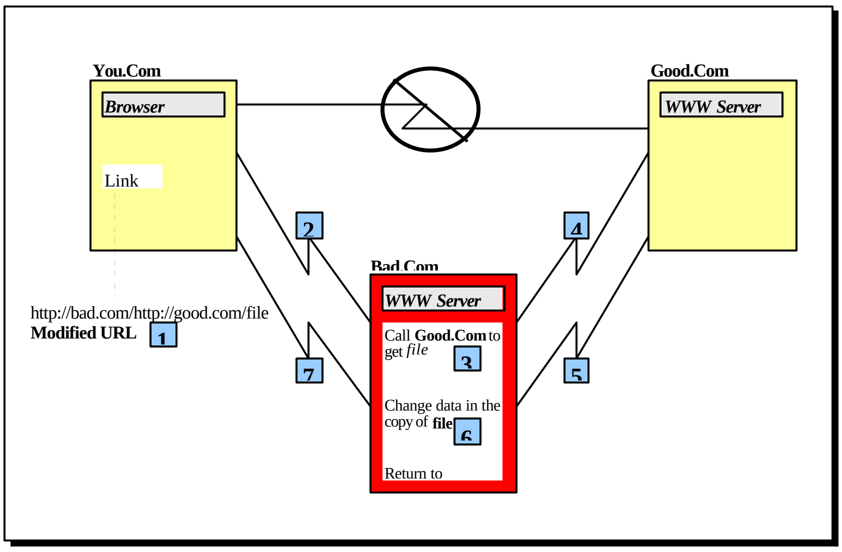
- Conferences We Speak At
- Online Presentations
- Literature
- Employment Opportunities

Last Updated: March 13, 2000
Copyright SystemExperts Corporation, 1998 - 2000. All rights reserved.
All trademarks used herein are the property of their respective owners.

Web Spoofing explained

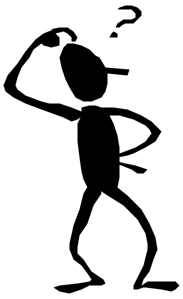
- Walk through:
  - the wanted URL is prefaced with the intruder’s URL
  - normal HTTP protocol will handle this just fine
  - the intruder site calls the REAL site and asks for the requested URL information
  - the REAL site returns the page as requested to the intruder
  - the intruder site massages the data (to change all URL references) and returns it to you

Web Spoofing Diagram


You.Com
Browser
Link
http://bad.com/http://good.com/file
Modified URL
1
2
Bad.Com
WWW Server
Call Good.Com to get *file*
3
4
Good.Com
WWW Server
5
Change data in the copy of **file**
6
Return to
7

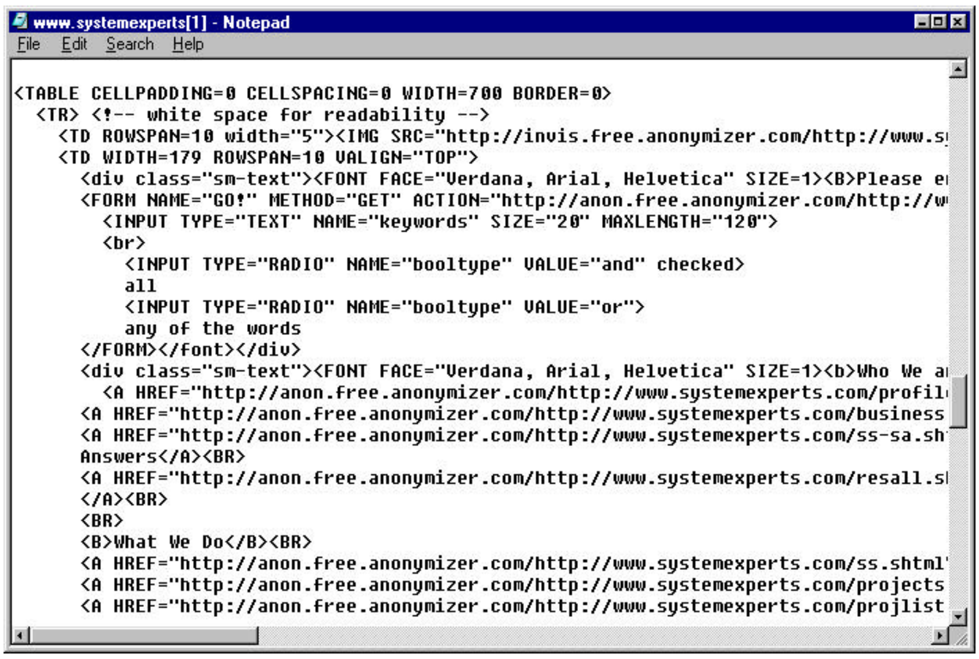
Web Spoofing:
How does that work again?

- You, the bad guy, must have an HTTP server that somehow gets in the middle of the client and the intended target, to be successful you need:
  - Web server
    - Apache, Netscape, IIS, etc.
  - an IP address



- Your server does URL rewriting
  - http://www.SystemExperts.com …is changed to…
  - http://www.intruder.com/http://www.SystemExperts.com

Web Spoofing Example, cont.



```
<TABLE CELLPADDING=0 CELLSPACING=0 WIDTH=700 BORDER=0>
  <TR> <!-- white space for readability -->
    <TD ROWSPAN=10 width="5"><IMG SRC="http://invis.free.anonymizer.com/http://www.s
    <TD WIDTH=179 ROWSPAN=10 VALIGN="TOP">
      <div class="sm-text"><FONT FACE="Verdana, Arial, Helvetica" SIZE=1><B>Please e
      <FORM NAME="GO!" METHOD="GET" ACTION="http://anon.free.anonymizer.com/http://w
        <INPUT TYPE="TEXT" NAME="keywords" SIZE="20" MAXLENGTH="120">
        <br>
          <INPUT TYPE="RADIO" NAME="booltype" VALUE="and" checked>
          all
          <INPUT TYPE="RADIO" NAME="booltype" VALUE="or">
          any of the words
      </FORM></font></div>
      <div class="sm-text"><FONT FACE="Verdana, Arial, Helvetica" SIZE=1><b>Who We a
        <A HREF="http://anon.free.anonymizer.com/http://www.systemexperts.com/profil
      <A HREF="http://anon.free.anonymizer.com/http://www.systemexperts.com/business
      <A HREF="http://anon.free.anonymizer.com/http://www.systemexperts.com/ss-sa.sh
      Answers</A><BR>
      <A HREF="http://anon.free.anonymizer.com/http://www.systemexperts.com/resall.s
      </A><BR>
      <BR>
      <B>What We Do</B><BR>
      <A HREF="http://anon.free.anonymizer.com/http://www.systemexperts.com/ss.shtml'
      <A HREF="http://anon.free.anonymizer.com/http://www.systemexperts.com/projects
      <A HREF="http://anon.free.anonymizer.com/http://www.systemexperts.com/projlist
```

How do you get in the middle?

