University of Colorado **Boulder**

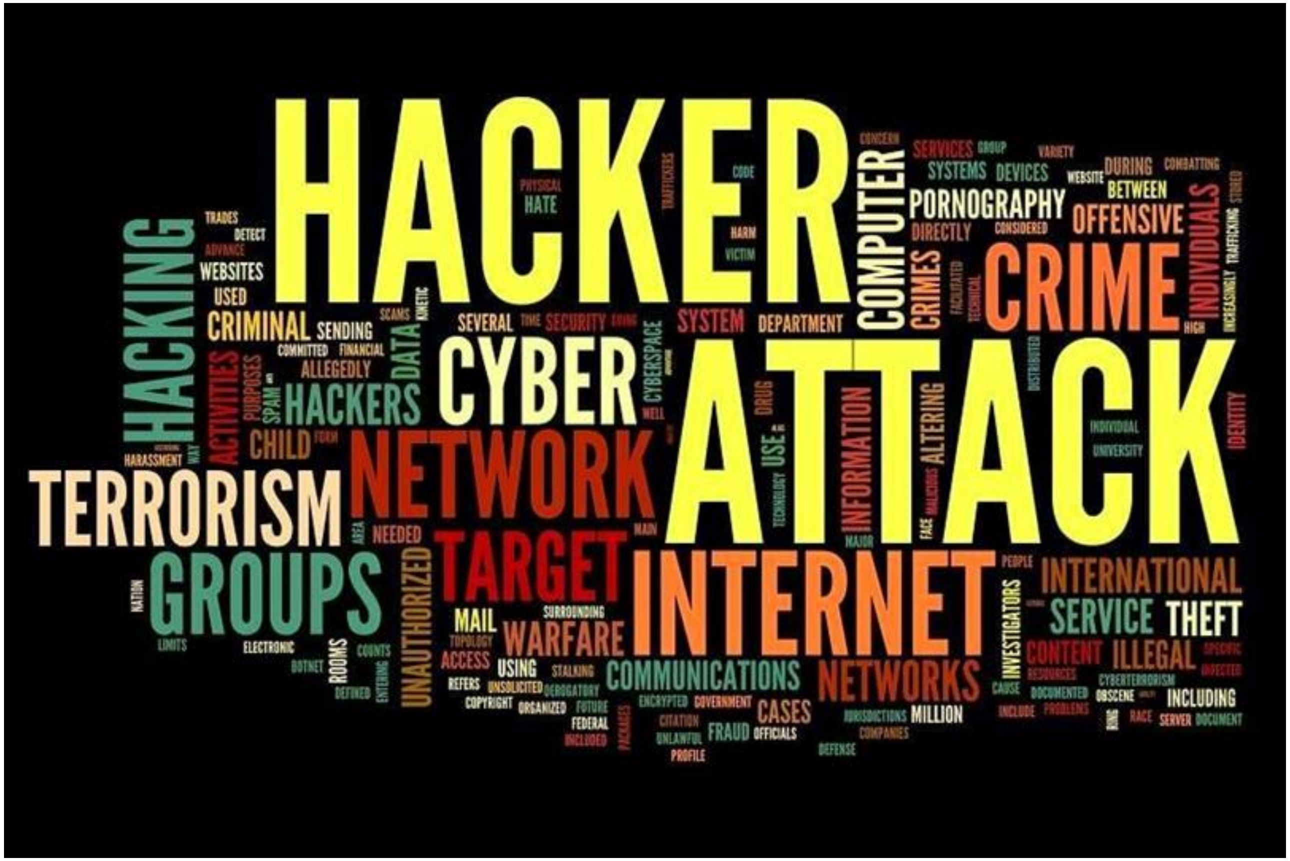
Fundamentals of Data Communications

Security

Levi Perigo, Ph.D.
University of Colorado Boulder
Department of Computer Science
Network Engineering

Review

Security (*Disclaimer)



Principles of Information Security

- – The need to defend against many attacks on technology has created a new element of IT known as information security.

- – Understanding basic principles of defense is an important first step in understanding security and its vulnerabilities.

What is Information Security?

- **Information security: Task of securing digital information**
  - Ensures protective measures properly implemented
  - Protects *confidentiality, integrity,* and *availability* (**CIA**) on the devices that store, manipulate, and transmit the information through products, people, and procedures

Challenges of Information Security

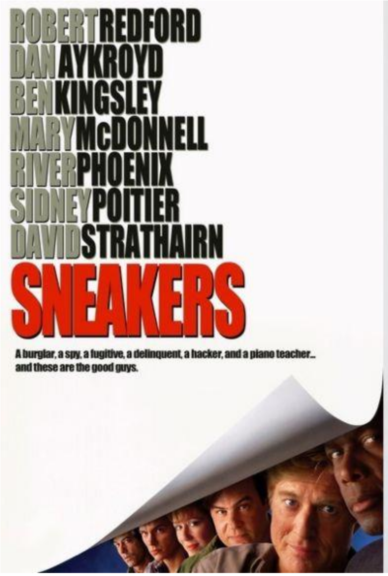
- **Trends influencing increasing difficultly in information security:**
  - Universally connected devices
  - Speed of attacks
  - Sophistication of attacks (ML)
  - Availability and simplicity of attack tools
  - Faster detection of vulnerabilities
  - Delays in patching
  - Distributed attacks
    - ***The "many against one" approach***
  - User confusion

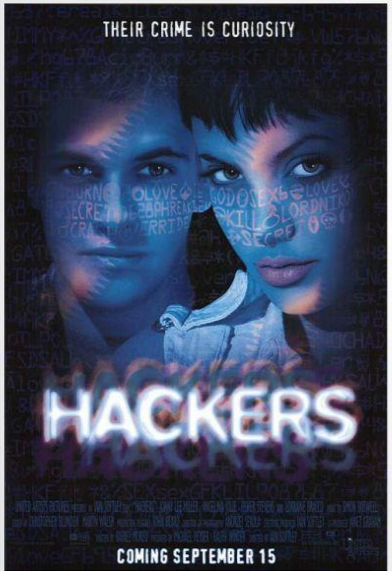
Security

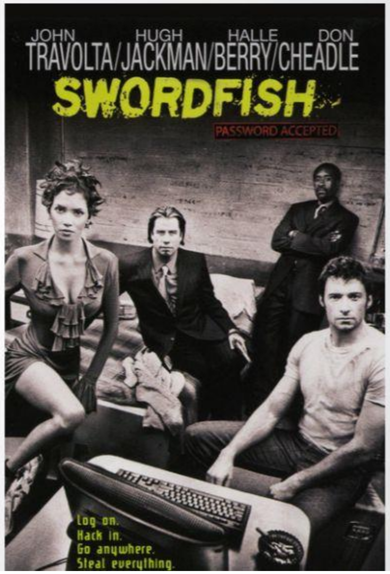
- **Hacker / Hacking**
- **Virus**
- **DDoS**
- **Social Engineering**

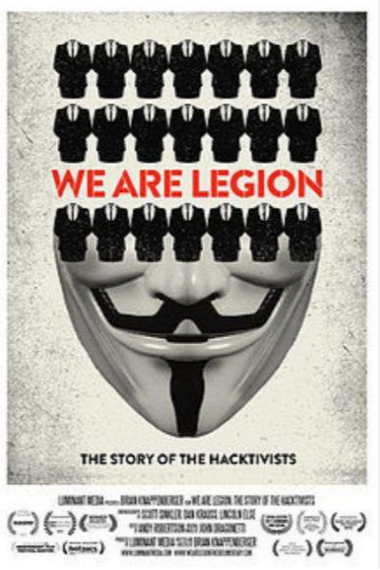
- **Financial Gain**
  - Business!
    - ***Bitcoin***

Media Glorifies “Hacking”


ROBERT REDFORD
DAN AYKROYD
BEN KINGSLEY
MARY McDONNELL
RIVER PHOENIX
SIDNEY POITIER
DAVID STRATHAIRN
SNEAKERS
A burglar, a spy, a fugitive, a delinquent, a hacker, and a piano teacher...
and these are the good guys.







Today’s Hackers

00 HACKER 10
100 DATA SECURITY 1001001001001001001
1010 PASSWORD 00100100100
IDENTITY THEFT

Why Hacking?

- **Financial Gain**
  - Steal & Return = 2x $
- **Notoriety / publicity**
- **Revenge**

- **State defense**
  - NSA
  - Nuclear
    - ***Stuxnet***
- **Hactivism**

Procedural Security Defenses

- **Security defenses go beyond technical solutions**

- **Involve implementing correct security procedures**

- **Procedural security defenses:**
  - Managing risk
  - Creating defenses against attacks

Managing Risk

- **Determine nature of risks to organization's assets**
  - First step in creating security policy

- **<u>Asset</u>: Any item that has value**
  - Cannot easily be replaced without a significant investment in expense, time, worker skill, and/or resources
  - Can form part of the organization's corporate identity

