



Ethical Hacking

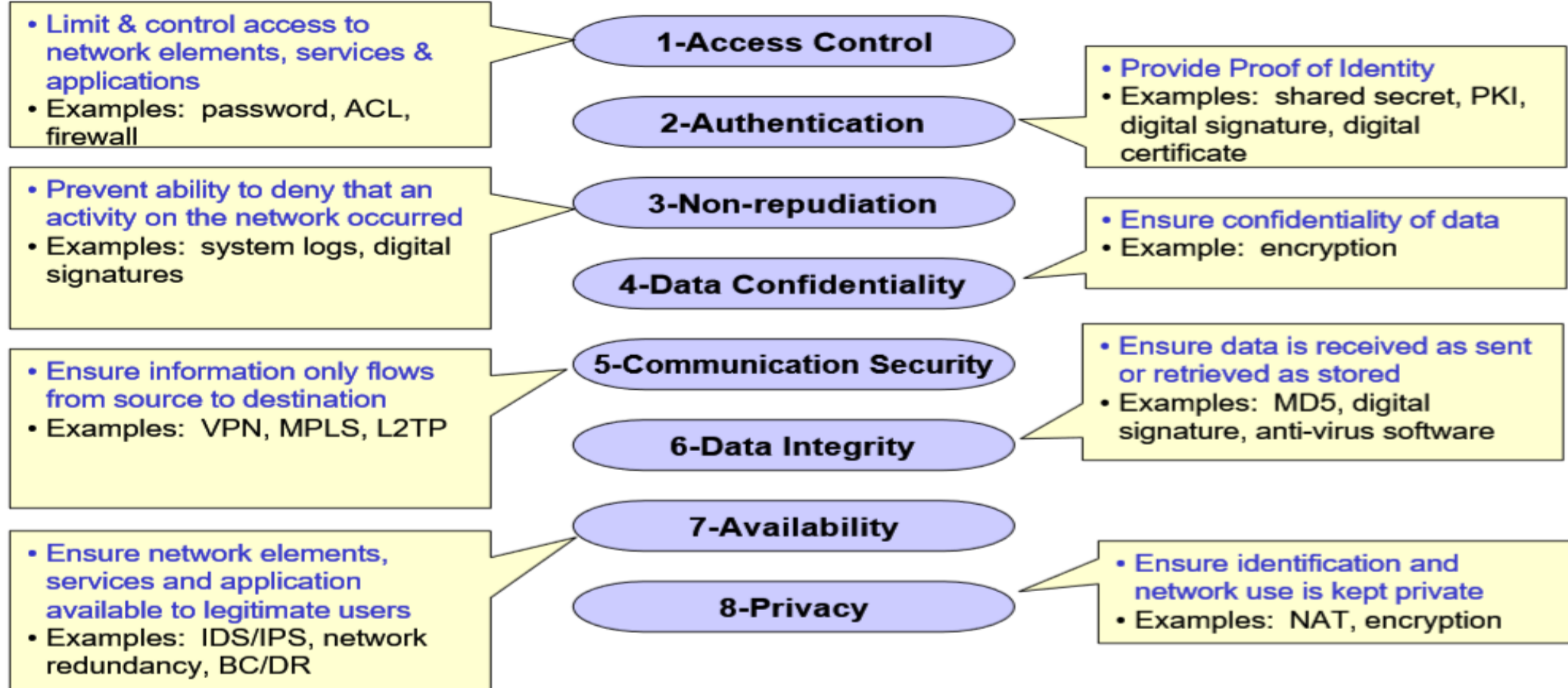


Hackers

- Types
 - White hat
 - Black hat
 - Grey hat
 - Suicidal
- Categories
 - Coder
 - Admin
 - Script Kiddies

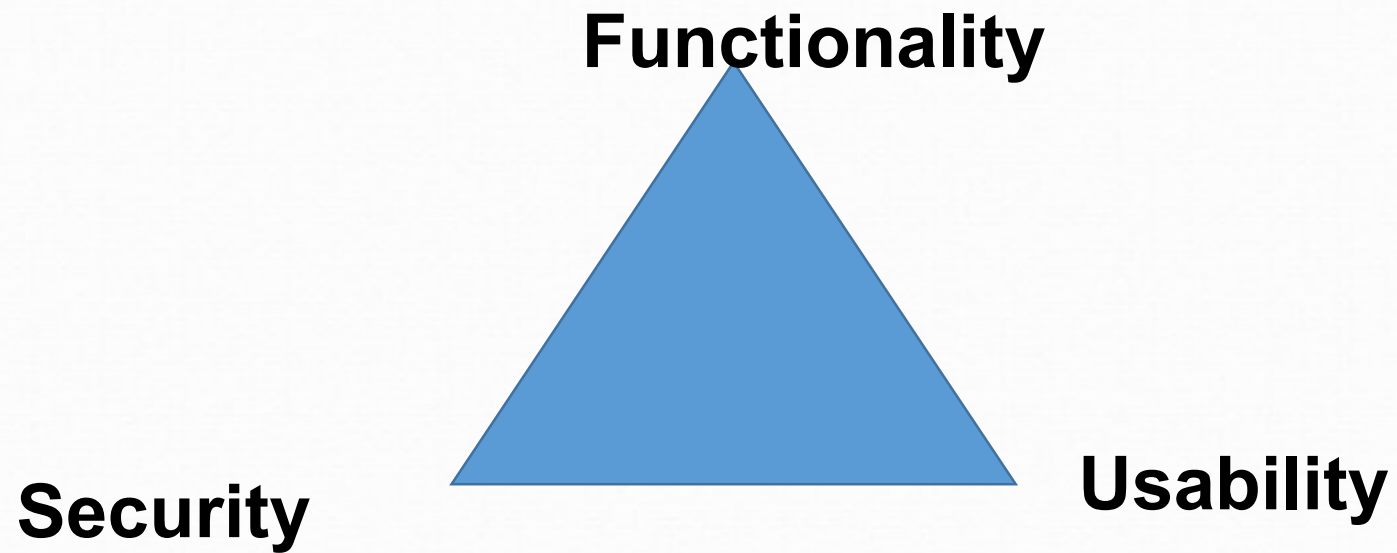


8 Security Dimensions ITU-T X.805 Recommendations





Security Triangle





Essential Terminologies

- Vulnerabilities
 - Weakness through which attacker can breach targeted systems security
- Exploits
 - Tools/keys through which security is breached
- Payload
 - Code that runs on targeted system
 - Single, Stager, & Stages

How does exploitation works



1. Vulnerability
2. Exploit
3. Payload



Process/ Phases

- Reconnaissance
 - Information gathering about the target
- Scanning
 - Networks, Ports, Vulnerabilities
- Gaining Access
 - Vulnerabilities, Exploits
- Maintaining Access
 - Backdoors
- Clearing Tracks
 - Daisy Chaining
- Reporting



Tools

- NMAP
- Angry IP Scanner
- Cain & Abel, John the ripper, THC Hydra, Aircrack-ng
- Ettercap
- Metasploit Framework
- SuperScan
- OWASP Zed Attack Proxy
- Burp Suite
- SQLmap
- Wireshark

Questions



- 1) Hacker who helps in strengthening security of cyber space in consent with the network owner is known as
- 2) A Coder could be
 - a) Black hat
 - b) White hat
 - c) Grey hat
 - d) Suicidal hacker
- 3) Getting domain name details using WHOIS is a part of
 - a) Reconnaissance
 - b) Scanning
 - c) Gaining access
 - d) None
- 4) Backdoors are used for
 - a) Reconnaissance
 - b) Scanning
 - c) Maintaining access
 - d) Reporting
- 1) Tools/keys through which security is breached are known as
 - a) Exploits
 - b) Payloads
 - c) Shell codes
 - d) None
- 5) ITU-T standard which defines Security Architecture for end to end communication security
 - a) X.25
 - b) X.509
 - c) G.783
 - d) X.805
- 7) Name of the Protocol Analyser
 - a) Nmap
 - b) Wireshark
 - 3) John the Ripper
 - 4) None