- Easy
  - DNS Poisoning (if available, direct and easy)
  - register a confusing or false URL entry in a search engine (easy but indirect)
  - have a “convincing” message using FAX, email, ad, or letter that encourages somebody to use your site (easy but also indirect)
- Hard
  - hack into the target server system (direct but hard)
  - you work for the target server system and are paid lots ‘O money to do it by the bad guys! (direct, but hard and costly)

How do you get in the middle? Part II

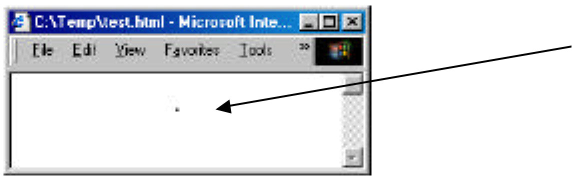
- Another new approach called:
  Web Page Pointer Theft
  - people steal/copy your meta tag data
    - potentially download your entire site!
  - then push their site (with your info) into search engines
  - end-users get tricked into thinking the “bad guys” are offering some desirable service and find themselves automatically transferred to someplace else
    - www.technoinsurance.com/website.htm
    - community.borland.com/devnews/article/1,1714,10429,00.html

Web Source Code: Things are REALLY different now

- Web applications are fundamentally different than historical business applications
  - much of the code is on-line
  - input data comes from an unpredictable source
  - more likely that bad guys have access
- Classes of problems include
  - special characters and practices
  - threshold input handling
  - modified pages
  - server exposures
    - validation of forms, format, and input

Special Practices Example

- Web Bugs
  - also known as transparent GIFs
- Simple embedded code has unexpected consequences
  - references other (server) sites
  - your system receives “unknown” cookies
- Code
  - <HTML><BODY><CENTER>
    <IMG SRC="http://www.toolzone.com/isuite/bin/counter.cgi?
    UID=TZ045288&APPID=webveil" **border="1"** >
    </CENTER></BODY></HTML>



There it is!!

Threshold Input Handling Exposures

- Unintended understanding of security characteristics
  - JavaScript code defines password characteristics
    - length, type, quality, life expectancy
- Unintended security design
  - implementation doesn’t match design
    - credentials only checked once
- Server doesn’t revalidate EVERYTHING
  - forms data
  - forms ACTION references
  - (re)authentication (e.g., User ID)

Modified (client-side) Pages and Examples

- Change client-side HTML source
  - download page
  - save to disk
  - edit page
  - reload into browser
  - send to server
    - file = “/etc/password” vs. file = “http://url”
    - file = “http://url/cgi-bin/” vs. file = “http://url”
    - <Input TYPE=HIDDEN NAME="CHK_PSWD" VALUE="NO" SIZE=0>
    - <AREA SHAPE="RECT" COORDS="15,170,290,228” HREF="/directory/page-code?USER_ID=1070">

HTTP Server Exposures Issues

- Used to exploit problems in the server code itself or to exploit problems with the release distribution
  - read files outside of server area
  - download server side scripts
  - execute arbitrary commands
- Exploits are normally the focus of hacker groups and well publicized
- For most people, only requires ability to find, read, and recreate exploits
  - that is, it’s easy for script kiddies to copy
    - e.g., whisker

(Old) HTTP Server Exposures Examples

- CA-97.24 Count CGI Program
  - www.cert.org/advisories/CA-1997-24.html
  - allows indirect file references
- What does it look like?
  - http://your.host/cgi-bin/Count.cgi?display=image&image=../../../../../../path_to_gif/file.gif
  - Thought this was old…but, if you forget to Chroot server_root…same thing can happen

(Newer) HTTP Server Examples, cont.

- IIS 4.0
  Administer site through http://localhost:5416/
  - allows viewing of all directories (not files)
  - What does it look like?
    - http://site/scripts/iisadmin/bdir.htr??d:\webs\
- IIS 4.0
  Sample pages section has active server page that supports virtual paths
  - allows access to any file on the same drive (need to give exact name)
  - What does it look like?
    - http://site/iissamples/exair/howitworks/codebrws.asp?source=/../../boot.ini
      - YOW!

(Newest) HTTP Server Examples, cont.

- Windows 2000 & IIS 5.0
  ISAPI extension to support Internet Printing Protocol (IPP)
  - buffer overflow that allows executing arbitrary code in the Local System security context: i.e., CONTROL
  - approximately 6 MILLION sites vulnerable
- What does it look like?
  - GET /NULL.printer HTTP/1.0
    Host: [buffer]

    Where [buffer] is approximately 420 characters
    http://marc.theaimsgroup.com/?l=bugtraq&m=98874912915948&w=2

    Program out there called jill.c that demonstrates the overflow

(Newest) HTTP Server Examples, cont.

