CYBER SECURITY

A new buzzword for an age old problem

THREAT, VULNERABILITY, AND RISK

- **Threat**- Potential danger to an asset such as data or the network.
- **Vulnerability and Attack Surface**
  - Weakness in a system or its design that could be exploited by a threat.
  - Attack surface describes different points where an attacker could get into a system and could get to the data (Example – operating system without security patches)
- **Exploit**
  - Mechanism used to leverage a vulnerability to compromise an asset.
  - Remote – works over the network.
  - Local – threat actor has user or administrative access to the end system.
- **Risk**
  - Likelihood that a threat will exploit a vulnerability of an asset and result in an undesirable consequence

CYBERCRIMINAL VERSUS CYBER HEROES

CYBERSECURITY CRIMINALS

- **Hackers** – This group of criminals breaks into computers or networks to gain access for various reasons.

White hat attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems.

Grey hat attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda.

Black hat attackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

CYBERCRIMINAL VERSUS CYBER HEROES

CYBERSECURITY CRIMINALS

Criminals come in many different forms. Each have their own motives:

- **Script Kiddies** - Teenagers or hobbyists mostly limited to pranks and vandalism, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks.
- **Vulnerability Brokers** - Grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
- **Hacktivists -** Grey hat hackers who rally and protest against different political and social ideas. Hacktivists publicly protest against organisations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.

CYBERCRIMINAL VERSUS CYBER HEROES

CYBERSECURITY CRIMINALS (CONT.)

Criminals come in many different forms. Each have their own motives:

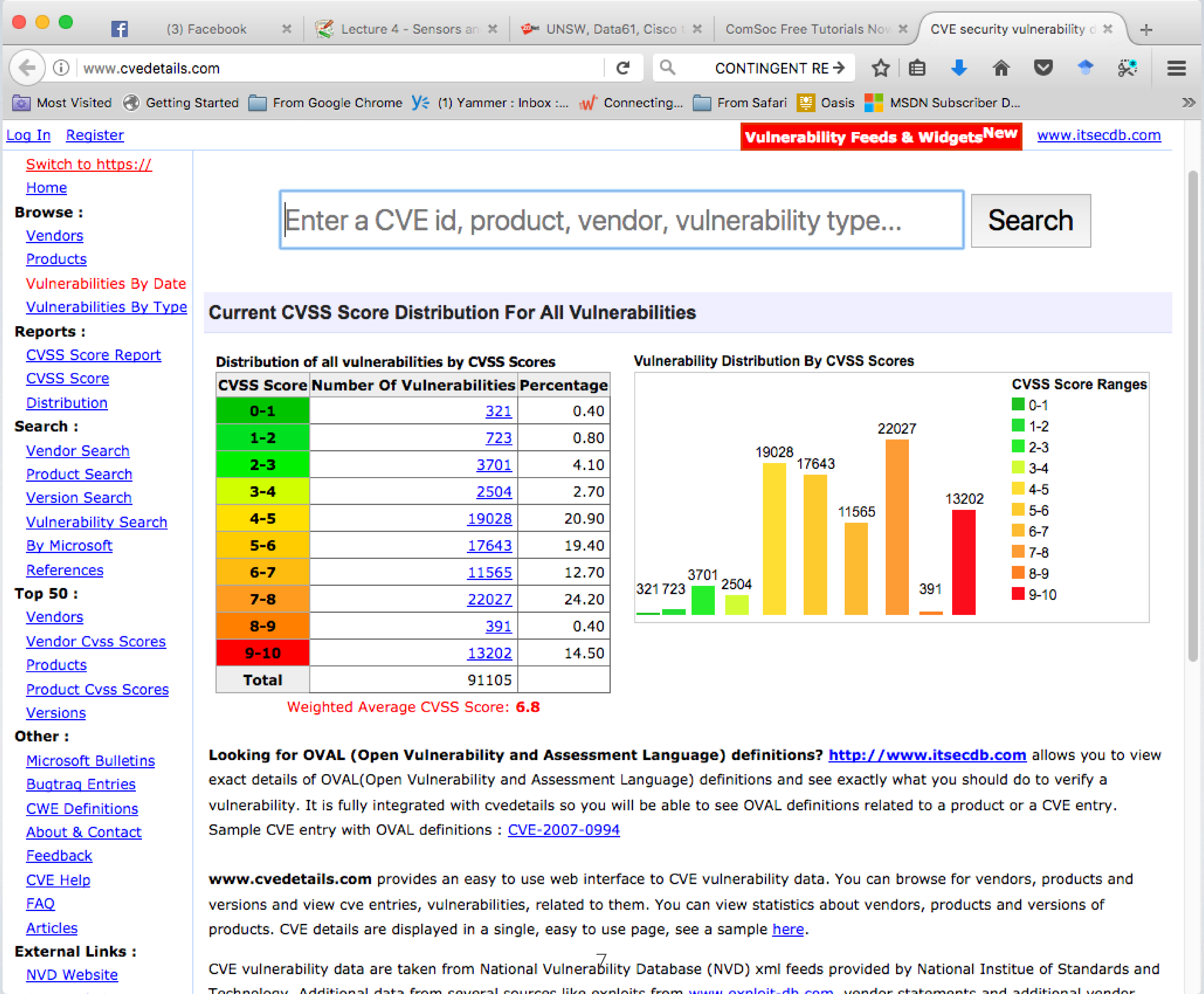
- **Cyber Criminals** - These are black hat hackers who are either self-employed or working for large cybercrime organisations. Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.
- **State Sponsored Hackers -** Depending on a person's perspective, these are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

CYBERCRIMINAL VERSUS CYBER HEROES

CYBERSECURITY SPECIALISTS

Thwarting the cyber criminals is a difficult task, company, government and international organisations have begun to take coordinated actions to limit or fend off cyber criminals. The coordinated actions include:

- **Vulnerability Database**: The Nation Common Vulnerabilities and Exposures (CVE) database is an example of the development of a national database. The CVE National Database was developed to provide a publicly available database of all know vulnerabilities. http://www.cvedetails.com/
- **Early Warning Systems**: The Honeynet project is an example of creating Early Warning Systems. The project provides a HoneyMap which displays real-time visualisation of attacks. https://www.honeynet.org/
- **Share Cyber Intelligence**: InfraGard is an example of wide spread sharing of cyber intelligence. The InfraGard program is a partnership between the US government and the private sector. The participants are dedicated to sharing information and intelligence to prevent hostile cyberattacks. https://www.infragard.org/ **- Use https://www.auscert.org.au/ similar organisation for our region**



Log In Register

Vulnerability Feeds & Widgets^New^ www.itsecdb.com

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website

Enter a CVE id, product, vendor, vulnerability type...

Search

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	321	0.40
1-2	723	0.80
2-3	3701	4.10
3-4	2504	2.70
4-5	19028	20.90
5-6	17643	19.40
6-7	11565	12.70
7-8	22027	24.20
8-9	391	0.40
9-10	13202	14.50
Total	91105	

Weighted Average CVSS Score: **6.8**

Vulnerability Distribution By CVSS Scores

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? http://www.itsecdb.com allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry. Sample CVE entry with OVAL definitions : CVE-2007-0994

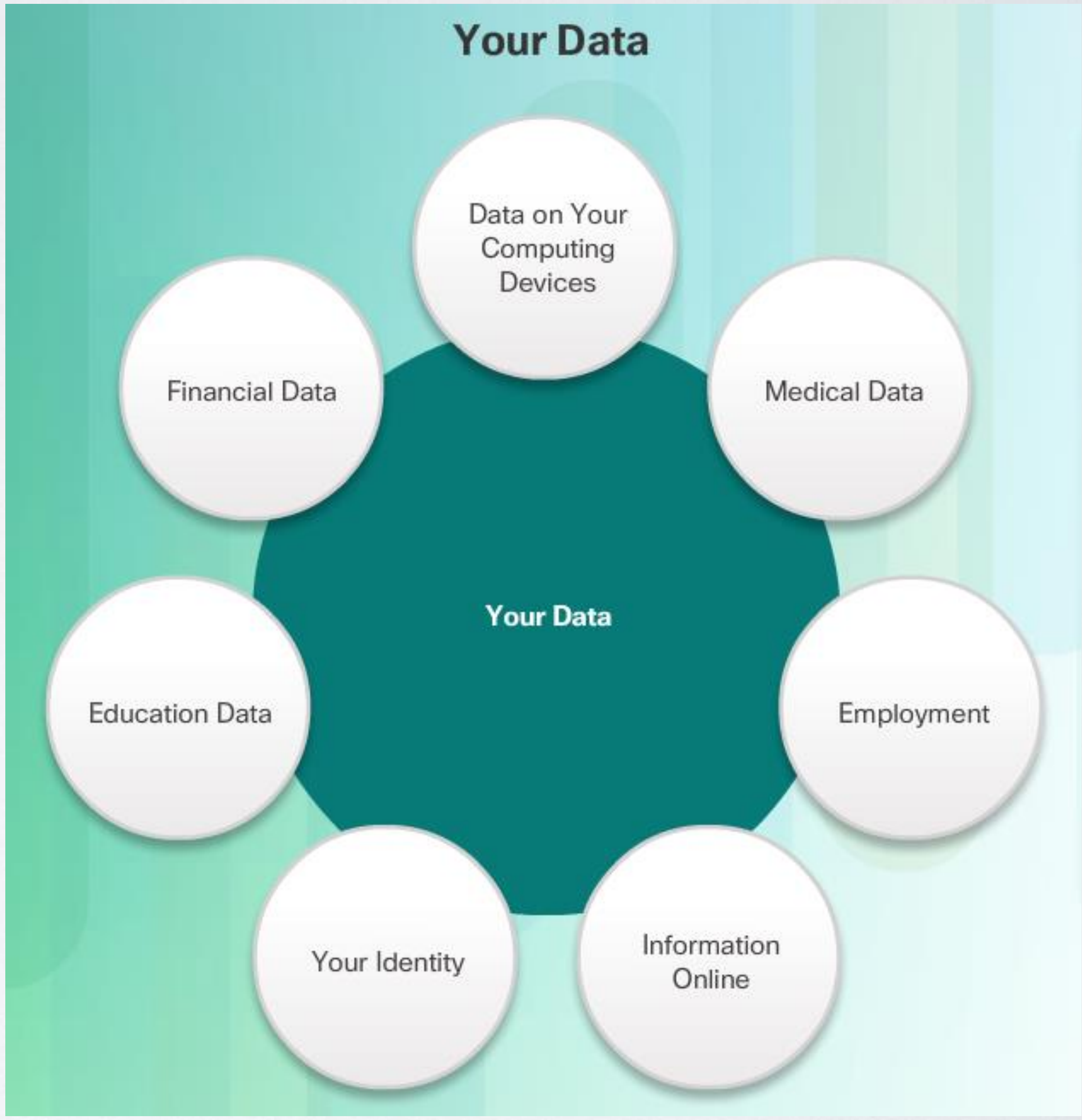
www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a sample here.

CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institue of Standards and Technology. Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor

THREAT ARENAS

The following examples are just a few sources of data that can come from established organisations:

- **Personal Information**
- **Medical Records**
- **Education Records**
- **Employment and Financial Records**



THREAT ARENAS

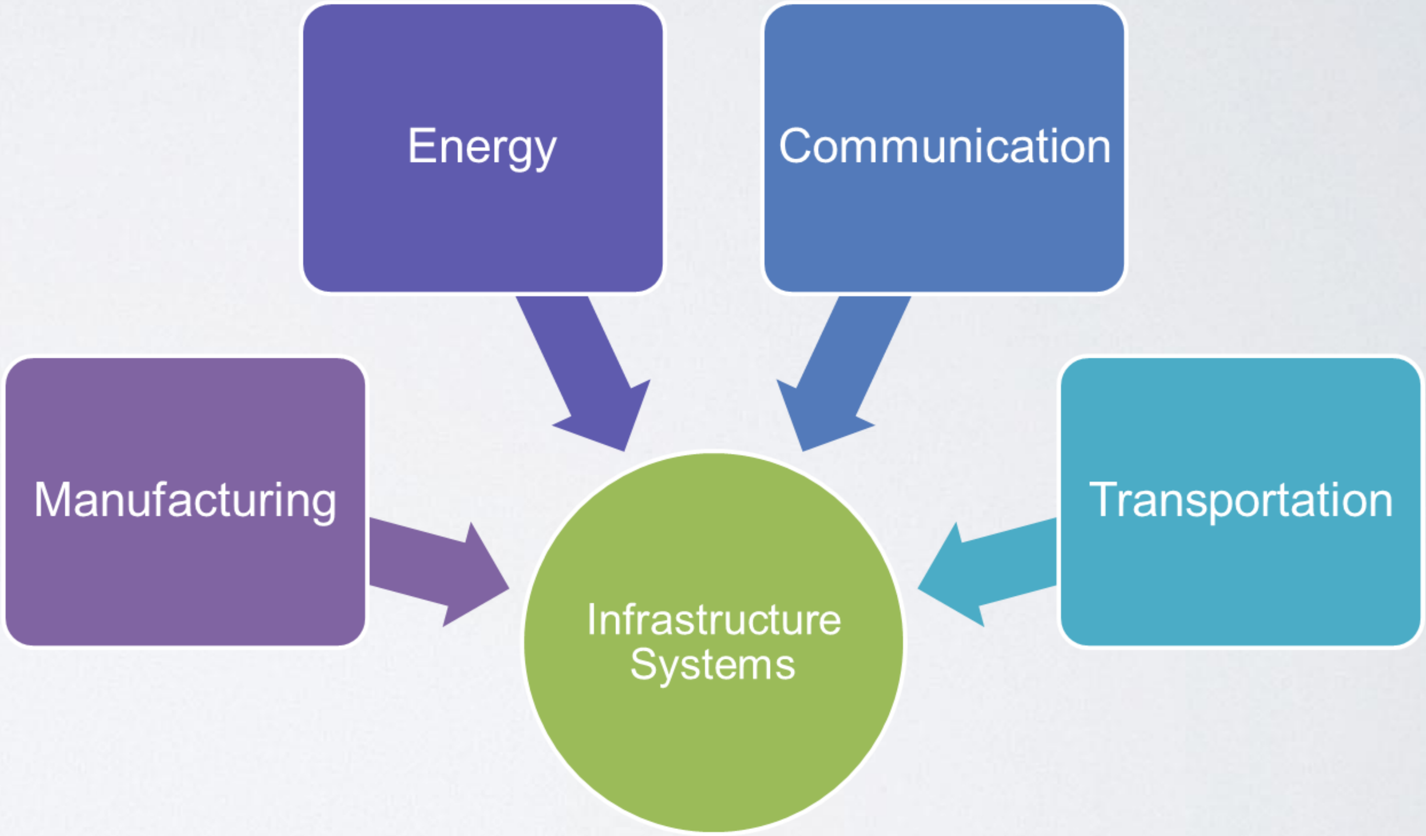
Network services like DNS, HTTP and Online Databases are prime targets for cyber criminals.

- Criminals use packet-sniffing tools to capture data streams over a network. Packet sniffers work by monitoring and recording all information coming across a network.
- Criminals can also use rogue devices, such as unsecured Wi-Fi access points.
- Packet forgery (or packet injection) interferes with an established network communication by constructing packets to appear as if they are part of a communication.

THREAT ARENAS

Sectors include:

- Manufacturing
  - Industry Controls
  - Automation
  - SCADA
- Energy Production and Distribution
  - Electrical Distribution and Smart Grid
  - Oil and Gas
- Communication
  - Phone
  - Email
  - Messaging
- Transportation systems
  - Air Travel
  - Rail
  - Over the Road



THE SPREAD OF THE DARK FORCES

Attacks can originate from within an organisation or from outside of the organisation

Internal Security Threats

- An internal user, such as an employee or contract partner (accidentally or intentionally)
- Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Internal attackers typically have knowledge of the corporate network, its resources, and its confidential data. They may also have knowledge of security countermeasures, policies and higher levels of administrative privileges.

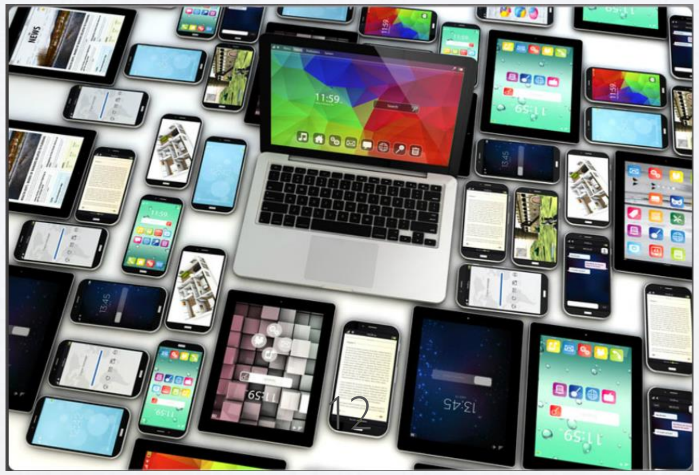
External Security Threats

- External threats from amateurs or skilled attackers can exploit vulnerabilities in networked devices, or can use social engineering, such as trickery, to gain access.
- External attacks exploit weaknesses or vulnerabilities to gain access to internal resources.

THE SPREAD OF THE DARK FORCES

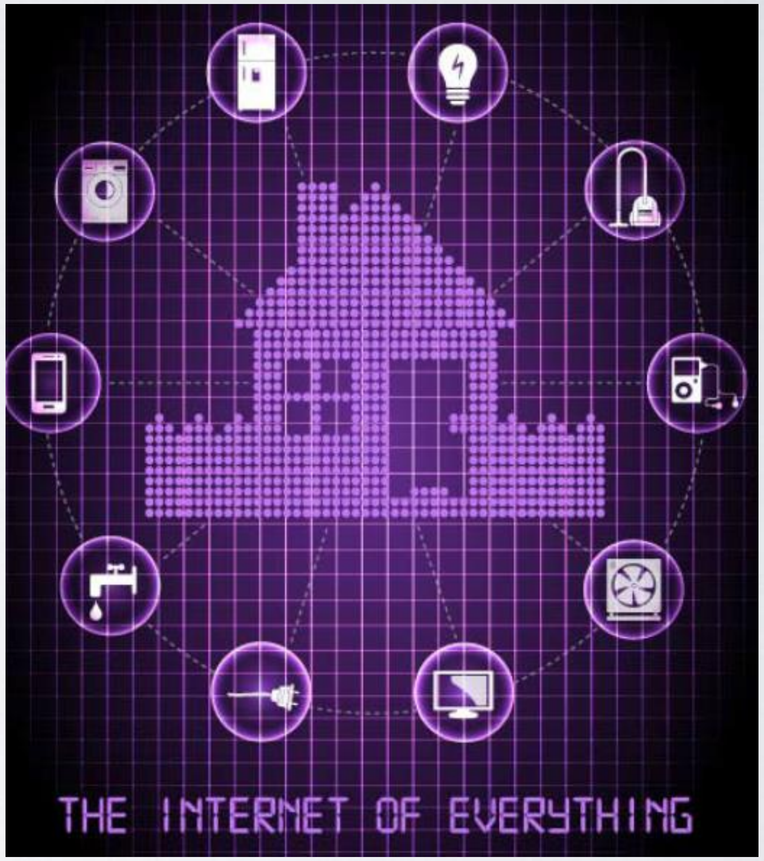
Vulnerabilities of Mobile Devices - In the past, employees typically used company-issued computers connected to a corporate LAN.

- Today, mobile devices such as iPhones, smartphones, tablets, are becoming powerful substitutes for, or additions to, the traditional PC.
- More and more people are using these devices to access enterprise information. Bring Your Own Device (BYOD) is a growing trend.
- The inability to centrally manage and update mobile devices poses a growing threat to organisations that allow employee mobile devices on their networks.



THE SPREAD OF THE DARK FORCES

- **Emergence Internet-of-Things** - The IoT) is the collection of technologies that enable the connection of various devices to the Internet.
- IoT technologies enable people to connect billions of devices to the Internet. These devices include appliances, locks, motors, and entertainment devices, to name just a few.
- This technology affects the amount of data that needs protection. Users access these devices remotely, which increases the number of networks requiring protection.
- With the emergence of IoT, there is much more data to be managed and secured. All of these connections, plus the expanded storage capacity and storage services offered through the Cloud and virtualisation, has led to the exponential growth of data.



THE SPREAD OF THE DARK FORCES

Impact of Big Data – Big data is the result of data sets that are large and complex, making traditional data processing applications inadequate. Big data poses both challenges and opportunities based on three dimensions:

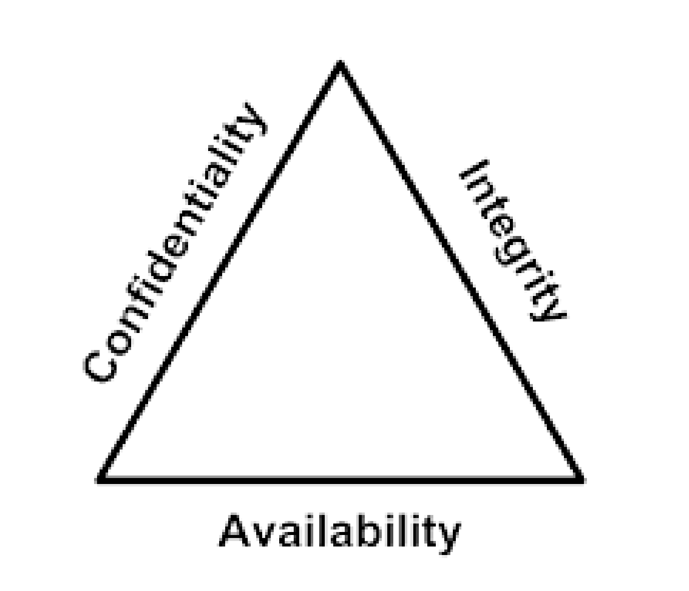
- The volume or amount of data
- The velocity or speed of data
- The variety or range of data types and sources

There are numerous examples of big corporate hacks in the news. As a result, enterprise systems require dramatic changes in security product designs and substantial upgrades to technologies and practices. Additionally, governments and industries are introducing more regulations and mandates that require better data protection and security controls to help guard big data.

THE THREE DIMENSIONS

The Principles of Security

- The first dimension identifies the goals to protect the cyber world.
- These three principles are confidentiality, integrity and availability.
- The principles provide focus and enable us to prioritise actions in protecting the cyber world.