- **<u>Threat</u>: type of action that has the potential to cause harm**

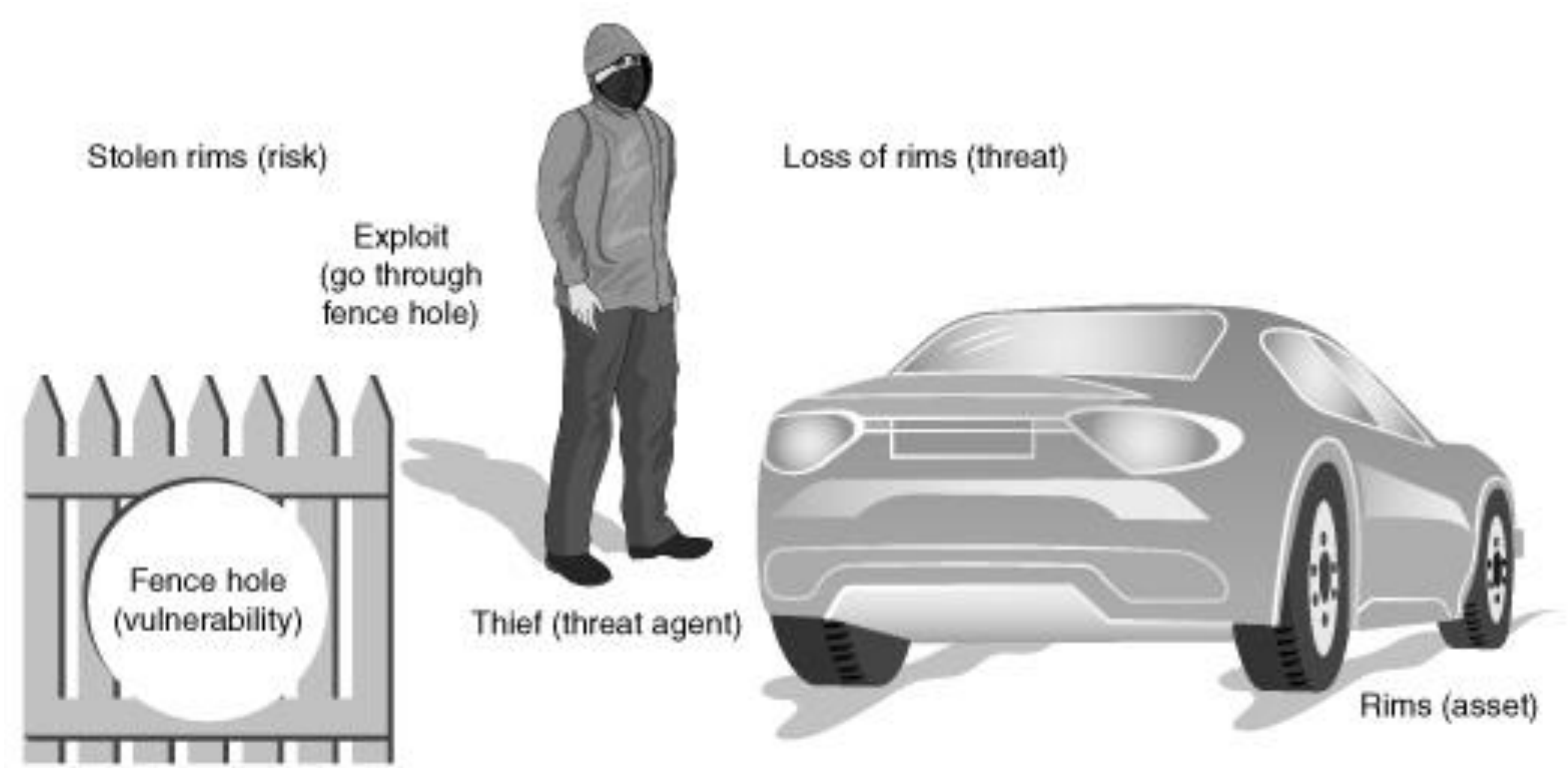
Managing Risk

- **Threat agent**: person or element that has the power to carry out a threat
  - ***In information security, could be a person attempting to break into a secure network***

- **Vulnerability**: flaw or weakness that allows a threat agent to bypass security

- **Exploiting**: taking advantage of a vulnerability

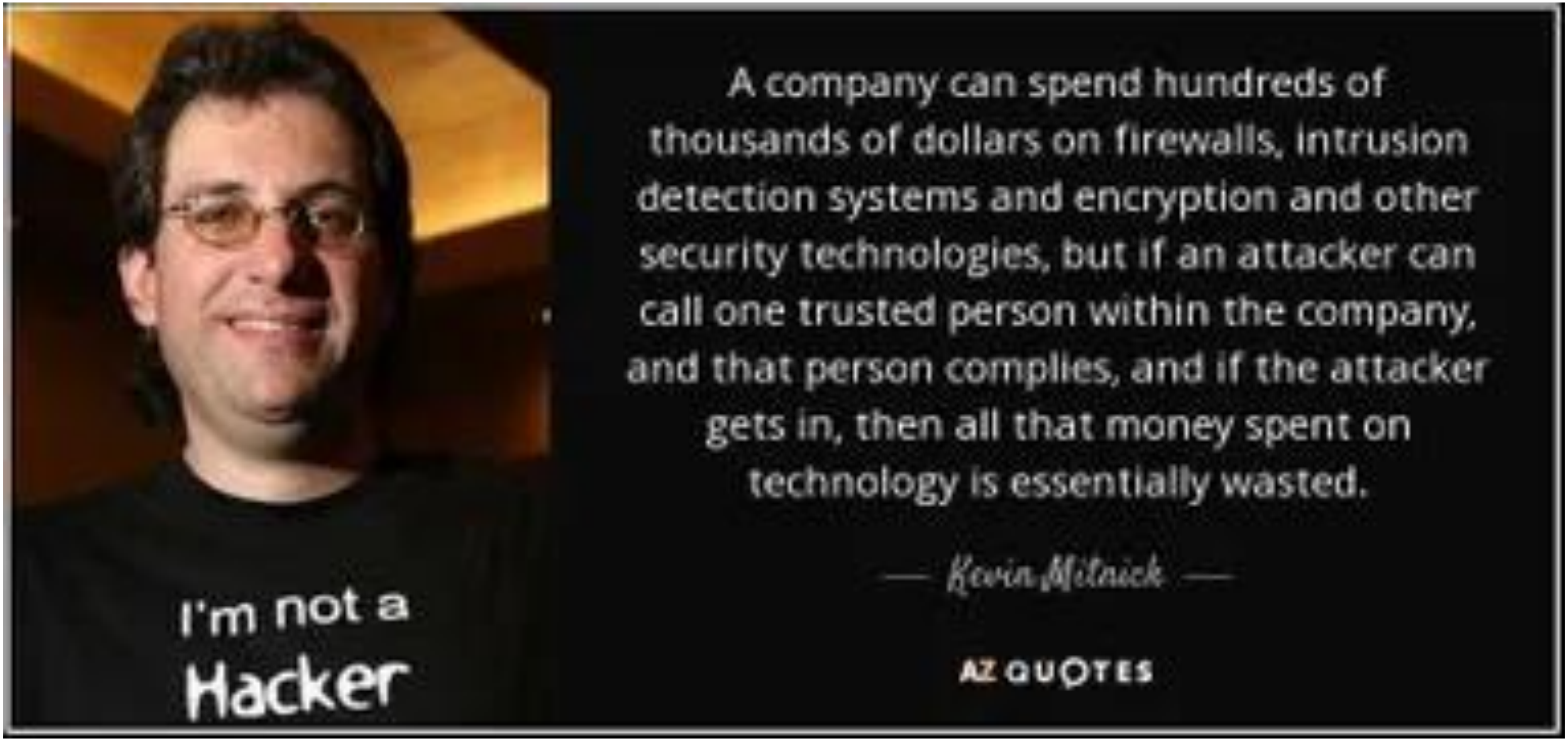
- **Risk**: the likelihood that a threat agent will exploit a vulnerability
  - ***Most risks should be diminished if possible***



© Cengage Learning 2013

Managing Risk

- **Social engineering attacks: Relies on tricking or deceiving someone to access a system**
  - Impersonation: create a fictitious character and then play out the role of that person on a victim
  - Phishing: sending an e-mail or displaying a Web announcement that falsely claims to be from a legitimate sender in order to trick the user into surrendering private information

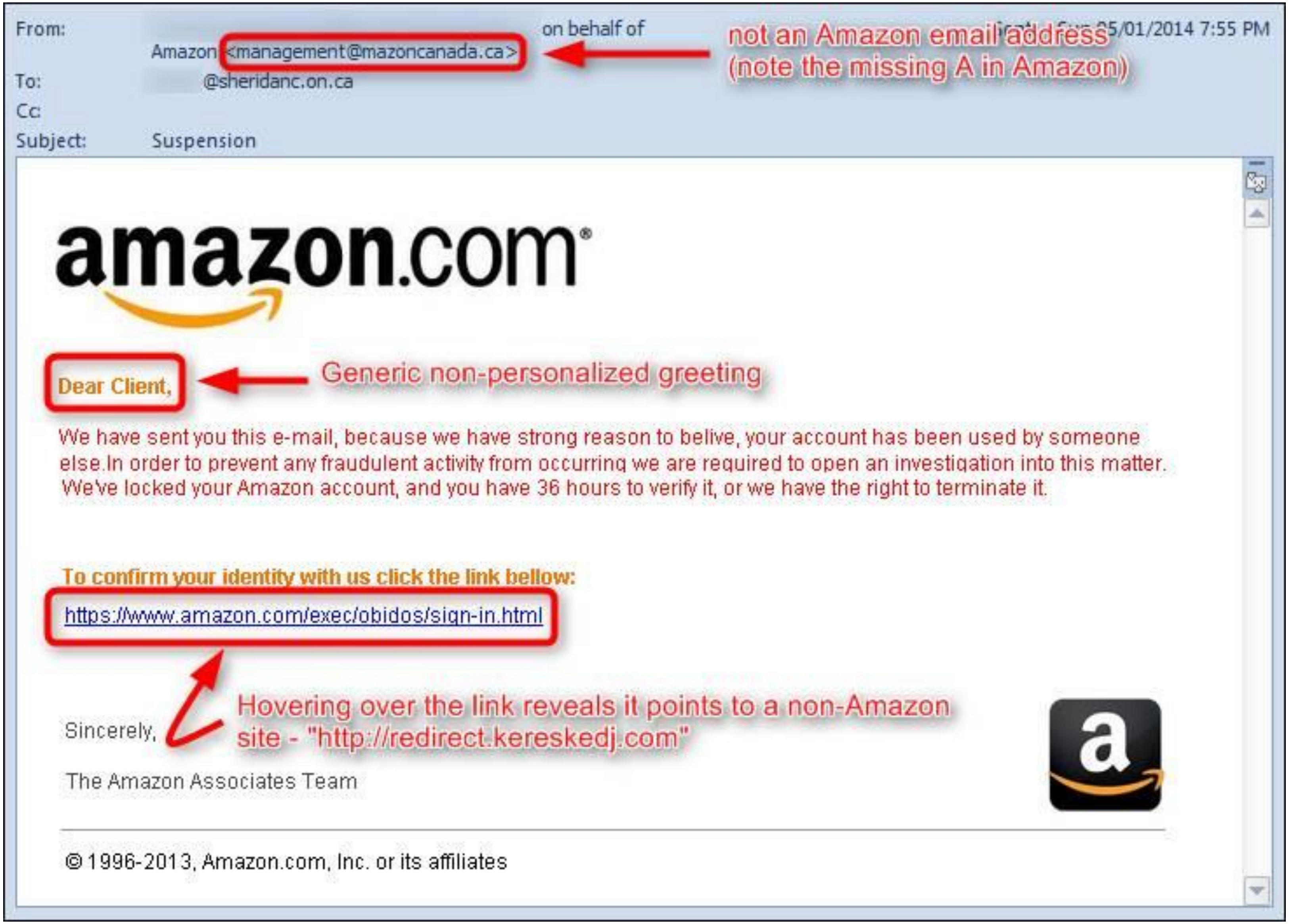


I'm not a
Hacker

A company can spend hundreds of thousands of dollars on firewalls, intrusion detection systems and encryption and other security technologies, but if an attacker can call one trusted person within the company, and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted.

— Kevin Mitnick —

AZ QUOTES



From: [redacted] on behalf of Amazon <management@mazoncanada.ca>   Sent: Sun 05/01/2014 7:55 PM

To: [redacted]@sheridanc.on.ca

Cc:

Subject: Suspension

not an Amazon email address (note the missing A in Amazon)

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

How do we prevent corporate phishing?