- Cisco IOS HTTP server authentication vulnerability
  - IOS using local authentication
    (i.e., not TACACS+ or Radius)
  - execute arbitrary commands at the highest level (15)
- What does it look like?
  - http://<address>/level/XX/exec/…
    - XX is between 16 and 99
    - all releases 11.3 and LATER are vulnerable
- What to do?
  - disable HTTP server (i.e., configure terminal “no ip http server”)
  - use TACACS+ or Radios
  - install fixed upgrade

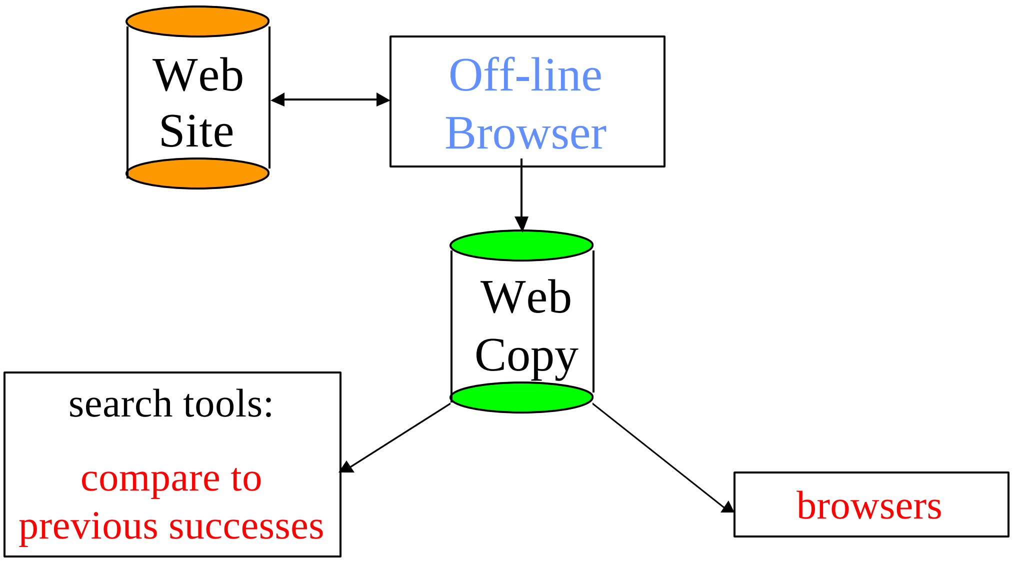
(Newest) HTTP Server Examples, cont.

- Code Red: IIS 4.0 and 5.0
  - **Buffer Overflow In IIS Indexing Service DLL**
    - http://www.cert.org/advisories/CA-2001-13.html
    - http://www.cert.org/advisories/CA-2001-19.html
    - http://www.cert.org/advisories/CA-2001-23.html
    - http://www.cert.org/incident_notes/IN-2001-10.html
    - http://www.cert.org/incident_notes/IN-2001-09.html
    - http://www.cert.org/incident_notes/IN-2001-08.html
- Web site defacement and possible performance degradation
  - …oh and execute arbitrary commands too

Offline Browser Technology

- Making it easy to review a Web site off line…in a way that probably wasn't intended
  - Web Snake
  - NavRoad
  - Black Widow (works with https !)
  - WeBCopier
  - Web VCR
  - Web ZIP
  - Offline Explorer
  - DISCo Pump

Using Off-line Browsers



Web Site

Off-line Browser

Web Copy

search tools:

compare to previous successes

browsers

What the Hacker KnOwZ… about the Web

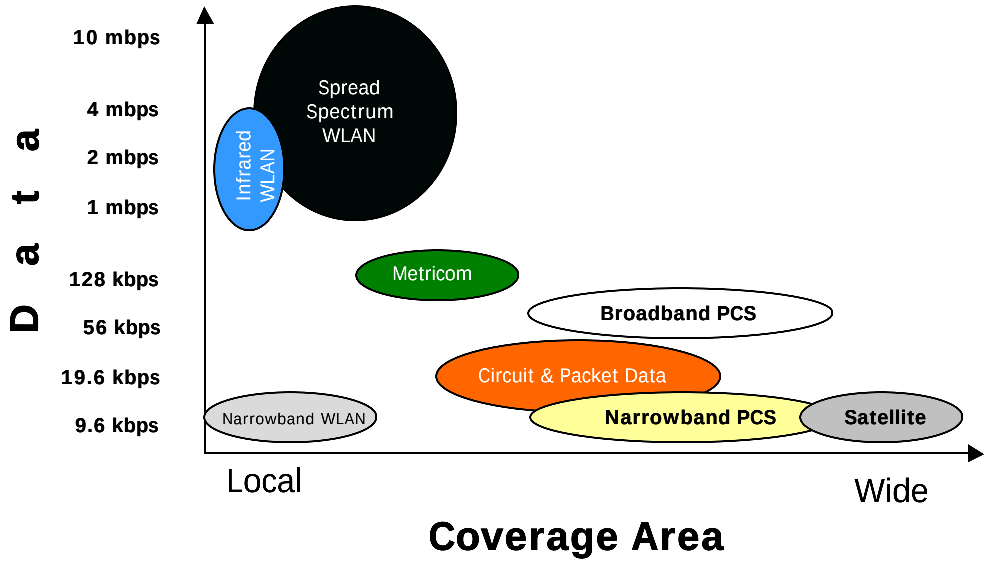
- Web Spoofing is a BIG/HUGE opportunity
  - lots of “hacking” efforts to increase the ways to do spoofing
- Many network applications are not rigorously tested for input handling issues
- Web code reveals a LOT about design, intention, conventions, and expectations of the server
- next…Wireless

Notes:

Where are We?