The States of Data

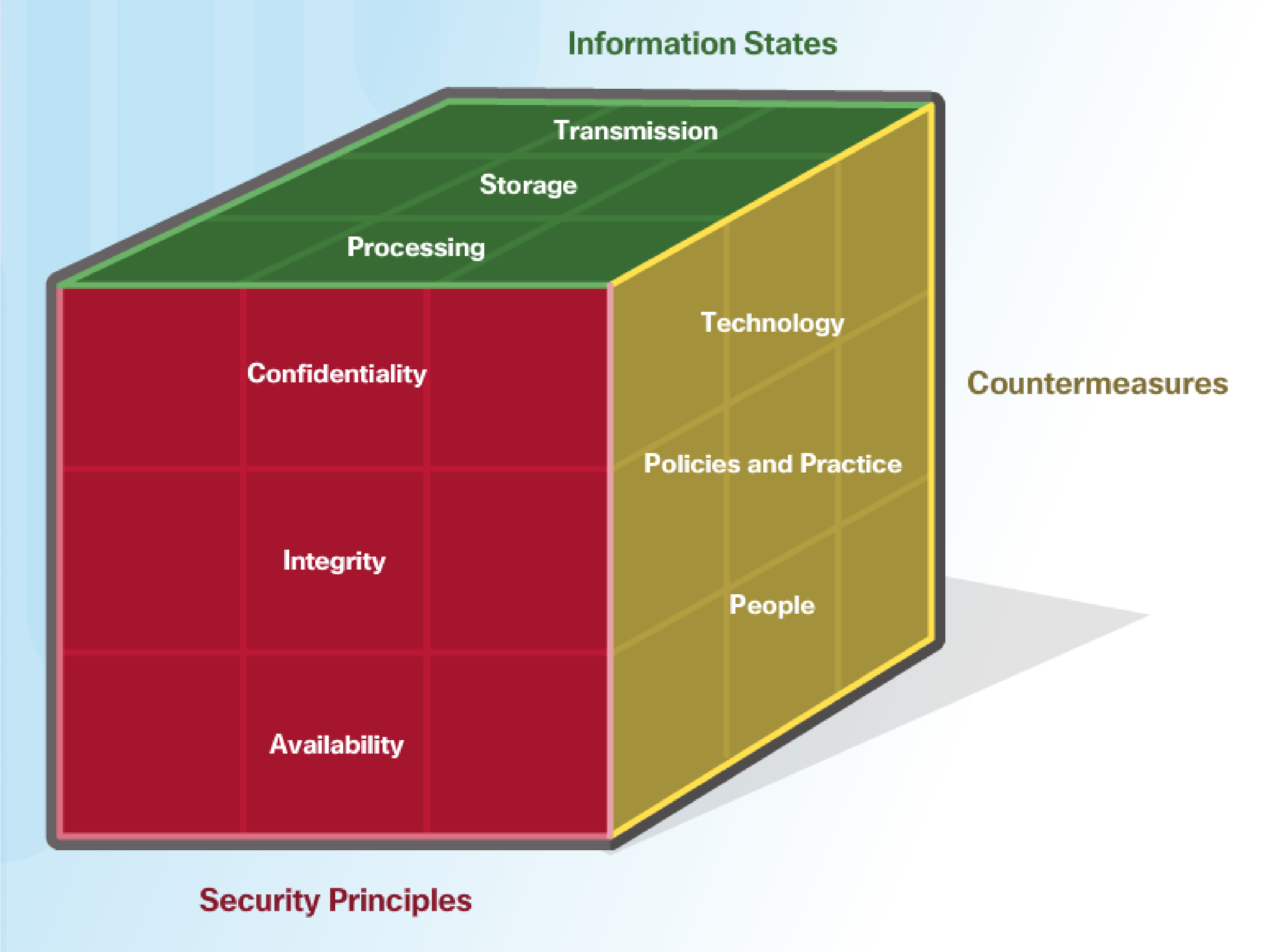
- The cyber world is a world of data; therefore focus on protecting data. The second dimension focuses on the problems of protecting all of the states of data in the cyber world. Data has three possible states:

1) Data at rest or in storage 2) Data in transit 3) Data in process

THE THREE DIMENSIONS (CONT.)

Cybersecurity Safeguards

- The third dimension of the cybersecurity cube defines the tools used to protect the cyber world.
- **Technologies -** devices, and products available to protect information systems and fend off cyber criminals.
- **Policies and Practices -** procedures, and guidelines that enable the citizens of the cyber world to stay safe and follow good practices.
- **People -** Aware and knowledgeable about their world and the dangers that threaten their world.



CONFIDENTIALITY

The Principle of Confidentiality

- Confidentiality or privacy, prevents the disclosure of information to unauthorised people, resources and processes. Organisations need to train employees about best practices in safeguarding sensitive information to protect themselves and the organisation from attacks.
- Methods used to ensure confidentiality include data encryption, authentication, and access control.

Protecting Data Privacy

- Organisations collect a large amount of data and much of this data is not sensitive because it is publicly available, like names and telephone numbers.
- Other data collected, though, is sensitive. Sensitive information is data protected from unauthorised access to safeguard an individual or an organisation.

CONFIDENTIALITY

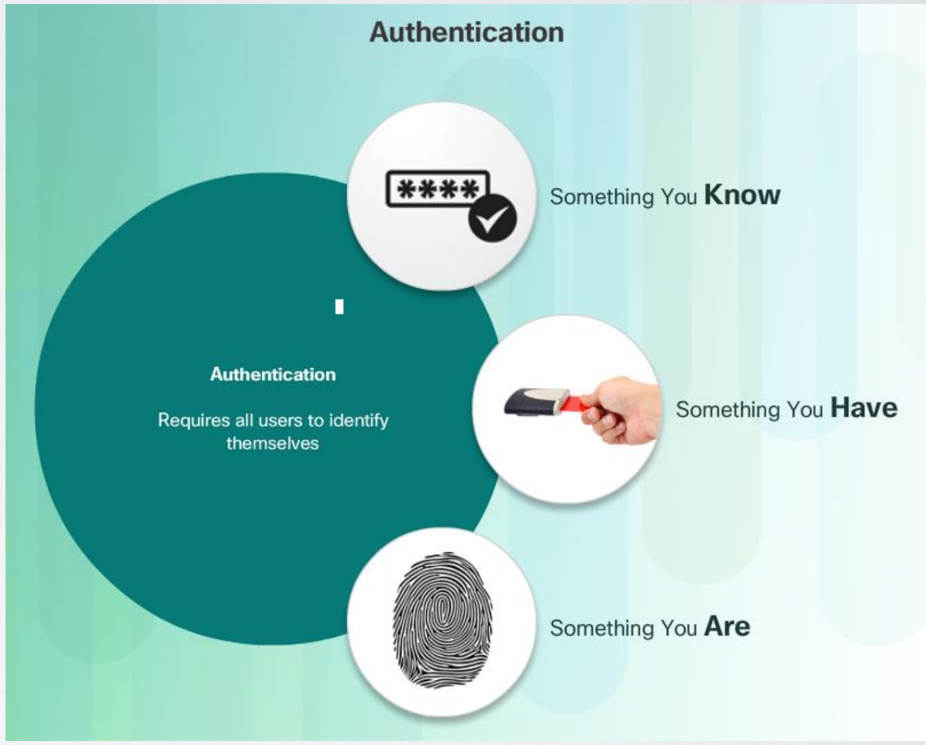
Controlling Access

Access control defines a number of protection schemes that prevent unauthorised access to a computer, network, database, or other data resources. The concepts of AAA involve three security services: **Authentication, Authorisation and Accounting.**

Authentication verifies the identity of a user to prevent unauthorised access.

Authorisation services determine which resources users can access, along with the operations that users can perform.

Accounting keeps track of what users do, including what they access, the amount of time they access resources, and any changes made.



CONFIDENTIALITY

Confidentiality and privacy seem interchangeable, but from a legal standpoint, they mean different things.

- Most privacy data is confidential, but not all confidential data is private. Access to confidential information occurs after confirming proper authorisation. Financial institutions, hospitals, medical professionals, law firms, and businesses handle confidential information.
- Confidential information has a non-public status. Maintaining confidentiality is more of an ethical duty.
- Privacy is the appropriate use of data. When organisations collect information provided by customers or employees, they should only use that data for its intended purpose.

INTEGRITY

Principle of Data Integrity

- Integrity is the accuracy, consistency, and trustworthiness of data during its entire life cycle.
  - Another term for integrity is quality.
- Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls.

Need for Data Integrity

- The need for data integrity varies based on how an organisation uses data. For example, Facebook does not verify the data that a user posts in a profile.
- A bank or financial organisation assigns a higher importance to data integrity. Transactions and customer accounts must be accurate.
- Protecting data integrity is a constant challenge for most organisations. Loss of data integrity can render entire data resources unreliable or unusable.

Integrity Checks

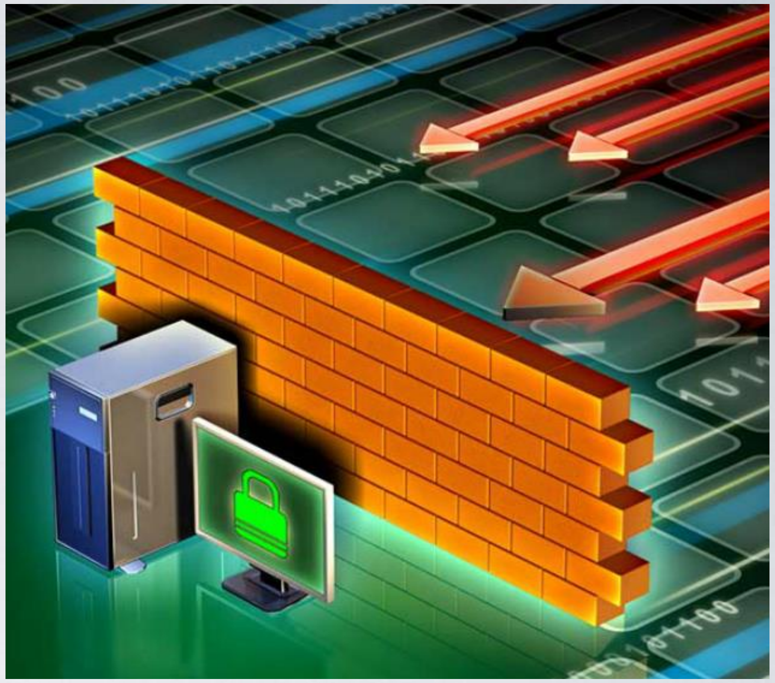
- An integrity check is a way to measure the consistency of a collection of data (a file, a picture, or a record). The integrity check performs a process called a hash function to take a snapshot of data at an instant in time.

AVAILABILITY

- Data availability is the principle used to describe the need to maintain availability of information systems and services at all times.
- Methods used to ensure availability include system redundancy, system backups, increased system resiliency, equipment maintenance, up-to-date operating systems and software, and plans in place to recover quickly from unforeseen disasters.
- High availability systems typically include three design principles: eliminate single points of failure, provide for reliable crossover, and detect failures as they occur.

Organisations can ensure availability by implementing the following:

1. Equipment maintenance
2. OS and system updates
3. Test backups
4. Plan for disasters
5. Implement new technologies
6. Monitor unusual activity
7. Test to verify availability



Cybersecurity Countermeasures
Technologies

Software-based Technology Safeguards

- Software safeguards include programs and services that protect operating systems, databases, and other services operating on workstations, portable devices, and servers.

Hardware-based Technology Safeguards

- Hardware based technologies are appliances that are installed within the network faculties. They can include: Firewall appliances, Intrusion Detection Systems (IDS),Intrusion Prevention Systems (IPS) and Content filtering systems.

Cybersecurity Countermeasures

Technologies

Network-based Technology Safeguards

Technological countermeasures can also include network-based technologies.

- **Virtual Private Network (VPN)** is a secure virtual network that uses the public network (i.e., the Internet). The security of a VPN lies in the encryption of packet content between the endpoints that define the VPN.
- **Network access control (NAC)** requires a set of checks before allowing a device to connect to a network. Some common checks include up-to-data antivirus software or operating system updates installed.
- **Wireless access point security** includes the implementation of authentication and encryption.

Cybersecurity Countermeasures

Technologies

Cloud-based Technology Safeguards

- Cloud-based technologies shift the technology component from the organisation to the cloud provider.
- **Software as a Service (SaaS)** allows users to gain access to application software and databases. Cloud providers manage the infrastructure. Users store data on the cloud provider's servers.
- **Infrastructure as a Service (IaaS)** provides virtualised computing resources over the Internet. The provider hosts the hardware, software, servers, and storage components.
- **Virtual security appliances** run inside a virtual environment with a pre-packaged, hardened operating system running on virtualised hardware.

Cybersecurity Countermeasures

Implementing Cybersecurity Education and Training

A security awareness program is extremely important for an organisation. An employee may not be purposefully malicious but just unaware of what the proper procedures are.

There are several ways to implement a formal training program:

- Make security awareness training a part of the employee's on-boarding process
- Tie security awareness to job requirements or performance evaluations
- Conduct in-person training sessions
- Complete online courses

Cybersecurity Countermeasures

Cybersecurity Policies and Procedures

- A security **policy** is a set of security objectives for a company that includes rules of behaviour for users and administrators and specifies system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems within an organisation.
- **Standards** help an IT staff maintain consistency in operating the network. Standards provide the technologies that specific users or programs need in addition to any program requirements or criteria that an organisation must follow.
- **Guidelines** are a list of suggestions on how to do things more efficiently and securely. They are similar to standards, but are more flexible and are not usually mandatory. Guidelines define how standards are developed and guarantee adherence to general security policies.
- **Procedure** documents are longer and more detailed than standards and guidelines. Procedure documents include implementation details that usually contain step-by-step instructions and graphics.