Defenses Against Attacks

- **Defenses against attacks include:**
  - Using security policies
  - Conducting effective security training for users
  - Implementing physical security procedures

Security Policy

- **Security policy**
  - Document that states how an organization plans to protect the company's information technology assets

- **Can serve several functions:**
  - Describe an overall intention and direction
  - Details specific risks and explains how to address them
  - Help to install security awareness in the organization's culture
  - Help ensure that employee behavior is directed and monitored to ensure compliance with security requirements

Security Policy

- **Security policy cycle:**
  - First phase involves a vulnerability assessment (an evaluation of exposure of assets to attackers, forces of nature, or any other harmful entity)
  - Five key elements:
    - ***Asset identification***
    - ***Threat evaluation***
    - ***Vulnerability appraisal***
    - ***Risk assessment***
    - ***Risk mitigation***

Security Policy

- **Security policy cycle (continued):**
  - – Second phase: use the information from the vulnerability assessment study to create the policy
  - – Final Phase: review the policy for compliance
    - ***When new assets that need protection are identified or new risks need to be addressed, the cycle begins over again***

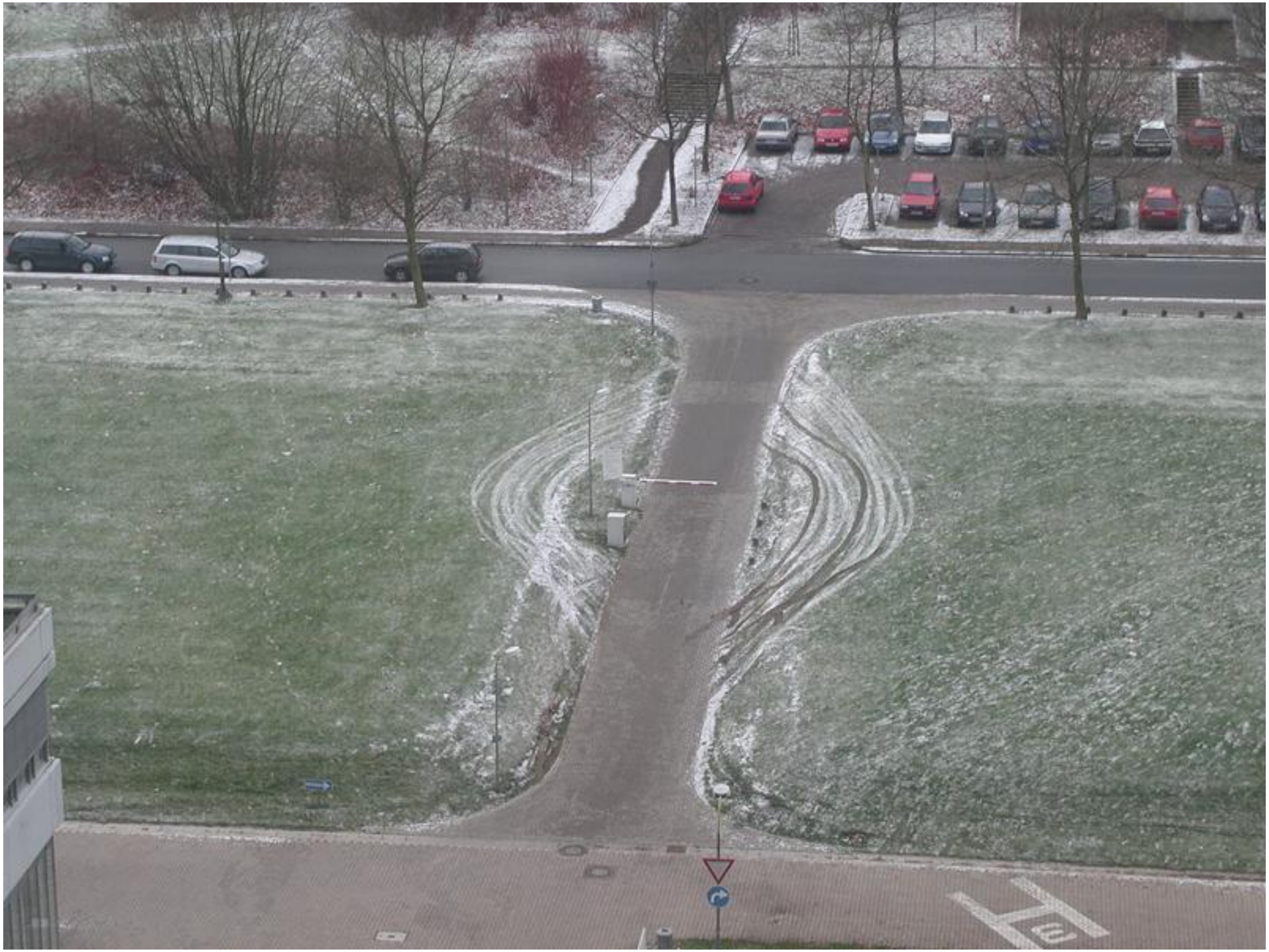
Security Policies

- **Types of security policies:**
  - **Acceptable use policy (AUP)**: defines the actions users may perform while accessing systems and networking equipment
  - **Password policy**: addresses how passwords are created and managed
  - **Wireless policy**: specifies the conditions that wireless devices must satisfy in order to connect to the organization's network

Security Policies

- **Effective security policy must balance trust and control**
  - Too much trust may lead to security problems
  - Too little trust may make it difficult to find and keep good employees

- ***Control must also be balanced**
  - If policies are too restrictive or too hard to comply with, employees will either ignore them or find ways to circumvent the controls

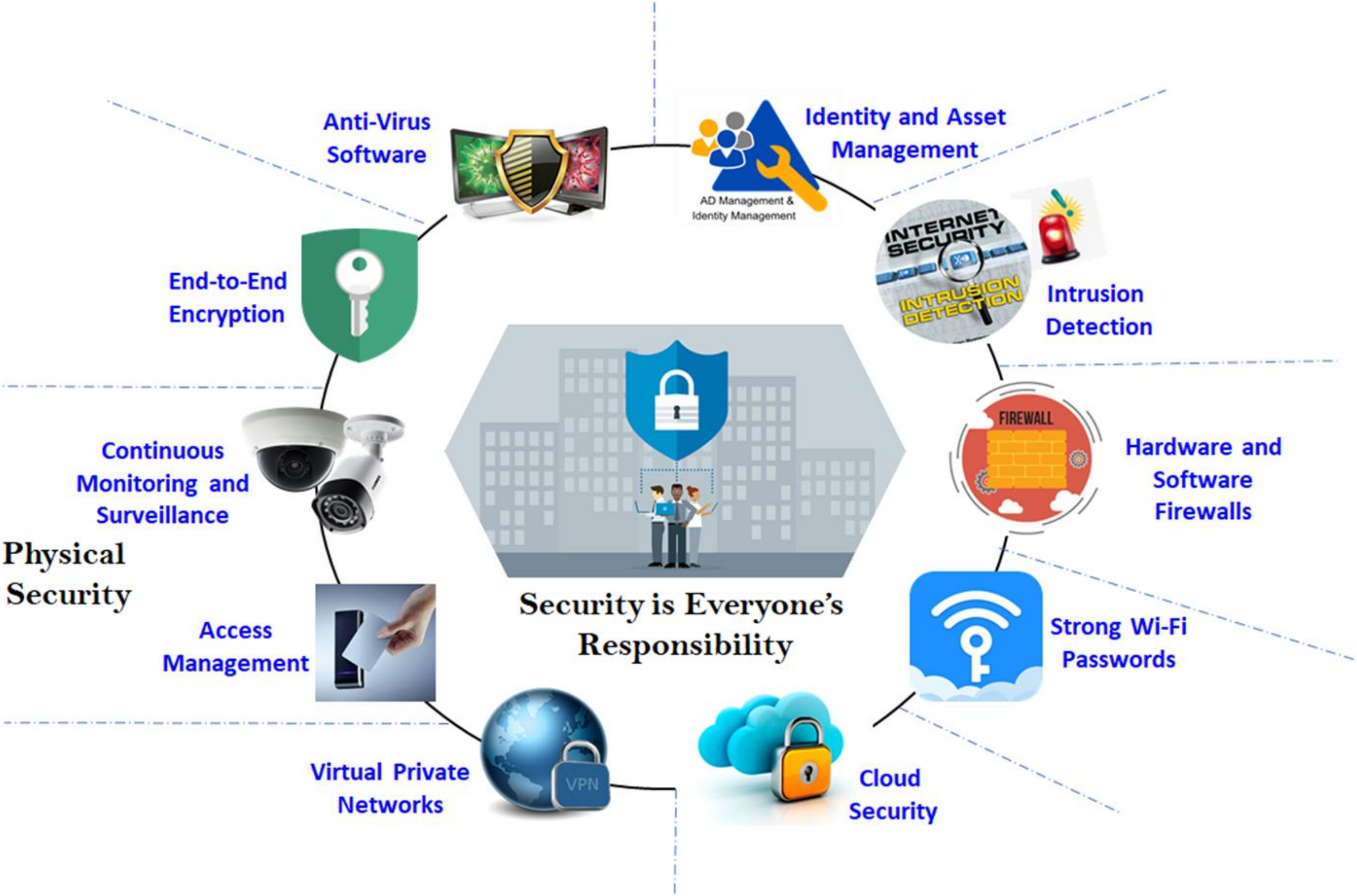


Awareness and Training

- **Opportunities for security education and training:**
  - When a new employee is hired
  - After a computer attack has occurred
  - When an employee is promoted or given new responsibilities
  - During an annual departmental retreat
  - When new user software is installed
  - When user hardware is upgraded

Network Device Security and Hardening

- **What are some best practices to secure networking equipment?**
  - Passwords / User account control
    - All the rules apply
      - » Strength, length, change
    - Passwords can be used to limit access to users that have been given the password (AAA – RADIUS / TACACS+)
  - Physical Security
    - ***Keycard / biometrics / physical key***
  - Logging
  - PCI Compliance


Anti-Virus Software
Identity and Asset Management
AD Management & Identity Management
End-to-End Encryption
INTERNET SECURITY
INTRUSION DETECTION
Intrusion Detection
Continuous Monitoring and Surveillance
FIREWALL
Hardware and Software Firewalls
Physical Security
Access Management
Security is Everyone's Responsibility
Strong Wi-Fi Passwords
Virtual Private Networks
VPN
Cloud Security

Common Threats to Physical Installations

- – Hardware threats
- – Environmental threats
- – Electrical threats
- – Maintenance threats

