SENG 460 / ECE 574
Practice of Information Security and Privacy

Attacks/Breaches

Best Practices

Prevention

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

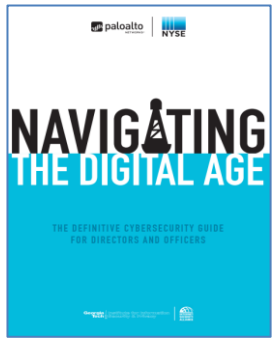
About the Course

- Class: SENG 460 – ECE 574
  - location: ELL 168 day/time: Friday 15:30 – 18:20
- Office hours:
  - location: ELL 168 day/time: on request
- TAs:
  - Mehrab Najafian
  - Araya Chaowalit
  - Sathvik Divilli
  - Ahmed Ahmer
  - Hadeer Ahmed
- Instructor:
  - Gary Perkins
    garyperkins@uvic.ca
- Discord:
  - Invite on BrightSpace

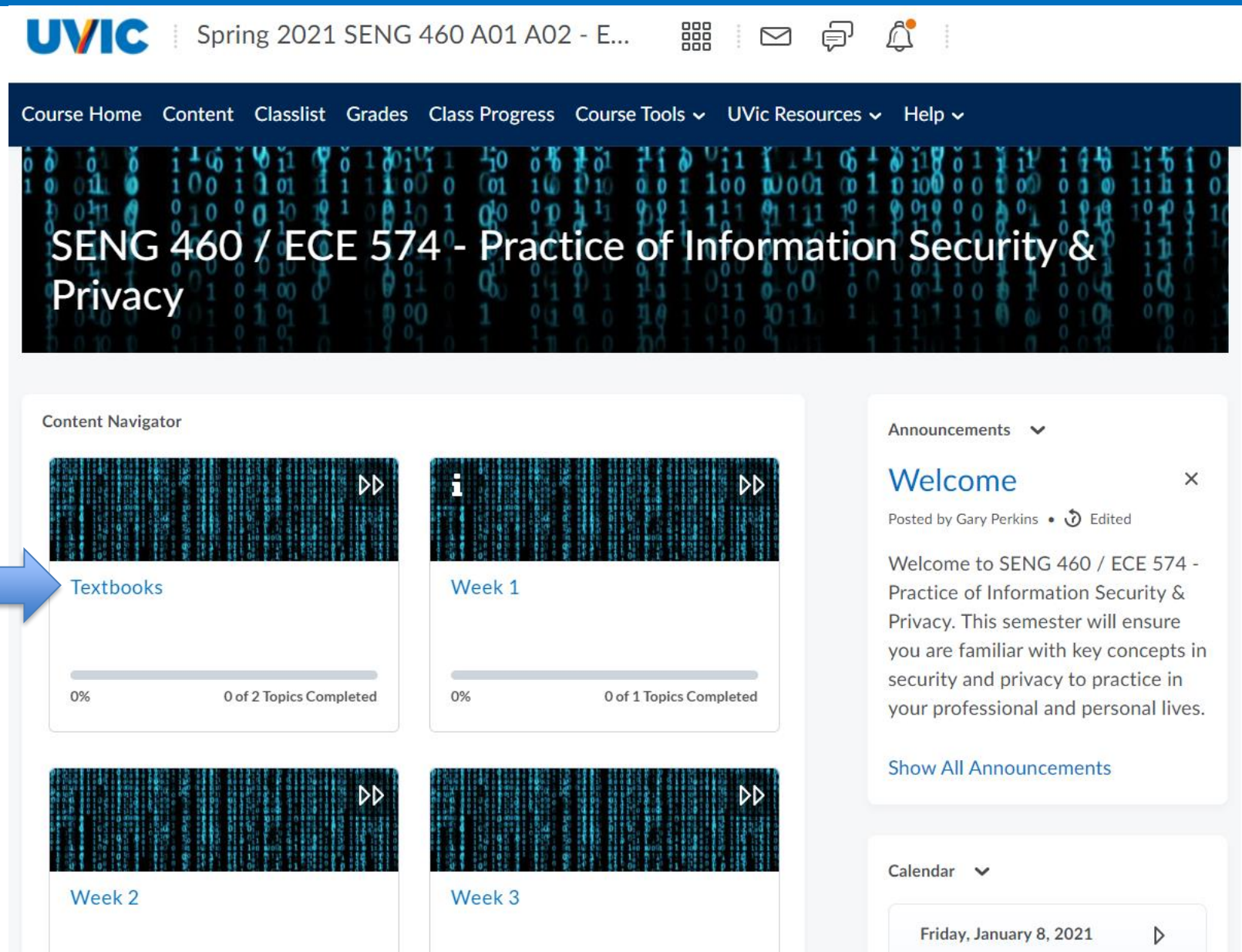
University of Victoria

Website (on BrightSpace)

- course website is on BrightSpace



University of Victoria



Grading

- SENG 460
  - Quizzes 20% Jan 27, Mar 10, Mar 31
  - Midterm 40% Feb 10
  - Final 40% TBD

- ECE 574
  - Quizzes 20% Jan 27, Mar 10, Mar 31
  - Midterm 20% Feb 10
  - Project 20% Mar 24
  - Final 40% TBD

University of Victoria

Lab Assignment

- weekly labs are posted; many are quite short, a few are longer
- all are aimed at providing hands-on exposure to tools
- access https://labs.engr.uvic.ca, use SSH, or use your home linux
- labs this semester are optional

Submit the Standards of Conduct

University of Victoria

ECE 574 Project Information

- ECE 574 students are also required to complete a project
- plan to benefit the industry by contributing to an online repository by producing a video to educate others on a security topic of your choice
- work either individually or in teams of two or three
- 4-5 minutes of content per student
- more details and examples available on the website

University of Victoria

Security Certifications

- Comptia: A+, Network+, Security+, PenTest+ $
- ISACA: CISM, CISA, CRISC $$
- ISC2: SSCP ($300), CISSP ($750) $$
- SANS: GSEC, GCIH, GPEN, GWAPT, many $$$
- EC-Council: CEH, LPT, CCISO
- Offensive Security: OSCP, others
- Cisco: CCNA Cyber Ops, others
- IAPP: CIPP, CIPM, CIPT (privacy pro, mgr, tech)

University of Victoria

Why certify?

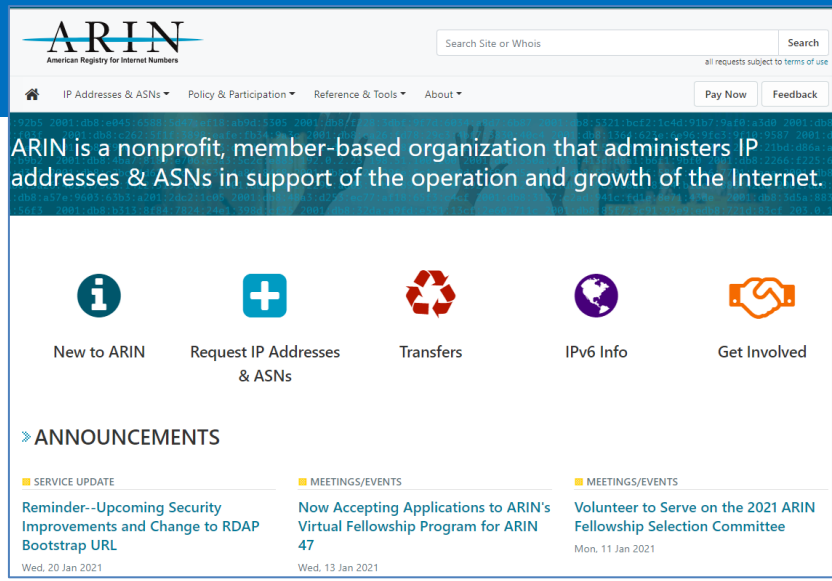
Review

- not every job requires significant technology knowledge
- most common certification requested is CISSP along with CISM and CISA
- incidents are increasing in frequency and sophistication
- no organization is immune to attack
- organizations don’t choose whether they are attacked – they are attacked if there is something of value or the perception there is
- security is not an IT problem, it’s business enterprise risk

University of Victoria

Review

- six types of attackers:
  - juveniles, insiders, organized crime, hacktivists, nation-states, cyber terrorists
- each has different access to resources, sophistication, motivation
  - lowest sophistication and skills are juveniles and highest are nation-states
- different reasons organizations are targeted, different impacts & attack vectors
- ARIN and Shodan are sites to conduct passive reconnaissance, intelligence gathering
- CIA triad is confidentiality, integrity, availability – **RIP Nickelback**
  - preventing unauthorized disclosure, unauthorized modification, disruption of activity



University of Victoria

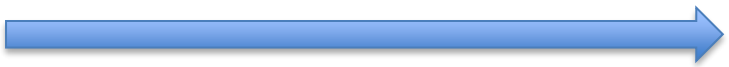
Review - Five tenets

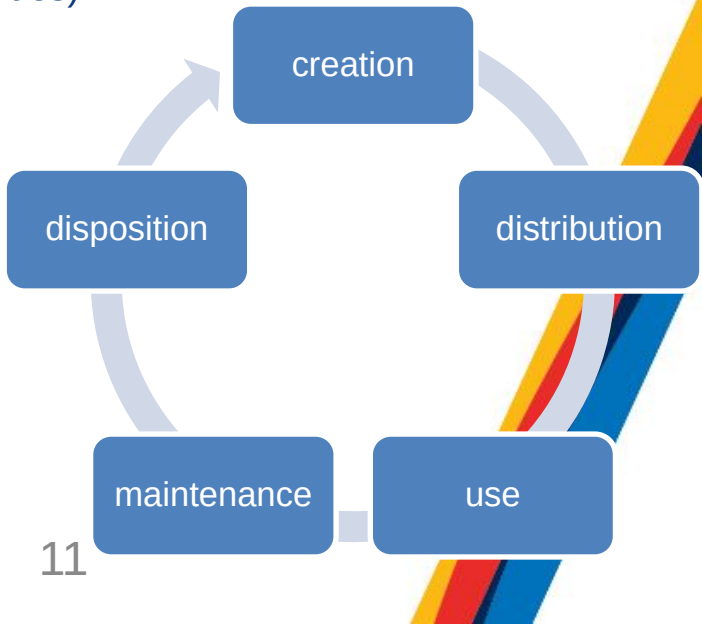
- **strong authentication**
  - more than one type of authentication (two-factor)
  - something you know, something you have, something you are
- **least privilege**:
  - ie. people have the access to do their job – nothing more, nothing less; similar to ‘need to know’
- **non-repudiation**:
  - ie. achieving the assurance that something could only have been done by a specific person
- **separation of duties**:
  - ie. separating tasks, responsibilities such that no-one person should be able to complete an act alone
- **defense in depth**:
  - layers of security so that any one layer failing will not in itself result in compromise
  - eg. systems should be built off a standard image that has been hardened with unnecessary services disabled and additional protections on the system but should also have authentication, firewalls, intrusion prevention, etc.

University of Victoria

Other concepts

- **privileged account management**
  - provide sparingly; only giving these permissions to users who need it
  - only use privileged accounts when necessary (eg. should not be logging in routinely as root)
  - monitor/check on these accounts and the use of them
- **job rotation**
  - reduce the length of time a person is in a job
  - if you manage access properly then prevents people from having too much access
  - reduces chance for fraud as well (also gives professional development/career progression opportunities)
- **information lifecycle management**
  - creation, distribution, use, maintenance, disposition
- **service level agreements (SLA)**
  - agreement between organization and vendor that a service will perform to a certain level
  - availability/uptime, throughput, capacity, accuracy, response time, resolution time, mean time to resolution (MTTR), mean time between failures (MTBF)





University of Victoria

Review

- what is security about?
  - enabling the business to make conscious decisions around risk
  - ensuring decisions are aligned with the risk appetite of the business
  - managing risk to an acceptable level

- it's still not an IT issue **though it won't feel like it after this lecture**

- …but first.. left off from last time…

University of Victoria

Best Practices

- Remember different kinds of controls
  - administrative, procedural — eg. policies, standards
  - technical, logical — eg. firewalls
  - physical — eg. fences
- COBIT (good practice framework)
- ITIL (IT Service Management)
- NIST (cybersecurity framework)
- ISO/IEC 27001 (information security standard)
- ISO/IEC 27002 (information security standard)

University of Victoria

Best Practices

- CIS (Center for Internet Security; best practices)
- SOX (Sarbanes Oxley)
- SAS70/SSAE16 (Statement on Standards for Attestation)
- PCI DSS (payment card industry data security standard; set of controls)
- FOIPPA (freedom of information and protection of privacy act)
  - previously required personal information be stored, accessed, and disclosed only in Canada
  - there were exceptions (eg. temporarily while travelling)
  - later amendments allow processing, routing
  - later amendments allow storage outside of Canada

University of Victoria

Best Practices

Framework Altitudes

Governance Objective

Stakeholder Needs: Value Creation

- **Benefits Realization**
- **Resource Optimization**
- **Risk Optimization**

Governance Drivers

Performance (*Business Goals*)

Conformance (*Legal, Regulatory*)

Enterprise Governance

- **Balanced Scorecard**
- **COSO**

Governance of Enterprise IT

COBIT

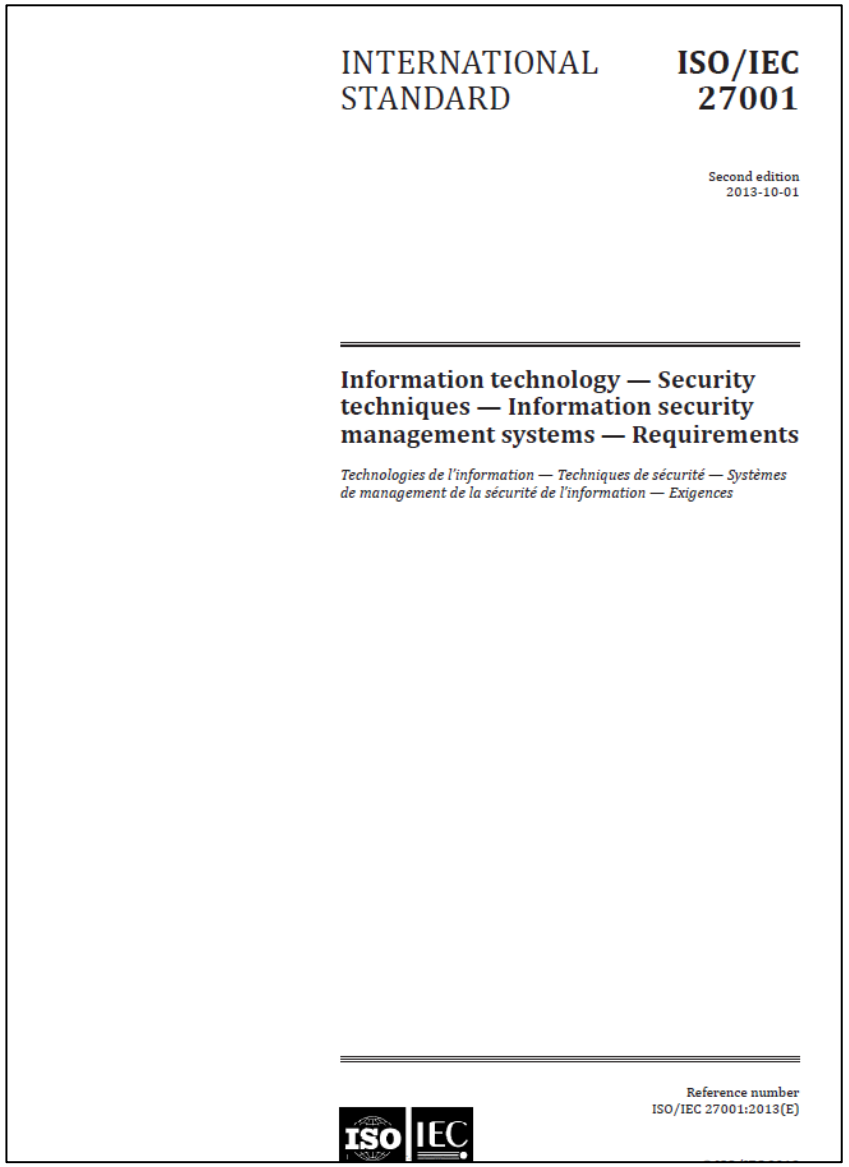
Standards

ISO, NIST, etc.

Good Practices

ITIL, TOGAF, BOKs, etc.