Reconnaissance

- Footprinting, Scanning & Enumeration
- Covertly discover and collect information about target system
- Initial information
 - Network range
 - Active machines
 - Open ports and Access Points
 - Fingerprint the OS
 - Services on Ports
 - Map the Network
- Active/Passive Reconnaissance



Footprinting

- Getting Possible information about target
- Active/ Passive
 - Domain name, IP Addresses, Namespaces
 - Employee Information, Phone Numbers, E-mails
 - Job Information
- <http://www.whois.com/whois> for information on domain name, ip2location.com for further details of website, IP Address Ranges of a multiple IP addresses serving different domains and sub-domains, can be obtained for a particular company using American Registry for Internet Numbers (ARIN) and www.archive.org for history of any website



Fingerprinting

- Used to determine what OS is running on a remote computer
- Active/ Passive
- To determine OS we look at
 - TTL, Window size, DF, TOS
 - (Method not 100% accurate but works better for some OS than others)
- Once OS is Known where the website is hosted, Use NMAP for OS, Open Ports associated with IP/Domain name
- Ping Sweep/ ICMP sweep: Which IP address from a range of IP Addresses map to live host



Scanning

- Port Scanning Techniques
 - Non-stealth scanning
 - Stealth scanning
- Defence
 - Configure firewall and IDS rule to detect and block probes
 - Block unwanted ports at the firewall
 - Hide sensitive Information from public view
 - Use custom rule set to lock down the network
- Tools: NMAP, Angry IP Scanner



Nmap

```
root@bt:~# nmap -sV -n 192.168.1.150
```

```
Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2011-12-07 08:03 CST
```

```
Nmap scan report for 192.168.1.150
```

```
Host is up (0.0042s latency).
```

```
Not shown: 995 closed ports
```

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
1025/tcp	open	msrpc	Microsoft Windows RPC
5000/tcp	open	upnp	Microsoft Windows UPnP

MAC Address: 08:00:27:FA:D6:C6 (Cadmus Computer Systems) x

```
Service Info: OS: Windows
```

```
Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 7.21 seconds
```

```
root@bt:~#
```

```
root@bt:~#
```



Enumeration

- Attacker **creates active connections to the target** and **perform direct queries** to gain more information about the target
- Use extracted information to identify system attack points and perform password attack to gain unauthorised access
- Conducted in Intranet environment
- Enumeration Techniques
 - Extract usernames from email ids
 - Extract information using default passwords
 - Extract user name using SNMP, Brute force using active directory, Extract user groups from windows
 - Information from DNS Zone transfer



DNS Enumeration

- DNS enumeration is the process of locating all the DNS servers and their corresponding records for an organization.
 - Get the host's addresses
 - Get the nameservers
 - Get the MX record
 - Perform **axfr** queries on nameservers
 - Get extra names and subdomains via **Google scraping**
 - Brute force subdomains from file can also perform recursion on subdomain that has NS records
 - Calculate C class domain network ranges and perform **whois** queries on them
 - Perform **reverse lookups** on **netranges**



Kali Linux

- World's most powerful and popular penetration testing platform
- Used by security professionals in a wide range of specializations, including penetration testing, forensics, reverse engineering, and vulnerability assessment.
- Built on the work of the Debian project and adds over 300 special-purpose packages of its own, all related to information security, particularly the field of penetrating testing.
- Used for Information gathering, vulnerability analysis, web application analysis, reverse engineering, sniffing and spoofing, exploitation tools, post exploitation, forensics, and reporting purposes



Metasploit Framework

- The Metasploit Framework (Msf) is a free, open source penetration testing solution developed by the open source community and Rapid7
- It was initially written in Perl (2003) and later re-written in Ruby in 2007
- **Metasploit Framework:**
- The basic steps for exploiting a system using the Framework include:
- Choosing and configuring an *exploit* (code that enters a target system by taking advantage of one of its vulnerabilities; about 900 different exploits for **Windows, Unix/Linux** and **Mac OS X** systems are included);



Metasploit Framework

- Optionally checking whether the intended target system is susceptible to the chosen exploit;
- Choosing and configuring a **payload** (code that will be executed on the target system upon successful entry; for instance, a remote shell or a VNC server);
- Choosing the encoding technique so that the intrusion-prevention system (IPS) ignores the encoded payload;
- Executing the exploit.
- Clearing Tracks



Kali Linux and Metasploit

- World's most powerful and popular penetration testing & digital forensic platform which includes Metasploit Framework among other several Penetration Testing tools such as Information Gathering tools NMAP/ ZenMAP, Searchsploit, DNS tools dnsenum.pl, DNSMAP, dnstracer, Hping3 etc.
- From Kali, one can run metasploit directly through command line, access a Metasploit GUI front end called Armitage or use Metasploit packages available in tools like the Social Engineering Toolset (SET)



Wireshark: Packet Analyser

- Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports
- Used for **network** troubleshooting, analysis, software and communications protocol development, and education
- Terminal based version (non-GUI) is called Tshark
- OS: Cross Platform written in c, c++



Wireshark

- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, Tshark
- Data display can be refined using a display filter.



Wireshark : Packet Analyser

- Plug-ins can be created for dissecting new protocols.
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured
- Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic.

The screenshot displays the Wireshark interface with a packet capture list and a detailed view of a selected packet. The packet list shows various protocols including TCP, UDP, and ICMP. The details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol, User Datagram Protocol, and Data. The raw data pane shows the hexadecimal and ASCII representation of the packet data.

No.	Time	Source	Destination	Protocol	Length	Info
10684	11:05:51.330278	192.168.10.126	192.168.10.130	UDP	210	Source port: 4723 Destination port: 60729
10685	11:05:51.338450	192.168.1.33	192.168.1.4	TCP	196	xgrid > 55061 [PSH, ACK] Seq=331001 Ack=1 win=8706 Len=142
10686	11:05:51.338644	192.168.1.4	192.168.1.33	TCP	54	55061 > xgrid [ACK] Seq=1 Ack=331145 win=16070 Len=0
10687	11:05:51.338874	192.168.1.33	192.168.1.4	TCP	196	xgrid > 55061 [PSH, ACK] Seq=331145 Ack=1 win=8706 Len=142
10688	11:05:51.339258	192.168.1.33	224.0.1.0	UDP	184	Source port: 41475 Destination port: 4770
10689	11:05:51.346775	192.168.10.126	192.168.10.130	UDP	210	Source port: 4723 Destination port: 60729
10690	11:05:51.353886	192.168.1.33	224.0.1.0	UDP	184	Source port: 41475 Destination port: 4770
10691	11:05:51.357375	192.168.1.33	192.168.1.4	TCP	196	xgrid > 55061 [PSH, ACK] Seq=331287 Ack=1 win=8706 Len=142
10692	11:05:51.357573	192.168.1.4	192.168.1.33	TCP	54	55061 > xgrid [ACK] Seq=1 Ack=331429 win=16425 Len=0
10693	11:05:51.361889	192.168.1.34	224.0.1.0	UDP	148	Source port: 61227 Destination port: 10126
10694	11:05:51.362733	192.168.1.35	224.0.1.0	UDP	390	Source port: 60632 Destination port: 10127
10695	11:05:51.363542	192.168.10.126	192.168.10.130	UDP	210	Source port: 4723 Destination port: 60729
10696	11:05:51.369624	192.168.1.33	224.0.1.0	UDP	184	Source port: 41475 Destination port: 4770
10697	11:05:51.380278	192.168.10.126	192.168.10.130	UDP	210	Source port: 4723 Destination port: 60729
10698	11:05:51.382020	192.168.1.33	192.168.1.4	TCP	196	xgrid > 55061 [PSH, ACK] Seq=331429 Ack=1 win=8706 Len=142
10699	11:05:51.386170	192.168.1.33	224.0.1.0	UDP	184	Source port: 41475 Destination port: 4770
10700	11:05:51.393149	192.168.1.34	224.0.1.0	UDP	148	Source port: 61227 Destination port: 10126
10701	11:05:51.396134	192.168.1.35	224.0.1.0	UDP	390	Source port: 60632 Destination port: 10127
10702	11:05:51.396898	192.168.10.126	192.168.10.130	UDP	210	Source port: 4723 Destination port: 60729
10703	11:05:51.402645	192.168.1.33	224.0.1.0	UDP	184	Source port: 41475 Destination port: 4770
10704	11:05:51.406757	192.168.1.33	192.168.1.4	TCP	196	xgrid > 55061 [PSH, ACK] Seq=331571 Ack=1 win=8706 Len=142
10705	11:05:51.407067	192.168.1.4	192.168.1.33	TCP	54	55061 > xgrid [ACK] Seq=1 Ack=331713 win=16154 Len=0
10706	11:05:51.407237	192.168.1.33	192.168.1.4	TCP	196	xgrid > 55061 [PSH, ACK] Seq=331713 Ack=1 win=8706 Len=142
10707	11:05:51.413467	192.168.10.126	192.168.10.130	UDP	210	Source port: 4723 Destination port: 60729