- Profiling
  - An example
  - Intrusions
- **Protocols**
  - SSL
  - DNS
  - SNMP
  - Web
  - **Wireless**
- Discovery and DoS
  - Discovery
  - Denial of Service
- Epilog
  - Top 10ish TTD
  - References

What is Wireless



802.11

- 2.4 GHz band
- 1 - 11 Mbps from a distance of about 150 to 2000 feet (without special antenna)
- Home business and business markets

- Peer-to-peer (a.k.a. Ad-Hoc)
  - official name is IBSS, Independent Basic Service Set
  - no Access Point (AP)
    - i.e., with just your wireless client cards
- BSS or Basic Service set
  - uses an AP to connect clients to a wired network
- ESS or Extended Service Set
  - uses multiple APs
  - clients may roam between APs

Exposures

- Technology problems
- Theft of hardware
- Eavesdropping
- Insecure configuration information

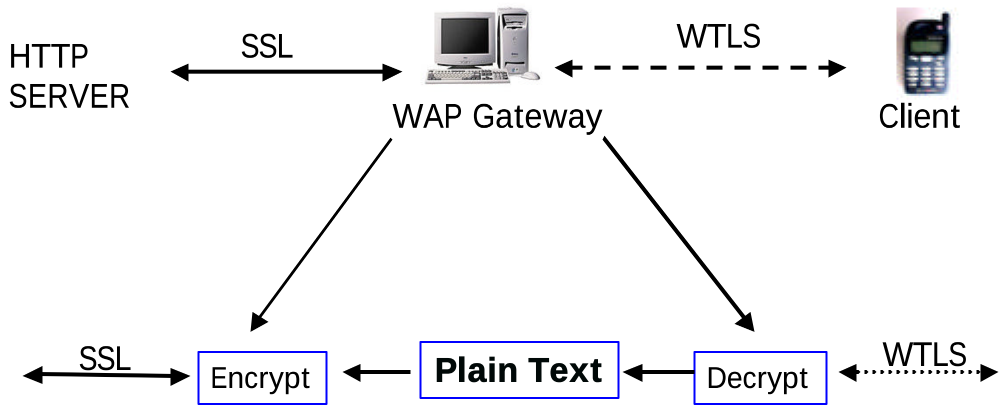
Technology Problems

- What does “technology” mean?
  - The current state of common hardware and software solutions, examples include
    - protocol issues
      - the raging debate over WEP
    - interoperability issues
      - the Gap in WAP
    - specification issues
      - WEP doesn’t encrypt the SSID and, in general, management packets
    - configuration issues
      - default AP is WEP disabled, open authentication, default SNMP community string

The Gap in WAP

- Not to be confused with WAP Gap
  - …which is hundreds of millions of devices that are NOT using WAP
- What is the Gap in WAP?
  - WAP handset to WAP server handled by WTLS
  - WAP server to Internet handled by SSL
  - Once decrypted by WTLS, data is exposed until it is re-encrypted by SSL

Gap in WAP



HTTP SERVER

SSL

WAP Gateway

WTLS

Client

SSL

Encrypt

Plain Text

Decrypt

WTLS

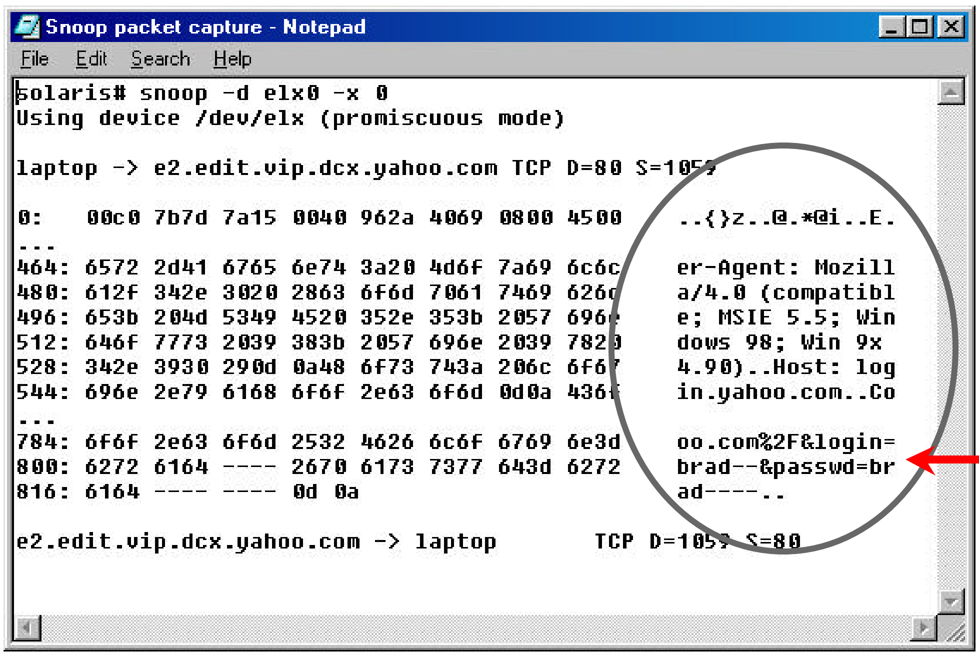
Theft of hardware

- Wireless stuff is small
  - Wireless cards fit in a shirt-pocket
  - Most of the APs fit in a jacket pocket or are easily hidden in any kind of bag
    - should they be tagged like clothes in a store?
- Cisco 340 cards write WEP keys to the card
- If a laptop were stolen, how long would it take to re-key your Wireless network?
- APs have WEP Keys in them
  - Data is stored locally