Layer 2 Security

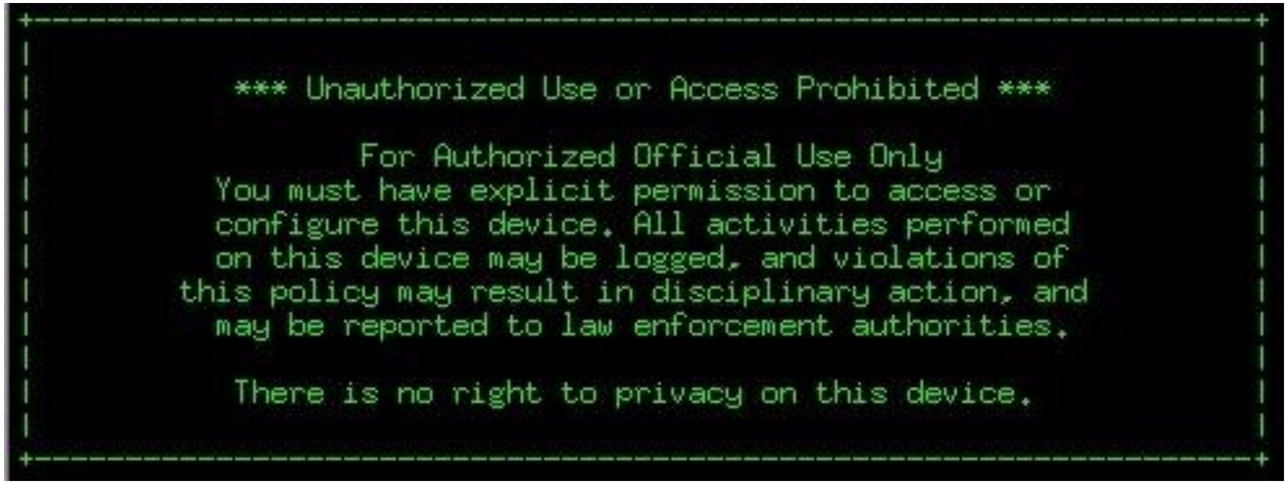
- **MAC limiting & filtering**
  - Allow known, deny unknown
- **802.1x**
  - RADIUS
  - Typically wireless networks
- **Disable unused ports**
- **Disable native VLAN**
- **Protected Ports**
- **MAC-based ACLs**
- **Rogue Machine Detection**
- **Administration Security**
- **Port Security**

Securing Unused Ports

- Unsecured ports can create a security hole
  - ***Why / How?***
- A switch plugged into an unused port will be added to the network.
  - ***VTP (DoS)***
  - ***Wireless Router***
  - ***Lobby ports***
- Secure unused ports by disabling interfaces (ports).
  - ***What's the downside of this?***

Configuring the Login Banner

- Defines and enables a customized banner to be displayed before the username and password login prompts.
- The login banner can be used to display a message before the user is prompted for a username.
- Organizational POLICY!!



```
+--------------------------------------------------------------------+
|                                                                    |
|           *** Unauthorized Use or Access Prohibited ***            |
|                                                                    |
|                   For Authorized Official Use Only                 |
|            You must have explicit permission to access or          |
|            configure this device. All activities performed         |
|            on this device may be logged, and violations of         |
|          this policy may result in disciplinary action, and        |
|            may be reported to law enforcement authorities.         |
|                                                                    |
|             There is no right to privacy on this device.           |
|                                                                    |
+--------------------------------------------------------------------+
```

Telnet vs. SSH Access

- Telnet
  - ***Most common access method***
  - ***Insecure (clear-text)***
  - ***Recommended to disable***
- SSH-encrypted

```
!- The username command create the username
and password for the SSH session
!
username cisco password  cisco

ip domain-name mydomain.com

crypto key generate rsa

ip ssh version 2

line vty 0 4
   login local
   transport input ssh
```

Firewall

Firewall

- **First and last line of defense**
  - – Sits on ingress/egress of the network (also acts as a router)

- **Filters traffic by port number**
  - – OSI Layer 4
  - – Some firewalls can filter through OSI layer 7

Firewall

- **Can encrypt traffic into/out of the network**
  - Protect traffic between sites

- **Proxy traffic**

- **Stateless or stateful**
  - Allows traffic out from LAN/Trusted

Firewall Rules

- **Security is procedural**
  - Technical and non-technical (security badge, keycard, etc.)

- **Firewall rules, packet filtering rules, email filter rules, etc.**

- **Technical rules follow procedural rules**

Firewall Rules

- **Allow or block traffic**
  - Groupings of categories
    - ***SRC IP; DST IP; port number, time of day, application, etc.***

- **A logical path**
  - Usually top-to-bottom

- **General or specific**
  - Specific rules are usually at the top
    - ***“OIT IPs can access the surveillance system”***
    - ***“Anyone can access Internet”***

Firewall Rules

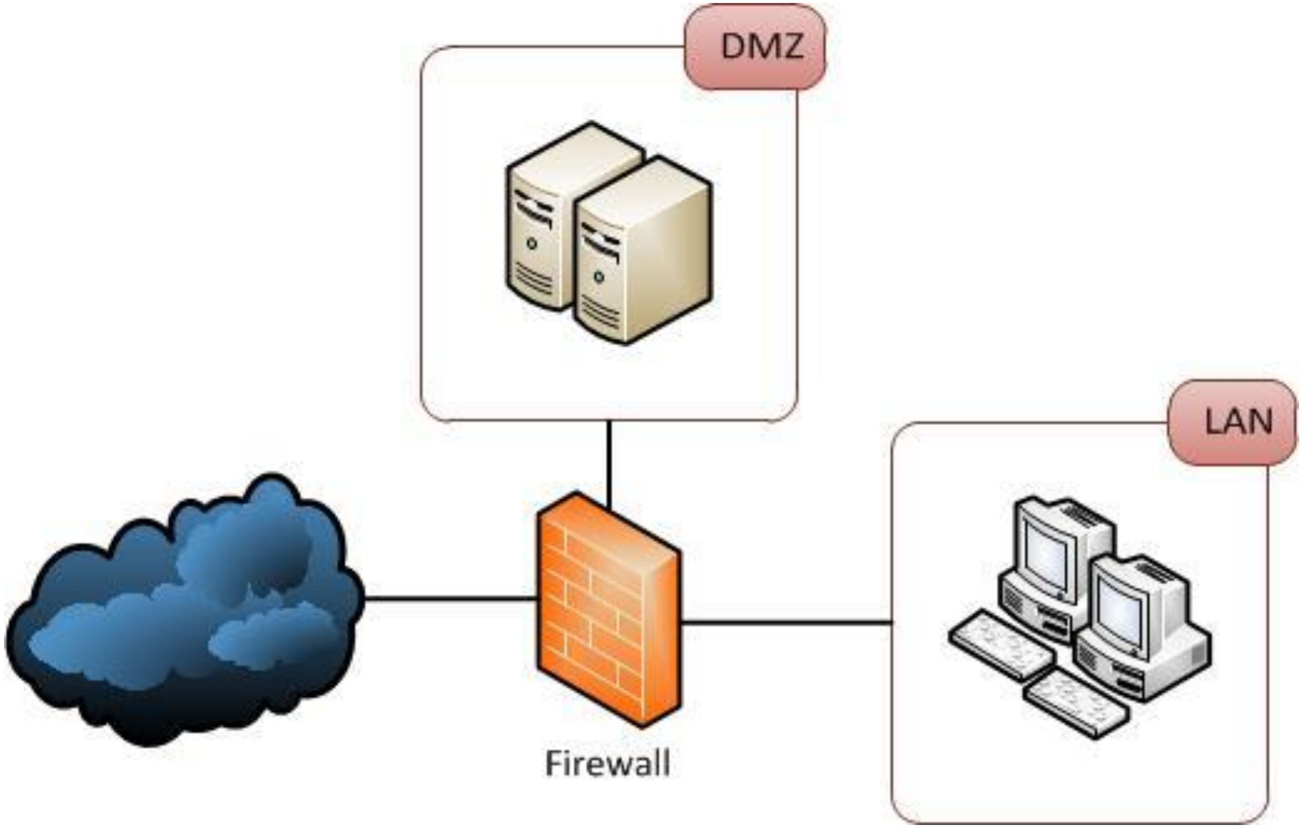
- **Implicit deny**
  - Most firewalls include a “deny all” at the bottom
    - ***Implicit vs explicit***
      - Logs

- **Caution: have console access!**

Demilitarized Zone (DMZ)

- **Where you put things that need to be accessed from the Internet**
  - Mail, Web, etc.
- **If compromised, attackers don’t have access to the rest of the network (only things in DMZ)**
- **Jump host in secure DMZ / Data Center**

DMZ Diagrams

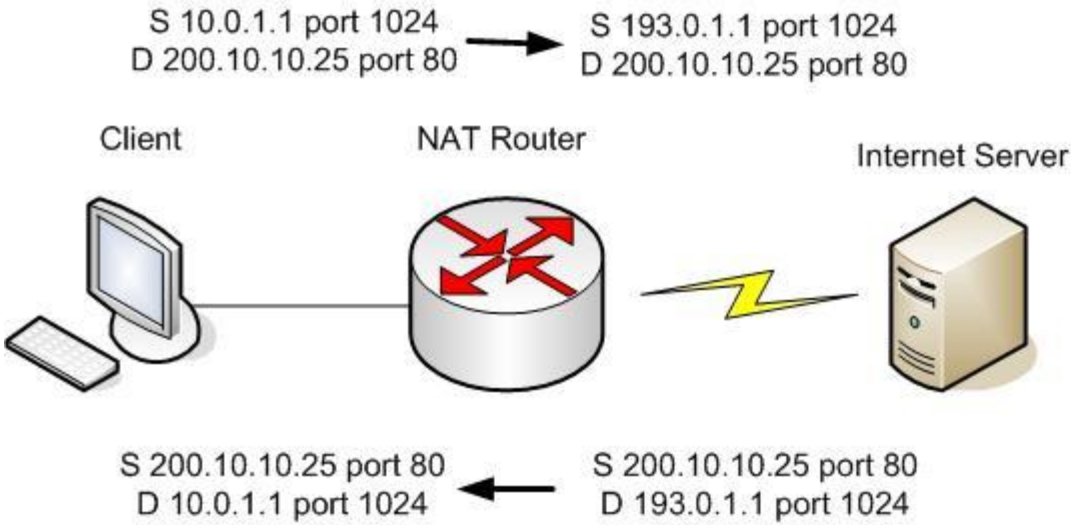


Network Address Translation (NAT)

- **What is the purpose of NAT?**
- **What is the purpose of Port Address Translation (PAT)?**
- **How is NAT/PAT different?**
- **Note: Most SMB routers/firewalls have NAT enable by default!**