ISO/IEC 27001



INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

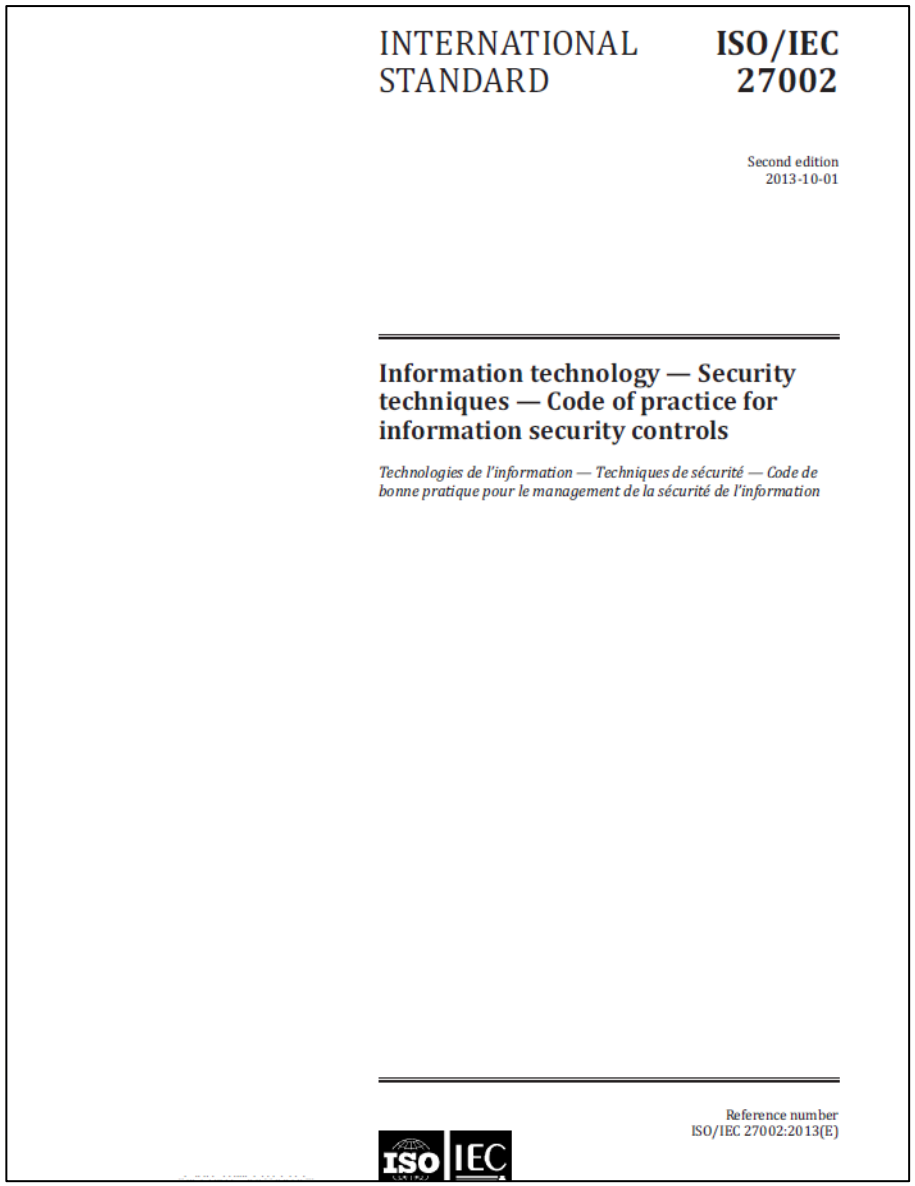
Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

ISO IEC

Contents

ISO/IEC 27002



INTERNATIONAL STANDARD

ISO/IEC 27002

Second edition
2013-10-01

Information technology — Security techniques — Code of practice for information security controls

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

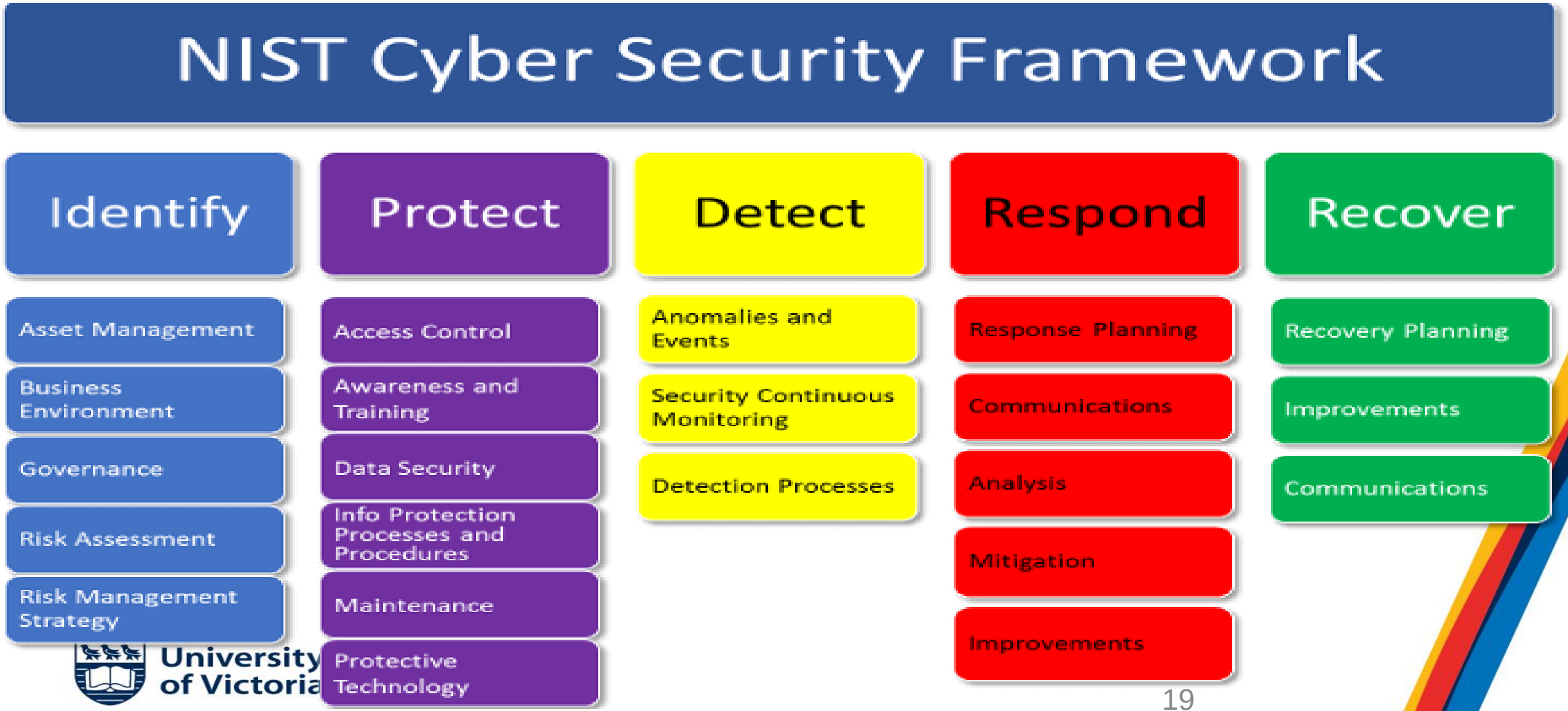
Reference number
ISO/IEC 27002:2013(E)

ISO IEC

Contents

ISO/IEC 27002:2013

NIST



https://securityaffairs.co/wordpress/58163/laws-and-regulations/nist-cybersecurity-framework-2.html

NIST

IDENTIFY (ID)	**Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.**
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
PROTECT (PR)	**Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.**
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

University of Victoria

NIST

DETECT (DE)	Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.
RESPOND (RS)	Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RECOVER (RC)	Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Hygiene Controls (procedural)

Security Controls	
Information Security Policy	Identify what employees may and may not do that will impact risk to systems and data
Risk Register	Conscious identification and treatment of physical and logical risks to systems and data
Risk Assessments	Review risk each time a new system is introduced or upon material change to an existing system
Incident Response Plan	Respond to inevitable security incidents in a consistent and scalable way
Incident Response Team	Team that is dedicated, virtual, or on retainer with third party provider to respond to security incidents
Security Education and Awareness	Humans represent the easiest method for attackers to gain unauthorized access to systems and data

Hygiene Controls (technical)

Security Controls	
Firewall	Modern version designed to prevent illegitimate network traffic
Intrusion Prevention	Sensors to prevent unauthorized access to networks and data
Website Content Filtering	System to detect employee access to inappropriate and infected websites
Email Content Filtering	System to detect infected email and spam messages
Anti-virus/ Malware	Software to detect malware and viruses on workstations and servers

SENG 460 / ECE 574
Practice of Information Security and Privacy

Lecture 2: Back to Basics

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Back to Basics

A long time ago, in a laboratory far, far away….

- binary was first referenced in the 17th century
- two-symbol system consisting of 0's and 1's

University of Victoria

Binary

- all you have are 0's and 1's

  to make numbers

- how do you go above 1?

  add more digits & push left

0001

0010

0011

0100

0101

0110

0111

1000

University of Victoria

Binary

1	0001	6	0110	A	01000001
2	0010	7	0111	B	01000010
3	0011	8	1000	C	01000011
4	0100	9	1001	D	01000100
5	0101	10	1010	E	01000101

01000011 01000001 01010100 = ???

01000101 01111000 01100001 01101101 01110000 01101100 01100101

University of Victoria

TCP/IP

- TCP/IP = Transmission Control Protocol / Internet Protocol
- TCP/IP is the most widely implemented protocol in networks today
- to communicate on the network

  each host needs an address
- two versions of IP addressing

  are IPv4 and IPv6

University of Victoria

IP addressing

IP address

- identifies a system on a network
- 4 numbers from 0-255 with periods in between

Examples:

157.240.3.174

216.232.63.190

123.45.67.89

_____

_____

University of Victoria

IP addressing

- IPv4 address
  - eg. 192.168.1.1
  - 4 groups of decimals
  - 4 groups of 8 bits (1 octet) = 32 bits
  - 11000000.10101000.00000001.00000001 where each bit refs to 128,64,32,16,8,4,2,1
- IPv6 address
  - eg. 2001:0db8:85a3:0000:0000:8a2e:0370:7334
  - 8 groups of 4 hexadecimal digits
  - 8 groups of 16 bits (2 octets) = 128 bits
  - 0010000000000001:0000110110111000:1000010110100011:0000000000000000:0000000000000000:1000101000101110:0000001101110000:0111001100110100

IP addresses are grouped into classes

Class	Range	Network	Host	# Networks	# Hosts
A	1-127	8 bits	24 bits	128	16,777,216
B	128-191	16 bits	16 bits	16,384	65,536
C	192-223	24 bits	8 bits	2,097,152	256
D	224-239	reserved for multicast			
E	240-254	reserved for future use			

missed opportunity to improve security

University of Victoria

IP addressing

IP address

- some IP addresses are routable — eg. 216.232.63.190
- some IP addresses are non-routable — eg. 192.168.1.1
- some IP addresses are reserved — eg. 127.0.0.1
- 127.0.0.1 refers to “localhost” or “home” (the machine you are on at the time)

Subnetting

- subnet masks take the same form as IP addresses but are used to determine which portions of the IP are for network and which are host addresses
- 192.168.1.1 with subnet mask 255.255.255.0 means network is 192.168.1 and host is 1

Default Subnet Masks Associated with IP Address Classes

Address Class	Default Subnet Mask
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

University of Victoria

IP address assignment

- IP address may be
  1) routable
  2) non-routable

- whether your IP address changes
  1) dynamic (changes)
  2) static (stays the same)

- how your computer gets an IP
  1) requests through DHCP
  2) manually hardcoded

University of Victoria

DHCP

- DHCP (Dynamic Host Configuration Protocol)

- DHCP servers assign:
  - IP address — each computer has unique IP on network
  - subnet mask — lets systems know what portion of IP is the network
  - default gateway — lets computer communicate with remote networks
  - DNS servers — lets computer convert hostname to IP and reverse

Address Assignment

- systems are identified by their MAC address
  - MAC = Media Access Control address – eg. 00:0d:93:78:b6:02
  - MAC = physical address = hardware address
  - intended to be unique but can be the same or changed / spoofed
  - 6 byte hexadecimal address that allows the network interface card (NIC) to be identified on the network
  - 3 bytes identify the manufacturer 00:0d:93

    3 bytes are the serial number assigned to device 78:b6:02

Helper Systems

- DNS (domain name system) servers translate hostname to IP and IP to hostname
  - www.cheese.com to 195.149.84.153
  - 195.149.84.153 to cheese.wn.com
- ARP protocol translates IP to MAC address
  - address resolution protocol
  - 10.200.1.23 to 00:0d:93:78:b6:02
- RARP protocol translates MAC to IP address
  - reverse address resolution protocol (obsolete)
  - 00:0d:93:78:b6:02 to 10.200.1.23

CIDR & Loopbacks

- CIDR (Classless Inter-Domain Routing)
  - allows more flexible allocation of IP addresses
  - CIDR notation refers to the network bits
  - eg. 255.255.255.0 is 24 bits or /24 for Class C
- 127 is not used as it is reserved for the loopback address 127.0.0.1, or localhost, or ‘home’
- broadcast address is an address all devices are connected to and can receive traffic from
  - the address is derived from a bitwise OR between subnet bits and host IP address though for our purposes “255” is often a clue

Bonus:
unicast
broadcast
multicast
anycast

University of Victoria

Demo: ping, traceroute, dig/nslookup, telnet

Routing

- different devices transmit traffic different ways

Device	Traffic	Note
hub	repeats traffic to all ports	inefficient
switch	sends traffic by MAC address	fast
router	send traffic by IP address	smart

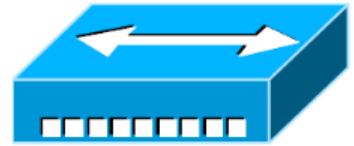
- systems determine if host is on a local or remote network
- if remote then system looks in the routing table to determine whether it has an entry for the network
- if it does it uses that route, if not then uses default gateway
- if no known route static or learned then uses default route

Hub

- device that can be used for networking
- “dumb” device that sends all signals to all ports

Example:
If a device on port 1 wants to send to port 5 a copy of the traffic is sent to ports 2, 3, and 4 as well

hub icon



University of Victoria

Switch

- smarter device that can be used for networking
- understands physical addresses and sends traffic only to the port with the correct physical address

Example:
If a device on port 1 wants to send to port 5 it only sends to 5 based on MAC address. A MAC address looks like 76-E5-F9-DD-6B-07 and identifies the network card.

switch icon 

University of Victoria

Router

- “smartest” device of the three that is used for networking
- understands IP addresses and networks and sends traffic only to the port with correct IP or network

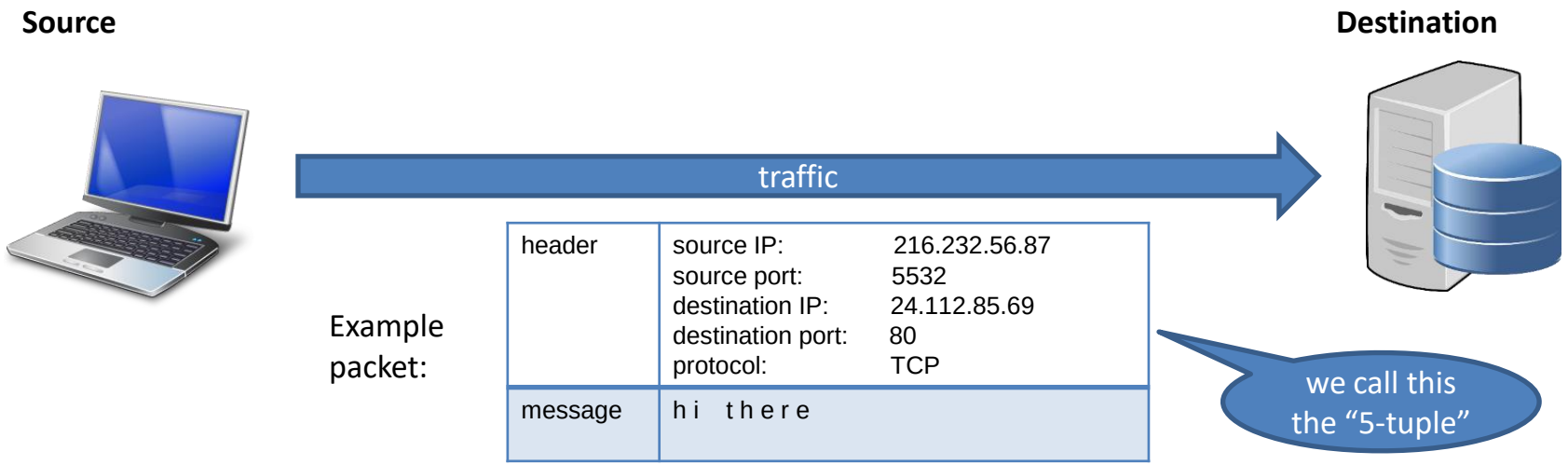
Example:
If a device on port 1 wants to send to port 5 it only sends to 5 based on IP address. An IP address looks like 24.14.82.67.

router icon

University of Victoria

Packets

- unit of data carried by a network

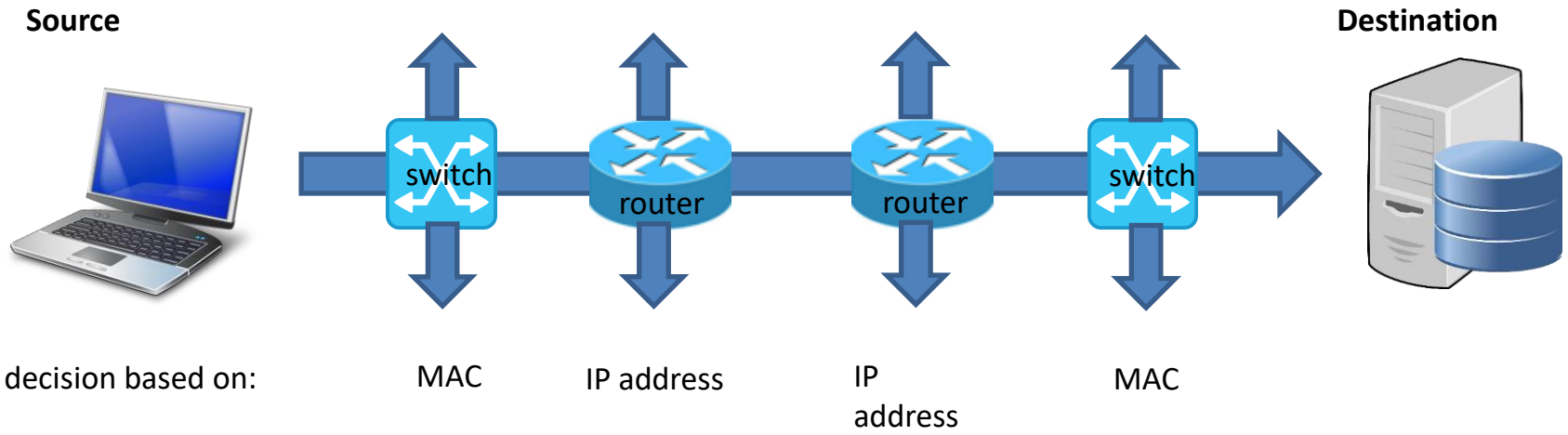


Demo: Wireshark

University of Victoria

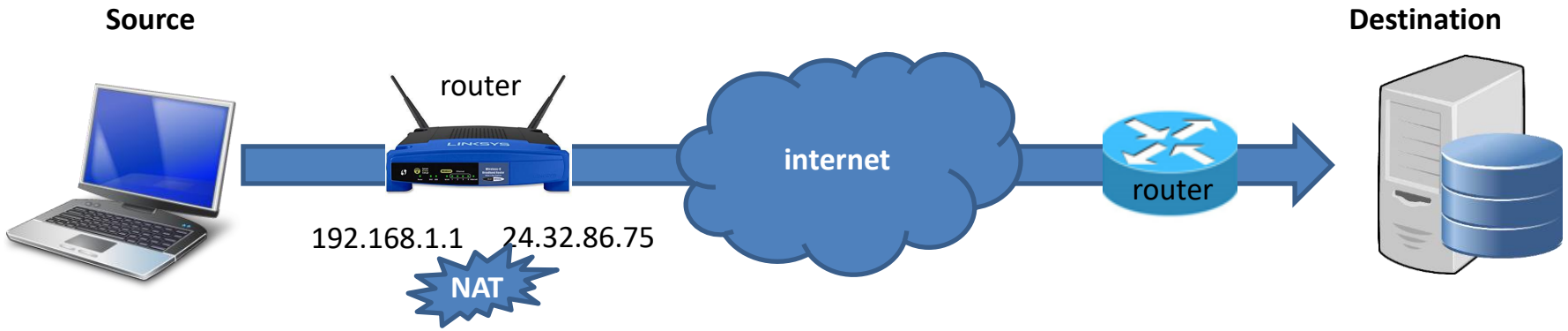
Routing

- how packets get from one place to another



NAT (Network Address Translation)