Security Management Framework
The ISO Model

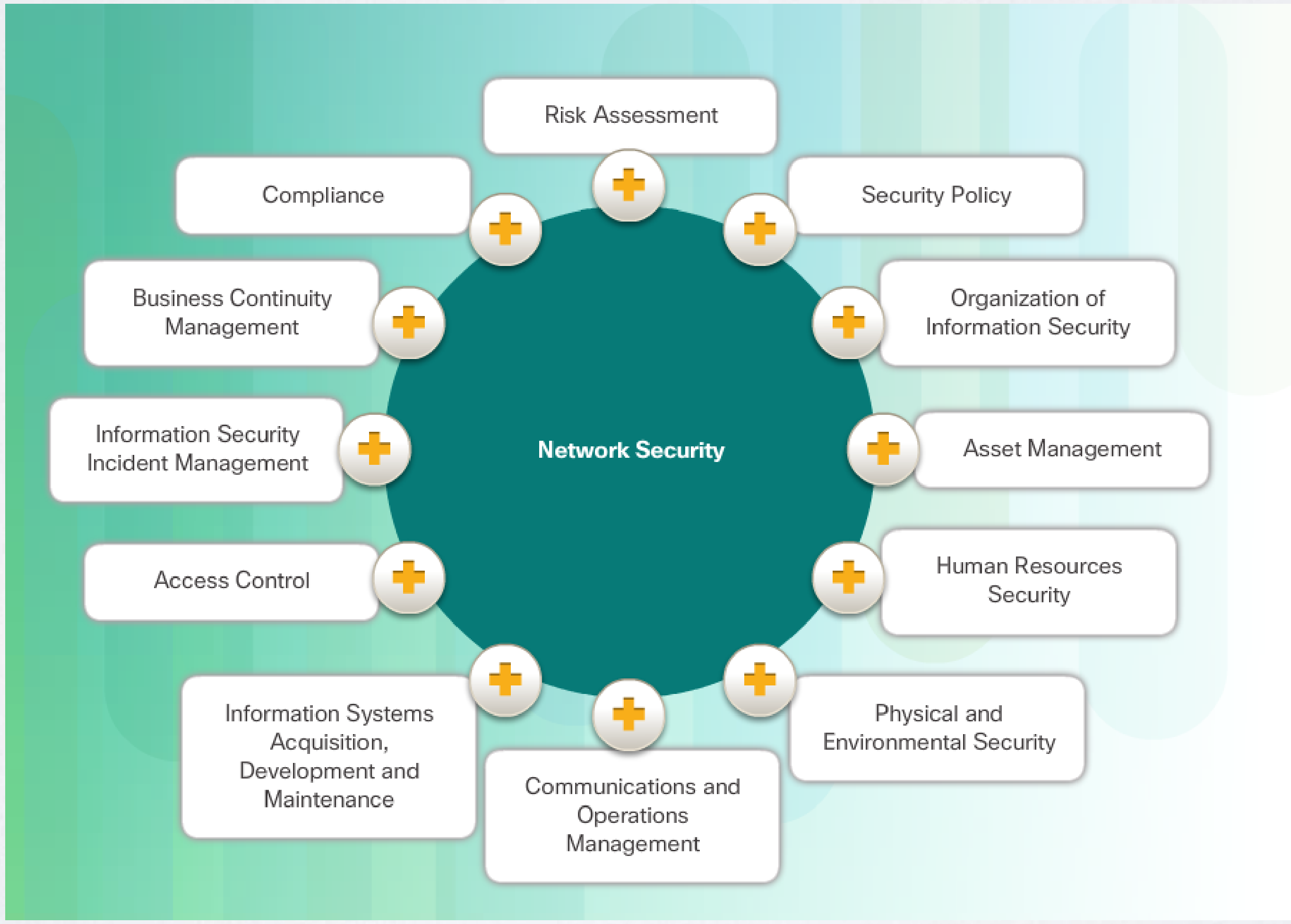
Security professionals need to secure information from end-to-end within the organisation. This is a monumental task, and it is unreasonable to expect one individual to have all of the requisite knowledge.

The **International Organisation for Standardisation (ISO)/International Electrotechnical Commission (IEC)** developed a comprehensive framework to guide information security management.

The ISO cybersecurity model is to cybersecurity professionals what the OSI networking model is to network engineers. Both provide a framework for understanding and approaching complex tasks.

Security Management Framework
The ISO Model

ISO/IEC 27000 is an information security standard published in 2005 and revised in 2013. ISO publishes the ISO 27000 standards. Even though the standards are not mandatory, most countries use them as a de facto framework for implementing information security.



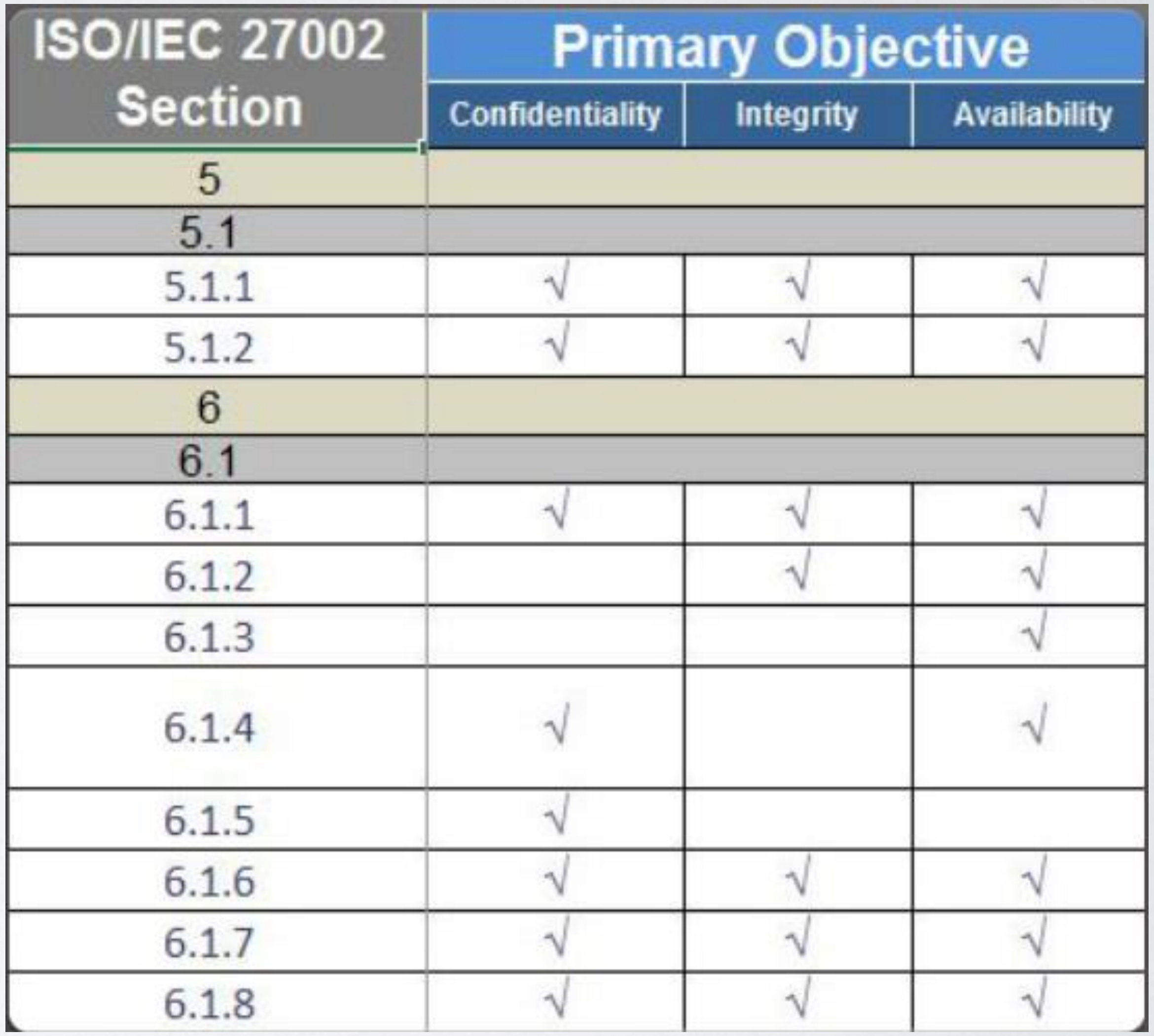
Network Security
Risk Assessment
Security Policy
Organization of Information Security
Asset Management
Human Resources Security
Physical and Environmental Security
Communications and Operations Management
Information Systems Acquisition, Development and Maintenance
Access Control
Information Security Incident Management
Business Continuity Management
Compliance

Available here: http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip#en

Security Management Framework

Using the ISO Cybersecurity Model

- The ISO 27000 is a universal framework
  - In order to use the framework effectively, an organisation must narrow down which domains, control objectives, and controls apply to its environment and operations.
- The ISO 27001 control objectives serve as a checklist.
  - The first step an organisation takes is to determine if these control objectives are applicable to the organisation.



ISO/IEC 27002 Section	Primary Objective		
	Confidentiality	Integrity	Availability
5			
5.1			
5.1.1	√	√	√
5.1.2	√	√	√
6			
6.1			
6.1.1	√	√	√
6.1.2		√	√
6.1.3			√
6.1.4	√		√
6.1.5	√		
6.1.6	√	√	√
6.1.7	√	√	√
6.1.8	√	√	√

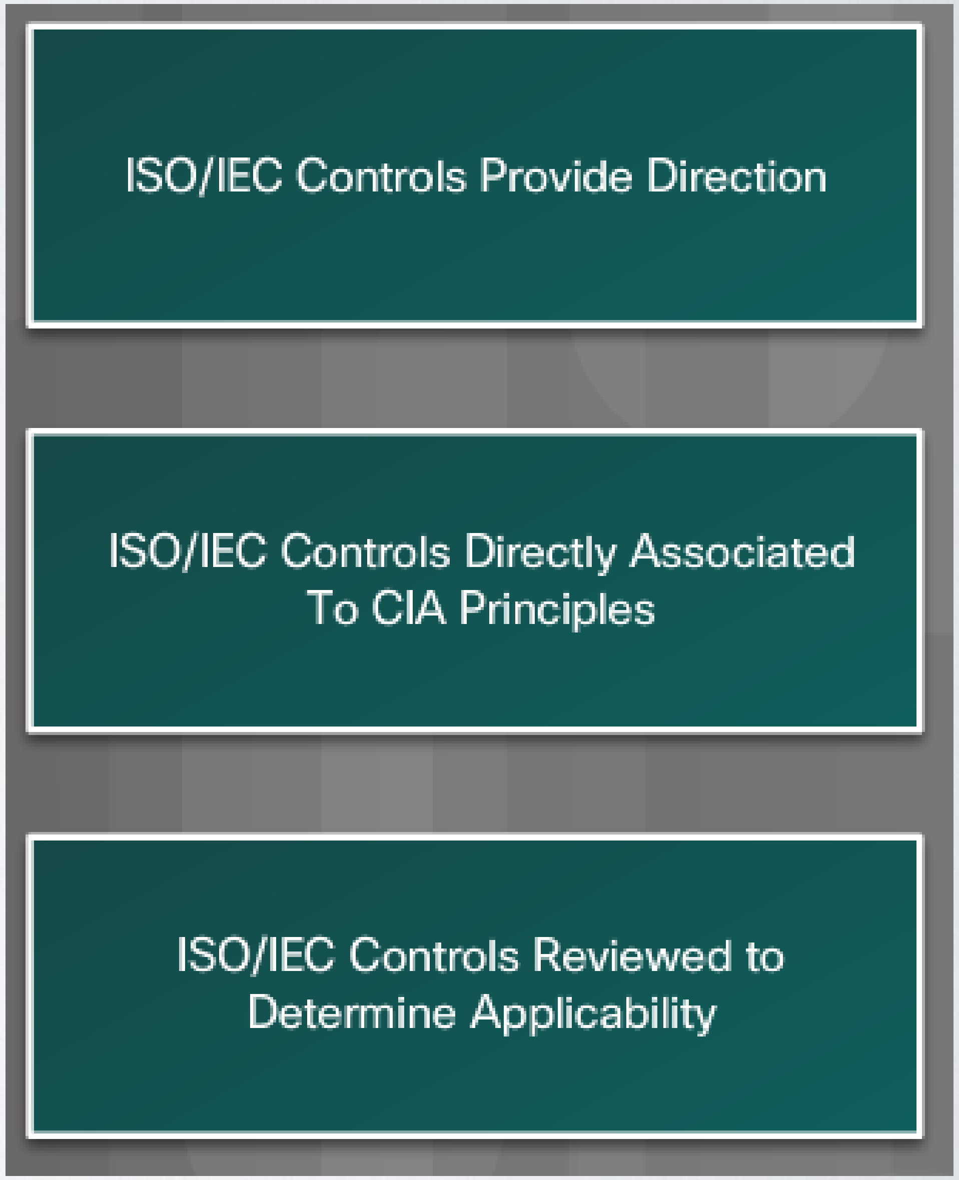
Security Management Framework

Using the ISO Cybersecurity Model

The ISO Cybersecurity Model and the States of Data

- Different groups within an organisation may be responsible for data in each of the various states.
- For example, the network security group is responsible for data during transmission.
- Programmers and data entry people are responsible for data during processing.
- The hardware and server support specialists are responsible for stored data.