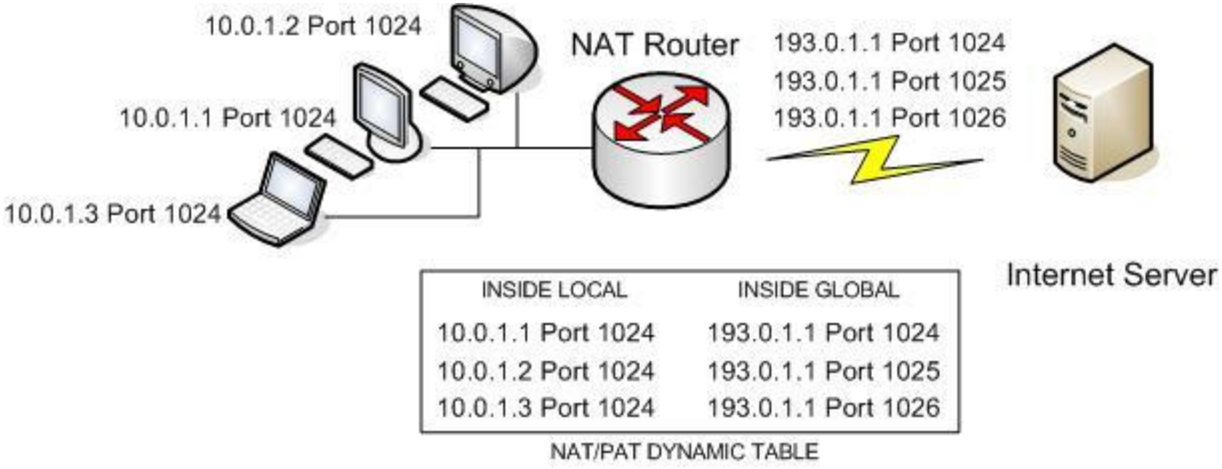
Network Address Translation (NAT)

- NAT allows networks with private IP address space to connect to the Internet
- NAT “translates” a private IP into a public (typically) IP address, while keeping a dynamic table of such translations



Overloading NAT (PAT)

- **PAT (Port Address Translation)**
  - Additional feature of NAT
  - Permits multiple connections using a single IP address
  - Translates both IP and port numbers (Socket)
  - NAT/PAT router keeps a table entry for each IP/port combination
  - Up to 64000 connections with a single IP

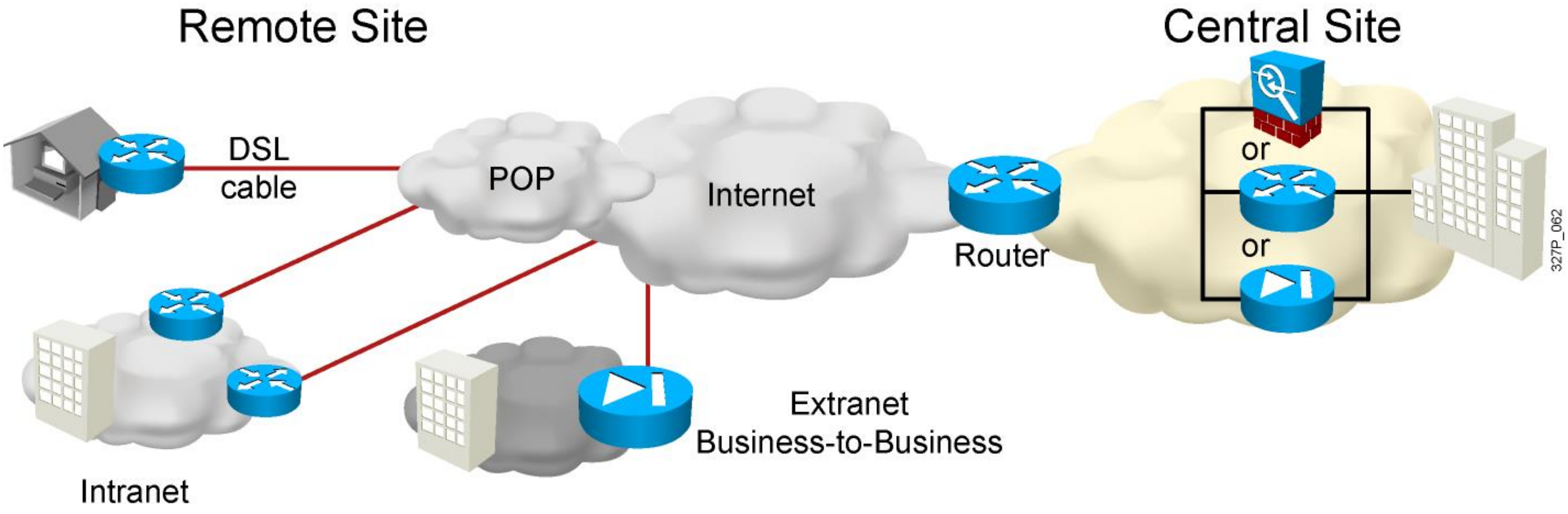


INSIDE LOCAL	INSIDE GLOBAL
10.0.1.1 Port 1024	193.0.1.1 Port 1024
10.0.1.2 Port 1024	193.0.1.1 Port 1025
10.0.1.3 Port 1024	193.0.1.1 Port 1026

NAT/PAT DYNAMIC TABLE

NAT/PAT Example (Port Forward)

Site-to-Site VPNs



- Site-to-site VPN: extension of classic WAN
- VPN Selectors – ACLs
- Router must support IPSec (software/hardware feature)

VPN Benefits and Negatives

- **Benefits**
  - Cost
  - Security
  - Scalability
  - Flexibility

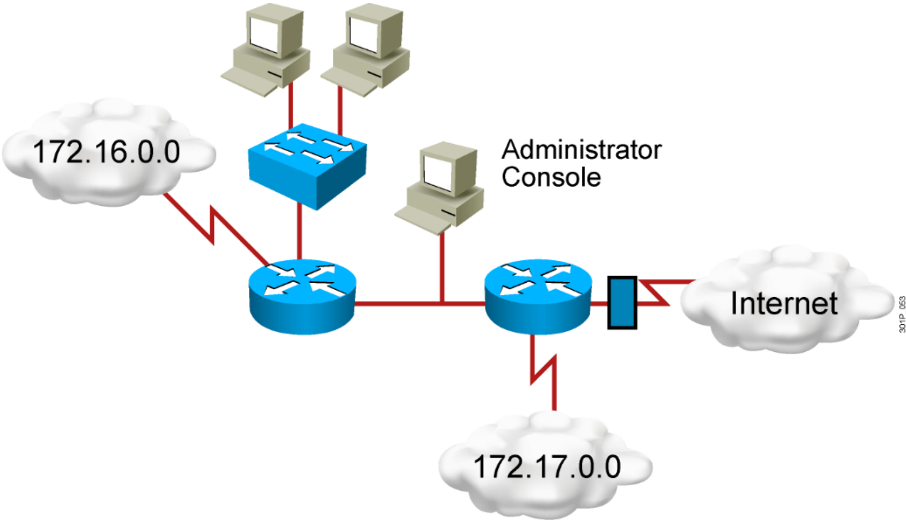
- **Negatives**
  - Cost
  - Security
  - Administrative Overhead
  - Delay/Latency/Overhead

Access-control Lists (ACLs)

- **What are access-control lists and why do we need ACLs?**
  - Make a router discard packets based on defined criteria
  - Prevent unwanted traffic on the network
  - Prevent hackers from penetrating the network
  - Prevent employees from accessing network resources
  - Filter routing updates (redistribution)
  - To match packets for prioritization (QoS), VPN tunneling (interesting traffic / encryption)
  - Control Bandwidth
  - Debug
  - Router Management

Why Use ACLs?

- Filtering: Manage IP traffic by filtering packets passing through a router
- Classification: ***Identify*** traffic for special handling
- Permit or deny packets moving through the router
- Permit or deny admin access to or from the router
- Without ACLs, all packets could be transmitted to all parts of your network



Features of ACL’s

- Packets can be filtered as they enter the interface before routing decision

- Packets can be filtered before they exit the interface, after the routing decision

- Filtering logic is configured in the ACL

- *Terminology:
  - Deny (don’t match): packet will be filtered
  - Permit (match): packet will not be filtered

Features of ACL’s

- Most vendor operating systems search the ACL sequentially (top down), until the **FIRST** statement match

- First match stops the search and an action is taken

- “Implicit Deny” / Don’t Match
  - Any packet that does not match any entry on the ACL will be discarded (or not matched)

- Steps to implement an ACL
  - Determine location of ACL
  - Create the ACL
  - Apply it on an interface (either for inbound or outbound traffic)

Types of ACLs

- Standard ACL
  - ***Checks SOURCE address***
  - ***Generally permits or denies entire protocol suite (IP)***

- Extended ACL
  - ***Checks source and/or destination address***
  - ***Generally permits or denies specific protocols and applications (IP / TCP / UDP / ICMP / RTP / etc.)***

- Two methods used to identify standard and extended ACLs:
  - ***Numbered ACLs use a number for identification***
  - ***Named ACLs use a descriptive name or number for identification***

ACL Configuration Guidelines

- Standard or extended indicates what can be filtered.
- Only one ACL per interface, per protocol, and per direction is typically allowed.
- The order of ACL statements controls testing, therefore, the most specific statements go at the top of the list.
- The **last ACL test is always an implicit deny everything else statement**, so every list needs at least one permit statement.
- ACLs are created globally and then applied to interfaces for inbound or outbound traffic.
- An ACL can filter traffic going through the router, or traffic to and from the router, depending on how it is applied.
- When placing ACLs in the network:
  - ***Place extended ACLs close to the source***
  - ***Place standard ACLs close to the destination***

Diagram of where to place ACLs

Extended ACLs

- **Extended ACL commands**
  - **access-list** *acl_number action source (IP/SPort) destination (IP/DPort)*
  - *Note:* When configuring remember “From” (source first) and “To” (destination second)
    - ***If arguments after source, applies to source port and vice versa***

- *access-list 101 deny tcp 10.1.1.0 0.0.0.255 10.1.2.0 0.0.0.255 eq 80*
- *access-list 101 deny ip any host 10.1.1.1*
- *access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23*
- *access-list 101 deny tcp any host 10.1.1.1 eq 23*
- *access-list 101 deny tcp any host 10.1.1.1 eq telnet*
- *access-list 101 deny udp 1.0.0.0 0.255.255.255 lt 1023 any*

Linux iptables

- **A Linux command that allows you to add firewall/security rules to secure your system**

- **Example:**
  - Block all “input” traffic from source IP 33.33.33.33
    - ***Incoming traffic will hit the input table which has the below rule. If the traffic has SIP=33.33.33.33, it will be dropped.***
    - ***iptables -A INPUT -s 33.33.33.33 -j DROP***

Linux iptables

- **Example:**
  - To be more specific, we can block input HTTP traffic from webserver 33.33.33.33
    - ***iptables -A INPUT -p tcp --sport=80 -s 33.33.33.33 -j DROP***
  - Order in a firewall is very important since rules get executed in order. If a firewall rule before the above one allowed traffic from the webserver, the packet would not get dropped. Therefore, add more specific rules at the top.
  - You can flush all firewall rules with **iptables –F** command

How do we keep business safe?

- **Planning**
- **Mitigation strategies**
- **Incident response**
- **Remediation strategies**
- **Backups and backup plan**
- **Securing the network and devices**
- **Policies**
- **Physical security**

Securing the Network

- **Continuous monitoring/logging**
- **Network Security**
  - Hosts
  - Network infrastructure
- **Physical**
- **Social**

Monitoring and Diagnosing Networks

- **Logging**
  - Syslog
  - Netflow
  - TACACS+
  - RADIUS

- **IDS**

- **IPS**

- **Patches**
  - Keep OS up to date!