- how private and public networks communicate



Source 192.168.1.5 connects to gateway 192.168.1.1 which NATs to 24.32.86.75 which connects to destination 52.71.209.23

(private network with non-routable IP address)

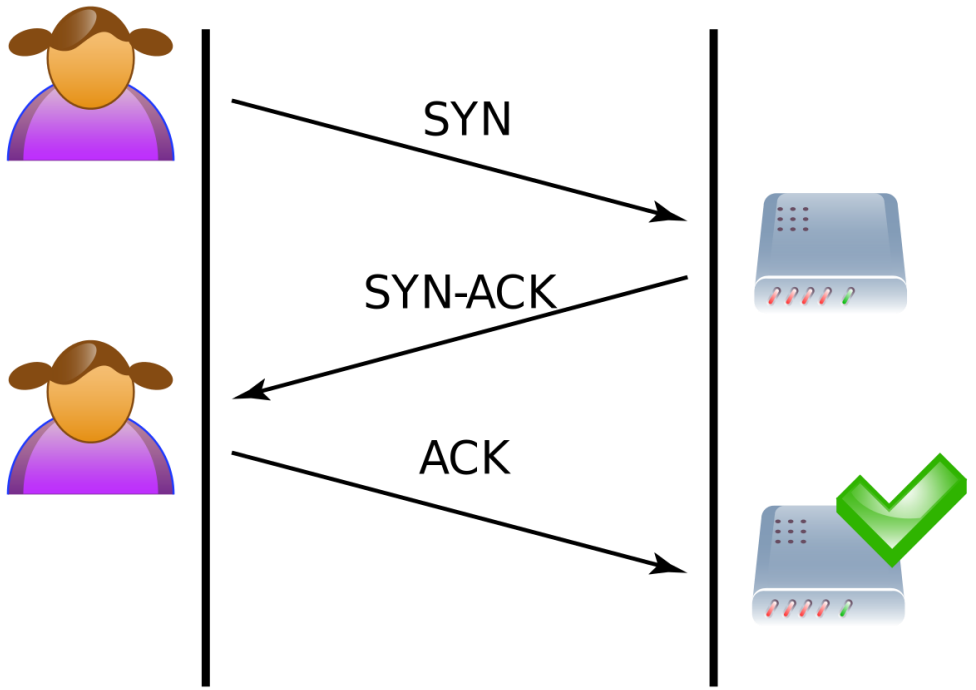
(public network with routable IP address)

Example: Findmyip

3-way Handshake

3-way Handshake

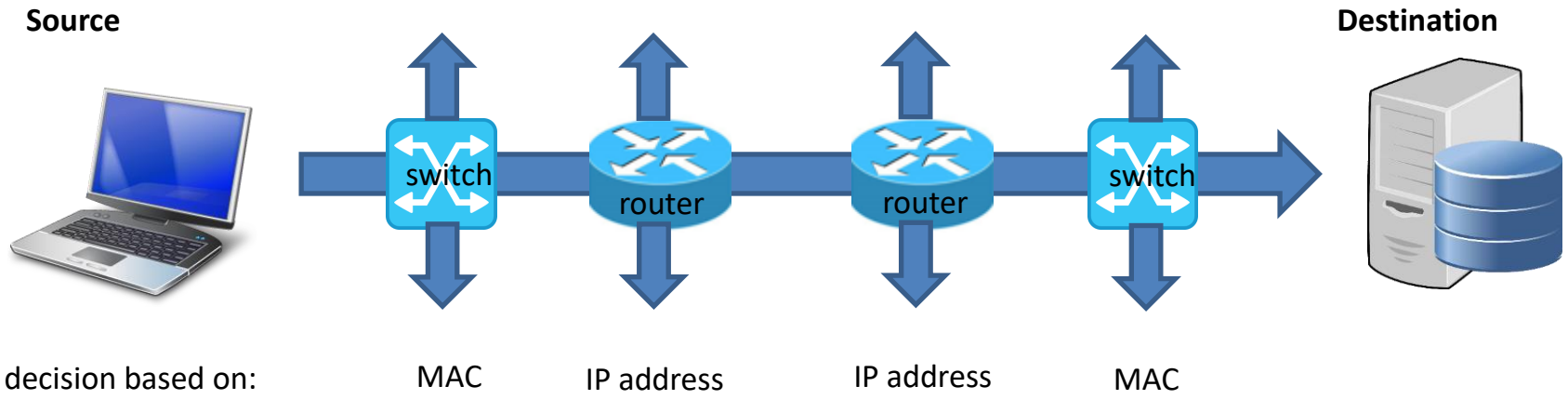
1. SYN
2. SYN-ACK
3. ACK



Example: SYN flood

Default Gateway

- each “hop” either knows where to send the traffic or sends it out the default

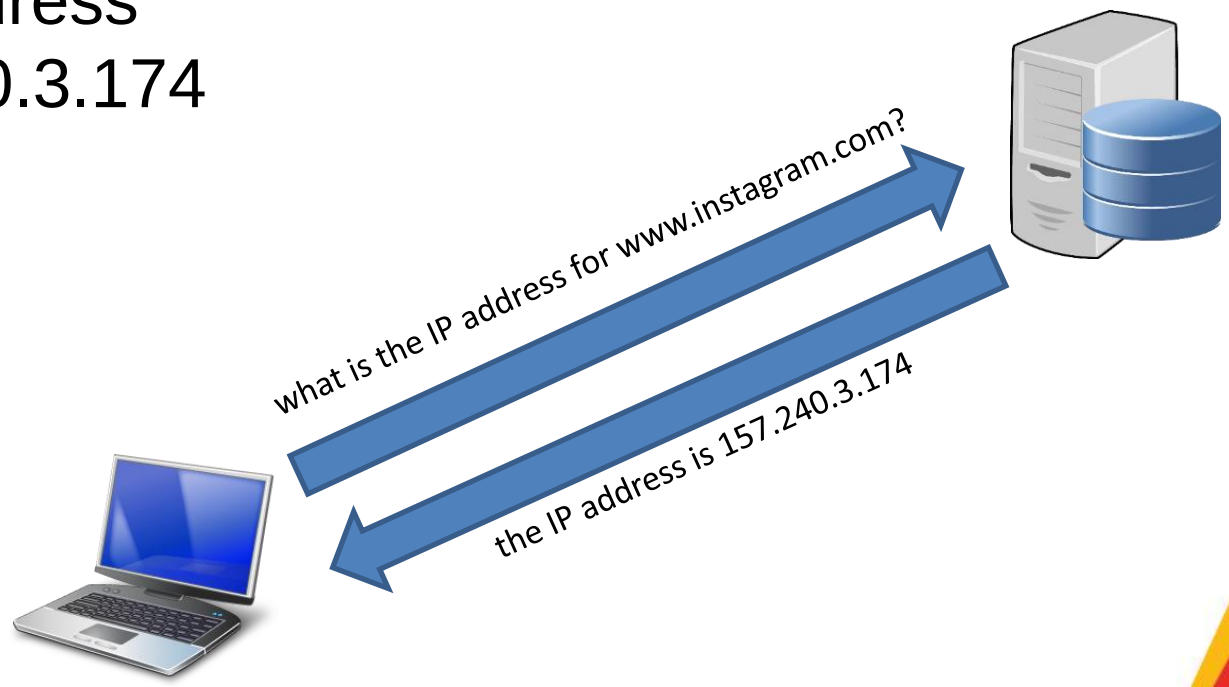


Example: Netstat & Routing Table

DNS (Domain Name System)

- allows computers to translate IP address to hostname and hostname to IP address
- eg. www.instagram.com = 157.240.3.174

- commands are nslookup or dig (or even host)



Address Translation

- different types of addresses
  - external, public addresses
  - internal, private addresses
- network address translation allows many hosts to ‘hide’ behind a single address
  - internally can run whatever addresses are desired
- NAT translates between the external and internal address and vice versa
- PAT is port address translation and allows multiple devices to use the same IP but with different ports

University of Victoria

…double NAT, secure NAT, source NAT
difference with a Proxy?

TCP vs UDP

- TCP (Transmission Control Protocol)
  - connection-oriented, expects and waits for responses, will re-transmit, can slow down
  - client: SYN
  - server: SYN-ACK
  - client: ACK

  } 3-way handshake

- UDP (User Datagram Protocol)
  - connection-less, does not wait for responses
  - send, send, send, send, send….

University of Victoria

Ports

- used for communicating between systems
- 65,535 TCP ports and 65,535 UDP ports

Port	Purpose
20/21	FTP
22 ✓	SSH
23	Telnet
25	SMTP
53	DNS
67/68 (U)	DHCP

Port	Purpose
69 (U)	TFTP
80	HTTP
110	POP
143	IMAP
443 ✓	HTTPS
1433	SQL

Port	Purpose
0-1023	well-known
1024-49,151	registered
49,152-65,535	dynamic / private

Example: Telnet to test web, send email

3306? 31337? 3389? 5800-5900? 6667? 25565? 1935, 3478-3480?
Secure protocols vs not…

University of Victoria

Nmap

- using nmap to identify open ports/services

nmap –Pn 192.168.1.1	scan without ping first
nmap –open 192.168.1.1	find open ports
nmap 192.168.1.1 –p80,443	specify ports to scan
nmap -A -T4 192.168.1.1	scan with OS detection fast
nmap -sV 192.168.1.1	detect server, service versions
nmap –Pn –script vuln 192.168.1.1	vulnerability scan

```
$ nmap -Pn 192.168.1.1 -p21,22,23,80,443
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-18 16:53 Pacific Daylight Time
Nmap scan report for 192.168.1.1
Host is up (0.010s latency).

PORT    STATE    SERVICE
21/tcp  closed   ftp
22/tcp  filtered ssh
23/tcp  filtered telnet
80/tcp  open     http
443/tcp open     https
MAC Address: 00:FC:8D:DE:F7:32 (Hitron Technologies.)

Nmap done: 1 IP address (1 host up) scanned in 9.87 seconds
```

University of Victoria

OSI Model (Open Systems Interconnection)

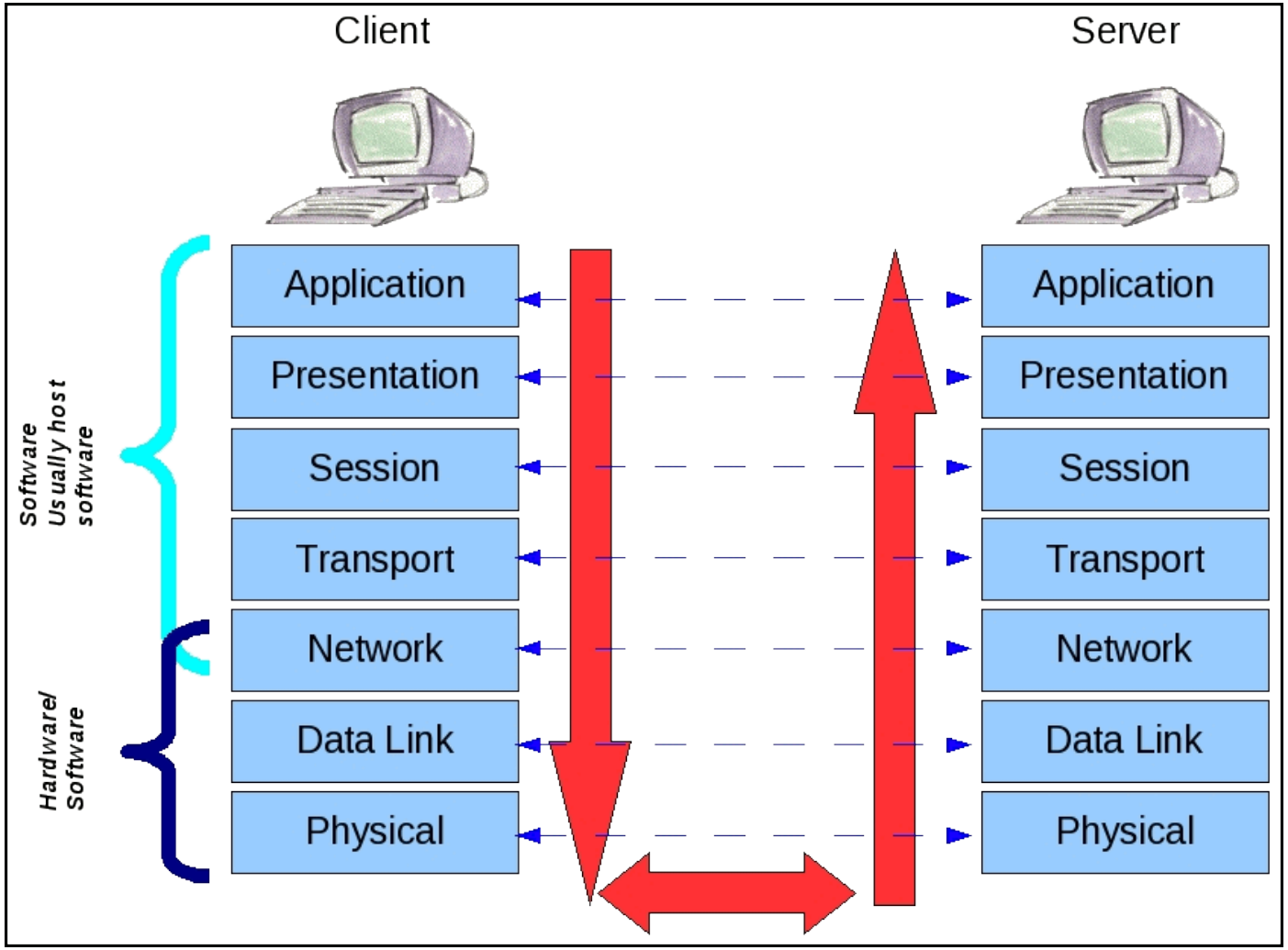
#	Layer	Purpose	Examples	DOD Model
7	Application	end user layer	SMTP, HTTP, FTP	Application
6	Presentation	encryption, decryption	JPEG, GIF	
5	Session	session management	logical ports RPC, SQL, NFS	
4	Transport	flow control	TCP, UDP	Transport
3	Network	router	IP, ICMP packets	Internet
2	Data Link	switch	frames	Network
1	Physical	hub/repeater	volts, bits	

PDNTSPA

also unofficial Layers 8, 9, and 10

University of Victoria

OSI Model (Open Systems Interconnection)



https://osimultimedia.weebly.com/how-the-osi-model-works.html

University of Victoria

SENG 460 / ECE 574
Practice of Information Security and Privacy

Lecture 2: Attacks, Breaches, Prevention & Best Practices

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Video

Oceans 8: https://www.youtube.com/watch?v=_qcW81eke6U

University of Victoria

Definitions

- vulnerability: an exposure that exists in a system

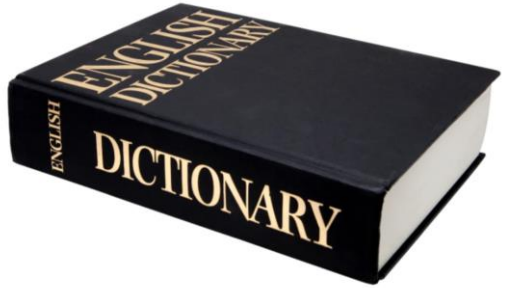
  - unintended flaw in software code or a system that leaves it open to the potential for exploitation in the form of unauthorized access or malicious behavior

- exploit: turns a vulnerability into an incident

  - code that takes advantage of a software vulnerability

- incident: a vulnerability that has been exploited

  aka. breach, compromise



University of Victoria

Vulnerabilities

Where do vulnerabilities come from?

- misconfigured systems
- poor coding
- insufficient security controls

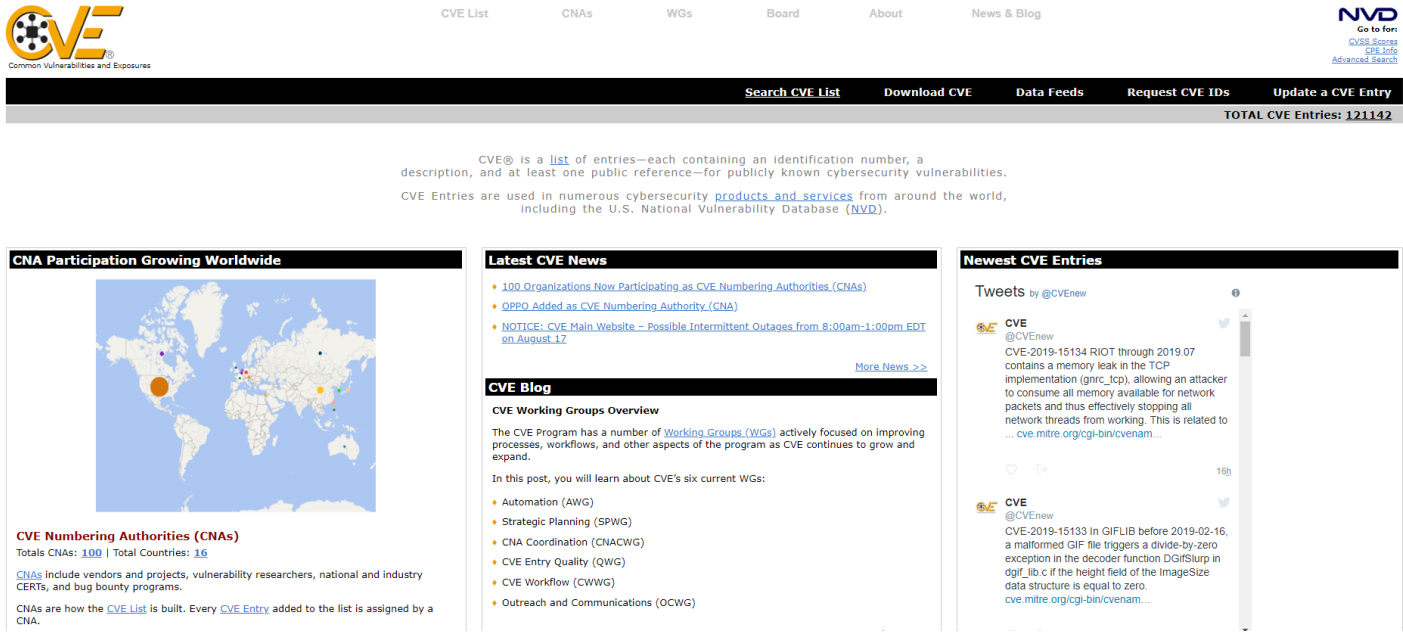
…and people… lots of people…

University of Victoria

Vulnerabilities

Identifying Vulnerabilities

- MITRE website (https://cve.mitre.org)
- CVE (common vulnerability & exposures)
- many other sources for vulnerability info



University of Victoria

Common Vulnerabilities & Exposures (CVE)

CVE List CNAs WGs Board About News & Blog

NVD
Go to for:
CVSS Scores
CPE Info
Advanced Search

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 121142

HOME > CVE > SEARCH RESULTS

Search Results

There are **81** CVE entries that match your search.