Eavesdropping

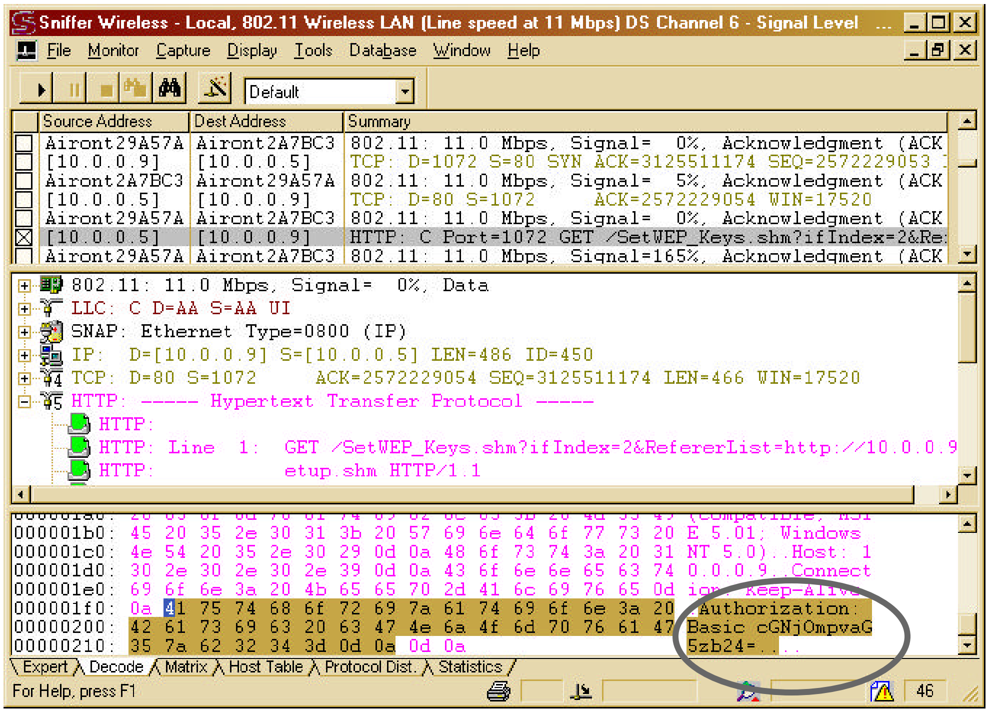
- Indirect: listening to the network that the wireless access point is connected to (PROMISC)
  - Remember: WEP only encrypts data between the client and the access point!
  - Quite frankly, this is what most people are doing when they talk about “sniffing wireless”
- Direct: listening to the airwaves (RFMON)
  - Sender can not detect eavesdropping
  - Frequency band largely determines range
    - it is quite possible that it goes outside the building
    - special electromagnetic shielding is needed to “stop” leakage

Eavesdropping, Indirect



```
solaris# snoop -d elx0 -x 0
Using device /dev/elx (promiscuous mode)

laptop -> e2.edit.vip.dcx.yahoo.com TCP D=80 S=1059

0:    00c0 7b7d 7a15 0040 962a 4069 0800 4500    ..{}z..@.*@i..E.
...
464: 6572 2d41 6765 6e74 3a20 4d6f 7a69 6c6c    er-Agent: Mozill
480: 612f 342e 3020 2863 6f6d 7061 7469 626c    a/4.0 (compatibl
496: 653b 204d 5349 4520 352e 353b 2057 696e    e; MSIE 5.5; Win
512: 646f 7773 2039 383b 2057 696e 2039 7820    dows 98; Win 9x
528: 342e 3930 290d 0a48 6f73 743a 206c 6f67    4.90)..Host: log
544: 696e 2e79 6168 6f6f 2e63 6f6d 0d0a 436f    in.yahoo.com..Co
...
784: 6f6f 2e63 6f6d 2532 4626 6c6f 6769 6e3d    oo.com%2F&login=
800: 6272 6164 ---- 2670 6173 7377 643d 6272    brad--&passwd=br
816: 6164 ---- ---- 0d 0a                       ad----..

e2.edit.vip.dcx.yahoo.com -> laptop       TCP D=1059 S=80
```

Eavesdropping, Indirect or Direct



Sniffer Wireless - Local, 802.11 Wireless LAN (Line speed at 11 Mbps) DS Channel 6 - Signal Level ...
File Monitor Capture Display Tools Database Window Help
Default

```
Source Address  Dest Address  Summary
□ Airont29A57A  Airont2A7BC3  802.11: 11.0 Mbps, Signal=  0%, Acknowledgment (ACK
□ [10.0.0.9]    [10.0.0.5]    TCP: D=1072 S=80 SYN ACK=3125511174 SEQ=2572229053 ]
□ Airont2A7BC3  Airont29A57A  802.11: 11.0 Mbps, Signal=  5%, Acknowledgment (ACK
□ [10.0.0.5]    [10.0.0.9]    TCP: D=80 S=1072     ACK=2572229054 WIN=17520
□ Airont29A57A  Airont2A7BC3  802.11: 11.0 Mbps, Signal=  0%, Acknowledgment (ACK
☒ [10.0.0.5]    [10.0.0.9]    HTTP: C Port=1072 GET /SetWEP_Keys.shm?ifIndex=2&Re:
□ Airont29A57A  Airont2A7BC3  802.11: 11.0 Mbps, Signal=165%, Acknowledgment (ACK
```

```
+ 802.11: 11.0 Mbps, Signal=  0%, Data
+ LLC: C D=AA S=AA UI
+ SNAP: Ethernet Type=0800 (IP)
+ IP:  D=[10.0.0.9] S=[10.0.0.5] LEN=486 ID=450
+ TCP: D=80 S=1072     ACK=2572229054 SEQ=3125511174 LEN=466 WIN=17520
- HTTP: ----- Hypertext Transfer Protocol -----
    HTTP:
    HTTP: Line  1:  GET /SetWEP_Keys.shm?ifIndex=2&RefererList=http://10.0.0.9
    HTTP:           etup.shm HTTP/1.1
```

```
000001b0: 45 20 35 2e 30 31 3b 20 57 69 6e 64 6f 77 73 20 E 5.01; Windows
000001c0: 4e 54 20 35 2e 30 29 0d 0a 48 6f 73 74 3a 20 31 NT 5.0)..Host: 1
000001d0: 30 2e 30 2e 30 2e 39 0d 0a 43 6f 6e 6e 65 63 74 0.0.0.9..Connect
000001e0: 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d ion: Keep-Alive.
000001f0: 0a 41 75 74 68 6f 72 69 7a 61 74 69 6f 6e 3a 20 .Authorization:
00000200: 42 61 73 69 63 20 63 47 4e 6a 4f 6d 70 76 61 47 Basic cGNjOmpvaG
00000210: 35 7a 62 32 34 3d 0d 0a 0d 0a                   5zb24=....
```