Security Audits

- **Review security logs**
- **Review policies and compliance with policies**
- **Check security device configuration**
- **Penetration testing**
- **How often should they happen?**
- **Remediation Policy**
  - Minor
  - Serious
  - Critical

Security Audits

- **Understanding Attacks**
  - – Malware
  - – Virus
  - – Worm
  - – Trojan Horse
  - – Ransomware
  - – Spoofing Attacks
  - – DoS & DDoS
  - – Phishing
  - – MitM
  - – Replay

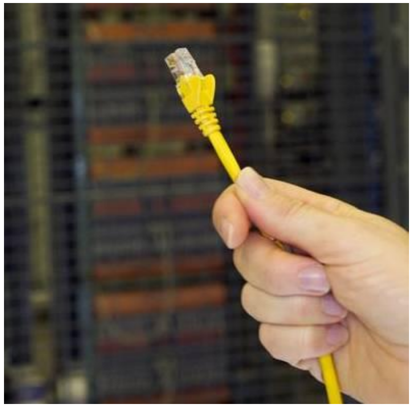
Remediation Policy

- **Disaster Recovery**
  - Data backup
  - Failover

- **Security Policy!!**

- **Reporting Security Issues**
  - Alarms
  - Alerts
  - Trends

We are under attack?!



WARNING!

We're Under Attack!

Incidence Response

- – Outside agencies should be contacted
- – Resources used to deal with an incident
- – Procedures to gather and secure evidence
- – List of info that should be collected about an incident
- – Outside experts who can be used to address issues if needed
- – Policies and guidelines regarding how to handle an incident

Incident Response

- **Identify the incident**
- **Investigating the incident**
- **Repairing the damage**
- **Documenting and reporting the response**
- **Adjusting procedures**
  - – What does this entail?

Adjusting Procedures

- **Raise awareness**

- **Education and training**
  - – Importance of security
  - – Responsibilities of people in the organization
  - – Policies and procedures
  - – Usage policies
  - – Account and password-selection criteria
  - – Social engineering prevention

Know your weakness

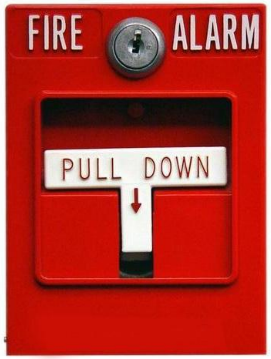
- **To protect your computer/network/company you must know where weaknesses are**

- **This is only efficient with automated tools**

- **Prioritize targets**
  - What area of the network has the highest risk

- **Prioritize results**
  - What is the area with the highest severity and likelihood of attack

Incident Response Plan



- **"Fire Drill"**
  - Was the evidence gathered and the chain of custody maintained?
  - Did the escalation procedures follow the correct path?
  - Given the results of the investigation, would you be able to find and prosecute the culprit?
  - What was done that should not have been done?
  - What could have been done better?

While that is happening…

- **Knowing where to scan is important**
- **Ask the right questions**
- **Ask multiple groups**
- **Ask where would you attack if you were an attacker?**
- **Ask what are you most scared of breaking**

Penetration Testing

- **Pen Test**
  - Authorized, simulated attack on a computer system, performed to evaluate the security of the system
    - ***Identify weaknesses (vulnerabilities)***
    - ***Strengths***
    - ***Risk Assessment***
  - Component of full security audit

What/how should you test?

- **Intrusive vs. Non-intrusive**

- **Black box**
  - No knowledge of the system (outside attacker)

- **White box**
  - Significant knowledge of the system (rogue employee)

- **Gray box**
  - Some limited knowledge of the system

Pen Test - Design

- **Find an exploitable vulnerability.**
- **Design an attack around it.**
- **Test the attack.**
- **Seize a line in use.**
- **Enter the attack.**
- **Exploit the entry for information recovery.**

Network Intrusion Detection and Prevention Systems

- **Intrusions**
  - Exploits against operating systems, application vulnerabilities, buffer overflows, etc.

- **Detection vs. Prevention**
  - Detection – alarm or alert
  - Prevention – stop it before

Identification Technologies

- **Signature-based**
  - Look for a perfect match
- **Anomaly-based**
  - Build a baseline of what’s “normal”
- **Behavior-based**
  - Observe and report
- **Heuristics**
  - Use artificial intelligence or machine learning to identify

Network Based Intrusion Prevention

- **Software**
  - Snort
  - Load it and go

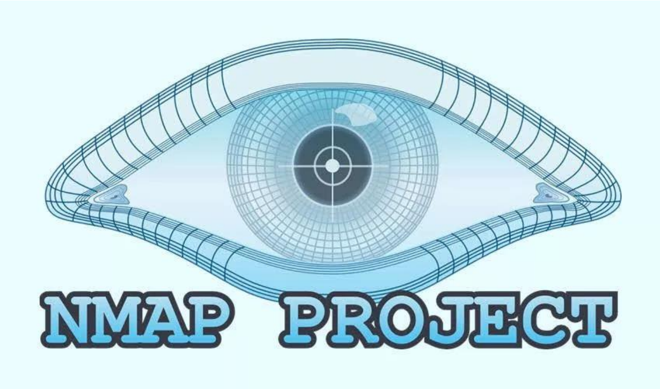
- **Hardware**
  - Specialized high-speed appliances
  - Enterprise features
    - ***High availability***
    - ***External logging***

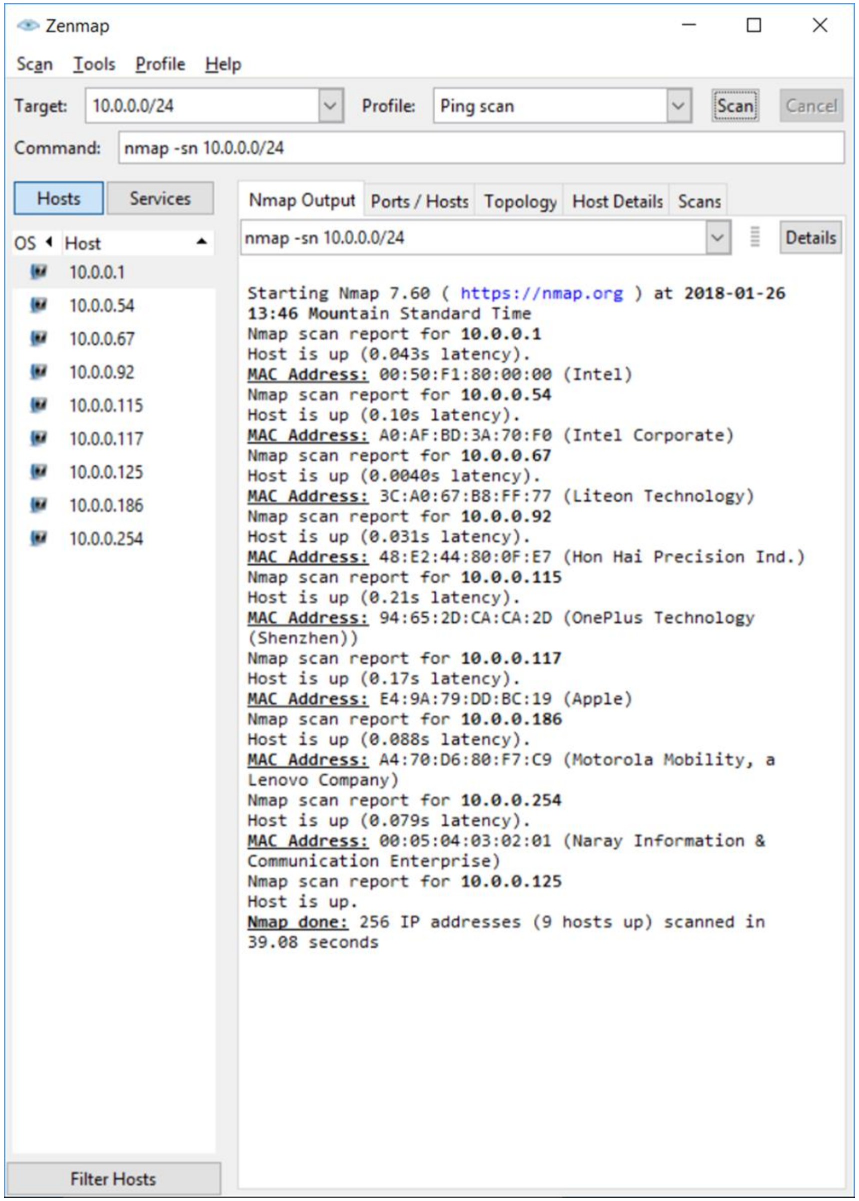
Network Mapping (Nmap)

- **Nmap and Zmap**
- **Uses**
- **IDS**
- **IPS**
- **Firewall**

Nmap & Zenmap

- **Free Open-Source Tool**
  - – Network Scanning and Security Functions
  - – Creates a “map” of the network
  - – Sends specific packets to target host (or hosts); analyzes responses
  - – Zmap GUI for Nmap
- **https://nmap.org/**