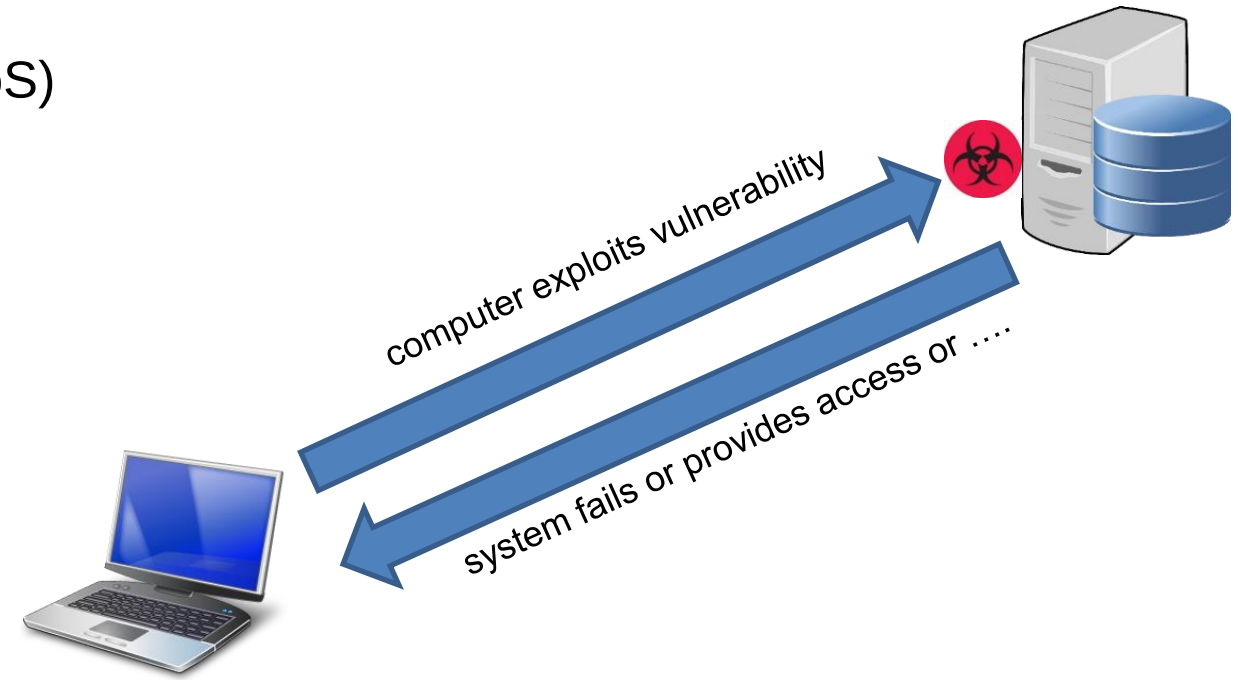
Name	Description
CVE-2018-1327	The Apache Struts REST Plugin is using XStream library which is vulnerable and allow perform a DoS attack when using a malicious request with specially crafted XML payload. Upgrade to the Apache Struts version 2.5.16 and switch to an optional Jackson XML handler as described here http://struts.apache.org/plugins/rest/#custom-contenttypehandlers. Another option is to implement a custom XML handler based on the Jackson XML handler from the Apache Struts 2.5.16.
CVE-2018-11776	Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 suffer from possible Remote Code Execution when alwaysSelectFullNamespace is true (either by user or a plugin like Convention Plugin) and then: results are used with no namespace and in same time, its upper package have no or wildcard namespace and similar to results, same possibility when using url tag which doesn't have value and action set and in same time, its upper package have no or wildcard namespace.
CVE-2017-9805	The REST Plugin in Apache Struts 2.1.1 through 2.3.x before 2.3.34 and 2.5.x before 2.5.13 uses an XStreamHandler with an instance of XStream for deserialization without any type filtering, which can lead to Remote Code Execution when deserializing XML payloads.
CVE-2017-9804	In Apache Struts 2.3.7 through 2.3.33 and 2.5 through 2.5.12, if an application allows entering a URL in a form field and built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL. NOTE: this vulnerability exists because of an incomplete fix for S2-047 / CVE-2017-7672.
CVE-2017-9793	The REST Plugin in Apache Struts 2.1.x, 2.3.7 through 2.3.33 and 2.5 through 2.5.12 is using an outdated XStream library which is vulnerable and allow perform a DoS attack using malicious request with specially crafted XML payload.
CVE-2017-9791	The Struts 1 plugin in Apache Struts 2.1.x and 2.3.x might allow remote code execution via a malicious field value passed in a raw message to the ActionMessage.
CVE-2017-9787	When using a Spring AOP functionality to secure Struts actions it is possible to perform a DoS attack. Solution is to upgrade to Apache Struts version 2.5.12 or 2.3.33.
CVE-2017-7672	If an application allows enter an URL in a form field and built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL. Solution is to upgrade to Apache Struts version 2.5.12.
CVE-2017-5638	The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.
CVE-2017-15707	In Apache Struts 2.5 to 2.5.14, the REST Plugin is using an outdated JSON-lib library which is vulnerable and allow perform a DoS attack using malicious request with specially crafted JSON payload.
CVE-2017-14589	It was possible for double OGNL evaluation in FreeMarker templates through Struts FreeMarker tags to occur. An attacker who has restricted administration rights to Bamboo or who hosts a website that a Bamboo administrator visits, is able to exploit this vulnerability to execute Java code of their choice on systems that run a vulnerable version of Bamboo. All versions of Bamboo before 6.1.6 (the fixed version for 6.1.x) and from 6.2.0 before 6.2.5 (the fixed version for 6.2.x) are affected by this vulnerability.
CVE-2017-12611	In Apache Struts 2.0.0 through 2.3.33 and 2.5 through 2.5.10.1, using an unintentional expression in a Freemarker tag instead of string literals can lead to a RCE attack.
CVE-2016-8738	In Apache Struts 2.5 through 2.5.5, if an application allows entering a URL in a form field and the built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL.
CVE-2016-6795	In the Convention plugin in Apache Struts 2.3.x before 2.3.31, and 2.5.x before 2.5.5, it is possible to prepare a special URL which will be used for path traversal and execution of arbitrary code on server side.
CVE-2016-4465	The URLValidator class in Apache Struts 2 2.3.20 through 2.3.28.1 and 2.5.x before 2.5.1 allows remote attackers to cause a denial of service via a null value for a URL field.
CVE-2016-4461	Apache Struts 2.x before 2.3.29 allows remote attackers to execute arbitrary code via a "%{}" sequence in a tag attribute, aka forced double OGNL evaluation. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-0785.

Impacts of Vulnerabilities

- Denial of Service (DoS), system crash, degradation
- remote code execution
- disclosure of information, information exposure
- unauthorized access, authentication by-pass
- elevation of privilege/privilege escalation

Exploiting a vulnerability

- service is open on a system
- vulnerability exists
- attacker exploits vulnerability
- attacker achieves goal (eg. DoS)



Process

- theoretical vulnerability is identified (eg. by researchers)
- exploit developed
- exploit released (or others get access to)
- exploit seen being used “in the wild”
- exploit being seen used against organization

University of Victoria

you choose… will you patch, mitigate, or be exploited?

Example

[Critical Citrix Flaw May Expose Thousands of Firms to Attacks]

Bleeping Computer

3 weeks ago

Unpatched Citrix Flaw Now Has PoC Exploits

Threatpost

3 days ago

[Proof-of-concept code published for Citrix bug as attacks intensify]

ZDNet

4 days ago

[Hackers probe Citrix servers for weakness to remote code execution vulnerability]

ZDNet

1 week ago

Attackers Are Scanning for Vulnerable Citrix Servers, Secure Now

Bleeping Computer

1 week ago

University of Victoria

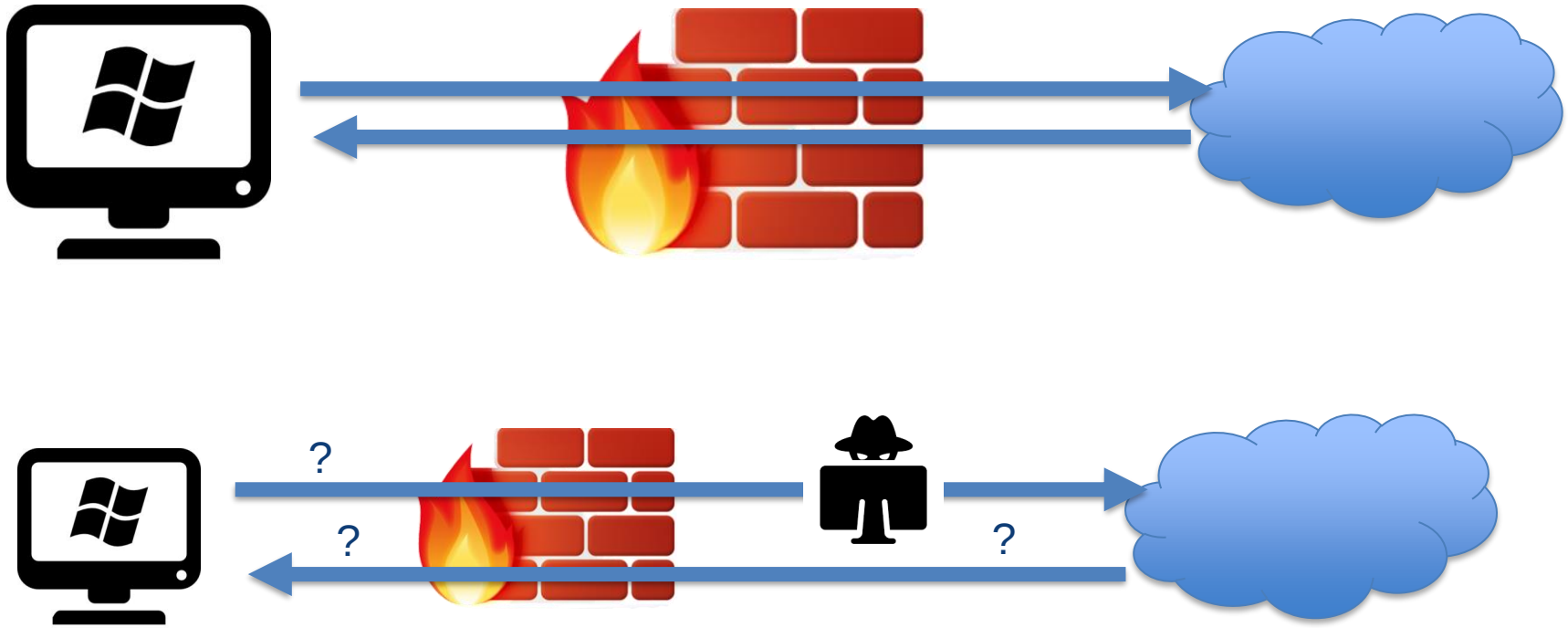
What to do about vulnerabilities…

- stay alert, pay attention to vendors
- patch them…. when a patch is available
- until then take steps to mitigate
- if can’t prevent then detect
- implement vendor workarounds
- restrict access
- implement IPS signatures

University of Victoria

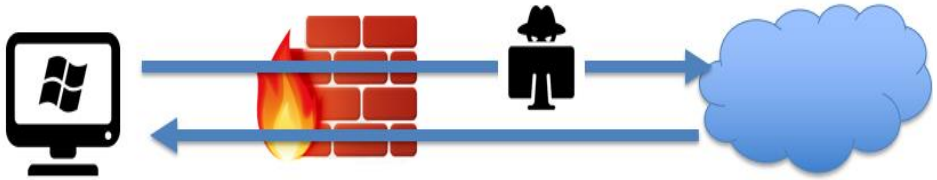
Types of Attacks

- Man-in-the-Middle (MITM)



Types of Attacks

- spoofing
  - TCP vs UDP
- wired, WiFi, wireless
  - tapping copper, fibre
  - intercepting WiFi, Pineapple
  - intercepting Wireless, IMSI Catchers,
  - Mobile Device Identifiers (MDIs), Stingrays, Radio/RAN
- host-based
  - physical, local – USB, hardware keyloggers
  - logical, remote



placement of MitM

University of Victoria

Types of Attacks

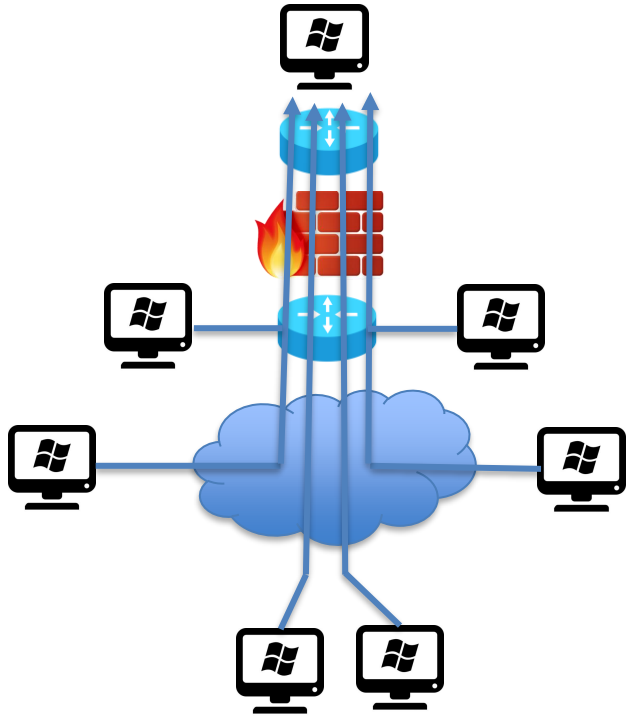
- virus — self-replicating program
- worm — self-sustaining running program
- trojan — program that does something other than it claims
- spyware — malware that enables surveillance
- exploit vulnerabilities to conduct
  - DoS (denial of service) and DDoS (distributed denial of service)
  - privilege escalation
  - remote code execution

Types of Attacks

- DDoS
  - volumetric/bandwidth attack sending more data than victim can accept
- Defacement
  - altering or replacing website
- Doxxing
  - revealing private information about a person publicly

Types of Attacks

- DDoS
  - distributed denial of service
  - multiple systems
  - high volume, high bandwidth
  - botnet, zombies
  - amplification attack
- Response
  - enable anti-spoofing if relevant
  - block traffic originating from places it shouldn't
  - if pattern then local ACL, call service provider for ACL upstream
  - on-premise anti-DDoS, cloud anti-DDoS (scrubbing)
  - blackhole source(s), destination(s), remove target



ACL = access control list

Types of Attacks

- ping flood — large volume or large size or both
- ping of death — size >65,535 when re-assembled
- SYN flood — syn, syn, syn, syn… w/o ACK
- UDP flood — fire and forget, large volume
- smurf — spoof IP of victim – ICMP/ping a bunch of hosts
- fraggle — spoof IP of victim – send UDP traffic to router's broadcast
- teardrop — jumbled packets – IP, 1 too small (also NewTear)
- land 

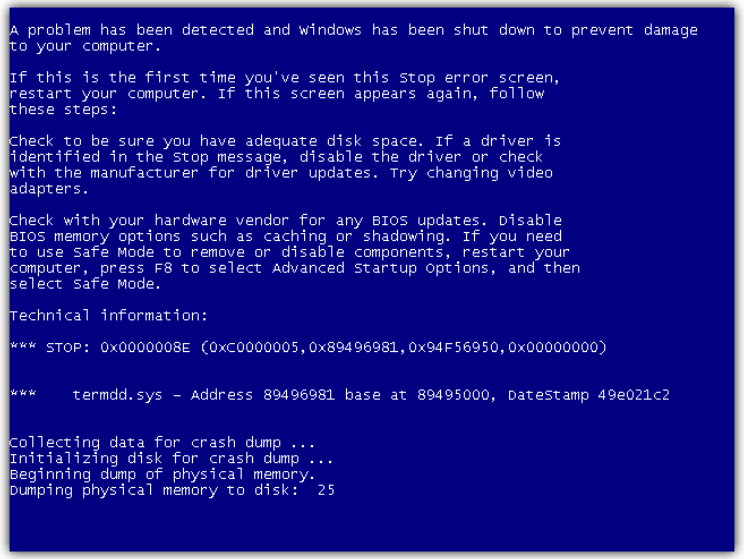
source and destination ports the same, causing loop

University of Victoria

Types of Attacks

- bonk — fragments of packets to port 53 can’t assemble
- boink — same as bonk but multiple ports
- jolt, ssping — similar just larger packets
- pepsi — udp flood with varied sources aimed at certain ports
- jizz — DNS spoofing, false caching
- ICMP nukes — send packets the destination OS can’t handle

  eg. OOB -> port 139 on Win 98 -> BSOD



University of Victoria

Types of Attacks

- buffer, heap, stack overflow
  - exceeding amount of data that can be received without problems
- ARP poisoning
  - sending illegitimate messages on the network to take over an IP address
- BGP hijacking (fake Border Gateway Protocol broadcasts)
  - China
  - Cryptocurrency
  - Google traffic through Russia

SQL

- lab is in Week 10
- important to know how databases work to understand SQL injection
- creating the database
  - mysql –u <user> -p
  - create database buysell;
  - use buysell;
  - create table users (username varchar(25), password varchar(25), name varchar(25), email varchar(25));
  - desc users;