The ISO Controls specifically address security objectives for data in each of the three states.



ISO/IEC Controls Provide Direction

ISO/IEC Controls Directly Associated To CIA Principles

ISO/IEC Controls Reviewed to Determine Applicability

Using the ISO Cybersecurity Model

The ISO Cybersecurity Model and Safeguards

- The ISO 27001 control objectives relate directly to the organisation's cybersecurity policies, procedures and guidelines which upper management determines.
- The ISO 27002 controls provide technical direction. For example, management establishes a policy specifying the protection of all data coming in to or out of the organisation. Implementing the technology to meet the policy objectives would not involve management.
- It is the responsibility of IT professionals to properly implement and configure the equipment used to fulfil the policy directives set by management.

ISO/IEC 27000

ISO/IEC 27001

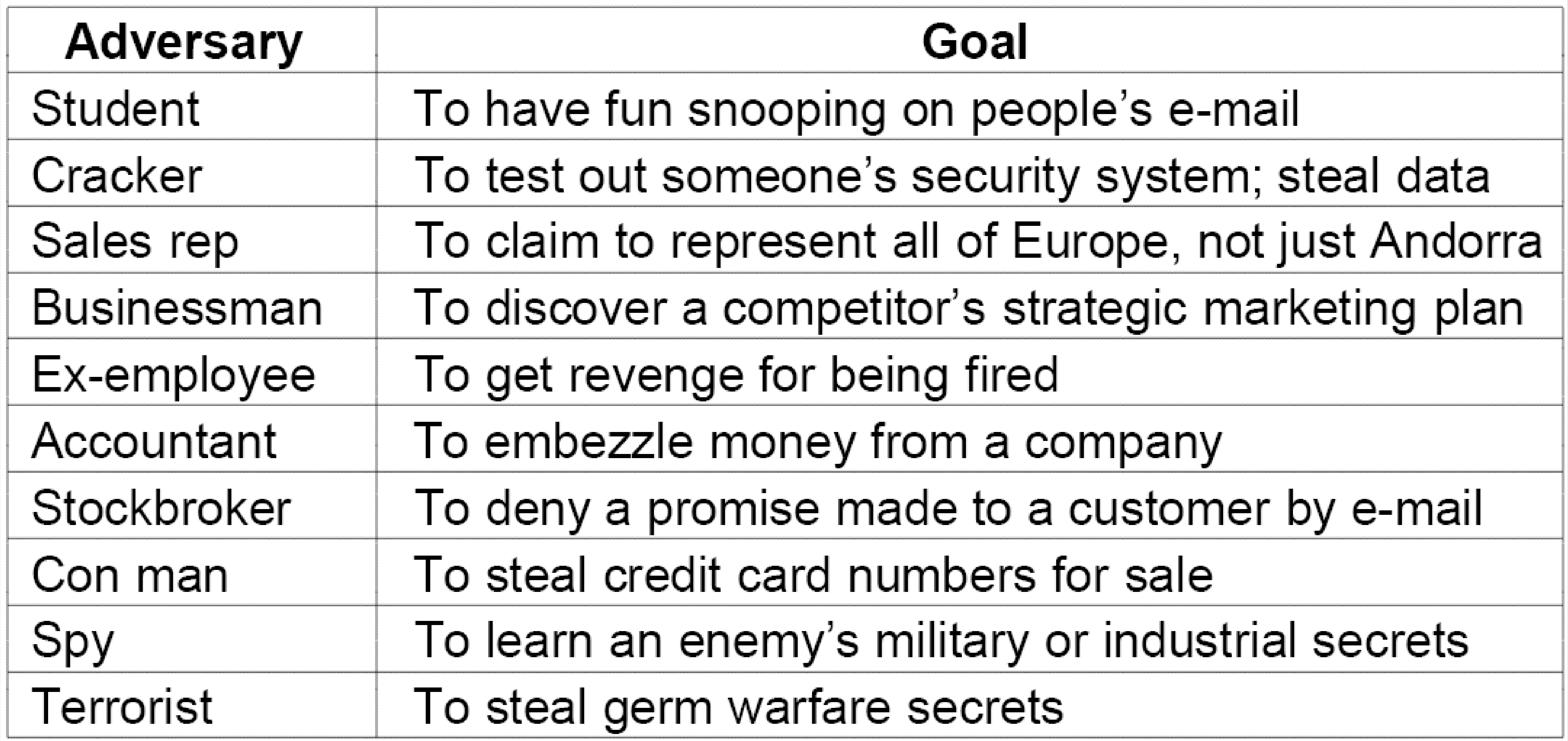
ISO/IEC 27002

SERVER SECURITY

WHAT IS A SECURE SYSTEM

- Secure system is an abstract concept
- Defined as “Robust”, it depends on
  - what you need
  - how much time you are willing to put in
  - and what resources are at your disposal

MOTIVATION FOR ATTACKS



Adversary	Goal
Student	To have fun snooping on people’s e-mail
Cracker	To test out someone’s security system; steal data
Sales rep	To claim to represent all of Europe, not just Andorra
Businessman	To discover a competitor’s strategic marketing plan
Ex-employee	To get revenge for being fired
Accountant	To embezzle money from a company
Stockbroker	To deny a promise made to a customer by e-mail
Con man	To steal credit card numbers for sale
Spy	To learn an enemy’s military or industrial secrets
Terrorist	To steal germ warfare secrets

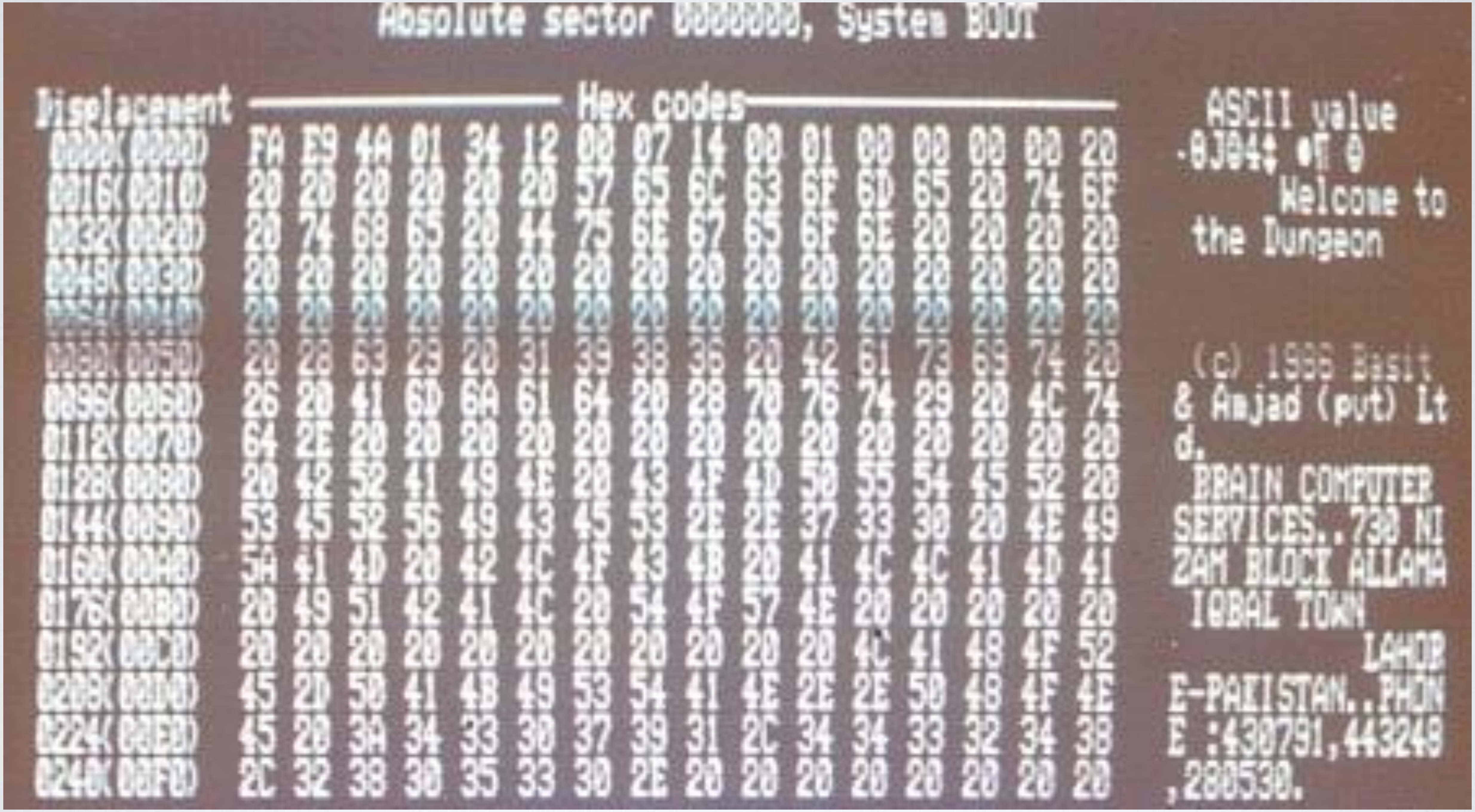
Source: “Computer Networks” by Andrew Tanenbaum

FIRST COMPUTER VIRUS

- Replaces the boot sector of a floppy
  - The real boot sector is moved to another sector and marked as bad.

Welcome to the Dungeon © 1986 Brain & Amjads (pvt) Ltd VIRUS_SHOE RECORD V9.0 Dedicated to the dynamic memories of millions of viruses who are no longer with us today - Thanks GOODNESS!! BEWARE OF THE er..VIRUS : this program is catching program follows after these messages....$#@%$@!!