Packet capture

Packet detail

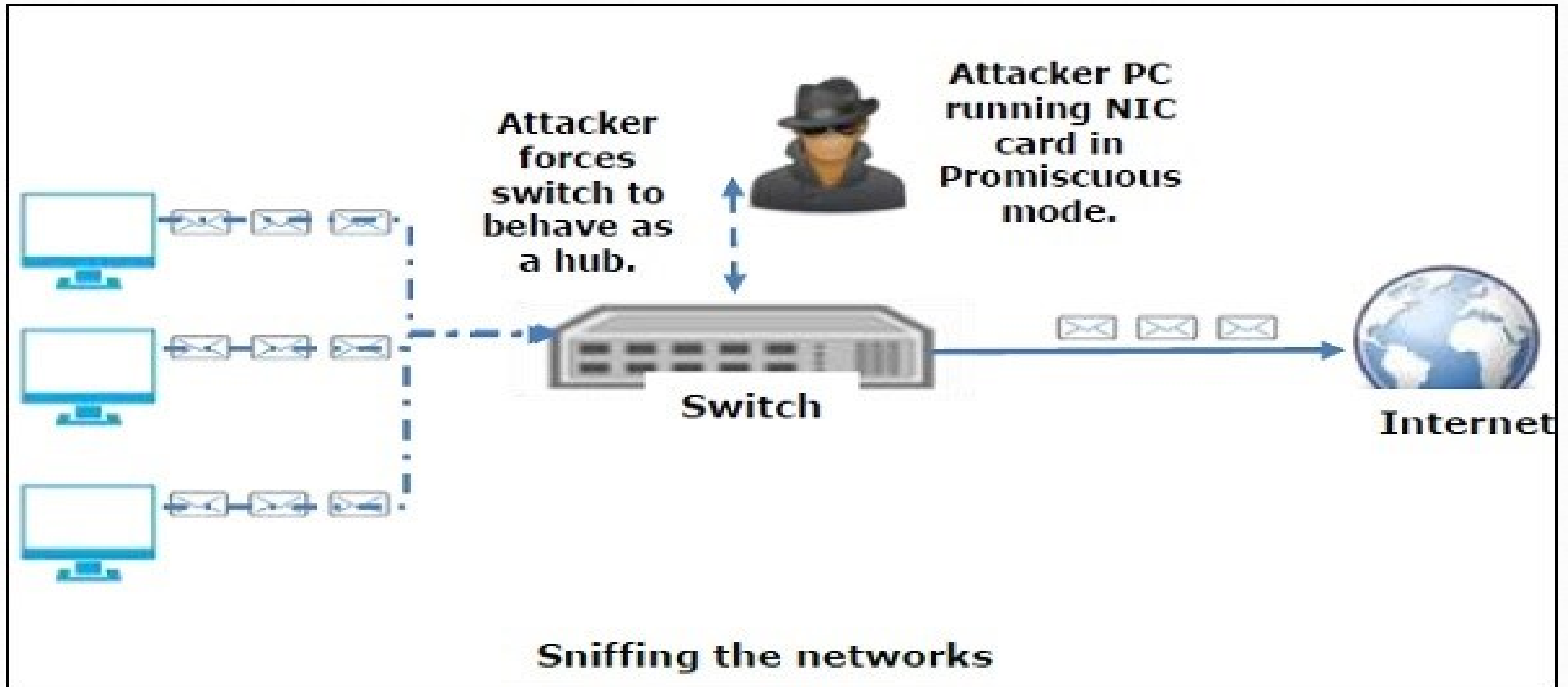
Raw data



Gaining Access: Sniffing

- Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.
- What can be sniffed?
 - Email/Web traffic, Chat sessions
 - FTP/Telnet passwords
 - Router configuration
 - DNS traffic

Sniffing...How ?





Sniffing contd....

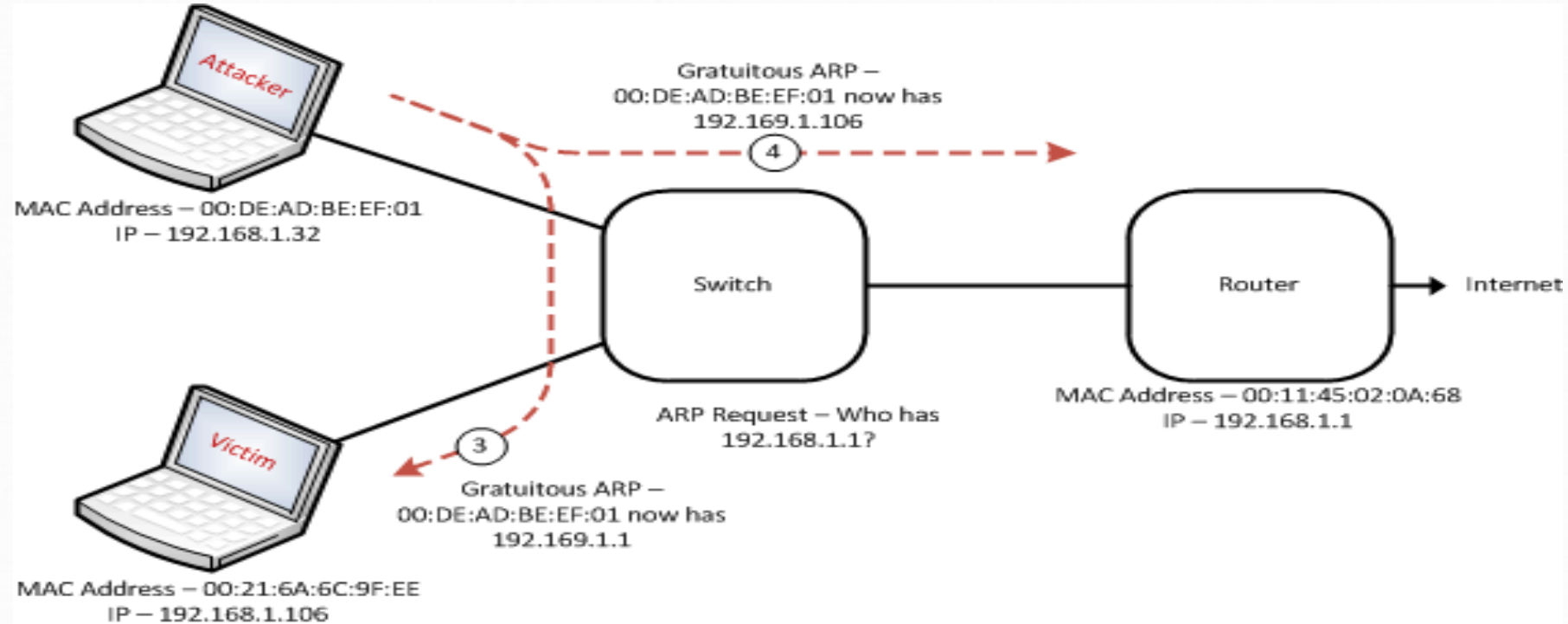
- Passive Sniffing
- Active Sniffing
 - MAC Flooding
 - ARP Poisoning
 - DHCP Attacks
 - DNS Poisoning
 - Spoofing Attacks
- Affected Protocols
 - HTTP, SMTP, NNTP, POP, FTP, IMAP, Telnet
- Hardware Analyser Tools, LI (wiretapping)