Field	Type	Null	Key	Default	Extra
username	varchar(25)	YES		NULL	
password	varchar(25)	YES		NULL	
name	varchar(25)	YES		NULL	
email	varchar(25)	YES		NULL	

SQL

- adding, updating, and deleting rows in the database:
  - insert into users (username,password,name,email) values ('lskywalker','chewbacca','Luke Skywalker','lskywalker@starwars.ca’);
  - select * from users where username like “lsky%”;
  - update users set password=“chewie” where username=“lskywalker”;
  - delete from users where username=“lskywalker”;

SQL

Other examples:

- select * from users order by email asc;
- select * from users where username not like “lsky%”;
- select * from users where username!=“lskywalker”
- drop table users;
- alter table users modify email varchar(25);

SQL

Example:

select * from users where username=“lskywalker” and password=“chewbacca“;

could become

select * from users where username=“” **or “1=1”;**
or
select * from users where username=“”; **drop table users;**

University of Victoria

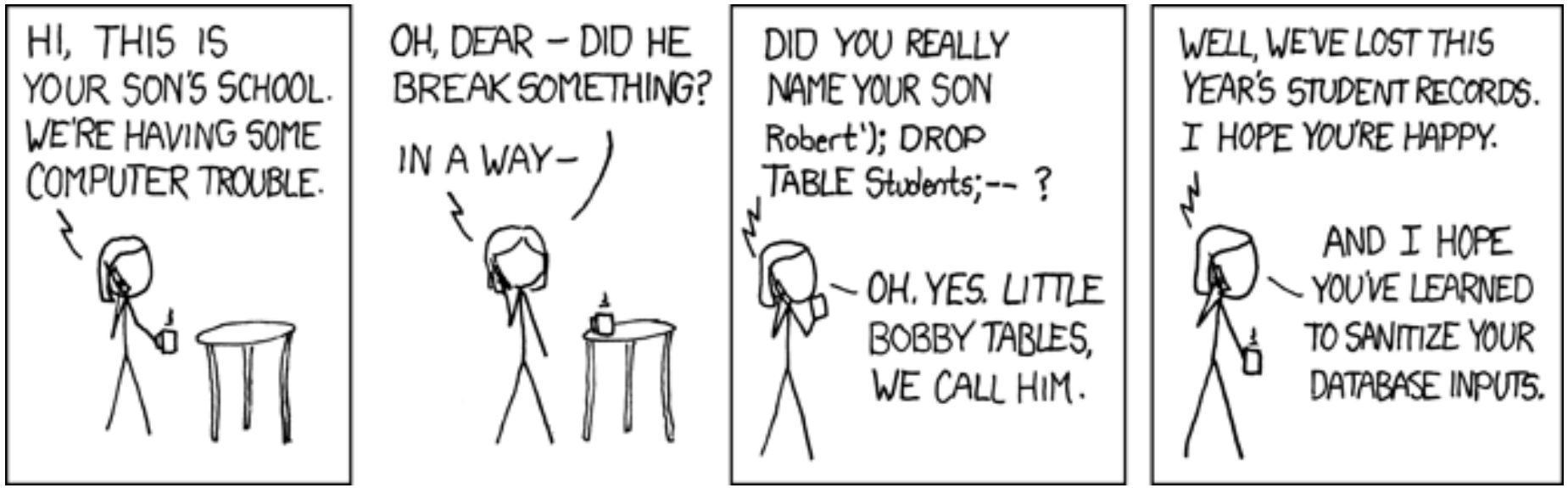
SQL Injection

- SQL injection (exploiting lack of error checking injecting additional SQL commands to input)

Logon page that shows an SQL injection string

SQL Injection

Little Bobby Tables



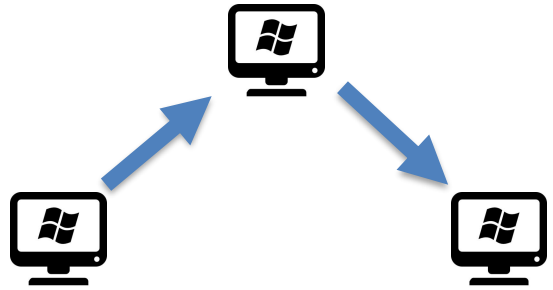
https://xkcd.com/327/

University of Victoria

SQL Injection (attempt?)

Types of Attacks

- reflection — spoof IP, send request, response goes to victim
- amplification — attacker ensures more traffic hits victim than attacker can send alone
- browser hijack — change home page, search, toolbars
- backdoors — covert method of bypassing authentication and gaining access to a system
- rootkits — program enables access to computer and masks existence
- password attacks — dictionary attacks, brute force, rainbow tables



University of Victoria


University
of Victoria

Types of Attacks

- social engineering — psychological manipulation of people into performing actions or divulging confidential info
- phishing, smishing, vishing — fraudulent attempt to obtain information over email, SMS, voice
- spearphishing — targeted phishing
- whaling — phishing targeted at executive
- zero day exploits — attack involving previously unknown vulnerability
- cross-site scripting — inject scripts into websites
- malvertising — displaying infected ads on legitimate websites
- waterholing — infecting a site that users are likely to visit

Securing the Humans

- tailgating / piggybacking
- shoulder surfing
- dumpster diving
- URL shorteners
- QR codes

…you don’t know where they go!

https://bit.ly/33G9wOP

University of Victoria

Example: https://web-capture.net/

Examples (not tested)

- Melissa
  - MS Word macro
  - disabled safeguards, lowered security settings
  - spread via infected email, sent to top 50 contacts
  - $1.2B damage
- ILoveYou
  - spread through email attachment
  - filename was Love-letter-for-you.txt.vbs (vbs didn’t show)
  - sent to all contacts, changed home page
  - stole passwords and sent to attacker
  - 10% of computers infected, $15B damage in Y2000

Examples (not tested)

- Code Red
  - buffer overflow, overwrote memory with instructions for virus
  - compromised system and instructions varied based on day of month
  - 1-19th target random IPs; 20th – 28th launch DDoS on White House, 29^{th+} sleep mode
  - 1-2 million infected, $2B damage

- Nimda
  - origin of the name, when it was released, rumours
  - compromised system, spread through variety of ways (email, network, vulnerabilities)
  - $635 million damage, over 2 million infected in 24 hours

Examples (not tested)

- SQL Slammer/Sapphire
  - spread via buffer overflow in MS SQL
  - infected random IPs after creating millions of copies
  - $750 million damage, significant impact on government, banks, 911
- Sasser ($500 million in damage)
  - exploited vulnerability in LSASS (local security authority subsystem service)
  - scanned until found a vulnerable IP
  - uploaded to Windows directory; target infected upon next reboot
- MyDoom
  - spread through KaZaa and emails; initiated DDoS, install backdoor
  - searched for email addresses, forged from address
  - 6-700k infected, $38 billion in damage

University of Victoria

Examples (not tested)

- Conficker
  - spread by infected USB drives over networks
  - disabled anti-malware; created backdoors
  - confusion regarding what it was intended to do on April 1, 2009
  - $9.1B damage with impact to government, military

Examples

- HeartBleed
  - OpenSSL, tricking servers into leaking information affecting CRA
- ShellShock
  - bash vulnerability
- Poodle (Padding Oracle on Downgrading Legacy Encryption)
  - MitM exploits fallback to SSL 3.0
- Freak (Factoring RSA Export Keys)
- Beast (Browser Exploit Against SSL/TLS)
  - exploited weak encryption
- Drown
  - attacks servers by using support for obsolete, insecure SSL v2

Examples

- **Stuxnet**
  - targeted Siemens, modified PLCs only used in Iran nuclear treatment plant
  - “world’s first digital weapon”
  - spun up Iranian centrifuges, disabled safety monitoring
  - attribution

To get Stuxnet to its target machines, the attackers first infect computers belonging to five outside companies that are believed to be connected in some way to the nuclear program. The aim is to make each "patient zero" an unwitting carrier who will help spread and transport the weapon on flash drives into the protected facility and the Siemens computers.

https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

Examples

- **Duqu**
  - very similar, digitally signed, information gathering/KL
  - MS Word dropper, download malware, execute payload
- **Flame** (most complex malware at the time of discovery)
  - information gathering, pretends to be Windows update proxy
- **Gauss**
  - information stealer – based on Flame

Stuxnet and Duqu same, Flame and Gauss similar

University of Victoria

Examples

- Cryptolocker (2013)
  - zip file with executable looks like PDF
- Cryptowall (2014)
  - ransomware through spam, malvertising
- Cerber (2016)
  - 150k devices, $195k ransom
- Locky (2016)
  - email fake invoice, tricks to enable macros, encrypts
- Wannacry (2017)
  - leveraged SMB vulnerability; 200k victims
- NotPetya (2017)
  - leveraged SMB vulnerability, infects MBR, encrypts MFT; $593 million (Merck)

- how ransomware works
- how to prevent
  - security awareness
  - patching
  - backups
  - email security
  - endpoint security

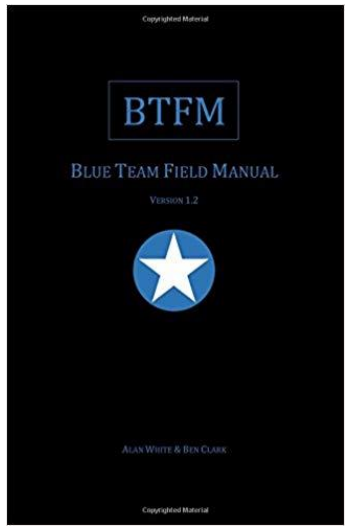
University of Victoria

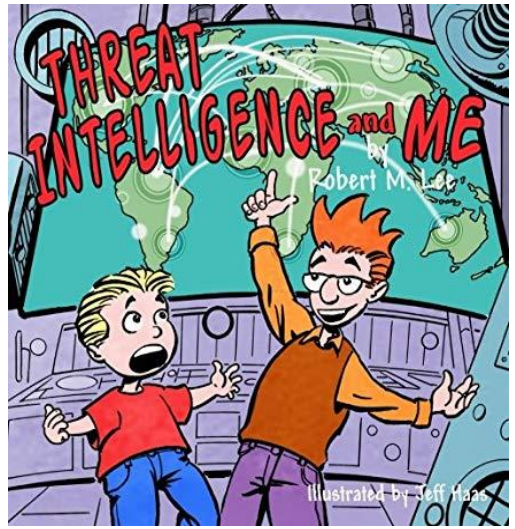
Summary

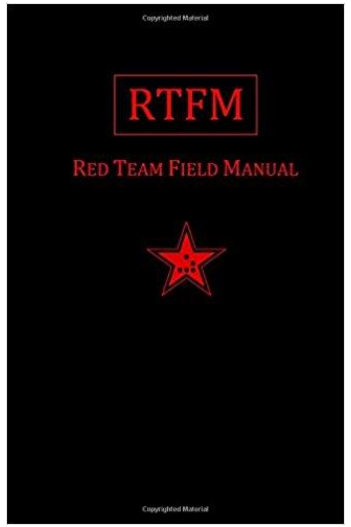
- compromised machines can never be trusted
- must permanently remove all traces
- best way to do this is to “flatten the system” and format and reinstall
- some infections can survive this process

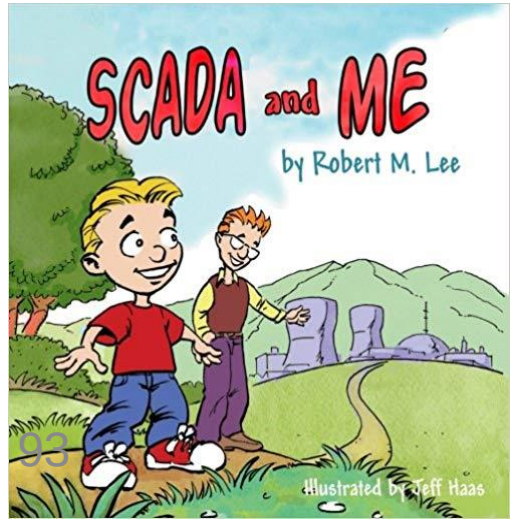
Prevention

- blue team
  - defenders, preventive
  - harden systems
- red team
  - attackers, external, blind
  - goal is to compromise the organization
- purple team
  - single group that does blue and red team
  - attacks and defends









University of Victoria

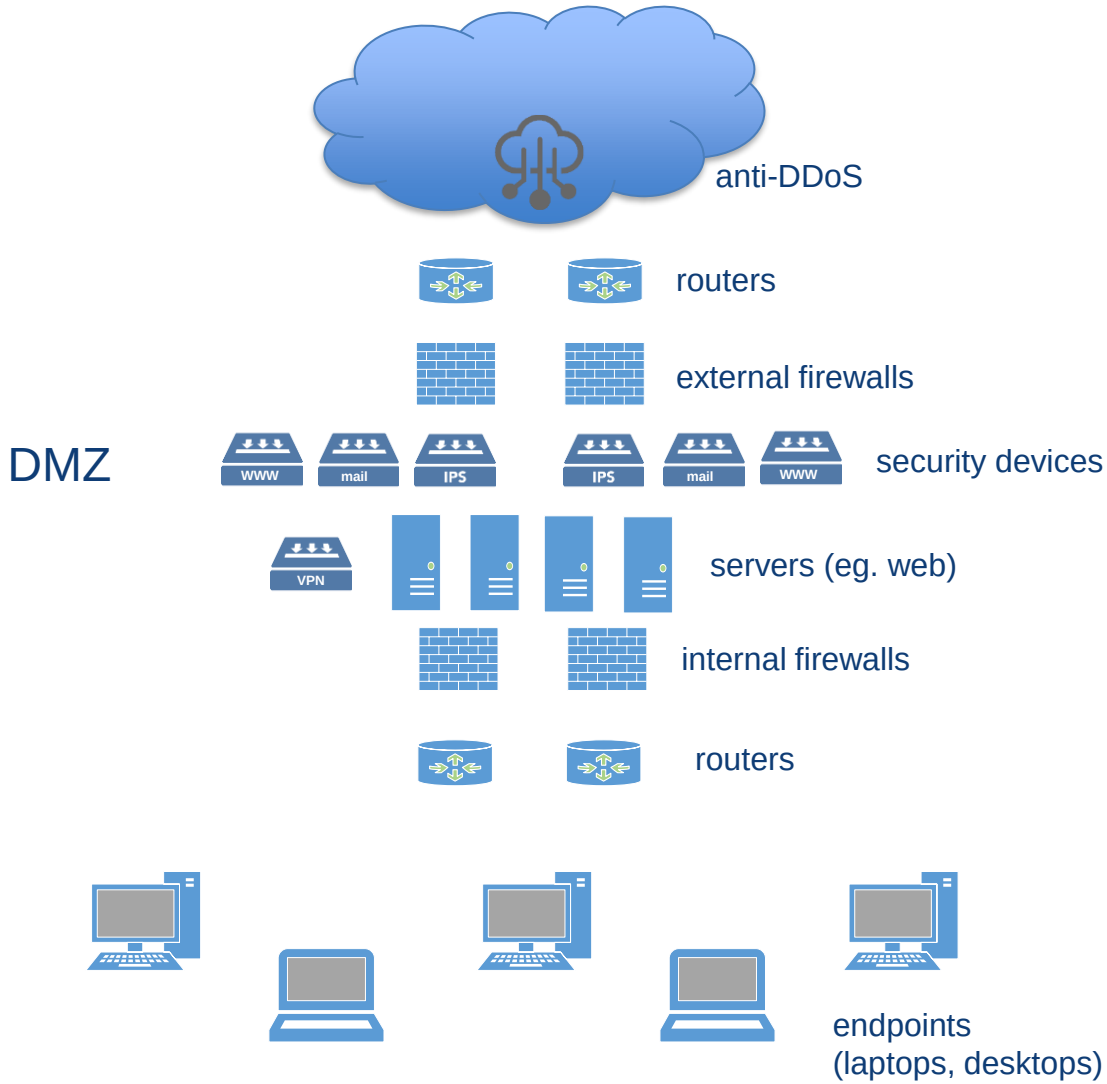
Prevention

- anti-DDoS (on-prem, cloud)
- firewall (packet filtering, stateful, NG)
- intrusion detection/prevention (HIDS, NIDS)
- web content filtering
- email content filtering
- SIEM
- VPN (client-to-site vs site-to-site; IPSec vs SSL)
- anti-malware

Sample Network Diagram

- simplified network diagram
- security stack
- DMZ
- direction of traffic
- redundancy & availability

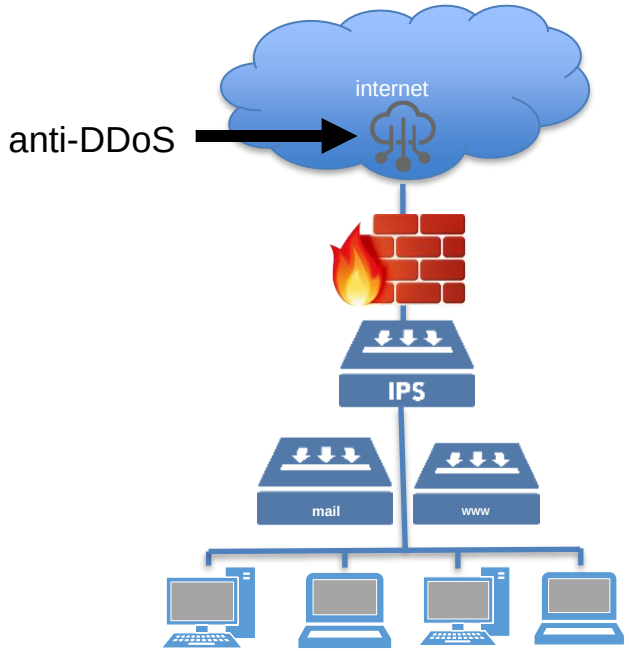
other topics
- impact of device placement (eg. IPS)
- impact of encrypted traffic
- naming conventions (eg. bcfw01.acme.com)