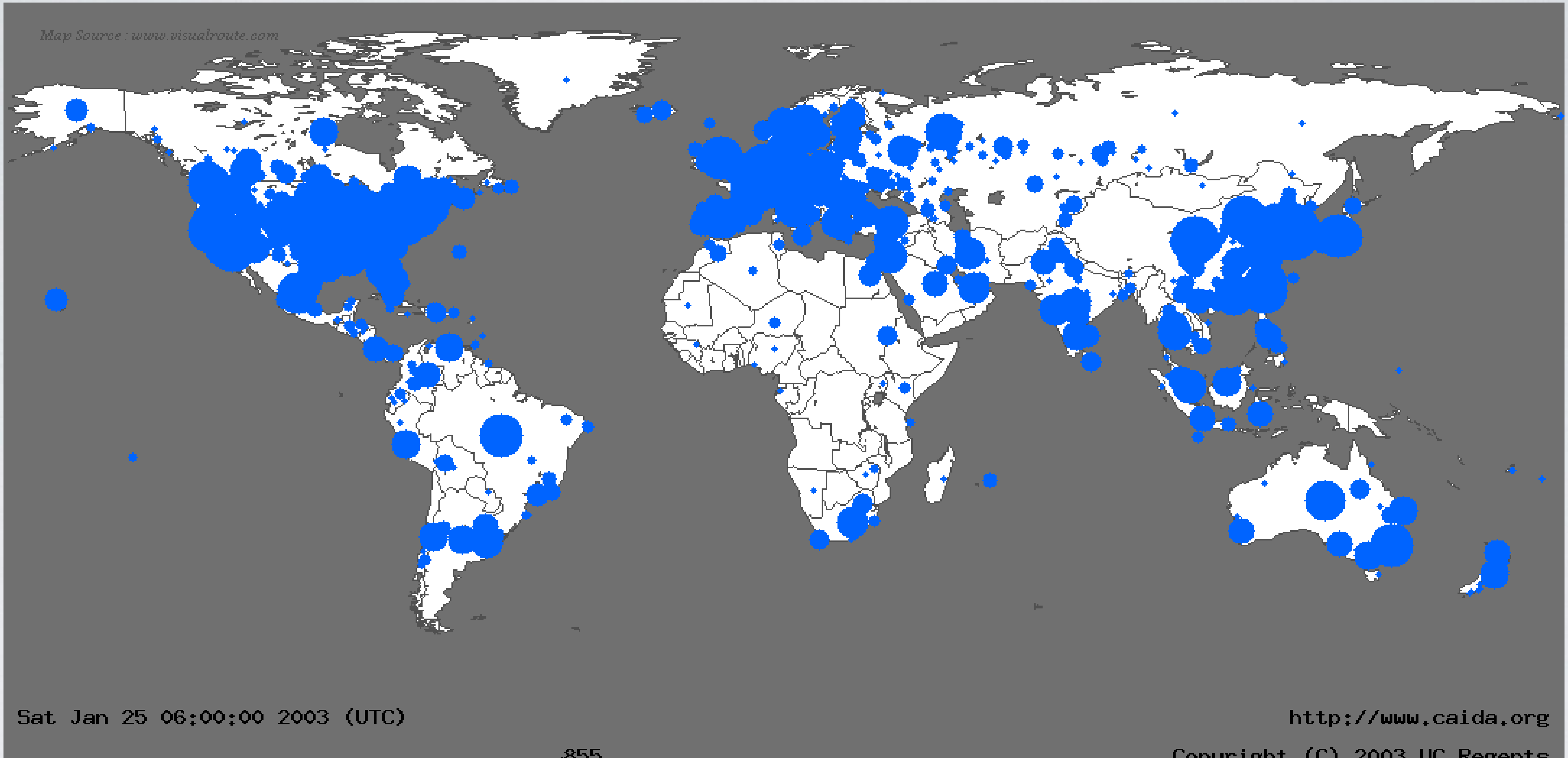
©BRAIN VIRUS 1986

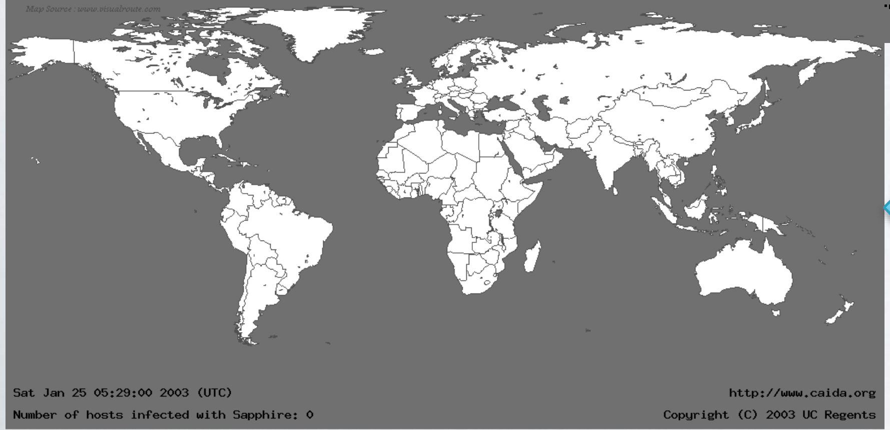


```
                      Absolute sector 0000000, System BOOT

Displacement ─────────── Hex codes ──────────────────────────   ASCII value
 0000(0000)   FA E9 4A 01 34 12 00 07 14 00 01 00 00 00 00 20   ·ΘJ☺4↕ •¶ ☺
 0016(0010)   20 20 20 20 20 20 57 65 6C 63 6F 6D 65 20 74 6F         Welcome to
 0032(0020)   20 74 68 65 20 44 75 6E 67 65 6F 6E 20 20 20 20    the Dungeon
 0048(0030)   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0064(0040)   20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
 0080(0050)   20 28 63 29 20 31 39 38 36 20 42 61 73 69 74 20    (c) 1986 Basit
 0096(0060)   26 20 41 6D 6A 61 64 20 28 70 76 74 29 20 4C 74   & Amjad (pvt) Lt
 0112(0070)   64 2E 20 20 20 20 20 20 20 20 20 20 20 20 20 20   d.
 0128(0080)   20 42 52 41 49 4E 20 43 4F 4D 50 55 54 45 52 20    BRAIN COMPUTER
 0144(0090)   53 45 52 56 49 43 45 53 2E 2E 37 33 30 20 4E 49   SERVICES..730 NI
 0160(00A0)   5A 41 4D 20 42 4C 4F 43 4B 20 41 4C 4C 41 4D 41   ZAM BLOCK ALLAMA
 0176(00B0)   20 49 51 42 41 4C 20 54 4F 57 4E 20 20 20 20 20    IQBAL TOWN
 0192(00C0)   20 20 20 20 20 20 20 20 20 20 20 4C 41 48 4F 52              LAHOR
 0208(00D0)   45 2D 50 41 4B 49 53 54 41 4E 2E 2E 50 48 4F 4E   E-PAKISTAN..PHON
 0224(00E0)   45 20 3A 34 33 30 37 39 31 2C 34 34 33 32 34 38   E :430791,443248
 0240(00F0)   2C 32 38 30 35 33 30 2E 20 20 20 20 20 20 20 20   ,280530.
```

WORM PROPAGATION


Map Source : www.visualroute.com
Sat Jan 25 06:00:00 2003 (UTC)
http://www.caida.org
855
Copyright (C) 2003 UC Regents


Map Source : www.visualroute.com
Sat Jan 25 05:29:00 2003 (UTC)
http://www.caida.org
Number of hosts infected with Sapphire: 0
Copyright (C) 2003 UC Regents

30 minutes earlier

SLAMMER

- The Sapphire Worm (also called Slammer) was the fastest computer worm in history.
- Doubled every 8.5 seconds infecting more than 90 percent of vulnerable hosts within 10 minutes.
- Infection started just before 05:30 UTC on Jan 25 2003.
  - Exploited a buffer overflow vulnerability in Microsoft's SQL Server or MSDE 2000
  - This weakness in an underlying indexing service **was** discovered in July 2002
- The worm infected at least 75,000 hosts
- Several disassembled versions of the source code of the worm are available.

SPOOFING

- Phishing
- Joe Job
- Look at headers
  - Compare the From address to the Message-ID domain
  - Note @scheduler
    - Not a valid dns or match

Message-ID:
1102074045742.1102067540733.15299.8.13145606@scheduler
From: Cell Labs wholesale@celllabsinc.com

Message-ID: <000a01c89b7b$05eea358$d988ba94@xwhhef>
From: "hezekiah nancy" <taylor@spamtest.com>

http://www.askdavetaylor.com/how_to_tell_if_email_is_spoofed_or_legit.html
Good article

```
220 dragon.cucat.org ESMTP Exim 4.72 Mon, 11 Apr 2011 11:21:58 +0800
HELO mail.here.org
250 dragon.cucat.org Hello chem-trebblem.eng.cage.curtin.edu.au [134.7.43.165]
MAIL FROM: "Santa Claus" <santaclaus@northpole.net>
250 OK
RCPT To: <Bill@here.com>
550 relay not permitted
RCPT To: <iain@cucat.org>
250 Accepted
DATA
354 Enter message, ending with "." on a line by itself
From: Santa Claus <santaclaus@northpole.net>
To: billgates@microsoft.com
Subject: Linux is better
Roses are #0000FF
Violets are #FF0000
All my base
Are belong to you!
.
250 OK id=1Q97kX-00057f-AK
quit
221 dragon.cucat.org closing connection
Connection closed by foreign host.
```

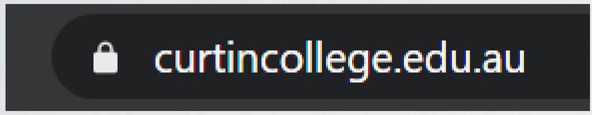
DNS lookup

Disable relay

Text entered

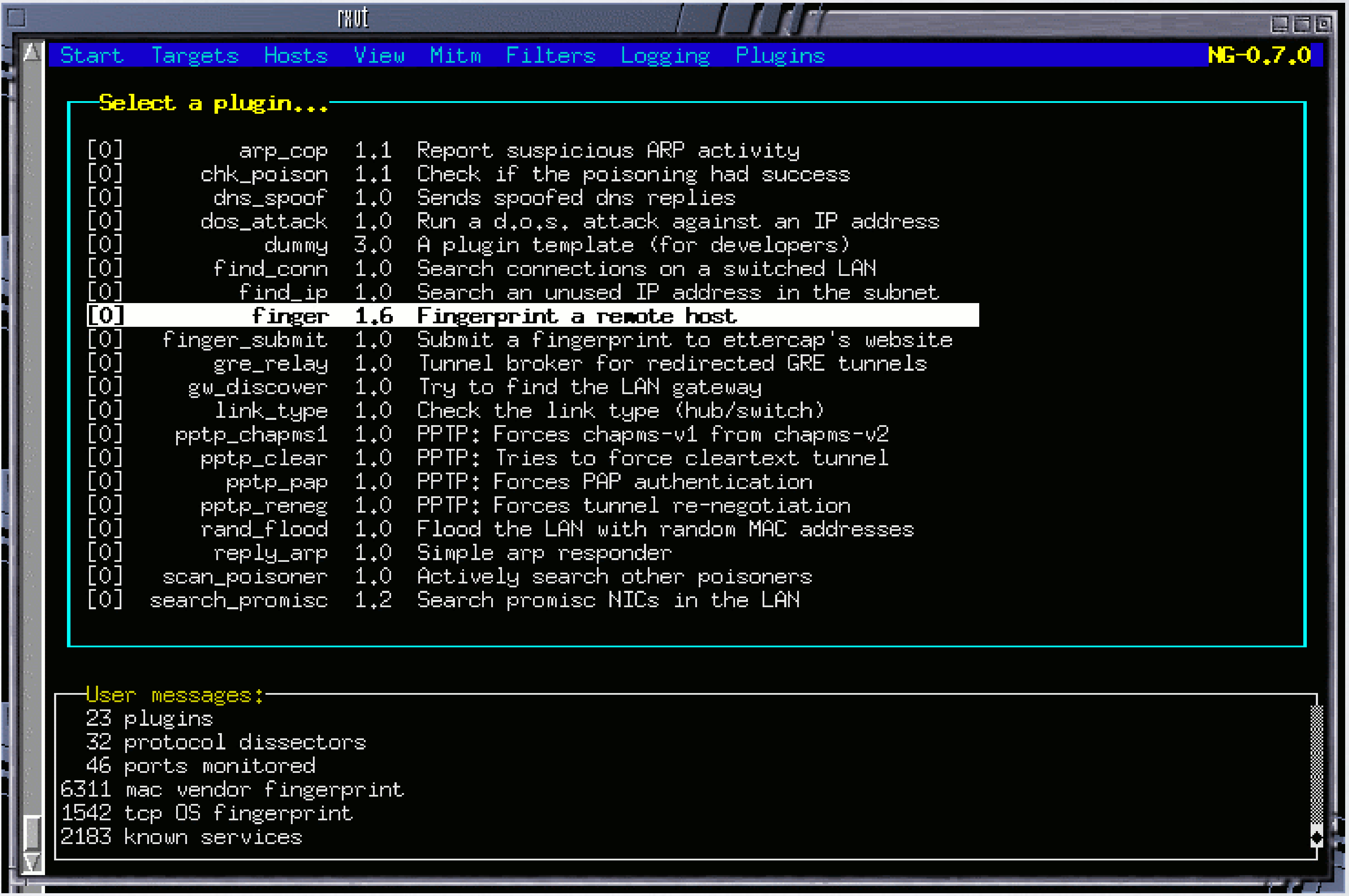
But a fake mail is created!!