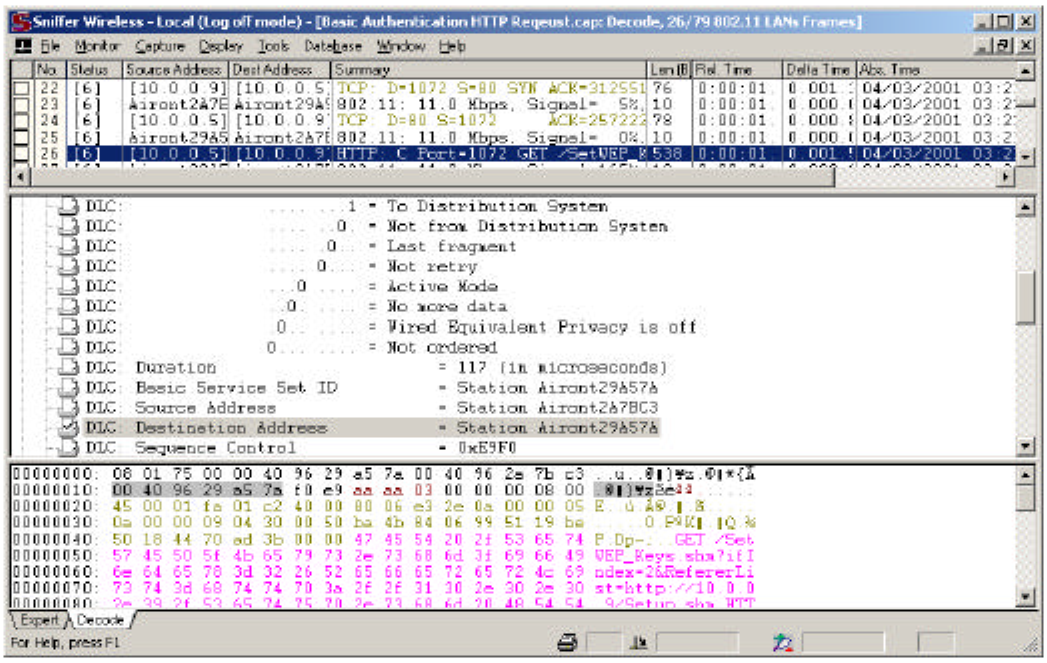
Indirect or Direct, cont.

- Take sniffed data
  - From wired or wireless network
  - cGNjOmpvaG5zb24=
- Apply just the right function

  -
    ```
    use MIME::Base64();
    $string = MIME::Base64::decode($ARGV[0]);
    printf("Password is $string\n");
    ```
- Look at the results
  - perl base64.pl cGNjOmpvaG5zb24=

    Password is pcc:johnson
  - hmm…Basic Auth isn't as helpful as you thought

Eavesdropping, Direct


Sniffer Wireless - Local (Log off mode) - [Basic Authentication HTTP Request.cap: Decode, 26/79 802.11 LANs Frames]
File Monitor Capture Display Tools Database Window Help
Expert
Decode
For Help, press F1

```
No. Status Source Address Dest Address  Summary                              Len (B Rel. Time  Delta Time Abs. Time
22  [6]    [10.0.0.9]     [10.0.0.5]    TCP: D=1072 S=80 SYN ACK=312551      76     0:00:01    0.001      04/03/2001 03:2
23  [6]    Airont2A7E     Airont29A5    802.11: 11.0 Mbps, Signal= 5%,       10     0:00:01    0.000      04/03/2001 03:2
24  [6]    [10.0.0.5]     [10.0.0.9]    TCP: D=80 S=1072       ACK=257222    78     0:00:01    0.000      04/03/2001 03:2
25  [6]    Airont29A5     Airont2A7E    802.11: 11.0 Mbps, Signal= 0%,       10     0:00:01    0.000      04/03/2001 03:2
26  [6]    [10.0.0.5]     [10.0.0.9]    HTTP: C Port=1072 GET /SetWEP_K      538    0:00:01    0.001      04/03/2001 03:2
```