Target: 10.0.0.0/24

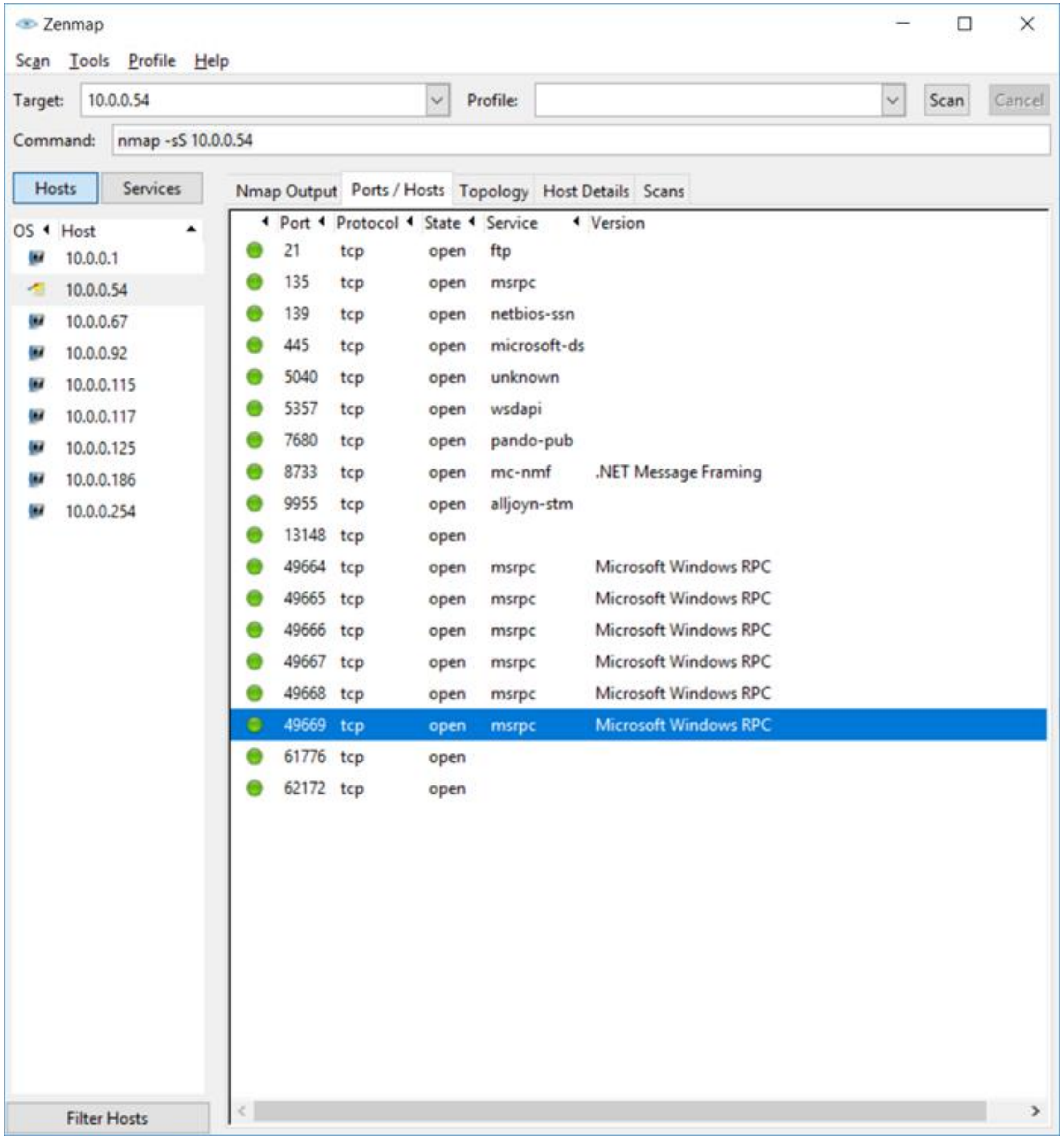
Profile: Ping scan

Command: nmap -sn 10.0.0.0/24

```
10.0.0.1
10.0.0.54
10.0.0.67
10.0.0.92
10.0.0.115
10.0.0.117
10.0.0.125
10.0.0.186
10.0.0.254
```

```
nmap -sn 10.0.0.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-26
13:46 Mountain Standard Time
Nmap scan report for 10.0.0.1
Host is up (0.043s latency).
MAC Address: 00:50:F1:80:00:00 (Intel)
Nmap scan report for 10.0.0.54
Host is up (0.10s latency).
MAC Address: A0:AF:BD:3A:70:F0 (Intel Corporate)
Nmap scan report for 10.0.0.67
Host is up (0.0040s latency).
MAC Address: 3C:A0:67:B8:FF:77 (Liteon Technology)
Nmap scan report for 10.0.0.92
Host is up (0.031s latency).
MAC Address: 48:E2:44:80:0F:E7 (Hon Hai Precision Ind.)
Nmap scan report for 10.0.0.115
Host is up (0.21s latency).
MAC Address: 94:65:2D:CA:CA:2D (OnePlus Technology
(Shenzhen))
Nmap scan report for 10.0.0.117
Host is up (0.17s latency).
MAC Address: E4:9A:79:DD:BC:19 (Apple)
Nmap scan report for 10.0.0.186
Host is up (0.088s latency).
MAC Address: A4:70:D6:80:F7:C9 (Motorola Mobility, a
Lenovo Company)
Nmap scan report for 10.0.0.254
Host is up (0.079s latency).
MAC Address: 00:05:04:03:02:01 (Naray Information &
Communication Enterprise)
Nmap scan report for 10.0.0.125
Host is up.
Nmap done: 256 IP addresses (9 hosts up) scanned in
39.08 seconds
```



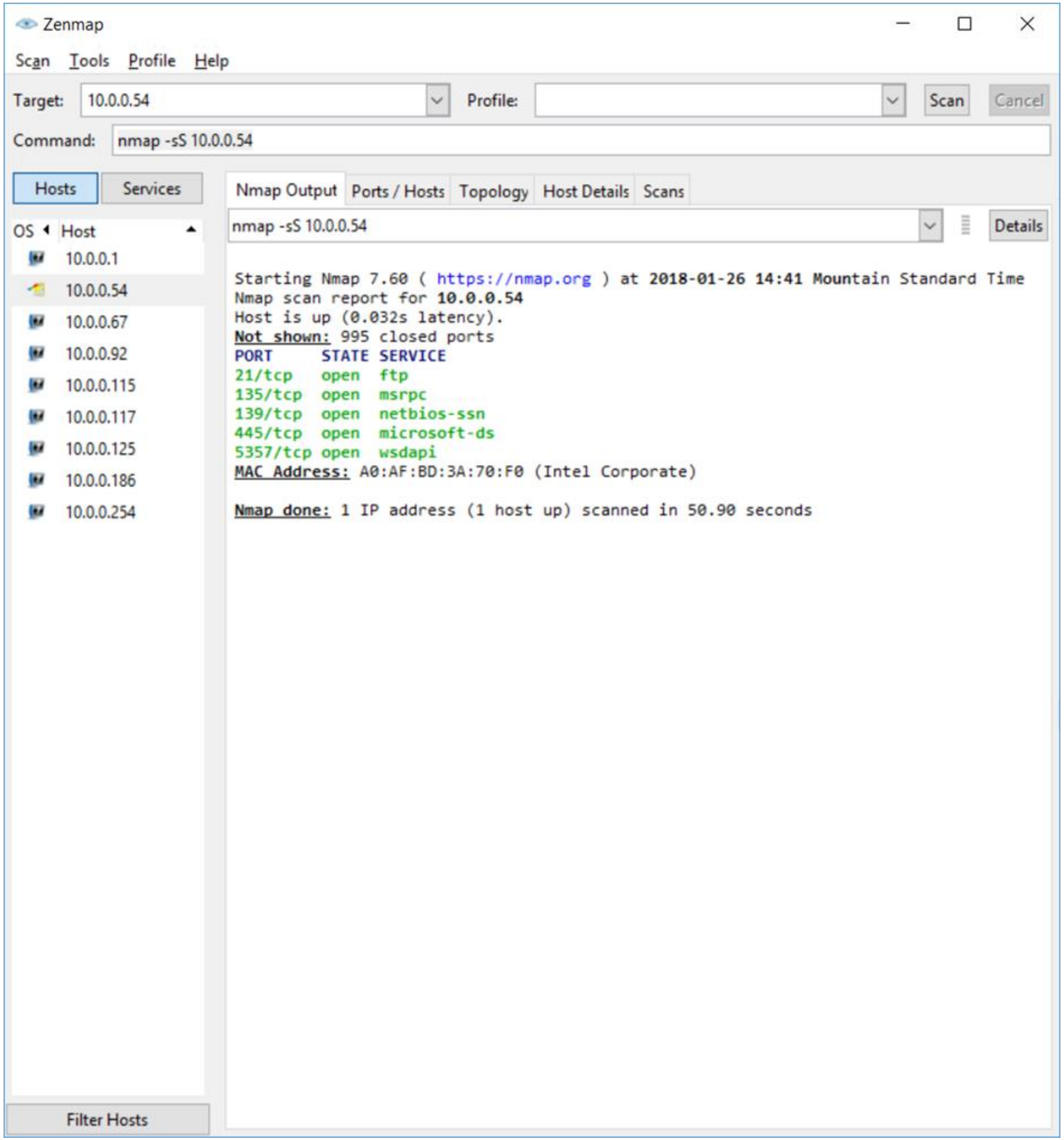
Target: 10.0.0.54

Profile:

Command: nmap -sS 10.0.0.54

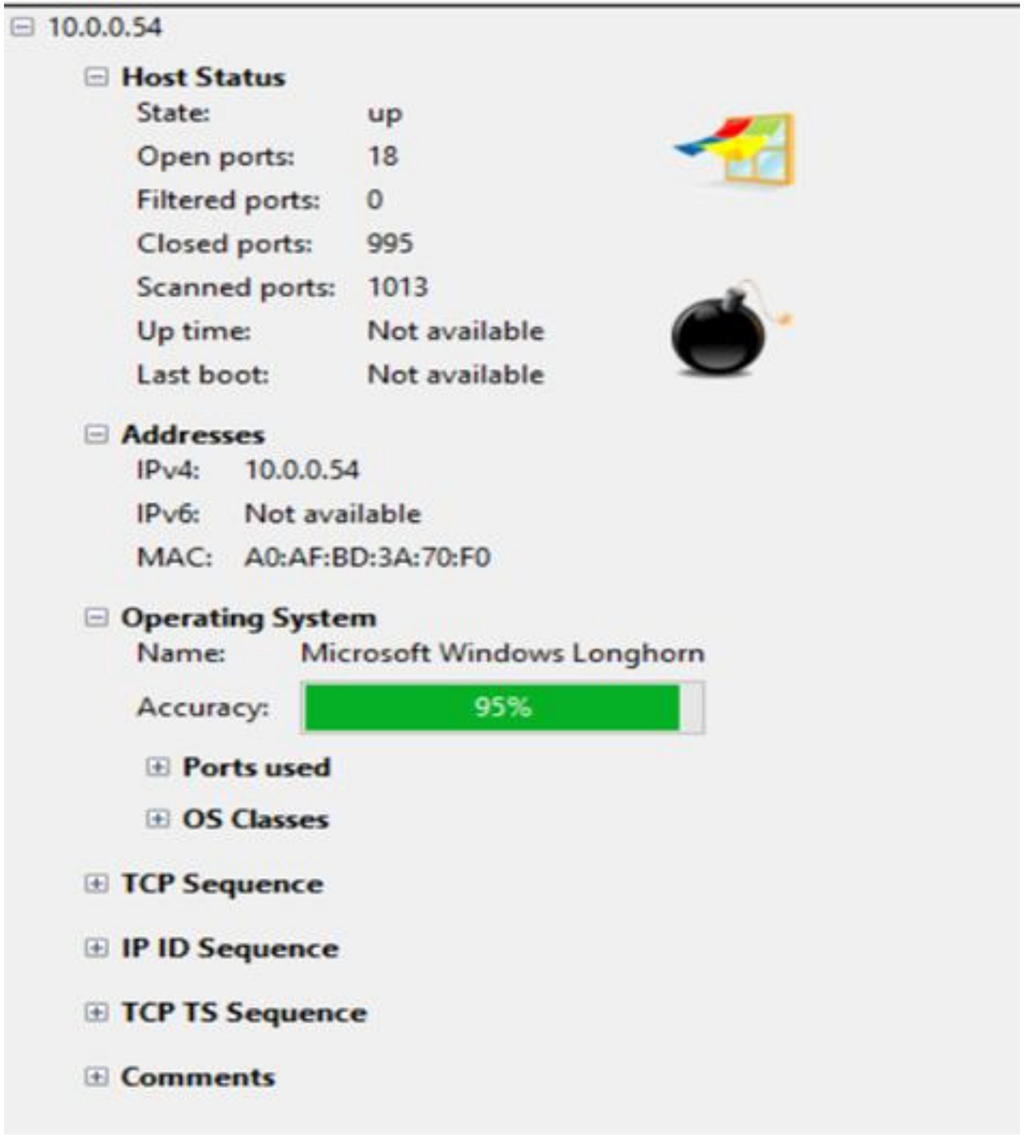
OS	Host
	10.0.0.1
	10.0.0.54
	10.0.0.67
	10.0.0.92
	10.0.0.115
	10.0.0.117
	10.0.0.125
	10.0.0.186
	10.0.0.254

