SENG 460 / ECE 574
Practice of Information Security and Privacy

Week 9

Application Security, Security Testing, Vulnerability Scanning,

Penetration Testing, Physical Security

Gary Perkins, MBA, CISSP

garyperkins@uvic.ca

University of Victoria

Guest Speaker

- AppSec is any and every activity you perform to ensure your software is secure
- discussed
  - SDLC and Waterfall
  - DevOps and DevSecOps
- discussed Pushing Left
  - security wants to be ‘invited to the party earlier and do security all the way through and not just at the end’
  - much more expensive to address defects in production
- mentioned OWASP and code reviews

University of Victoria

Secure Coding

- principles
  - least privilege
  - separation of duties
  - defence in depth
  - non-repudiation
  - strong authentication
- build security in from the ground up
  - easier, cheaper, faster, more effective
- don’t bolt it on after the fact because it’s
  - difficult, expensive, slower/delay, less effective

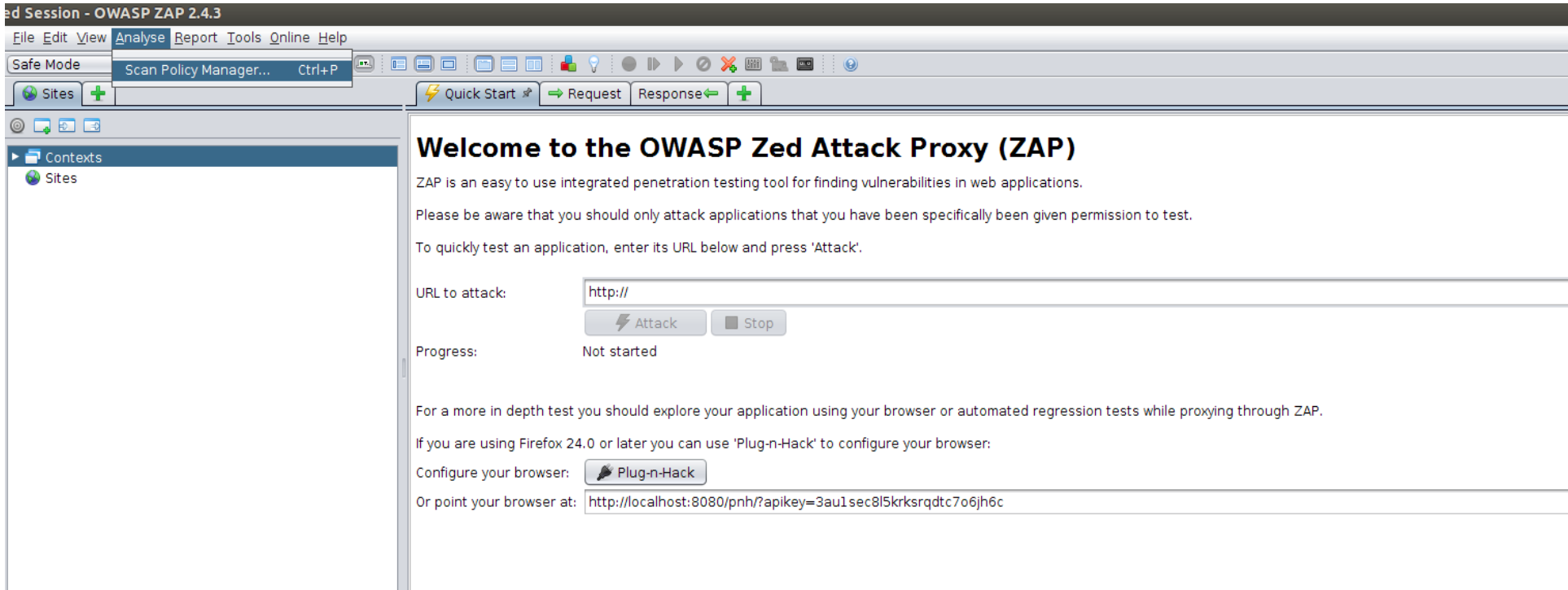
Secure Coding

- validate your input
  - never rely on the client
- use secure protocols
  - utilize encryption at rest and in transit
- don’t make assumptions
  - trust and verify
- never store or pass passwords in plain text
- don’t proceed with known vulnerabilities
  - patch new ones that arise

University of Victoria

Secure Coding

- OWASP
  - Open Web Application Security Project
- OWASP Zed Attack Proxy (ZAP)
  - finds vulnerabilities while you are developing and testing
- courses on OWASP on Cybrary