```
DLC:                .... ...1 = To Distribution System
DLC:                .... ..0. = Not from Distribution System
DLC:                .... .0.. = Last fragment
DLC:                .... 0... = Not retry
DLC:                ...0 .... = Active Mode
DLC:                ..0. .... = No more data
DLC:                .0.. .... = Wired Equivalent Privacy is off
DLC:                0... .... = Not ordered
DLC: Duration                  = 117 (in microseconds)
DLC: Basic Service Set ID      = Station Airont29A57A
DLC: Source Address            = Station Airont2A78C3
DLC: Destination Address       = Station Airont29A57A
DLC: Sequence Control          = 0xE9F0
```

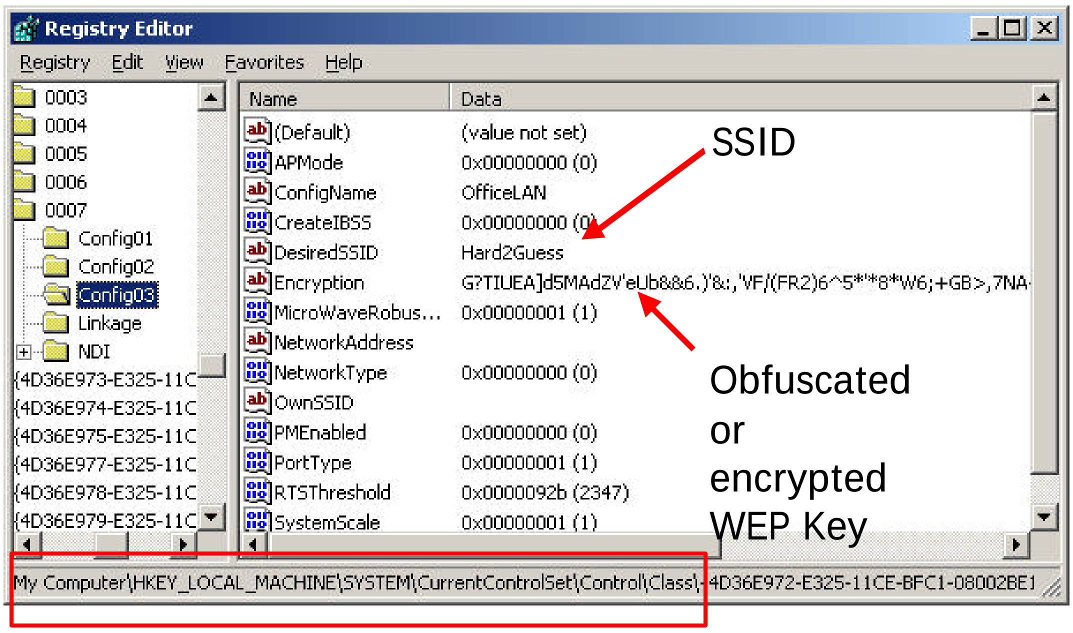
```
00000000: 08 01 75 00 00 40 96 29 a5 7a 00 40 96 2a 7b c3 ..u..@ )¥z.@ *{Ã
00000010: 00 40 96 29 a5 7a f0 e9 aa aa 03 00 00 00 08 00 .@ )¥zðéªª......
00000020: 45 00 01 fa 01 c2 40 00 80 06 e3 2e 0a 00 00 05 E..ú.Â@. .ã.....
00000030: 0a 00 00 09 04 30 00 50 ba 4b 84 06 99 51 19 ba .....0.PºK  Q.º
00000040: 50 18 44 70 ad 3b 00 00 47 45 54 20 2f 53 65 74 P.Dp-;..GET /Set
00000050: 57 45 50 5f 4b 65 79 73 2e 73 68 6d 3f 69 66 49 WEP_Keys.shm?ifI
00000060: 6e 64 65 78 3d 32 26 52 65 66 65 72 65 72 4c 69 ndex=2&RefererLi
00000070: 73 74 3d 68 74 74 70 3a 2f 2f 31 30 2e 30 2e 30 st=http://10.0.0
00000080: 2e 39 2f 53 65 74 75 70 2e 73 68 6d 20 48 54 54 .9/Setup.shm HTT
```

Eavesdropping, cont.

Insecure Configuration Information

- Where does the client store the information?
  - Cisco: On the card -> so steal it
  - Lucent:
    - on Windows, it’s in a world-readable registry key -> so copy the values and import them into your configuration
    - on other OSs, it’s stored in a file
  - Other cards are storing the data someplace too ☺
- Let’s take a closer look at the Lucent Windows example

Lucent Client Registry Entries



0003
0004
0005
0006
0007
Config01
Config02
Config03
Linkage
NDI
{4D36E973-E325-11C
{4D36E974-E325-11C
{4D36E975-E325-11C
{4D36E977-E325-11C
{4D36E978-E325-11C
{4D36E979-E325-11C

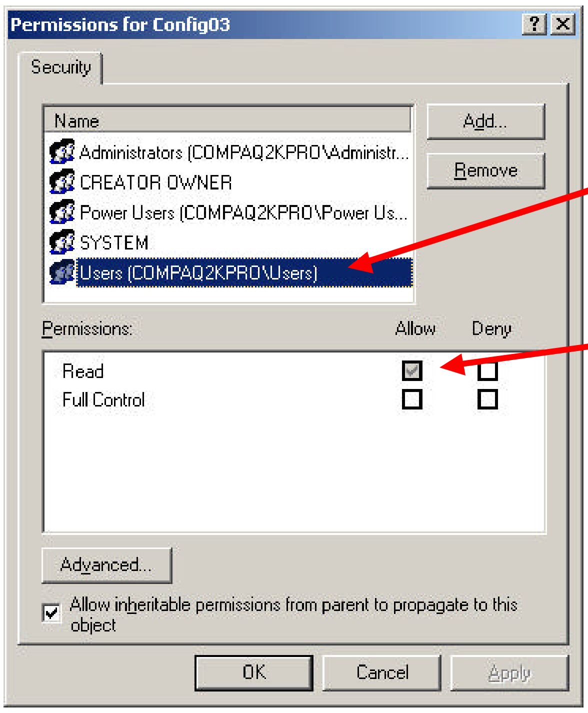
Name	Data
(Default)	(value not set)
APMode	0x00000000 (0)
ConfigName	OfficeLAN
CreateIBSS	0x00000000 (0)
DesiredSSID	Hard2Guess
Encryption	G?TIUEA]d5MAdZV'eUb&&6.)'&:,'VF/(FR2)6^5*'*8*W6;+GB>,7NA
MicroWaveRobus...	0x00000001 (1)
NetworkAddress	
NetworkType	0x00000000 (0)
OwnSSID	
PMEnabled	0x00000000 (0)
PortType	0x00000001 (1)
RTSThreshold	0x0000092b (2347)
SystemScale	0x00000001 (1)

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{4D36E972-E325-11CE-BFC1-08002BE1

SSID

Obfuscated
or
encrypted
WEP Key

Registry Permissions



Name
Administrators (COMPAQ2KPRO\Administr...
CREATOR OWNER
Power Users (COMPAQ2KPRO\Power Us...
SYSTEM
Users (COMPAQ2KPRO\Users)

Permissions:	Allow	Deny
Read	☑	□
Full Control	□	□

☑ Allow inheritable permissions from parent to propagate to this object

Any authenticated user

Can read and copy this data ☹

Wireless Medicine

- Enable WEP
- Change the SSID
  - and change it to something good
- Disable broadcast
  - otherwise, your SSID is there to see and it wants to associate with any clients near it
- Change the password on your AP
- Periodically survey your site
- Use MAC address filtering
- Reconsider using DHCP
- Consider using fixed IP addresses for your wireless NICs
- If you really need data privacy or confidentiality, look into other application level mechanisms like SSL or VPN technologies

What the Hacker KnOwZ… about Wireless

- Deployment is almost too easy, many organizations don’t harden their environment
- It’s a new space, many people don’t understand the issues involved
- next…Epilog

Notes:

Notes:

Where are We?

- Profiling
  - An example
  - Intrusions
- Protocols
  - SSL
  - DNS
  - SNMP
  - Web
  - Wireless
- Discovery and DoS
  - Discovery
  - Denial of Service
- **Epilog**
  - **Top 10ish TTD**
  - References

Top 10ish Things To Do

- Tools

vulnerability testing:	nessus or nsat
HTTP CGI checker:	whisker
OS identification and special scanner:	nmap
IDS:	network (e.g., snort) and integrity checker (e.g., Tripwire)

Top 10ish Things To Do, cont.

- Development
  - Use some scanner to create a template profile of your important systems: run the scanner every day and generate an alarm/email if the results are different
  - Define a list of 5-10 important issues and create/use any kind of script/program you can to check the logs for those things
  - Upgrade every version of BIND you can to the latest version (yours, your neighbors, your ISP)
  - If you’re using IIS…install all upgrade fixes, remove (if possible) all default/example software, and run assessments tools against your site…constantly!

Top 10ish Things To Do, cont.

- Process
  - Reduce the number of versions you have for every major OS, application, and library