	Port	Protocol	State	Service	Version
●	21	tcp	open	ftp	
●	135	tcp	open	msrpc	
●	139	tcp	open	netbios-ssn	
●	445	tcp	open	microsoft-ds	
●	5040	tcp	open	unknown	
●	5357	tcp	open	wsdapi	
●	7680	tcp	open	pando-pub	
●	8733	tcp	open	mc-nmf	.NET Message Framing
●	9955	tcp	open	alljoyn-stm	
●	13148	tcp	open		
●	49664	tcp	open	msrpc	Microsoft Windows RPC
●	49665	tcp	open	msrpc	Microsoft Windows RPC
●	49666	tcp	open	msrpc	Microsoft Windows RPC
●	49667	tcp	open	msrpc	Microsoft Windows RPC
●	49668	tcp	open	msrpc	Microsoft Windows RPC
●	49669	tcp	open	msrpc	Microsoft Windows RPC
●	61776	tcp	open		
●	62172	tcp	open		



```
Starting Nmap 7.60 ( https://nmap.org ) at 2018-01-26 14:41 Mountain Standard Time
Nmap scan report for 10.0.0.54
Host is up (0.032s latency).
Not shown: 995 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: A0:AF:BD:3A:70:F0 (Intel Corporate)

Nmap done: 1 IP address (1 host up) scanned in 50.90 seconds
```



⊟ 10.0.0.54

⊟ **Host Status**

State: up

Open ports: 18

Filtered ports: 0

Closed ports: 995

Scanned ports: 1013

Up time: Not available

Last boot: Not available

⊟ **Addresses**

IPv4: 10.0.0.54

IPv6: Not available

MAC: A0:AF:BD:3A:70:F0

⊟ **Operating System**

Name: Microsoft Windows Longhorn

Accuracy: 95%

⊞ **Ports used**

⊞ **OS Classes**

⊞ **TCP Sequence**

⊞ **IP ID Sequence**

⊞ **TCP TS Sequence**

⊞ **Comments**

Results

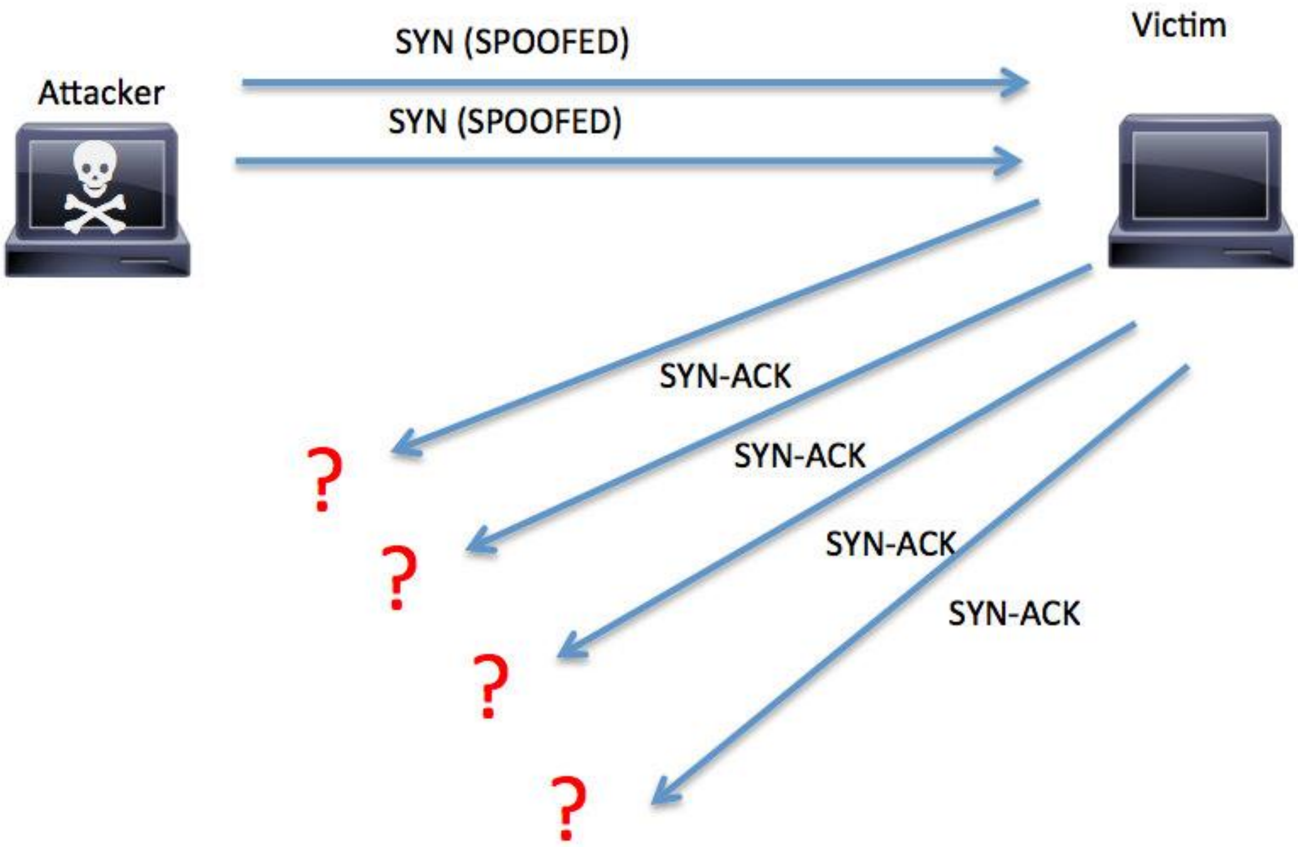
- **Now that you have results review them by priority and consider exposure to attack**

- **Prepare a report**
  - Executive Summary
    - ***manager does not get past first page***
  - pie charts
  - detail threats
  - show example of exploit
  - detail a plan to fix
    - ***multiple alternatives***

Hping3 (hping.org)

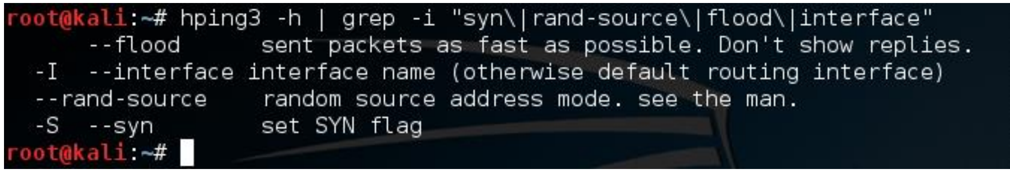
- **Packet generator**
- **Security Testing Tool**
  - Firewall testing
  - Advanced port scanning
  - Network testing, using different protocols, TOS, fragmentation
  - Manual path MTU discovery
  - Advanced traceroute, under all the supported protocols
  - Remote OS fingerprinting
  - Remote uptime guessing
  - TCP/IP stacks auditing

SYN Flooding



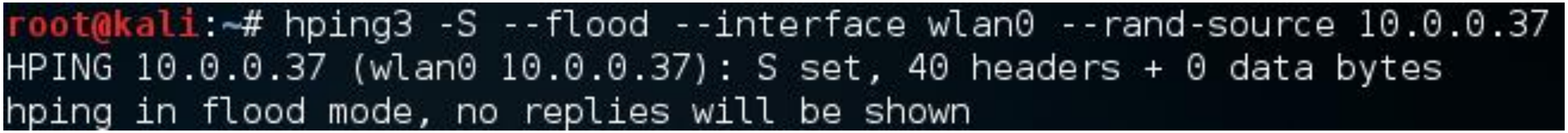
Hping flags

- **-flood**
  - – Flood mode
- **-interface**
  - – Egress interface of device
- **-S**
  - – SYN
- **-rand-source**
  - – Randomize the source address of each packet

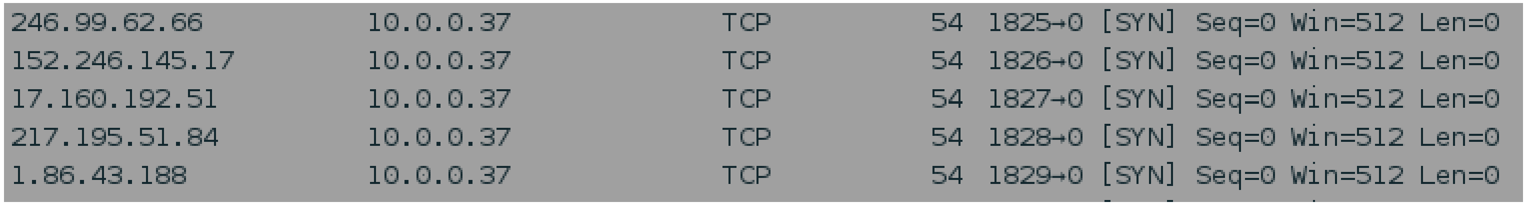


```
root@kali:~# hping3 -h | grep -i "syn\|rand-source\|flood\|interface"
      --flood      sent packets as fast as possible. Don't show replies.
  -I  --interface interface name (otherwise default routing interface)
  --rand-source     random source address mode. see the man.
  -S  --syn         set SYN flag
root@kali:~# 
```

Launch the attack



```
root@kali:~# hping3 -S --flood --interface wlan0 --rand-source 10.0.0.37
HPING 10.0.0.37 (wlan0 10.0.0.37): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```



```
246.99.62.66        10.0.0.37        TCP        54  1825→0 [SYN] Seq=0 Win=512 Len=0
152.246.145.17      10.0.0.37        TCP        54  1826→0 [SYN] Seq=0 Win=512 Len=0
17.160.192.51       10.0.0.37        TCP        54  1827→0 [SYN] Seq=0 Win=512 Len=0
217.195.51.84       10.0.0.37        TCP        54  1828→0 [SYN] Seq=0 Win=512 Len=0
1.86.43.188         10.0.0.37        TCP        54  1829→0 [SYN] Seq=0 Win=512 Len=0
```

How do we prevent DoS & DDoS?

Questions?