ARP Poisoning



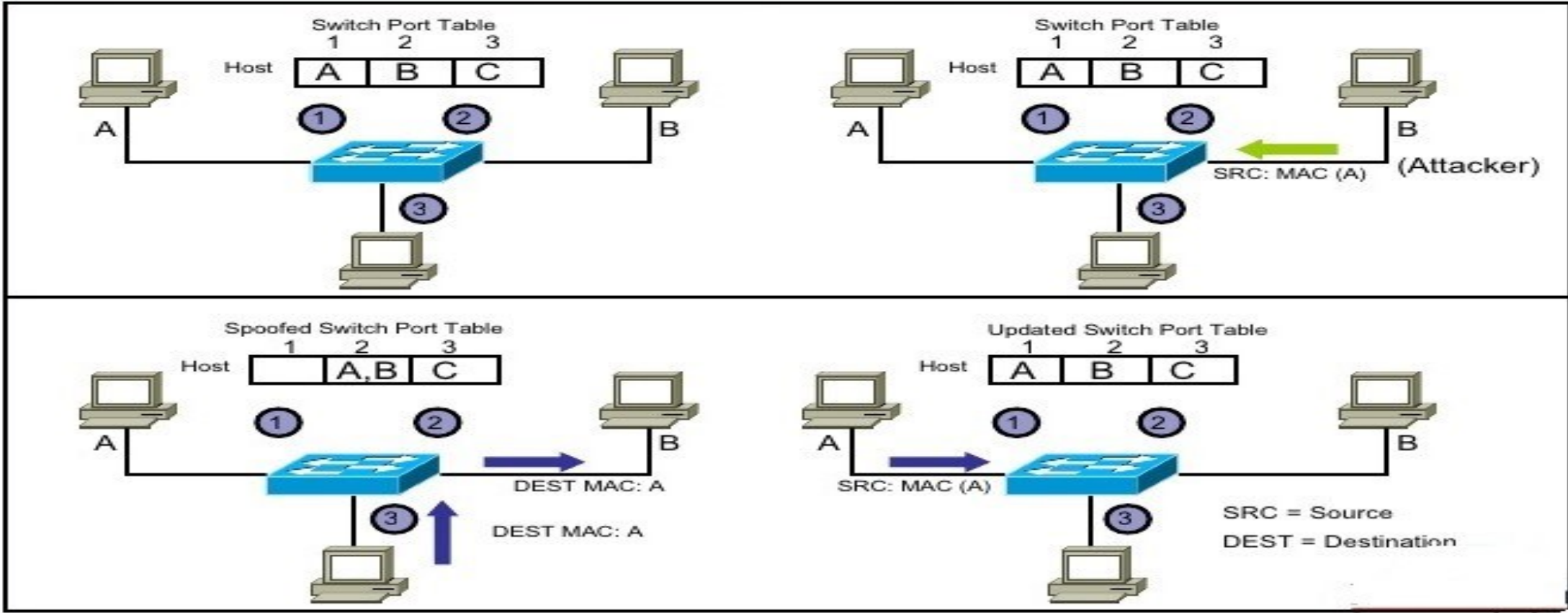
- ARP operates by broadcasting a message across a n/w, to determine the Layer 2 address (MAC address) of a host with a predefined Layer 3 address(IP address)
- The host at the destination IP address sends a reply packet containing its MAC address
- After initial ARP transaction , the ARP response is cached by the originating device
- In ARP spoofing attack, the ARP messages contain the **IP address** of network, such as **default gateway**, or a **DNS server** and replaces the **MAC address** for the corresponding **network resource** with its own **MAC address**
- With new ARP information, the attacker is in the **Man-In-The Middle**

ARP Spoofing



- Attack tools: Ettercap, Cain and Abel for MS Window platforms
- Mitigation: Dynamic ARP Inspection (DAI)-Interception and validation of IP-MAC address relationship of all packets on untrusted ports.

MAC Address Spoofing Attack





MAC Address Spoofing

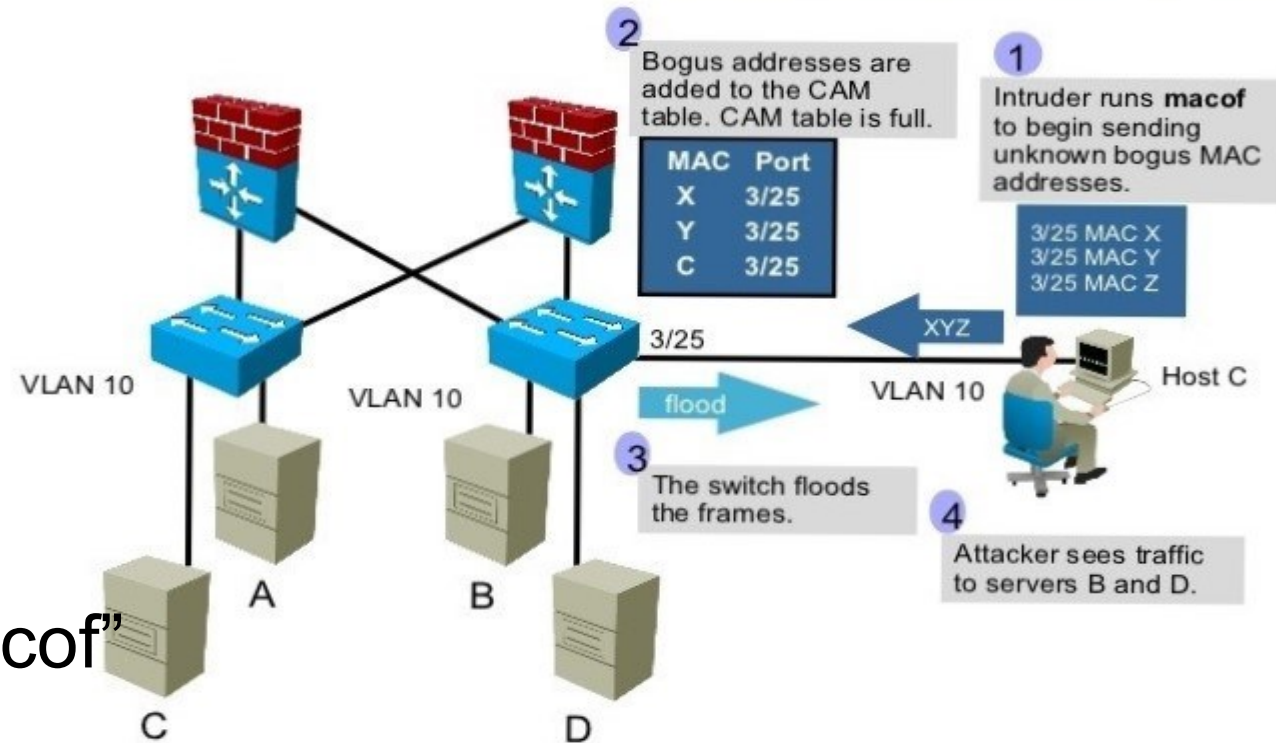
- Tools
 - Some OS allows changing MAC address from adaptor setting
 - Last shown attack could be executed with the tools used for ARP spoofing such as Nmap
- Mitigation
 - Port Security: It enables an administrator configure individual switch ports to allow only a specified number of source MAC addresses
 - Switch(config)# **interface f0/13**
 - Switch(config-if)# **switchport port-security**
 - configured on all user-facing interfaces