University of Victoria

Anti-DDoS

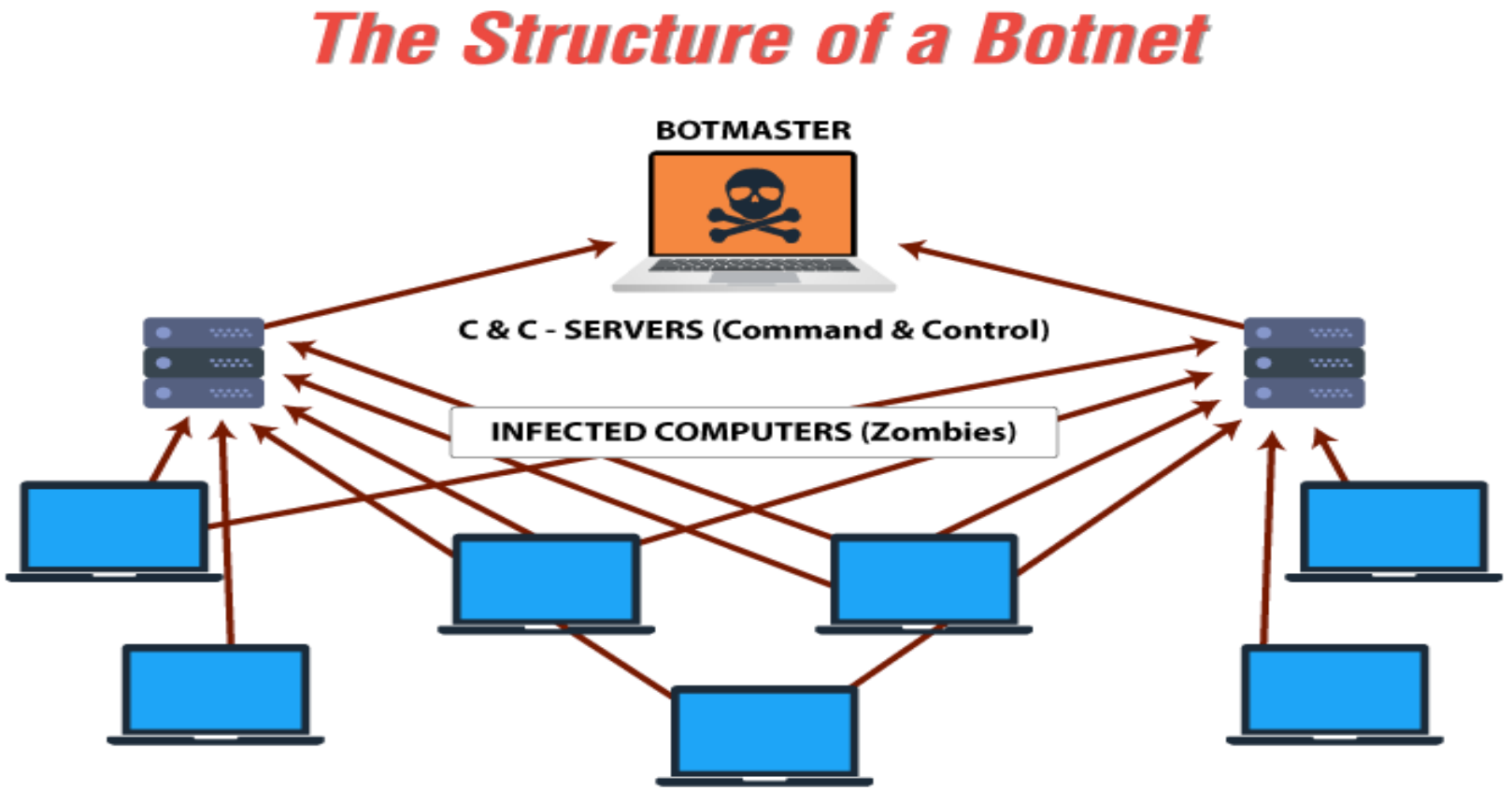
- prevents or mitigates high volume attacks
- types
  - on-prem may be effective up to amount of bandwidth
  - cloud redirect malicious traffic to scrubbing centre
- methods
  - manual human detects, human responds
  - hybrid human decides to invoke automated controls
  - automatic tools detect and respond



Considerations
- anti-spoofing
- reflection, amplification attacks

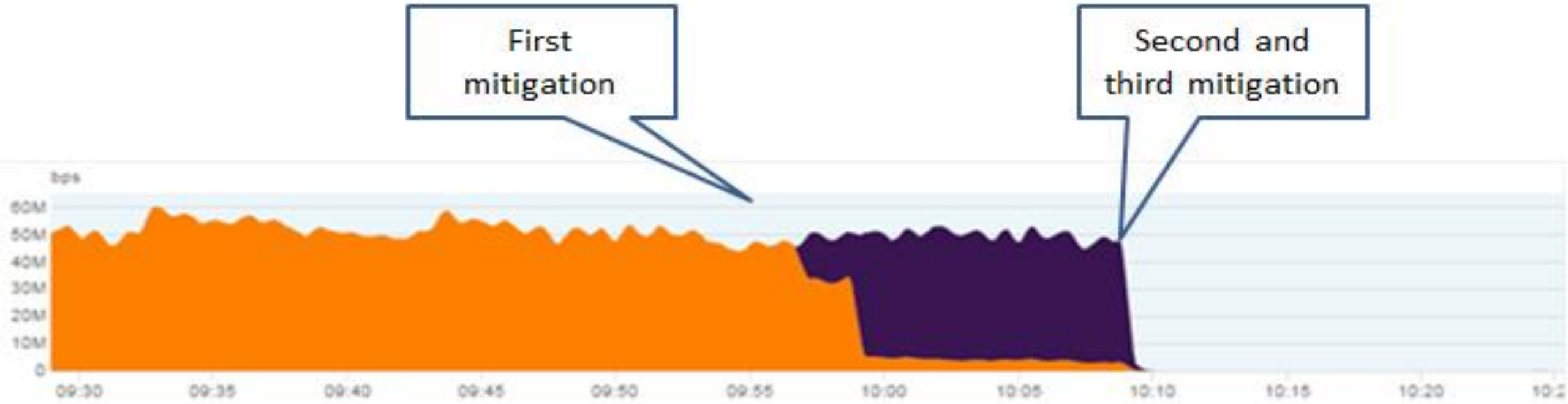
University of Victoria

Anti-DDoS



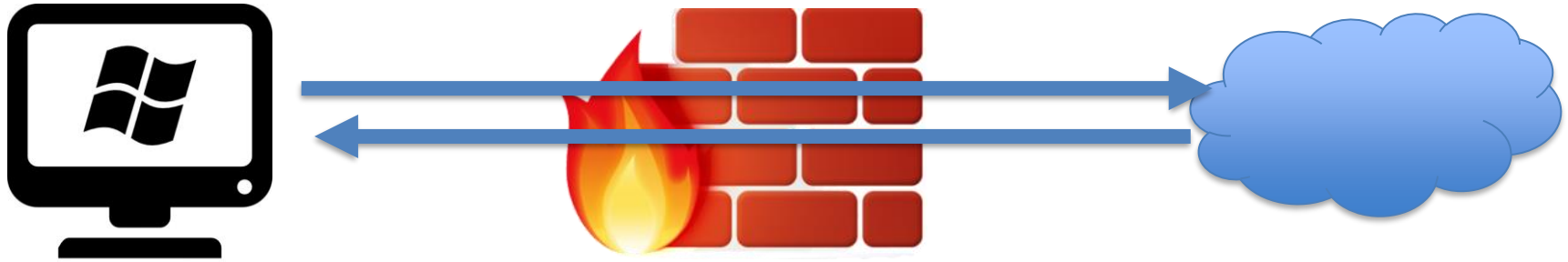
University of Victoria

Anti-DDoS

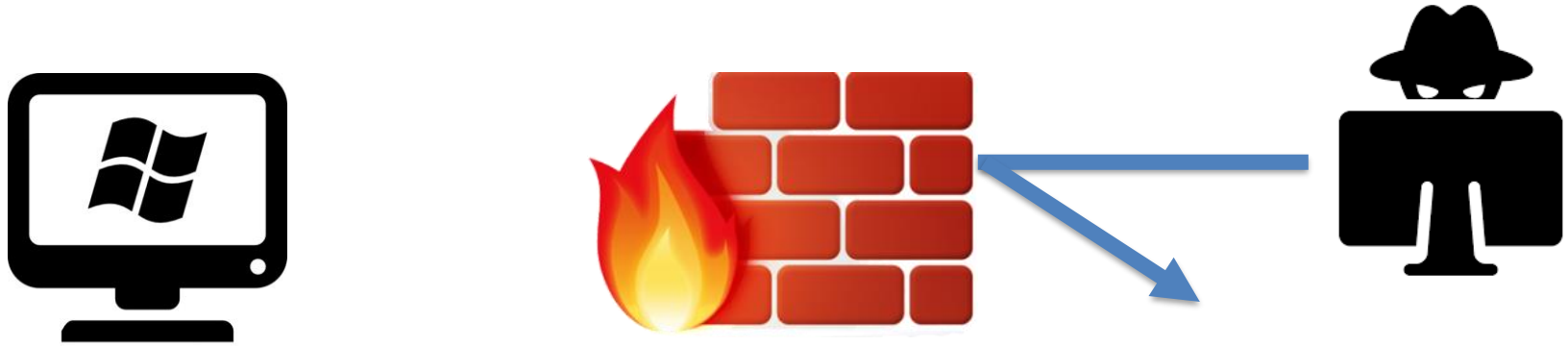


Key	Graph	Category	Bytes Blocked	bps Blocked	Packets Blocked	pps Blocked
		Spoofed SYN Flood Prevention	11.64 GB	25.87 Mbps	286.17 M packets	79.49 kpps
		Blacklisted Hosts	3.73 GB	8.29 Mbps	91.63 M packets	25.45 kpps
		ICMP Flood Detection	352.19 kB	782.63 bps	4.72 k packets	1.31 pps
		TCP SYN Flood Detection	215.48 kB	478.84 bps	721 packets	0.20 pps

Firewall

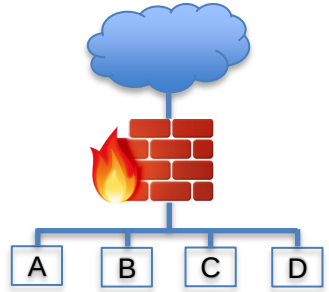


5-tuple: source IP/port, destination IP/port, protocol



Firewall

- different types
  - circuit-level (operates at transport/session)
  - packet-filtering (examines each packet)
  - stateless (does not track state, packet streams)
  - stateful (aware if packet is part of a larger stream, sometimes called shallow packet inspection)
  - application (operates at application layer, deep packet inspection)
  - next generation NG (combines intrusion prevention and more)



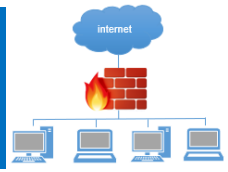
- determines whether packets should be permitted through
  - fundamentally rules are source, destination, port, action
  - start with a “cleanup rule” of “any – any – drop”
  - add exceptions above

Security | Address Translation | SmartDefense | VPN Manager | Desktop Security

NO.	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	Linux-racoon	cpmodule	Any Traffic	ICMP echo-request UDP IKE ?? ESP	accept	Log	Policy Targets	Any	IKE/ESP and ping
2	Net-172.16.1.0	Net-172.16.2.0	MyIntranet	Any	accept	Log	Policy Targets	Any	from local to remote
3	Net-172.16.2.0	Net-172.16.1.0	MyIntranet	Any	accept	Log	Policy Targets	Any	from remote to local
4	Any	Any	Any Traffic	NBT TCP microsoft-ds	drop	None	Policy Targets	Any	There are always some W* hosts around...which shouldn't fill the log
5	Any	Any	Any Traffic	Any	drop	Log	Policy Targets	Any	Drop all other traffic

University of Victoria

Firewall Ruleset Sample



Firewall Ruleset Sample

#	Source	Dest	Service	Action	Track
1	Bad People	Any	Any	Drop	No log
2	24.112.86.55	24.110.83.93	25565	Allow	Log
3	123.42.56.107	24.110.83.92	http/80 & https/443	Allow	Log
4	23.73.51.95	24.110.83.93	Any	Drop	Log
5	Any	Any	telnet/23	Drop	Log
6	23.73.51.95	24.110.83.92	Any	Drop	Log
7	Any	Any	Any	Drop	Log

University of Victoria

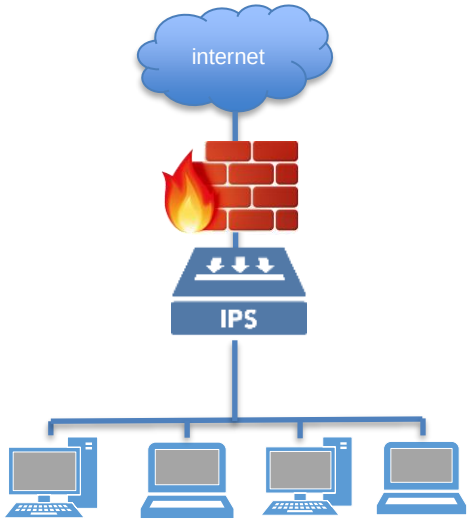
Firewall Ruleset Sample

#	Source	Dest	Service	Action	Track
1					
2					
3					
4					
5					
6					
7					

University of Victoria

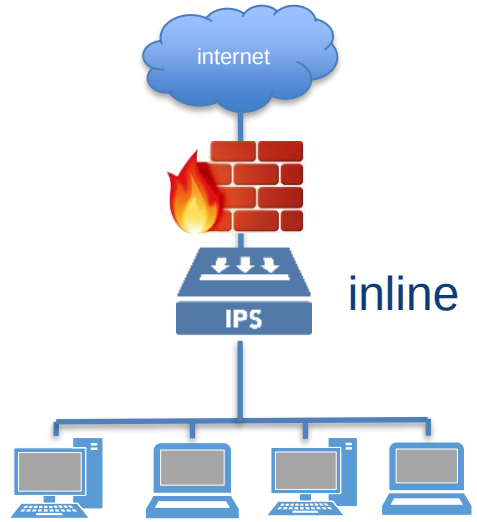
Intrusion Detection/Prevention

- two types
  - intrusion detection (only detects and notifies regarding intrusions)
  - intrusion prevention (detects and stops intrusions)
- two types (same as firewalls)
  - host-based IPS (on the host)
  - network-based IPS (on the network)
    - can be in-line or off a tap
    - can fail open or fail closed
- detection methods
  - signature-based
    - compare traffic against known attack patterns
  - anomaly based
    - create **baseline** of normal activity and identify deviations.. **anomalies**

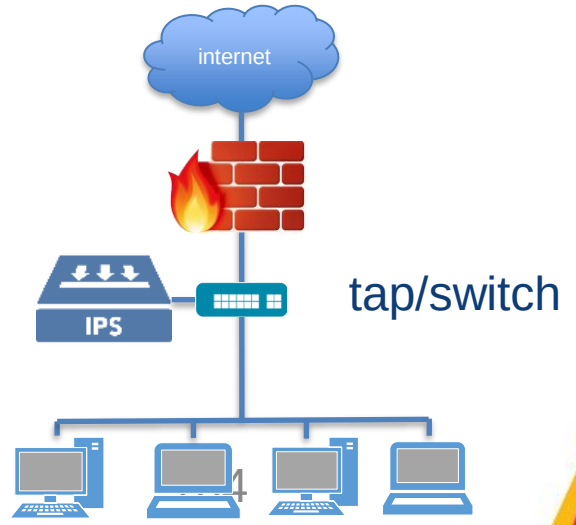


Intrusion Detection/Prevention

- positioning of security gear
  - do you put the IDS/IPS, for example, in-line or on a tap
  - what are the pros/cons
  - if the system is malfunctioning do you want it to fail open or closed?
  - firewall should fail closed
  - others it's up to the risk appetite of the organization



inline

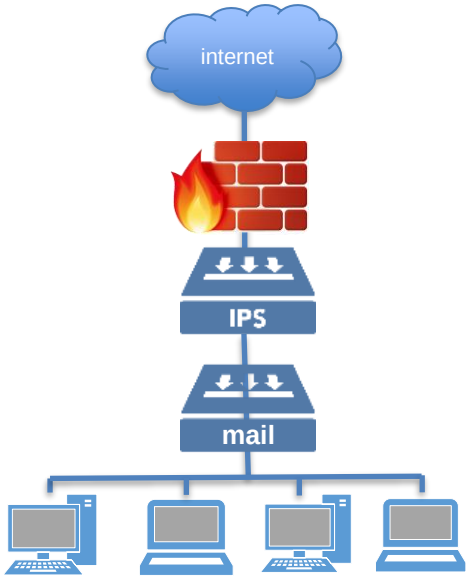


tap/switch

University of Victoria

Email Content Filtering

- determines whether emails should be let through
- focuses on matching
  - source IP address
  - source email address
  - destination email address
  - email content
  - email attachment
  - …others
- also consider whitelisting/blacklisting, SPF, DKIM, DMARC



University of Victoria

Example: Telnet

Email Content Filtering

- rate of effectiveness
- first check can be blacklist/whitelist
- second check can be reputation-based
  - low score means no connection allowed
  - could be rate-limited or prevented
  - earn negative reputation, earn positive
- third check can be anti-spam, anti-malware

University of Victoria

Email Content Filtering

- RBL = realtime blackhole list
  - how do you get on? get off?
- SPF = sender policy framework
  - identifies which IP addresses should be permitted to send email for your domain
  - does your organization have a record?
  - does your organization factor in SPF? enforce?

University of Victoria

also

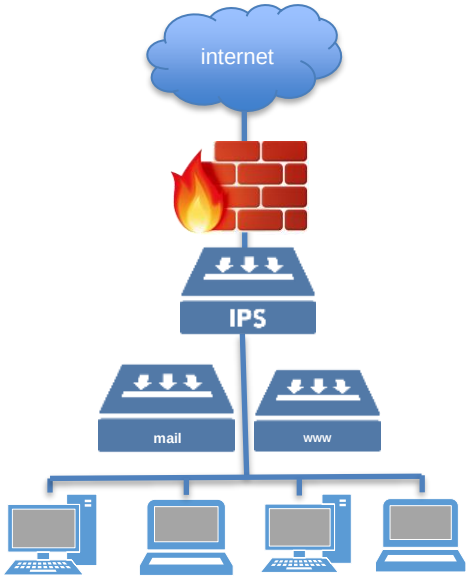
DKIM = Domain Keys Identified Mail

DMARC = Domain Message Authentication Reporting

Web Content Filtering

- lets companies pick which sites and categories are allowed
- how do you decide what sites to block?