OTHER SPOOFING



curtincollege.edu.au

- URL
- IP
- MAC
- DNS



```
Select a plugin...

[0]        arp_cop   1.1  Report suspicious ARP activity
[0]      chk_poison  1.1  Check if the poisoning had success
[0]       dns_spoof  1.0  Sends spoofed dns replies
[0]      dos_attack  1.0  Run a d.o.s. attack against an IP address
[0]           dummy  3.0  A plugin template (for developers)
[0]       find_conn  1.0  Search connections on a switched LAN
[0]         find_ip  1.0  Search an unused IP address in the subnet
[0]          finger  1.6  Fingerprint a remote host
[0]   finger_submit  1.0  Submit a fingerprint to ettercap's website
[0]       gre_relay  1.0  Tunnel broker for redirected GRE tunnels
[0]     gw_discover  1.0  Try to find the LAN gateway
[0]       link_type  1.0  Check the link type (hub/switch)
[0]    pptp_chapms1  1.0  PPTP: Forces chapms-v1 from chapms-v2
[0]      pptp_clear  1.0  PPTP: Tries to force cleartext tunnel
[0]        pptp_pap  1.0  PPTP: Forces PAP authentication
[0]      pptp_reneg  1.0  PPTP: Forces tunnel re-negotiation
[0]      rand_flood  1.0  Flood the LAN with random MAC addresses
[0]       reply_arp  1.0  Simple arp responder
[0]   scan_poisoner  1.0  Actively search other poisoners
[0]  search_promisc  1.2  Search promisc NICs in the LAN

User messages:
  23 plugins
  32 protocol dissectors
  46 ports monitored
6311 mac vendor fingerprint
1542 tcp OS fingerprint
2183 known services
```

PASSWORD MANAGEMENT

- You really don't want to be the second person to try to crack your users passwords
- Brute force tries every possibility
- Dictionary attacks try passwords based on words (and combinations of words in a dictionary)
- Password salts
  - Random values used as an input, along with a password, to a key derivation function
  - The result is stored as the encrypted password
  - The salt value may or may not be protected as a secret
  - The salt data makes it more difficult to conduct a dictionary attack using pre-encryption of dictionary entries, as each bit of salt used doubles the amount of storage and computation required

PASSWORD MANAGEMENT (CONT.)

- Windows
  - Stores local passwords in the SAM
  - Stores domain passwords in AD
- Linux
  - Stores local passwords in either /etc/passwd OR /etc/shadow
  - Stores network based passwords in the NIS database

PASSWORD MANAGEMENT

- L0phtCrack attempts to crack Windows passwords from hashes which it can obtain (given proper access) from stand-alone Windows workstations, networked servers, primary domain controllers, or Active Directory.
- In some cases it can sniff the hashes off the wire.
- It has numerous methods of generating password guesses (dictionary, brute force, etc).
  - LC5 was discontinued by Symantec in 2006, then re-acquired by the original L0pht guys and reborn as LC6 in 2009.
  - free alternatives ophcrack, Cain and Abel, or John the Ripper. For downloads and more information, visit the L0phtCrack homepage.

PERMISSIONS (YET AGAIN)

- SUID & SGID
  - Check when owned by root or wheel
  - Find using `find -perm 4000 /`
  - Remove if possible
  - Close all unnecessary services
  - Use TCP Wrappers all other ports
- Write permission to all (xx2) are dangerous
- .rhosts file
  - This sets which hosts are trusted, look out for + entries (matches any user eg name)

The term wheel refers to a user account with a wheel bit, a system setting that provides additional special system privileges that empower a user to execute restricted commands that ordinary user accounts cannot access

MONITOR YOUR COMPUTER

- Be the hacker yourself
  - Check for scripts and exploits which might be used against you
- Port scan your machine regularly
  - ensure no ports and services are open unless necessary
- Firewall
  - Hiding behind a firewall might help in reducing hackability
    - though those who pass it, are likely to be a better class of hacker

SCANNING

- Scanning, as a method for discovering exploitable communication channels, has been around for ages. The idea is to probe as many listeners as possible, and keep track of the ones that are receptive or useful to your particular need. Much of the field of advertising is based on this paradigm, and the "to current resident" brute force style of bulk mail is an almost perfect parallel to what we will discuss. Just stick a message in every mailbox and wait for the responses to trickle back. ….
- We send a blizzard of packets for various protocols, and we deduce which services are listening from the responses we receive (or don't receive).

– Fyodor, creator of nmap.

SCANNING (CONT.)

- Nmap – network port scanner
  - Checks hosts for servers listening on ports
    - -sP IP range scanning (via ICMP echo requests, called a “ping sweep”)

```
# nmap -sP 192.168.7.0/24
Starting nmap V. 2.12
Host (192.168.7.11) appears to be up.
Host (192.168.7.12) appears to be up.
Host (192.168.7.76) appears to be up.
Nmap run completed -- 256 IP addresses (3 hosts up)
  scanned in 1 second
```

SCANNING (CONT.)

- port scanning (TCP)
  - -sA (ACK flag scan – from SYN SYN/ACK ACK)
    - Does not determine open ports
    - Maps firewall rulesets (check if stateful and/or filtered)
    - On unfiltered systems, open/closed ports both return a RST
    - No response or error messages - labeled filtered
  - -sT (TCP connect() scan)
    - Attempts to make a standard TCP connection
    - Slower and more likely to be noticed by target
  - -sS (SYN flag scan or half-open scan)
    - Send SYN packet and then wait for a response
    - A SYN/ACK indicates the port is listening (open)
    - A RST (reset) is indicative of a non-listener
    - No response or error messages - labeled filtered
  - Other scans: Stealth FIN, Xmas tree, Null, OS detect

SCANNING (CONT.)

Sample results from an nmap scan:

Port	State	Protocol	Service
7	Open	tcp	echo
9	Open	tcp	discard
21	Open	tcp	ftp
23	Open	tcp	telnet
25	Open	tcp	smtp

SCANNING (CONT.)

- Nessus – “next generation” port scanner
  - Client/Server pair
  - Does not assume a given service will be running on the standard port
  - Attempts to exploit service to determine susceptibility
  - Modular design, so new security checks can be easily added
  - NeWT
    - essentially Nessus for Windows
    - Combines client/server into single package

SCANNING (CONT.)

Sample results from a NeWT scan:

- ftp (21/tcp)
  - Port is open Plugin ID : 11219
  - An unknown service is running on this port.
    It is usually reserved for FTP Plugin ID : 10330
  - An unknown service runs on this port. Solution: if a trojan horse is running, run a good antivirus scanner Risk factor : Low Plugin ID : 11157

- netbios-ssn (139/tcp)
  - Port is open Plugin ID : 11219
  - An SMB server is running on this port Plugin ID : 11011

FIREWALLS

- A firewall is hardware or software that regulates data flow to a secured network by filtering data originating from unsecured or untrusted sources.
  - Port Blocking
  - Application exception
  - ACLs

FIREWALLS

- Firewalls identify and block traffic to/from your network
  - Some forms of firewalls include
    - Packet filters
    - Stateful filters
    - Application level filters
    - Proxies

FIREWALLS (CONT.)

- **Packet filters**
  - Operate on packets, protocols, connections and ports.
  - Decision making based on:
    - Where a packet is **coming from**
    - Where a packet **is going**
    - What protocol the packet is using
    - What connection port it is wanting
  - Determine if the packet can pass, and if so where to send the packet

FIREWALLS (CONT.)

- **Stateful filtering**
  - Track significant attributes of connections. (ex. IP addrs., ports, packet sequence numbers.)
  - Basis in TCP's three-way handshake.
    - Client makes a request (SYN), server responds (SYN/ACK), client acknowledges response (ACK).
    - Once the handshake is complete, the connection is considered to be "established"
  - Other packets for this session are checked to determine whether they belongs to the existing, pre-screened session.
  - Once the session has ended, its entry in the state-table is discarded.
  - Some stateful firewalls pass all outgoing packets but only allow incoming packets that are part of an established connection.
  - UDP problem

FIREWALLS (CONT.)

- **Application level filter/gateway/proxy**
  - Filter based on packet contents;
    - these can filter packets at the application layer of the OSI model
  - Incoming or outgoing packets cannot access services for which there is no proxy.
    - (Eg. An application level filter that is configured for web traffic will not allow any other type of traffic through.)
  - This type of firewall can filter application specific commands (eg. http:post and get, etc.)
  - Application level filters can also be used to log user activity and logins
  - These are very secure, but come with a performance impact

FIREWALLS (CONT.)

- Proxy servers
  - A service that allows clients to make indirect network connections to other network services
  - The client sends its request for a resource to the proxy server
    - eg. a web connection
  - The proxy then makes the request on the client’s behalf (or in some cases, provides the resource via its cache)
  - In some cases, the proxy may alter the client's request or the server's response for various purposes

FIREWALLS (CONT.)

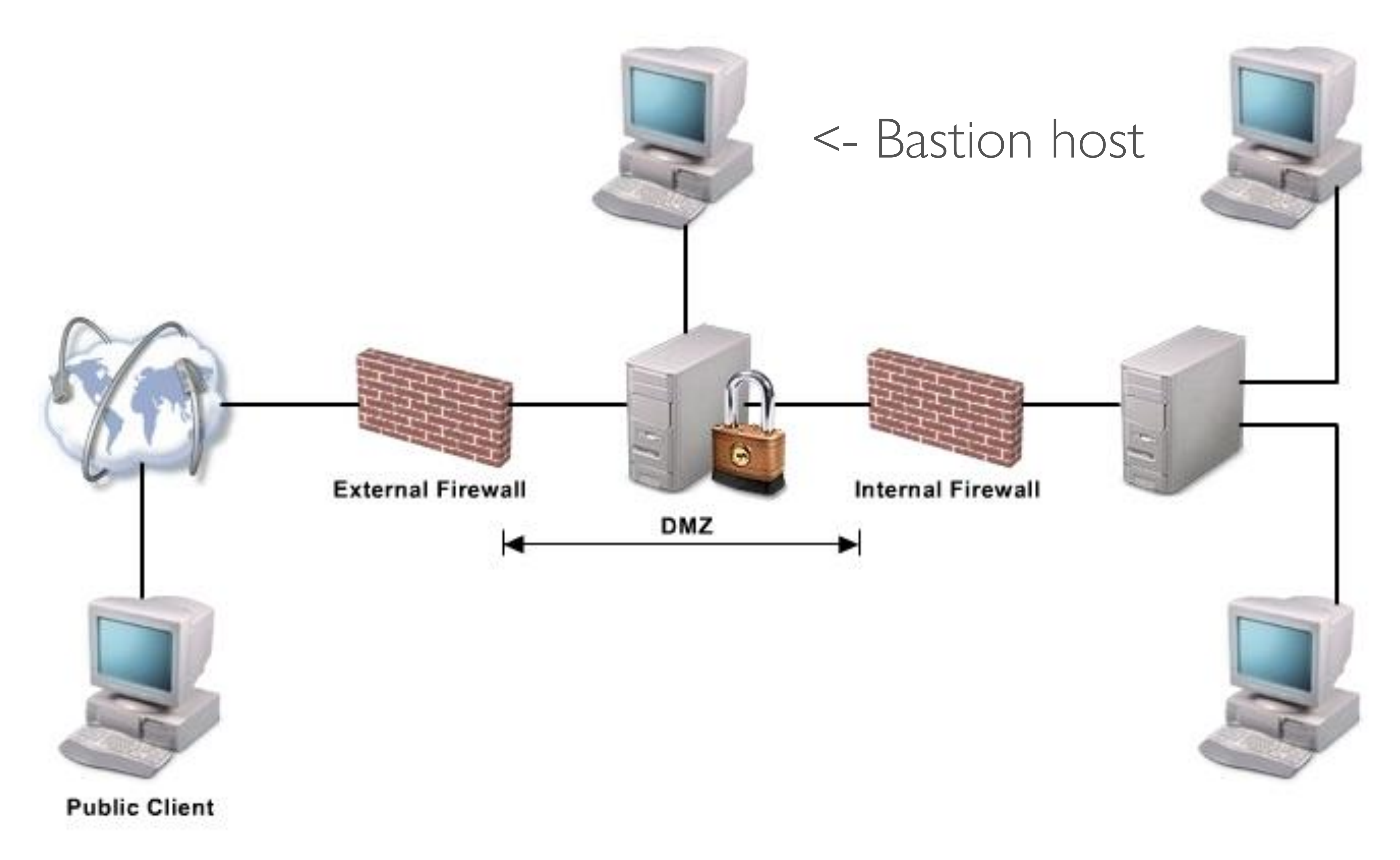
- Access control via “listing”
  - Blacklisting – control by blocking access
  - Whitelisting – control by allowing access
  - Greylisting – control by blocking, then allowing
- Think Blue Coat ProxySG (old)
  - Symantec ProxySG and Advanced Secure Gateway (ASG)

DMZ

- A Demilitarised Zone
  - allows connections from internal and external hosts, allows outward connections, but prohibits inward connections.