MAC Table Overflow

- Limited size of MAC table
- Attacker will flood the switch with a large number of invalid source MAC addresses until the MAC table fills up
- Switch will act as hub
- Applicable for single VLAN
- **Tool:** install “dsniff” and type “macof”
- **Mitigation :** Port Security

MAC Address Table Overflow Attack

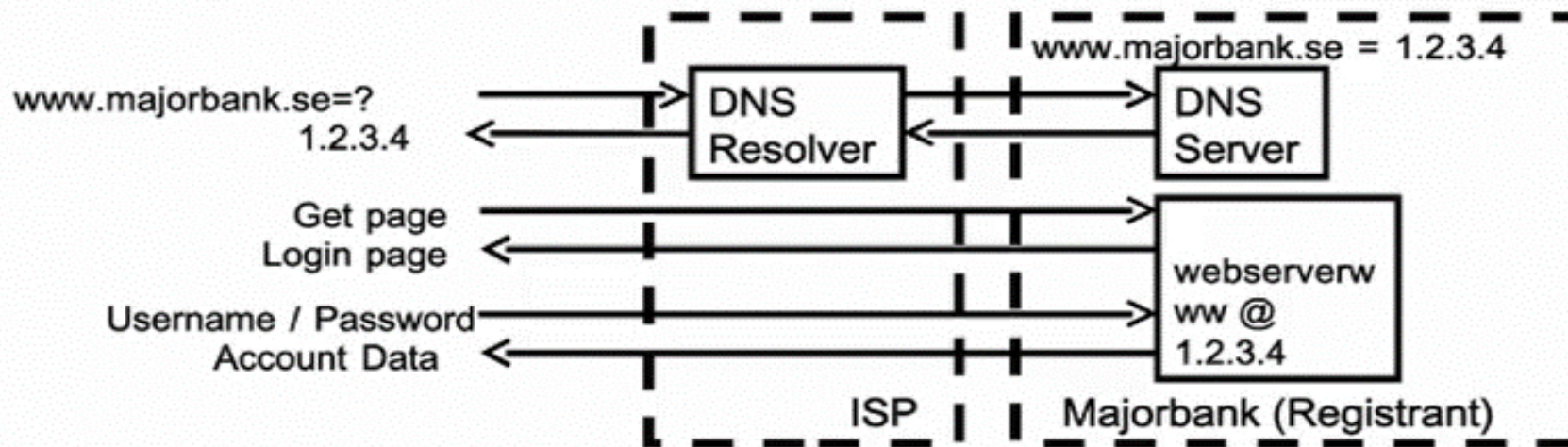




DNS Spoofing

DNS resolves IP address for a given Domain Name

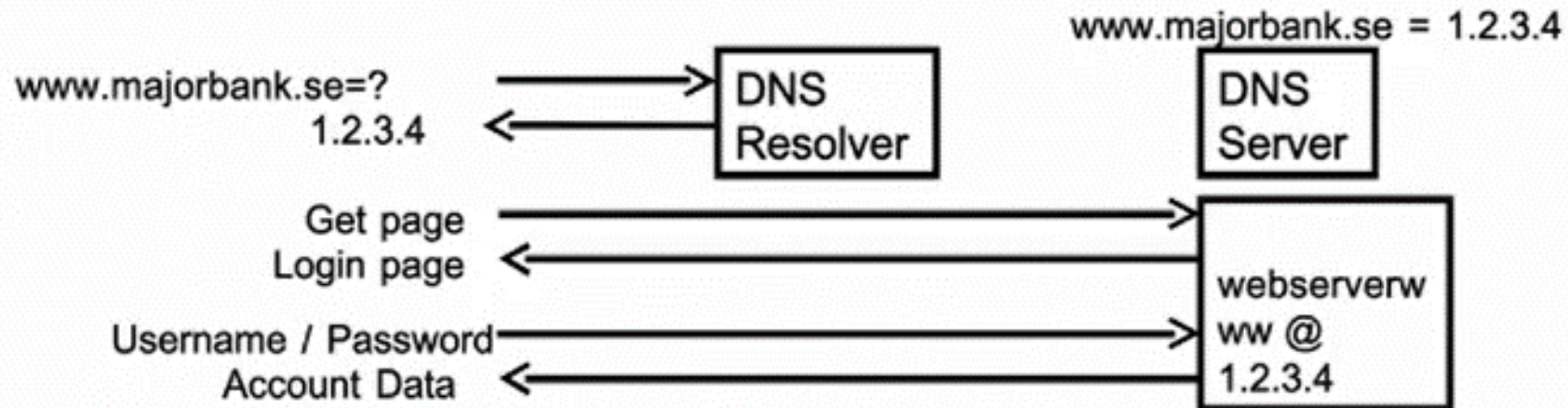
The Internet's Phone Book – Domain Name System (DNS)