  - Develop a 1-page “What To Do” checklist in the event of an intrusion for your administrators and their boss
  - Create a clone of your important systems, configurations, and applications
  - Do at least 5 of the things on the Wireless Medicine page

Remember the Themes..What to Watch for

- It’s the protocols
  - DDoS
  - Another bunch of DNS exploits
  - Continued problems in RPC, NetBIOS, POP, Imap, and Bind
- Intrusion awareness
  - New wireless hacking techniques
- SSL
  - More forged keys
  - Certificate granting and revocation issues
- Web Applications
  - Servers not handling modified forms/pages from client
  - More client-side language problems
  - More “clever” viruses, macros, Trojan horses

The End.

- Profiling is a big part of being prepared for an intrusion
- Executing many of the available profiling tools or techniques requires little actual knowledge
- There are a lot of tools, techniques, sites, and initiatives that you can use and should be aware of
- The hacker KnOwZ a lot
  - check out the What the Hacker KnOwZ pages for a quick reference

Where are We?

- Profiling
  - An example
  - Intrusions
- Discovery and DoS
  - Discovery
  - Denial of Service
- Protocols
  - SSL
  - DNS
  - SNMP
  - Web
  - Wireless
- **Epilog**
  - Top 10ish TTD
  - **References**

REFERENCES

- Incident and Response Centers
- Intrusion Tools
- Security Tool Libraries
- Mailing Lists
- Books

Incident and Response Centers

- CERT
  - www.cert.org/
- CIAC
  - ciac.llnl.gov/
- FIRST - association of response teams
  - www.first.org/

Intrusion Tools

- Mscan - limited but powerful exploit assessment
  Sscan - Mscan derivative, more powerful
  - packetstorm.decepticons.org
- Scotty - protocol agents (rpc,snmp,http,udp,etc.)
  - wwwsnmp.cs.utwente.nl/~schoenw/scotty/
- Nmap - many types of scans
  - www.insecure.org/nmap/index.html
- eEye Retina Scanner
  - www.eeye.com/html/Products/Retina/overview.html

Intrusion Tools, cont.

- SATAN/SAINT/SARA - exposure assessment
  - www.fish.com/~zen/satan/satan.html
  - SAINT - SATAN derivative
    - wwdsilx.wwdsi.com/saint/
  - SARA - another SATAN derivative
    - www-arc.com/sara/
- cURL - URL grabber
  - freshmeat.net/news/1999/08/27/935751207.html
- Whisker
  - www.wiretrip.net/rfp/p/doc.asp?id=21&iface=2

Intrusion Tools, cont.

- Typhoon
  - http://www.nextgenss.com/
- Nsat
  - packetstorm.securify.com/UNIX/scanners/indexdate.shtml
  - mixter.warrior2k.com/
- Nessus
  - www.nessus.org/

Intrusion Tools, cont.

- ISS - Internet Security Scanner
  - www.iss.net
- NetRecon
  - www.axent.com
- NetRanger
  - www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml
- Kane Security Analysis
  - www.intrusion.com/Products/analystnt.shtml

Security Tool Libraries

- ftp://ciac.llnl.gov/pub/ciac
- ftp://ftp.win.tue.nl/pub/security
- ftp://ftp.nec.com/pub/security
- www.alw.nih.gov/Security/
- sites.inka.de/lina/freefire-l/tools.html

Mailing Lists and related Courses and Sites

- Bugtraq mailing Lists
  - bugtraq: Go to www.securityfocus.com/
  - ntbugtraq: Go to www.ntbugtraq.com/
- Related Courses
  - LISA, SANS, USENIX: look for…
    - How to Audit Web-Based Applications, David Rhoades
    - Hacking Exposed: LIVE!, Eric Schultze, George Kurtz
    - Security Auditing with PERL, Dan Klein

Hacking Sites
WARNING

- Use protected/private network
- Use protected/private host
  - that you are willing to SCRUB
- Don’t accept binaries
  - look at the code

Books

- Hacking Exposed
  by McClure, Scambray, and Kurtz

  Paperback - 550 pages
  (September 1999)
  Published by McGraw-Hill
  ISBN: 0072121270

Books, cont.

- Maximum Security : A Hacker's Guide to Protecting Your Internet Site and Network
  by Anonymous *

  Paperback - 829 pages 2nd edition w/cd-rom
  (September 1998)
  Published by Sams
  ISBN: 0672313413

  Note *: “Anonymous” …give me a break!

Books, cont.

- Maximum Linux Security : A Hacker's Guide to Protecting Your Linux Server and Workstation
  by Anonymous *

  Paperback - 800 pages w/cd-rom
  (October 1999)
  Published by Sams
  ISBN: 0672316706

  Note *: "Anonymous" …give me a break, again!

Books, cont.

- Windows 2000 Security Handbook
  by Phil Cox and Tom Sheldon

  Paperback - 700 pages
  (November 2000)
  Published by Osborne McGraw-Hill
  ISBN: 0072124334

Books, cont.

- White-Hat Security Arsenal
  by Aviel D. Rubin

  Paperback - 330 pages
  (June 2001)
  Published by Addison Wesley
  ISBN: 0-201-71114-1

SystemEXPERTS
LEADERSHIP IN SECURITY

Brad C. Johnson
Vice President

Brad.Johnson@SystemExperts.com
401-348-3099 direct
401-348-3078 fax
978-440-9388 main
http://www.SystemExperts.com/

THE REAL END!

- Thank you for attending!
- Thank you for your comments!
- http://www.SystemExperts.com/tutors/profiles.pdf
- **Please fill out the Instructor Evaluation Form!!**