Alcohol & Tobacco
Anonymizer
Art / Culture
Blogs / Personal Pages
Botnets
Browser Plugin
Browser Toolbar
Business / Economy
Child Abuse
Cloud Services
Computers / Internet
Cryptocurrency
Download Manager
Education
Email
Encrypts communications
Entertainment
Fashion
File Storage and Sharing
File Upload
Financial Services
Friendster Widgets
Gambling
Games
General
Google Plus Widgets
Government / Military
Greeting Cards
Hacking
Hate / Racism
Health
High Bandwidth
IPTV
Illegal / Questionable
Illegal Drugs
Inactive Sites
Instant Chat
Instant Messaging
Job Search / Careers
Lifestyle
Lingerie and Swimsuit
LinkedIn Widgets
Marijuana
Media Sharing
Media Streams
Microsoft & Office365
Mobile Software
MySpace Widgets
Nature / Conservation
Network Protocols
Network Utilities
News / Media
Newsgroups / Forums
Ning.com Widgets
Non-profits & NGOs
Nudity
P2P File Sharing
Personals / Dating
Phishing
Political / Legal
Pornography
Real Estate
Recreation
Religion
Remote Administration
Restaurants / Dining / Food
SCADA Protocols
SMS Tools
Search Engines / Portals
Sex
Sex Education
Shopping
Social Networking
Social Plugins
Software Downloads
Software Update
Spam
Sports
Spyware / Malicious Sites
Stealth Tactics
Suspicious Content
Tasteless
Translation
Travel
Twitter Clients
URL Filtering
Uncategorized
Vehicles
Video Conferencing
Violence
Virtual Worlds
VoIP
Weapons
Web Advertisements
Web Browser
Web Browser Acceleration
Web Conferencing
Web Content Aggregators
Web Services Provider
Web Spider



University of Victoria

Web Content Filtering

- enables employers to determine which sites and categories of sites will and won’t be permitted
- ensure you have an appropriate use policy, information security policy, or other code of conduct document
- which sites do you block? how do you decide?

University of Victoria

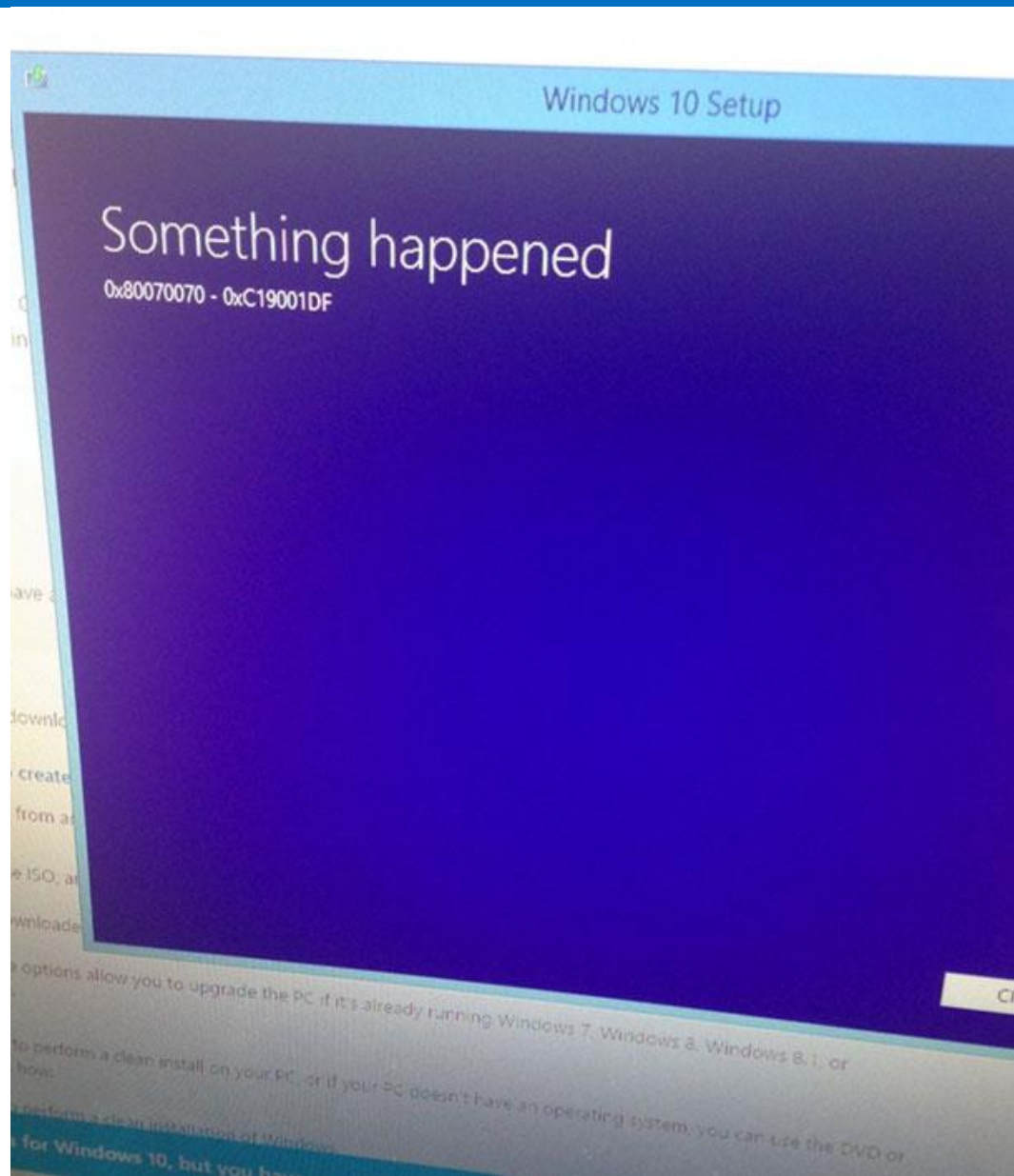
Web Content Filtering

Alcohol & Tobacco
Anonymizer
Art / Culture
Blogs / Personal Pages
Botnets
Browser Plugin
Browser Toolbar
Business / Economy
Child Abuse
Cloud Services
Computers / Internet
Cryptocurrency
Download Manager
Education
Email
Encrypts communications
Entertainment
Fashion
File Storage and Sharing
File Upload
Financial Services
Friendster Widgets
Gambling
Games
General
Google Plus Widgets
Government / Military
Greeting Cards
Hacking
Hate / Racism
Health
High Bandwidth
IPTV
Illegal / Questionable
Illegal Drugs
Inactive Sites
Instant Chat
Instant Messaging
Job Search / Careers
Lifestyle
Lingerie and Swimsuit
LinkedIn Widgets
Marijuana
Media Sharing
Media Streams
Microsoft & Office365
Mobile Software
MySpace Widgets
Nature / Conservation
Network Protocols
Network Utilities
News / Media
Newsgroups / Forums
Ning.com Widgets
Non-profits & NGOs
Nudity
P2P File Sharing
Personals / Dating
Phishing
Political / Legal
Pornography
Real Estate
Recreation
Religion
Remote Administration
Restaurants / Dining / Food
SCADA Protocols
SMS Tools
Search Engines / Portals
Sex
Sex Education
Shopping
Social Networking
Social Plugins
Software Downloads
Software Update
Spam
Sports
Spyware / Malicious Sites
Stealth Tactics
Suspicious Content
Tasteless
Translation
Travel
Twitter Clients
URL Filtering
Uncategorized
Vehicles
Video Conferencing
Violence
Virtual Worlds
VoIP
Weapons
Web Advertisements
Web Browser
Web Browser Acceleration
Web Conferencing
Web Content Aggregators
Web Services Provider
Web Spider

University of Victoria

Logging

- all of these platforms generate logs
- can log locally or remotely
- can log decentralized or centralized
- centralized provides visibility to variety of platforms
- common basic logging platform is ‘syslog’
- includes where the logs came from – hostname or IP
- timestamp – important to have common time
- then ensure sufficient level of detail in the logs to know who did what when
- ensure you are able to identify ‘events of interest’
  - eg. anomalies, intrusions, unauthorized access, unauthorized changes, other violations



University of Victoria

Security Logs (certification)

- firewall

2020-01-01 22:00:32 ALLOW TCP 192.168.0.1:45137 207.194.28.62:80 1532 0 1 SEND
2020-01-01 22:00:33 DENY TCP 54.12.34.15:45137 207.192.168.0.5:25 332 0 1 SEND
2020-01-01 22:00:35 ALLOW TCP 192.168.0.1:35437 207.194.28.62:80 7531 0 1 SEND
2020-01-01 22:00:38 DENY UDP 67.82.41.2:31337 192.168.0.123:54321 534 0 1 SEND

- IPS/IDS

Jan 19 16:18:40 HOST_SNORT snort: [116:55:1] (snort_decoder): Truncated Tcp Options {TCP} AAA.BBB.CCC.DDD:80 -> AAA.BBB.CCC.DDD:1589
Jan 19 16:18:40 HOST_SNORT snort: [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING {TCP} AAA.BBB.CCC.DDD:23564 -> AAA.BBB.CCC.DDD:80
Jan 19 16:18:40 HOST_SNORT snort: [1:2307:1] WEB-PHP PayPal Storefront arbitrary command execution attempt [Classification: Web Application Attack] [Priority:1]: {TCP} AAA.BBB.CCC.DDD:55023 -> AAA.BBB.CCC.DDD:80
Jan 19 16:18:40 HOST_SNORT snort: [119:7:1] (http_inspect) IIS UNICODE CODEPOINT ENCODING {TCP} AAA.BBB.CCC.DDD:55053 -> AAA.BBB.CCC.DDD:80
Jan 19 16:18:40 HOST_SNORT snort: [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING {TCP} AAA.BBB.CCC.DDD:49065 -> AAA.BBB.CCC.DDD:80
Jan 19 16:18:41 HOST_SNORT snort: [119:14:1] (http_inspect) NON-RFC DEFINED CHAR {TCP} AAA.BBB.CCC.DDD:49082 -> AAA.BBB.CCC.DDD:80
Jan 19 16:18:41 HOST_SNORT snort: [1:2003:2] MS-SQL Worm propagation attempt[Classification: Misc Attack] [Priority: 2]: {UDP} AAA.BBB.CCC.DDD:10000 -> AAA.BBB.CCC.DDD:1434
Jan 19 16:18:43 HOST_SNORT snort: [1:483:2] ICMP PING CyberKit 2.2 Windows [Classification: Misc activity] [Priority: 3]: {ICMP} AAA.BBB.CCC.DDD -> AAA.BBB.CCC.DDD

Security Logs (certification)

- proxy logs

172.29.10.1, James, -, Y, 2/4/96, 8:22:56, SERVERNAME, PROXYNAME, -, www.yahoo.com, -, 80, 5277, 4792, 890, http, TCP, GET, http://www.yahoo.com/, TEXT/HTML, Inet, 200, -
172.29.10.1, James, -, Y, 2/4/96, 8:22:58, SERVERNAME, PROXYNAME, -, www.cnn.com, -, 80, 401, 5501, 1104, http, TCP, GET, http://www.cnn.com, IMAGE/GIF, VCache, 304, -
172.29.10.1, James, -, Y, 2/4/96, 8:22:59, SERVERNAME, PROXYNAME, -, www.atw.fullfeed.com, -, 80, 471, 3280, 1104, http, TCP, GET, http://www.atw.fullfeed.com/atw/gfx/ispcdeco.gif, IMAGE/GIF, VCache, 304, -
172.29.10.1, James, -, Y, 2/4/96, 8:22:59, SERVERNAME, PROXYNAME, -, www.atw.fullfeed.com, -, 80, 231, 638, 1094, http, TCP, GET, http://www.atw.fullfeed.com/atw/gfx/www.gif, IMAGE/GIF, VCache, 304, -
172.29.10.1, James, -, Y, 2/4/96, 8:22:59, SERVERNAME, PROXYNAME, -, www.atw.fullfeed.com, -, 80, 371, 4745, 1112, http, TCP, GET, http://www.atw.fullfeed.com/atw/gfx/intouch-icon.gif, IMAGE/GIF, VCache, 304, -

- antivirus logs

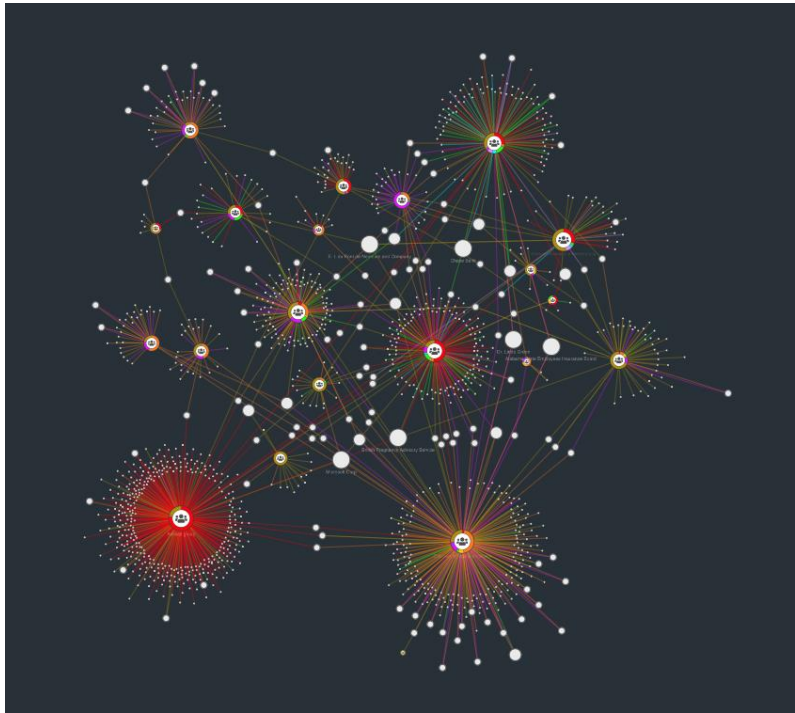
Date, Location, Malware Name, Action, Status, Alert

12/3/2019 08:30:00, c:\windows\system32\driver.exe, Trojan.Backdoor, Quarantine, Success
12/3/2019 08:30:00, c:\progra~1\flash\file.dll, Unwanted Application, Ask, Success
12/3/2019 08:30:00, c:\temp\ssaver.scr, BrowserHijack, Detect, Success
12/3/2019 08:30:00, c:\users\john\downloads\attachment.pdf, Adware, Quarantine, Success
12/3/2019 08:30:00, c:\windows\test.bat, HackTool, Detect, Success

- netflow data

Date flow start	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Pkts	Bytes	Flows
2010-09-01 00:00:00.459	0.000	UDP	127.0.0.1:24920	->	192.168.0.1:22126	1	46	1
2010-09-01 00:00:00.363	0.000	UDP	192.168.0.1:22126	->	127.0.0.1:24920	1	80	1

University of Victoria



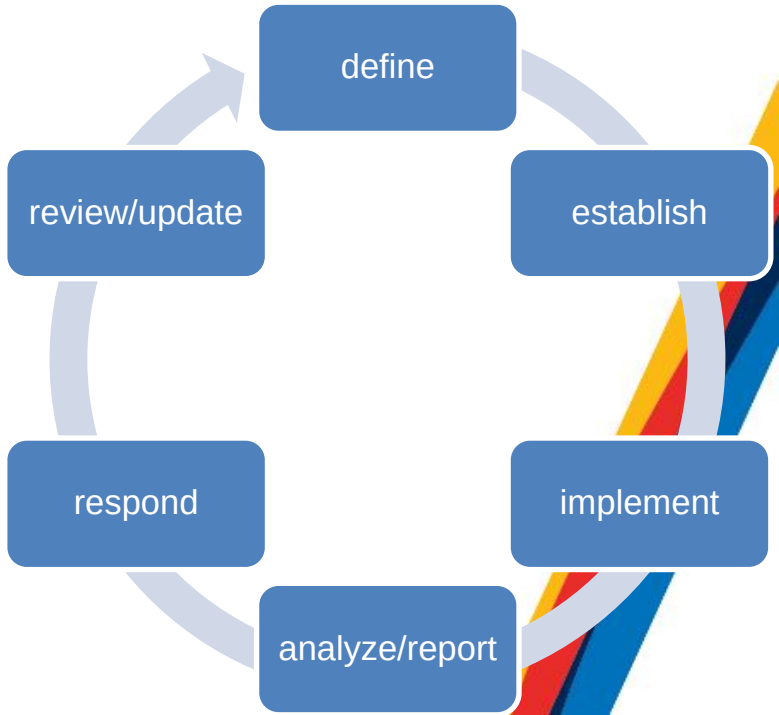
Helps to be able to visualize and analyze data (eg. Gephi)

Monitoring

- common to monitor up/down of systems and whether they are functioning
- are you monitoring for security events as well?
- tricky to determine what is permitted vs. not as there are often exceptions to rules

  eg. users shouldn't be deleted – but sysadmins have to delete
  when the user is no longer employed
- one example you always want to be alerted on is disabling logs
- also consider file integrity monitoring – good to know when certain files change
- sensitivity
  - false positive: something detected as bad and it's not (type 1 error)
  - false negative: something not detected as bad and it is (type 2 error – dangerous)
  - true positive: something detected as bad and it is
  - true negative: something not detected as bad and it's not

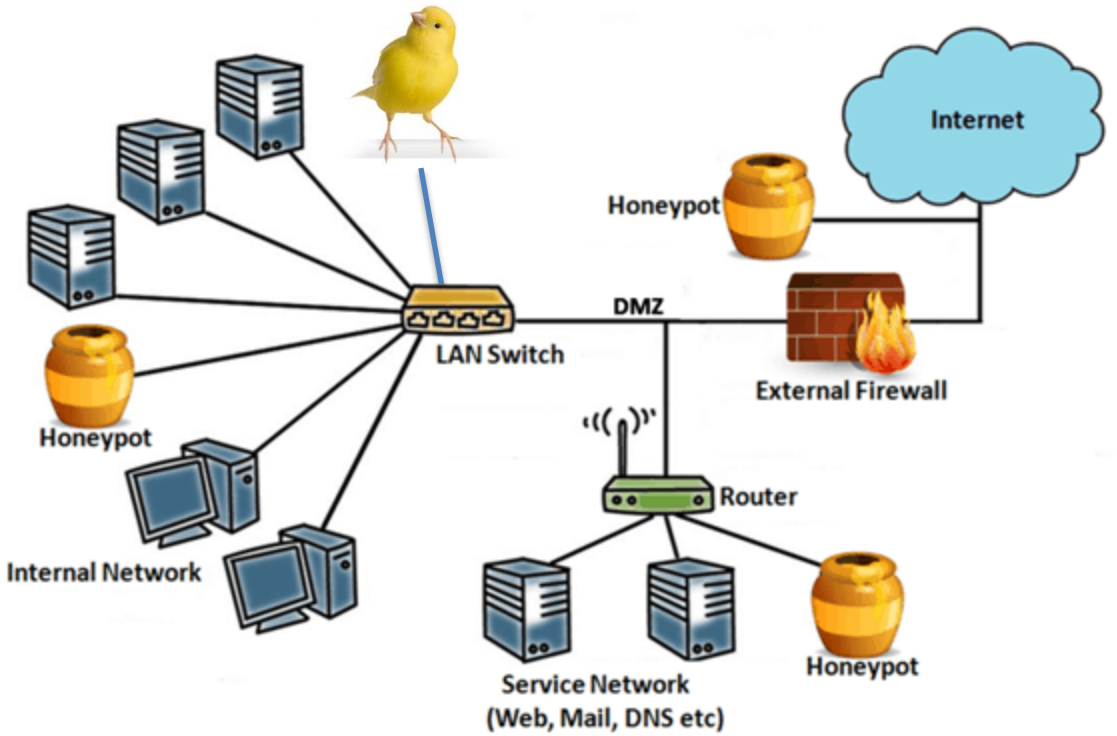
NIST monitoring:



University of Victoria

Honeypots/Honeynets

- honeypot
  - system designed to be an attractive target for attacks
  - can be used to detect them or distract from real targets
- honeynet
  - network designed to be an attractive target for attacks
  - may contain one or more honeypots
- tarpit
  - system designed to slow attackers down
- canary
  - system designed to provide early warning
  - eg. email account, top of GAL, default route alerting, system that should never receive traffic

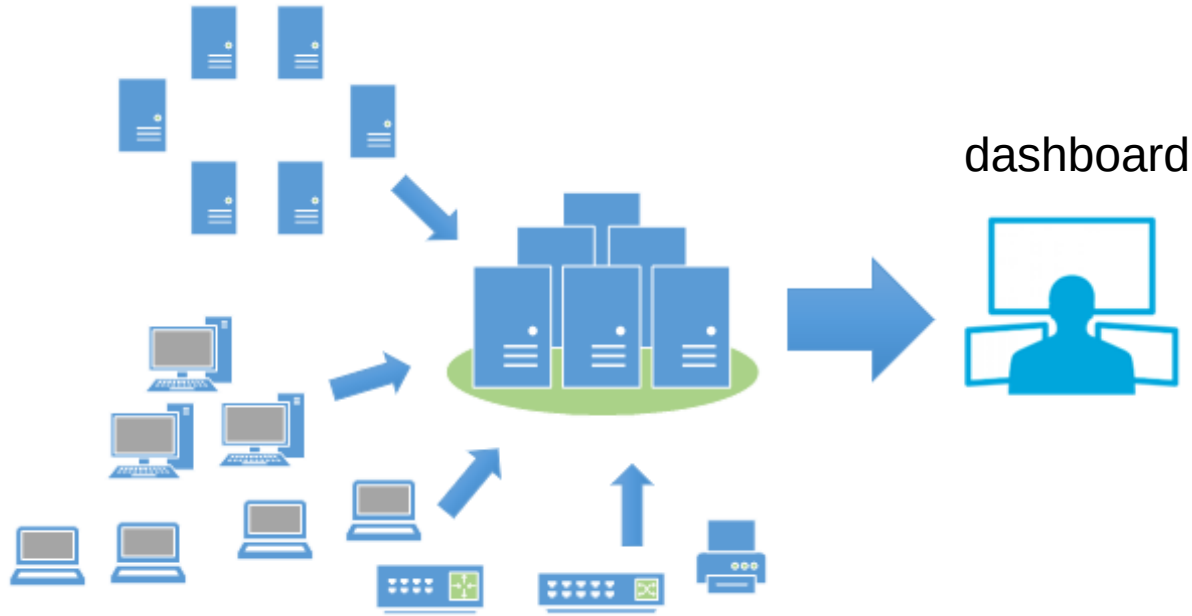


University of Victoria

SIEM (aka SIM, SEIM)

Security Information and Event Management

- must collect logs… good idea to aggregate them
- must look at them… log monitoring
- humans can't keep up
- need a system to correlate to find badness
- try not to send false alarms to humans …. alerting
- humans and their time are valuable



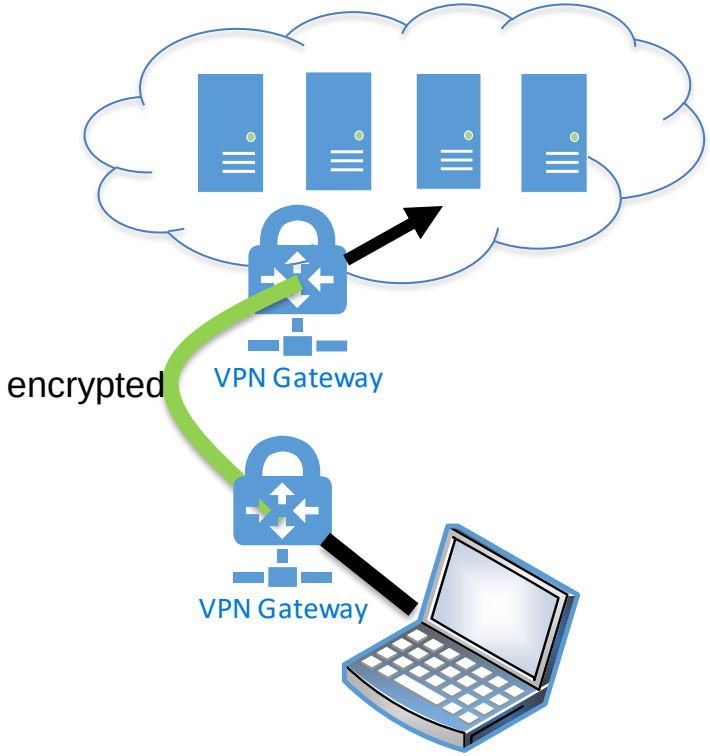
University of Victoria

SIEM

- organizations need to keep logs of who did what when
  - who doesn't keep logs?
- ineffective to have humans staring at glass
- need systems to do the collection, aggregation, correlation, monitoring, alerting
- **mandatory tuning**
- goal is to put actionable intelligence in the hands of the security analyst
- next evolution is SOAR (Security Orchestration Automation and Response) systems that help automate portions or all of response to potential attacks

VPN (Virtual Private Network)

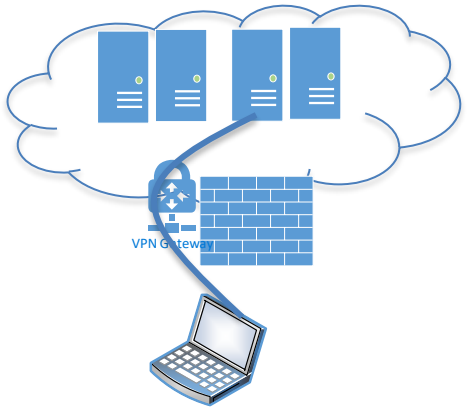
- secure access to other systems
- traffic is encrypted while in the “tunnel”
- best used with strong authentication



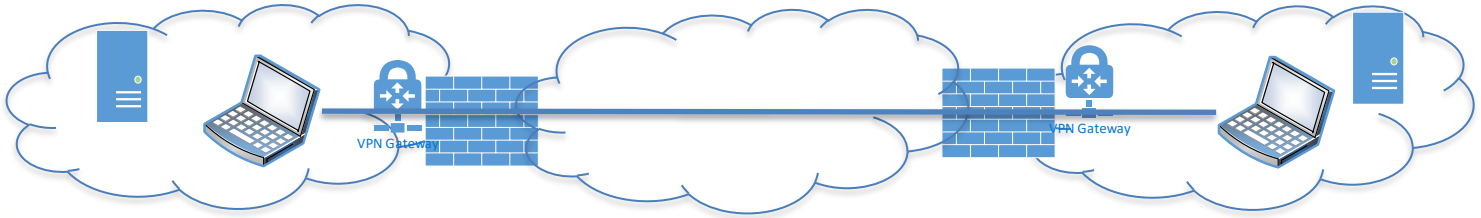
University of Victoria

VPN

- Client-to-Site VPN (C2S)
  - IPSec or SSL
  - provides secure remote access into organization network
  - best used with strong authentication / 2FA / MFA



- Site-to-Site VPN (S2S)
  - “always on”; allows secure access between organizations



University of Victoria

Strong Authentication

Multifactor Authentication

Factors:

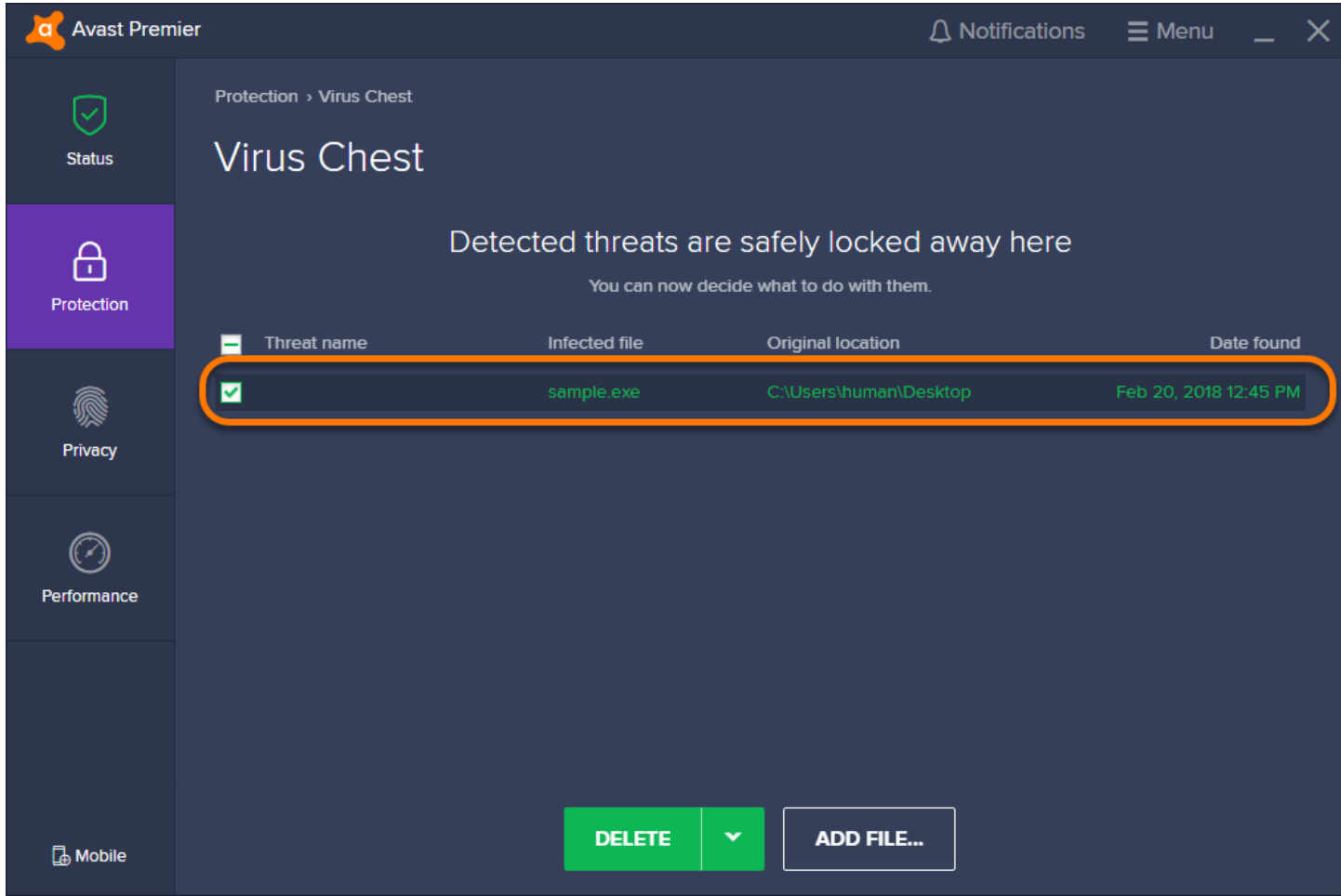
- something you know (eg. password, PIN)
- something you have (eg. token or phone)
- something you are (eg. fingerprint, iris)

…2 or more of the above…

University of Victoria

Anti-virus

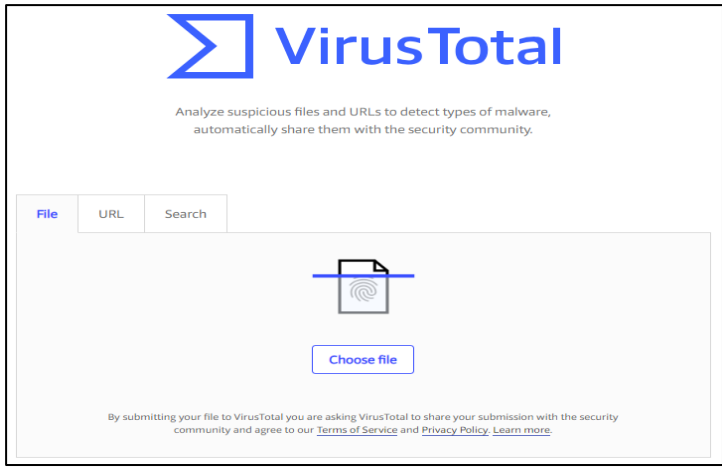
- some AV is very basic and offers very limited protection
- may use a software firewall in addition to a hardware firewall and anti-malware
- avoid virus, browser hijacking, infected attachments, malicious links, etc.

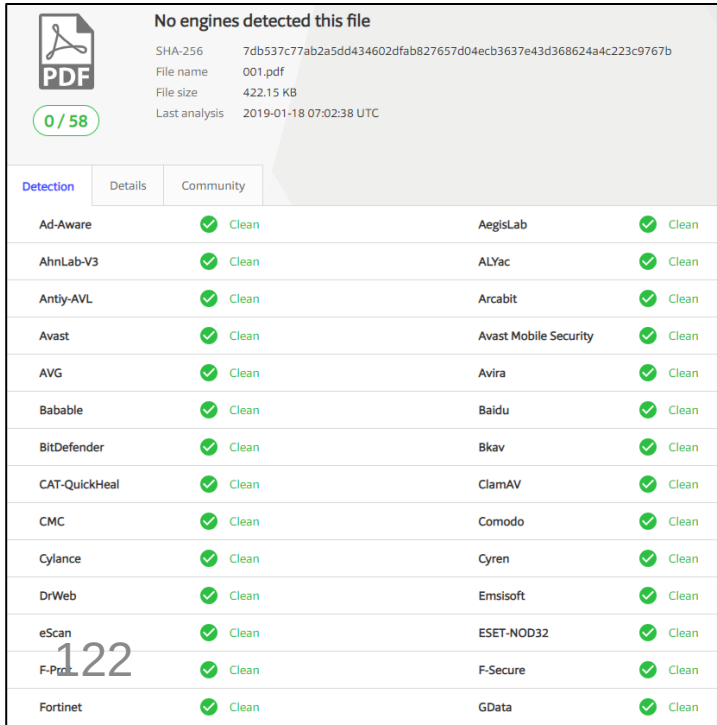


University of Victoria

Anti-Malware

- anti-malware
  - signature-based
  - behaviour-based
- online options
  - eg. HouseCall anti-virus
  - eg. VirusTotal
- install on desktops, laptops, mobiles, servers
- also sandboxing, quarantining, reverse engineering





University of Victoria

Example: Malware

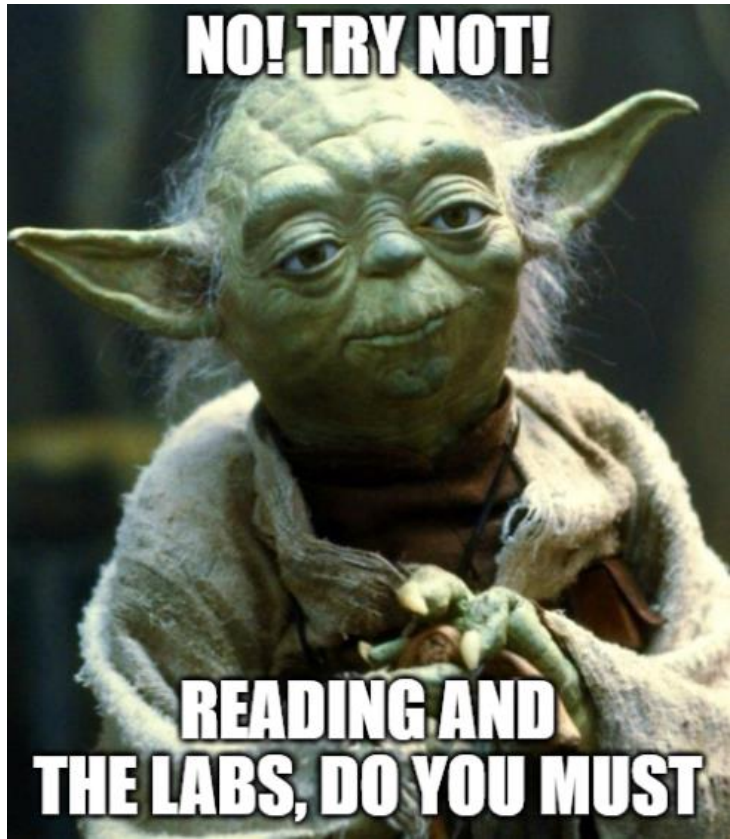
Certification

- data
  - full packet capture
  - session data — summary data between devices, conversations, flows
  - transaction data — application records derived from network traffic; more connection-level info (eg. HTTP, SMTP data)
  - statistical data — summary or profile of network traffic
  - metadata — data about the flow (eg. what netflow captures)
  - alert data — identified by tools as information about potential attacks

- also
  - agent-based and agentless protection – some solutions have an agent that goes on the system, others don't
  - evasion and obfuscation techniques (eg. tunneling, encryption, proxies)

Summary

- build security in from the ground up
  - security by design
  - build in layers, defence in depth
- no organization globally is immune to attack
- doing the basics stops 80% of the problems
  - do the basics well
- prepare for the known, deal with the unknown



University of Victoria

Assigned Reading

- next week is Incident Response & Recovery – don’t miss it!
- read Chapters 34-39
- consider the labs


University
of Victoria