DNS Cache



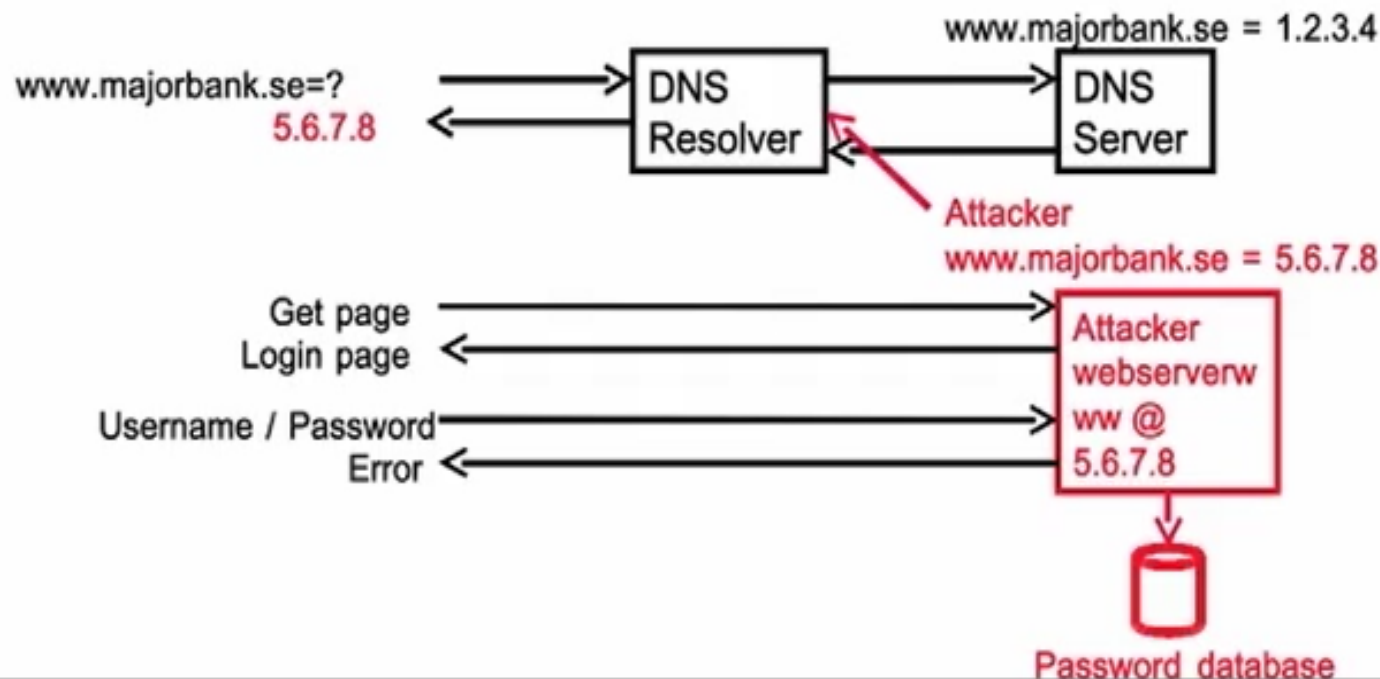
Caching Responses for Efficiency





DNS Cache Poisoning

The Problem: DNS Cache Poisoning Attack

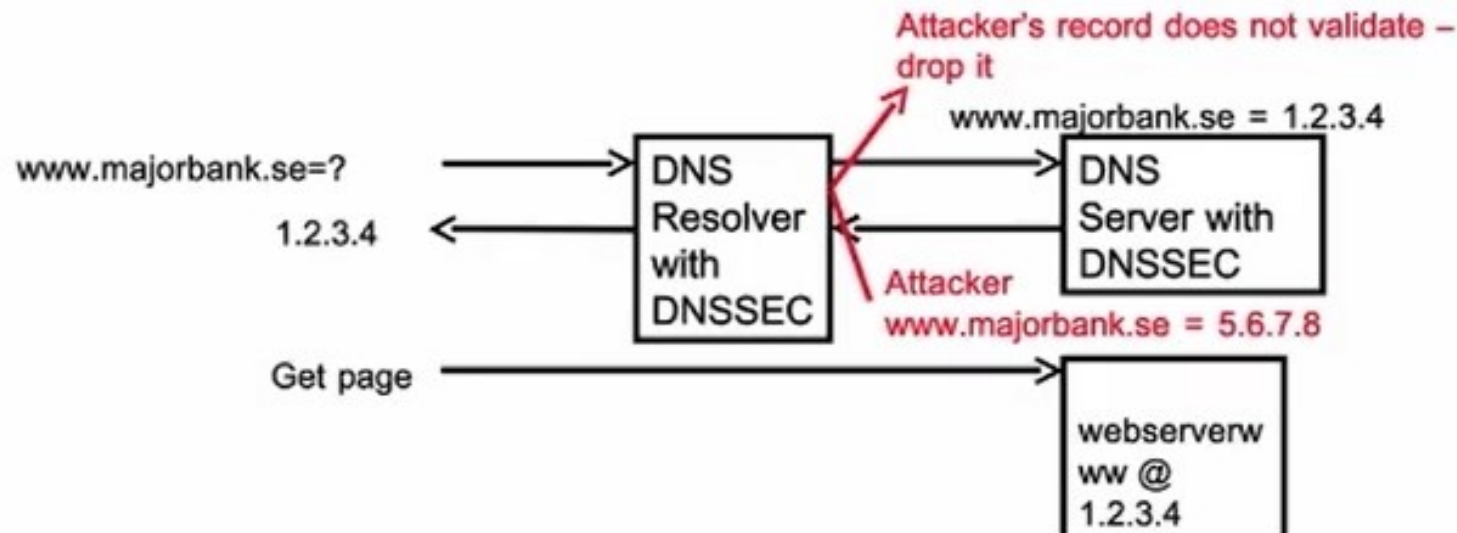


- Spread malware
- Man-In-The-Middle
- Denial of Service

Mitigation: DNSSEC

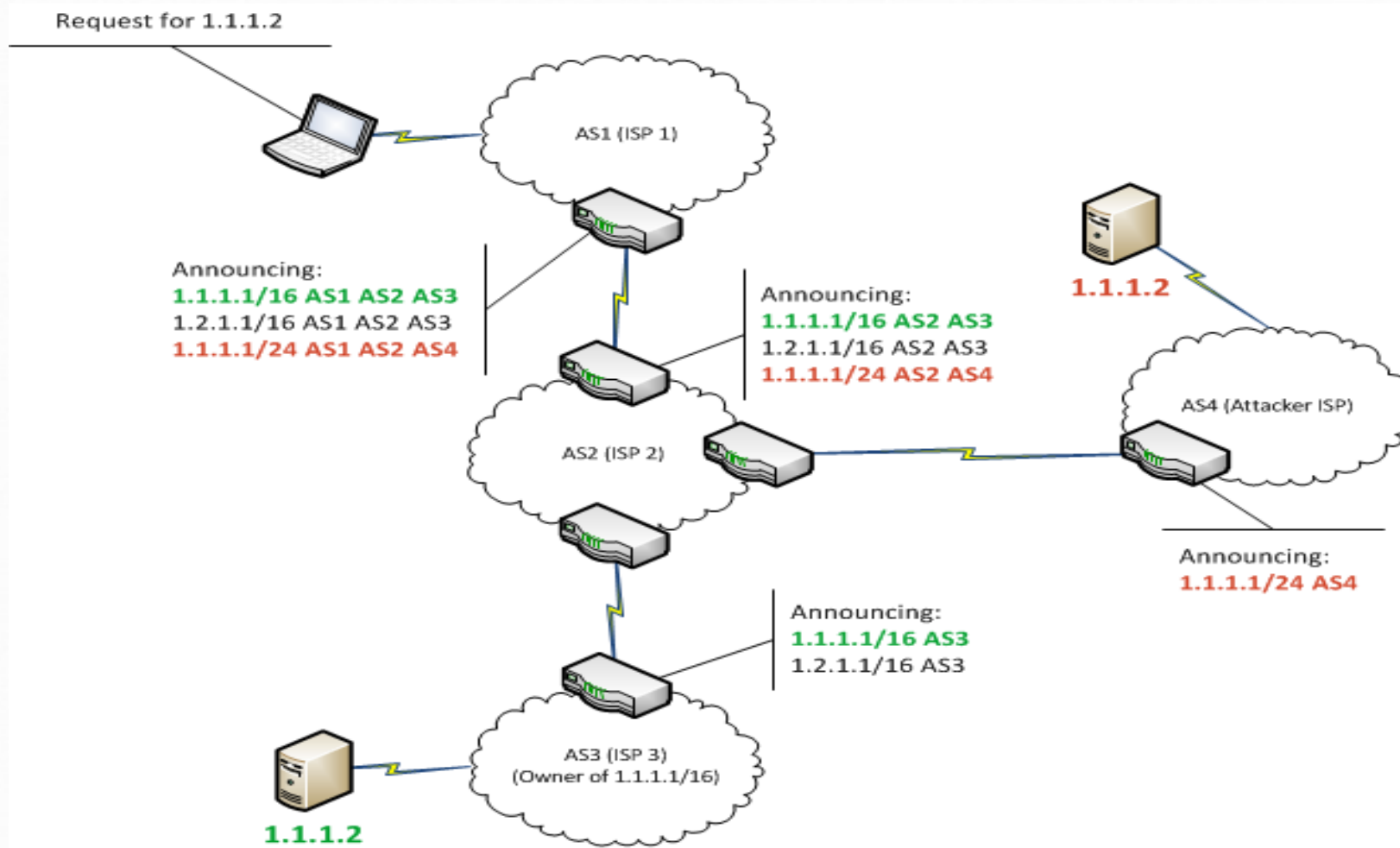


Securing The Phone Book – DNS Security Extensions (DNSSEC)





BGP Peer Hijacking





BGP Peer Hijacking

- Tools
 - MAC or ARP spoofing
 - Sniff routing traffic and then perform modification on routing updates
 - Control over devices due to very poor device security using Telnet/ SNMP

- Mitigation
 - Enable Security like 802.1x, ARP inspection, Port Security
 - Device hardening (Patch update, securing remote access, access hardening)



Exploitation

- Exploitation is a piece of programmed software or script which can allow hackers to take control over a system, exploiting its vulnerabilities.
- Metasploit is a powerful tool to locate vulnerabilities in a system.