- **Hosts in the DMZ's can provide external services while protecting the internal network in case a host in the DMZ is compromised.**
  - A small section of a private network is made available for public access.
  - A DMZ enables external clients to access data on private systems without compromising the security of the internal network as a whole.
  - The external firewall enables public clients to access the service; the internal firewall prevents them from connecting to protected internal hosts.

DMZ



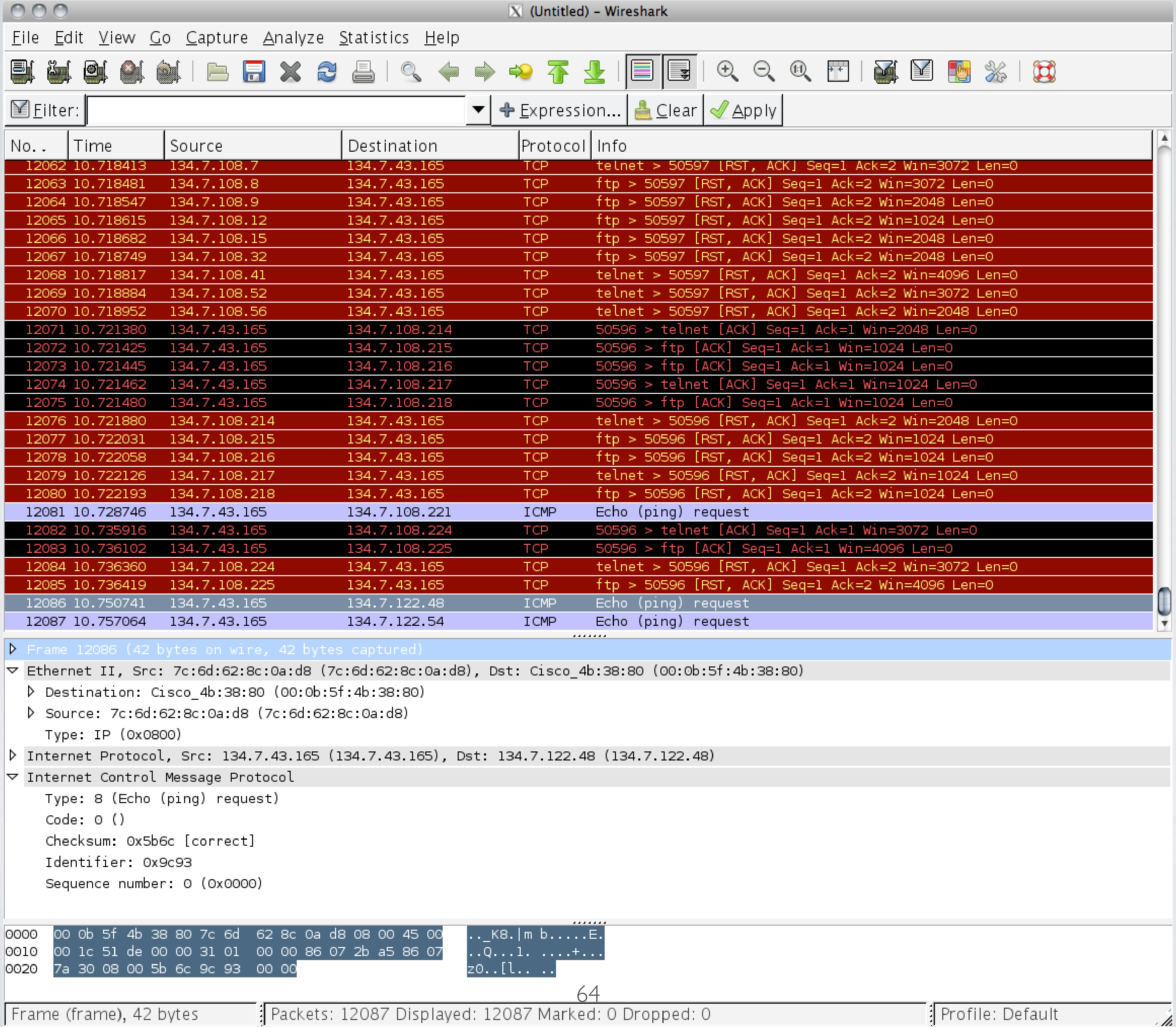
<- Bastion host

FIREWALLS (CONT.)

- Bastion host
  - Outside the DMZ, unprotected by a firewall or filtering router (possibly)
  - May be a secure gateway or may provide services.
  - Generally fulfils a specific role
  - All unnecessary services, protocols, programs, and network ports are disabled or removed
  - Do not share authentication services with trusted hosts within the network; so that if it is compromised the intruder will still not have 'the keys to the castle'
  - “Hardened” to limit potential methods of attack.

SYSTEM CHANGES

- Tripwire
    - Software driven/host based intrusion detection system
    - Intruders usually leave traces of their activities (changes in the system state)
    - Looks for and reports on state changes of the system
    - Tripwire monitors static attributes of files: binary signatures, size, expected changes in size, etc.
    - This can also be useful for integrity assurance, change management, policy compliance, etc.



```
No. .  Time       Source          Destination      Protocol  Info
12062 10.718413  134.7.108.7     134.7.43.165     TCP       telnet > 50597 [RST, ACK] Seq=1 Ack=2 Win=3072 Len=0
12063 10.718481  134.7.108.8     134.7.43.165     TCP       ftp > 50597 [RST, ACK] Seq=1 Ack=2 Win=3072 Len=0
12064 10.718547  134.7.108.9     134.7.43.165     TCP       ftp > 50597 [RST, ACK] Seq=1 Ack=2 Win=2048 Len=0
12065 10.718615  134.7.108.12    134.7.43.165     TCP       ftp > 50597 [RST, ACK] Seq=1 Ack=2 Win=1024 Len=0
12066 10.718682  134.7.108.15    134.7.43.165     TCP       ftp > 50597 [RST, ACK] Seq=1 Ack=2 Win=2048 Len=0
12067 10.718749  134.7.108.32    134.7.43.165     TCP       ftp > 50597 [RST, ACK] Seq=1 Ack=2 Win=2048 Len=0
12068 10.718817  134.7.108.41    134.7.43.165     TCP       telnet > 50597 [RST, ACK] Seq=1 Ack=2 Win=4096 Len=0
12069 10.718884  134.7.108.52    134.7.43.165     TCP       telnet > 50597 [RST, ACK] Seq=1 Ack=2 Win=3072 Len=0
12070 10.718952  134.7.108.56    134.7.43.165     TCP       telnet > 50597 [RST, ACK] Seq=1 Ack=2 Win=2048 Len=0
12071 10.721380  134.7.43.165    134.7.108.214    TCP       50596 > telnet [ACK] Seq=1 Ack=1 Win=2048 Len=0
12072 10.721425  134.7.43.165    134.7.108.215    TCP       50596 > ftp [ACK] Seq=1 Ack=1 Win=1024 Len=0
12073 10.721445  134.7.43.165    134.7.108.216    TCP       50596 > ftp [ACK] Seq=1 Ack=1 Win=1024 Len=0
12074 10.721462  134.7.43.165    134.7.108.217    TCP       50596 > telnet [ACK] Seq=1 Ack=1 Win=1024 Len=0
12075 10.721480  134.7.43.165    134.7.108.218    TCP       50596 > ftp [ACK] Seq=1 Ack=1 Win=1024 Len=0
12076 10.721880  134.7.108.214   134.7.43.165     TCP       telnet > 50596 [RST, ACK] Seq=1 Ack=2 Win=2048 Len=0
12077 10.722031  134.7.108.215   134.7.43.165     TCP       ftp > 50596 [RST, ACK] Seq=1 Ack=2 Win=1024 Len=0
12078 10.722058  134.7.108.216   134.7.43.165     TCP       ftp > 50596 [RST, ACK] Seq=1 Ack=2 Win=1024 Len=0
12079 10.722126  134.7.108.217   134.7.43.165     TCP       telnet > 50596 [RST, ACK] Seq=1 Ack=2 Win=1024 Len=0
12080 10.722193  134.7.108.218   134.7.43.165     TCP       ftp > 50596 [RST, ACK] Seq=1 Ack=2 Win=1024 Len=0
12081 10.728746  134.7.43.165    134.7.108.221    ICMP      Echo (ping) request
12082 10.735916  134.7.43.165    134.7.108.224    TCP       50596 > telnet [ACK] Seq=1 Ack=1 Win=3072 Len=0
12083 10.736102  134.7.43.165    134.7.108.225    TCP       50596 > ftp [ACK] Seq=1 Ack=1 Win=4096 Len=0
12084 10.736360  134.7.108.224   134.7.43.165     TCP       telnet > 50596 [RST, ACK] Seq=1 Ack=2 Win=3072 Len=0
12085 10.736419  134.7.108.225   134.7.43.165     TCP       ftp > 50596 [RST, ACK] Seq=1 Ack=2 Win=4096 Len=0
12086 10.750741  134.7.43.165    134.7.122.48     ICMP      Echo (ping) request
12087 10.757064  134.7.43.165    134.7.122.54     ICMP      Echo (ping) request
```

```
▷ Frame 12086 (42 bytes on wire, 42 bytes captured)
▽ Ethernet II, Src: 7c:6d:62:8c:0a:d8 (7c:6d:62:8c:0a:d8), Dst: Cisco_4b:38:80 (00:0b:5f:4b:38:80)
  ▷ Destination: Cisco_4b:38:80 (00:0b:5f:4b:38:80)
  ▷ Source: 7c:6d:62:8c:0a:d8 (7c:6d:62:8c:0a:d8)
    Type: IP (0x0800)
▷ Internet Protocol, Src: 134.7.43.165 (134.7.43.165), Dst: 134.7.122.48 (134.7.122.48)
▽ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0 ()
    Checksum: 0x5b6c [correct]
    Identifier: 0x9c93
    Sequence number: 0 (0x0000)
```

```
0000  00 0b 5f 4b 38 80 7c 6d  62 8c 0a d8 08 00 45 00   .._K8.|m b.....E.
0010  00 1c 51 de 00 00 31 01  00 00 86 07 2b a5 86 07   ..Q...1. ....+...
0020  7a 30 08 00 5b 6c 9c 93  00 00                     z0..[l.. ..
```

Frame (frame), 42 bytes | Packets: 12087 Displayed: 12087 Marked: 0 Dropped: 0 | Profile: Default