The screenshot displays the Metasploit web interface. At the top, there is a navigation bar with tabs for Overview, Analysis, Sessions, Campaigns, Web Apps, Modules, Tags, Reports (with a notification icon), and Tasks. Below this is a breadcrumb trail: Home > Dublin VV > Vulnerabilities. A toolbar contains various actions: Grouped View, Delete Vulnerabilities, Tag Hosts, Scan, Import, Nexpose, WebScan, Modules, Bruteforce, and Exploit. A secondary toolbar shows Hosts, Notes, Services, Vulnerabilities (selected), Captured Data, and Network Topology. A 'Push Exploited Vul' button is visible on the right. The main content area shows a table of vulnerabilities with columns for Host, Service, Name, Status, and References. A tooltip 'Found by Metasploit' points to a 'NEW' badge on one of the entries.

Host	Service	Name	Status	References
VULN71	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
VULNET01XPSPO	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823960)	Exploited	CVE-2003-0352 (13 Total)
metasploitable.localdomain	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)
VULN005W3K03SP0	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823960)	Exploited	CVE-2003-0352 (13 Total)
WIN2KASPP4	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
VULN71	445/tcp	MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution (958644)	Exploited	CVE-2008-4250 (18 Total)
WIN2KAS	135/tcp	MS03-026: Buffer Overrun in RPC Interface Could Allow Code Execution (823960)	Exploited	CVE-2003-0352 (13 Total)
metasploitable	80/tcp	PHP Vulnerability: CVE-2012-1823	Exploited	CVE-2012-1823 (18 Total)
metasploitable	445/tcp	Samba MS-RPC Shell Command Injection Vulnerability	Exploited	CVE-2007-2447 (31 Total)



Exploitation...

- www.exploit-db.com is the place where you can find all the exploits related to a vulnerability.

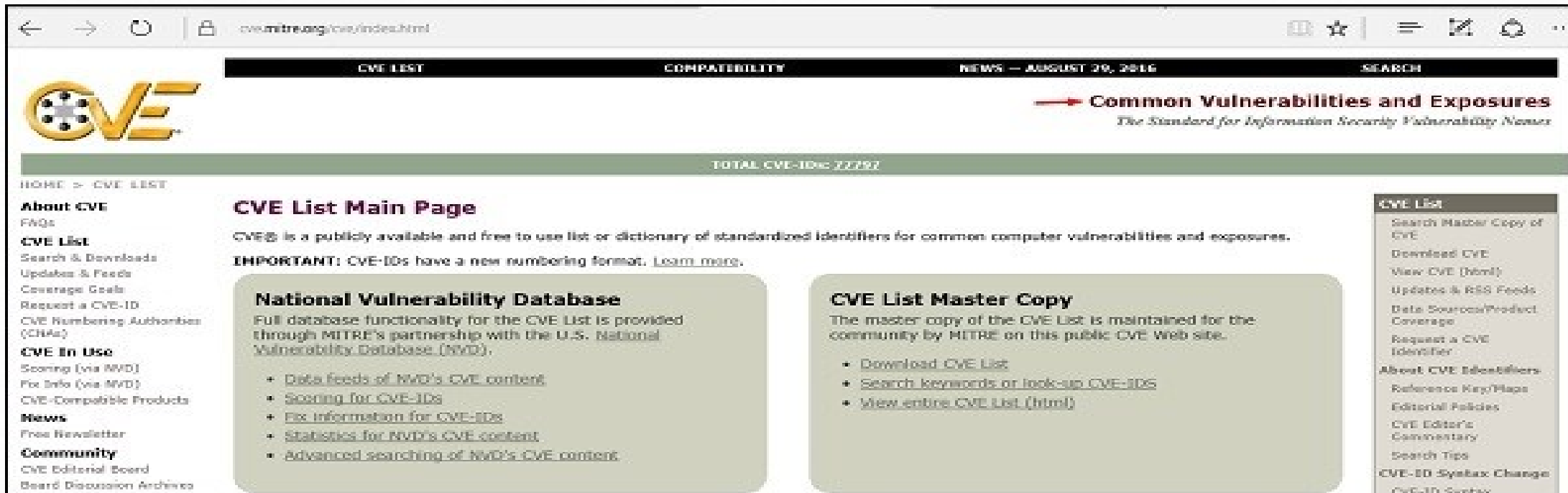
The screenshot shows the Exploit-DB website interface. At the top, there is a navigation menu with links for Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. Below the menu, the page title is 'Remote Exploits'. A description states: 'This exploit category includes exploits for remote services or applications, including client side exploits.' Below this, there is a table listing various exploits.

Date Added	D	A	V	Title	Platform	Author
2016-08-23	✓	-	✓	Phoenix Exploit Kit - Remote Code Execution (Metasploit)	PHP	Metasploit
2016-02-26	✓	-	✓	Microsoft Windows - SRV2.SYS SMB Code Execution Exploit (Python) (MS09-050)	Windows	ohnozzy
2016-02-26	✓	-	✓	Microsoft Windows - NetAPI32.dll Code Execution Exploit (Python) (MS08-067)	Windows	ohnozzy
2016-08-19	✓	-	✓	TOPSEC Firewalls - Remote Exploit (ELIGIBLEBACHELOR)	Hardware	Shadow Brokers
2016-08-18	✓	-	✓	Cisco ASA 8.x - Authentication Bypass (EXTRABACON)	Hardware	Shadow Brokers
2016-08-14	✓	-	✓	Samsung Smart Home Camera SNH-P-6410 - Command Injection	Hardware	PentestPartner.
2016-08-12	✓	-	✓	FreePBX 13 / 14 - Remote Command Execution With Privilege Escalation	Linux	pgt



Exploitation..

- Common Vulnerabilities and Exposures (CVE)
- CVE is a dictionary of publicly known information security vulnerabilities and exposures. It's free for public use. <https://cve.mitre.org>



The screenshot shows the CVE List Main Page on the MITRE website. The page features a navigation bar with links for CVE LIST, COMPATIBILITY, NEWS (dated August 29, 2016), and SEARCH. The CVE logo is prominently displayed on the left. A green banner indicates a total of 22,292 CVE-IDs. The main content area includes a 'National Vulnerability Database' section with a list of links for data feeds, scoring, fix information, statistics, and advanced searching. A 'CVE List Master Copy' section provides links to download the list, search keywords, and view the entire list. A sidebar on the right offers various utility links such as 'Search Master Copy of CVE', 'Download CVE', and 'Request a CVE Identifier'.

← → ↻ 🔒 cve.mitre.org/cve/index.html

CVE LIST COMPATIBILITY NEWS — AUGUST 29, 2016 SEARCH

CVE
Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

TOTAL CVE-IDs: 22292

HOME > CVE LIST

About CVE
FAQs
CVE List
Search & Downloads
Updates & Feeds
Coverage Goals
Request a CVE-ID
CVE Numbering Authority (CNA)
CVE In Use
Scoring (via NVD)
Fix Info (via NVD)
CVE-Compatible Products
News
Free Newsletter
Community
CVE Editorial Board
Board Discussion Archive

CVE List Main Page
CVE® is a publicly available and free to use list or dictionary of standardized identifiers for common computer vulnerabilities and exposures.
IMPORTANT: CVE-IDs have a new numbering format. [Learn more.](#)

National Vulnerability Database
Full database functionality for the CVE List is provided through MITRE's partnership with the U.S. National Vulnerability Database (NVD).
• [Data feeds of NVD's CVE content](#)
• [Scoring for CVE-IDs](#)
• [Fix information for CVE-IDs](#)
• [Statistics for NVD's CVE content](#)
• [Advanced searching of NVD's CVE content](#)

CVE List Master Copy
The master copy of the CVE List is maintained for the community by MITRE on this public CVE Web site.
• [Download CVE List](#)
• [Search keywords or look-up CVE-IDs](#)
• [View entire CVE List \(html\)](#)

CVE List
• [Search Master Copy of CVE](#)
• [Download CVE](#)
• [View CVE \(html\)](#)
• [Updates & RSS Feeds](#)
• [Data Sources/Product Coverage](#)
• [Request a CVE Identifier](#)
• [About CVE Identifiers](#)
• [Reference Key/Maps](#)
• [Editorial Policies](#)
• [CVE Editor's Commentary](#)
• [Search Tips](#)
• [CVE-ID Syntax Change](#)
• [CVE-ID Syntax](#)



Exploits....

- National Vulnerability Database
- You can locate this database at – <https://nvd.nist.gov>

Sponsored by DHS/NCSC/CERT

NIST National Institute of Standards and Technology

National Vulnerability Database

automating vulnerability management, security measurement, and compliance checking

Vulnerabilities | Checklists | 800-53/800-53A | Product Dictionary | Impact Metrics | Data Feeds | Statistics | FAQs

Home | SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments | Visualizations

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
78657 CVE Vulnerabilities
365 Checklists

Search CVE and CCE Vulnerability Database

(Advanced Search)
Keyword search:

Try a product or vendor name
Try a CVE standard vulnerability name or QVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

Search All
 Search Last 3 Months
 Search Last 3 Years

Show only vulnerabilities that have the following associated resources:
 Software Flaws (CVE)

- Remote exploits/ Local exploits



Maintaining Access— Trojans and Backdoors

- Trojan:
 - A program in which the **malicious code** is contained inside apparently harmless programming or data in such a way that it can **get control and cause damage** to your system
 - Replicate, spread, and get activated upon user's certain predefined actions



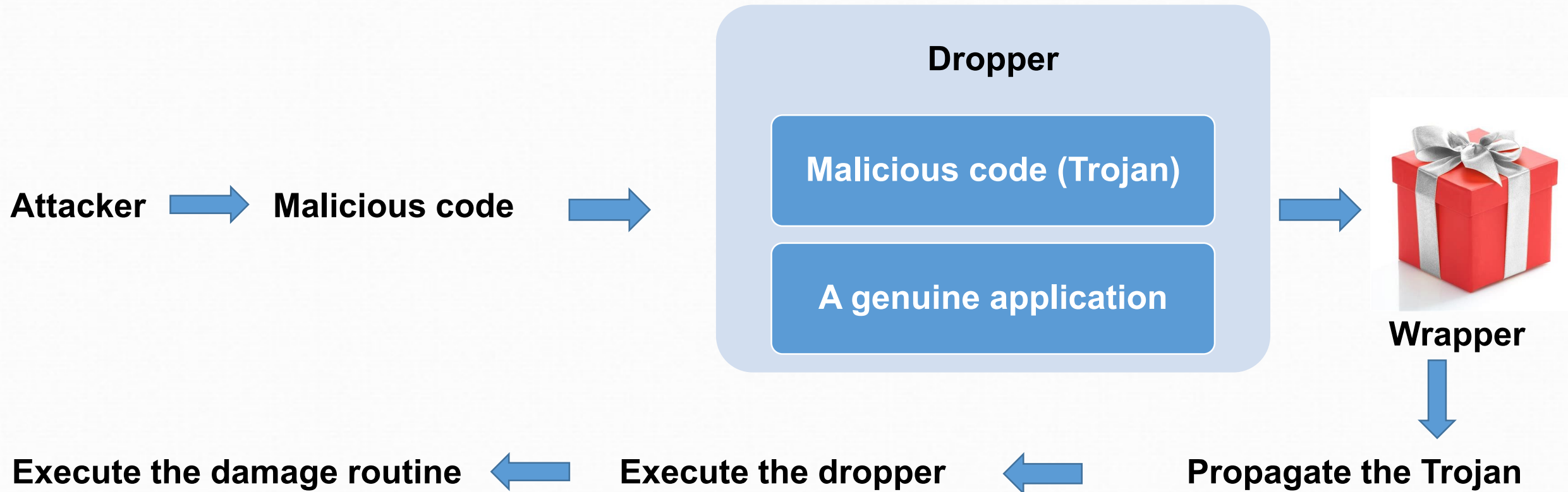
Maintaining Access- Trojans and Backdoors

- Purpose:

Delete or replace **OS's critical files**; generate **fake traffic** to create **DOS attack**; Download spyware, adware, and malicious files; disable **firewall** and **antivirus**; create **backdoors** to gain remote access; infect victim's PC as a **Proxy Server** for relaying attack; use victim's PC as a **botnet** to perform DOS attack; use victim's PC for spamming and blasting email messages; steal **password, security codes, credit card info** using keyloggers .



Maintaining Access: Trojan





Trojan/Backdoors

- Pen Testing for Trojans and Backdoors
 - Scan for open ports
 - Scan for running processes, registry entries, device drivers, window services, startup programs, files & folders, network activities, modification of OS files
 - Run Trojan scanner to detect Trojans
 - Document all the findings
 - If Trojans are detected, isolate the machine from network.
 - Update and run antivirus/ find other antivirus solution to clean Trojans



Maintaining Access: Trojan

Mitigation:

- Awareness and preventive measures
- Anti-Trojan tools such as TrojanHunter & Emsisoft
- Anti malware to detect and eliminate Trojans



Cryptography

- Ransomware
- Objectives (CIAN)
- Substitution Ciphers, Caesar ciphers, Transposition Cipher

Types

Symmetric
Encryption

AES, RC4, DES, RC5, RC6

Asymmetric
Encryption

RSA, DSA, ECT, PKCS



Cryptography Contd..

- SSH
- Digital signature
- PKI
- Cryptography tools
- Cryptography attacks
- Cryptanalysis



Clearing Tracks

- Ensure you go undetected is very important
- Kill all monitoring software
 - Anti Virus
 - Firewall
 - Host Based Intrusion Detection System (HIDS)
- Metasploit's meterpreter scripts (payload) could help in clearing logs and killing AV and Firewall
 - Killav
- Clean all logs
 - Event, application, and security



Rule of Engagement: Penetration Testing

- Objectives
- Rules of Engagement (Process, Skill & Reporting)
 - Process
 - First: Agreement with client i.r.o. Scope, Time-lines, Reporting format of results for technical specialists & Business Representatives
 - Code of conduct with company & individuals
 - Legal & regulatory issues
 - Structured, systematic & repeatable process
 - Organisations' security during information handling



Rules of engagement...Process

- Tools & methodologies are tested before being used in live tests
- Tests on applications with all levels of privileges, if applicable
- All modifications executed against a system to be documented, and returned to their original positions, if possible
- Access to compromised system to be maintained through proper authentication
- Any action that could affect normal operation of system to be taken after written approval
- All data to be destroyed once the report has been accepted
- No logs to be removed, cleared or modified unless specifically authorised



Rules of engagement..

- Skills
 - Latest threats and countermeasures in various areas
 - Consider all stages of potential cybercrime attacks
 - Threat analysis on own research and other sources like SANS, P1, OWASP, Top-10
 - Specially tailored, manual test rather than running a set of automated tests using standard tools
 - Evaluate whole target environment rather than a particular system



Rules of engagement..

- Reporting
 - Clear, insightful reports to technical specialists & Business representatives
 - Constructive, expert remediation advice
 - Quantify findings & business implications of technical weaknesses
 - Cause of delay, if any
 - Detailed list of action taken against compromised systems
 - No passwords to be included in the final report
 - Sensitive data in the report to be masked, if any



Thanks