University of Victoria

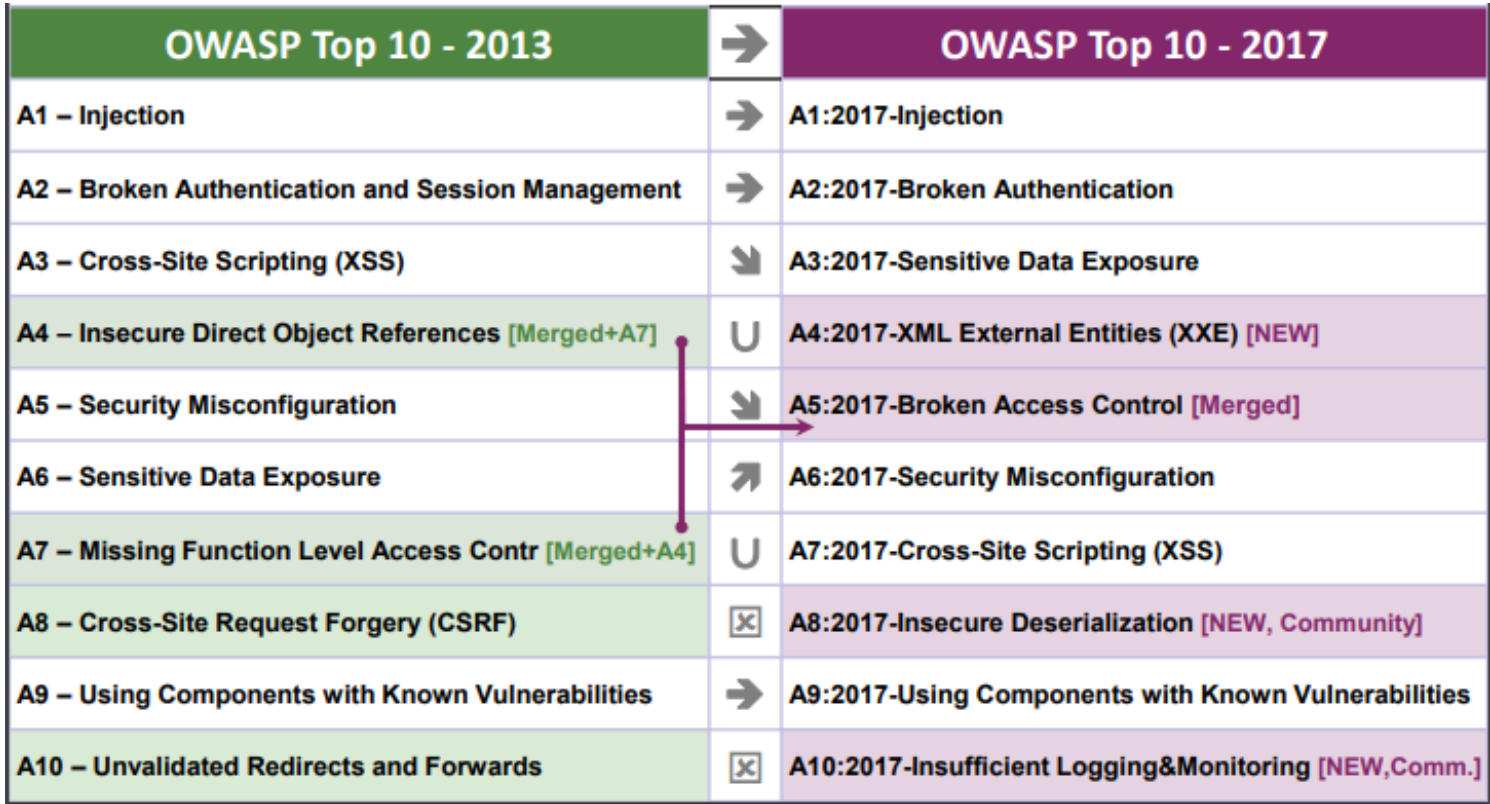
Secure Coding

OWASP Top 10 Security Risks

1) Injection
2) Broken authentication
3) Sensitive data exposure
4) XML External Entities (XXE)
5) Broken Access Control
6) Security Misconfigurations
7) **Cross-Site Scripting (XSS)**
8) Insecure Deserialization
9) Using Components with Known Vulnerabilities
10) Insufficient Logging and Monitoring

Common issues:

- Cross-site Request Forgery (CSRF)
- Cross-site Scripting (XSS)
- SQL Injection
- Session Hijacking

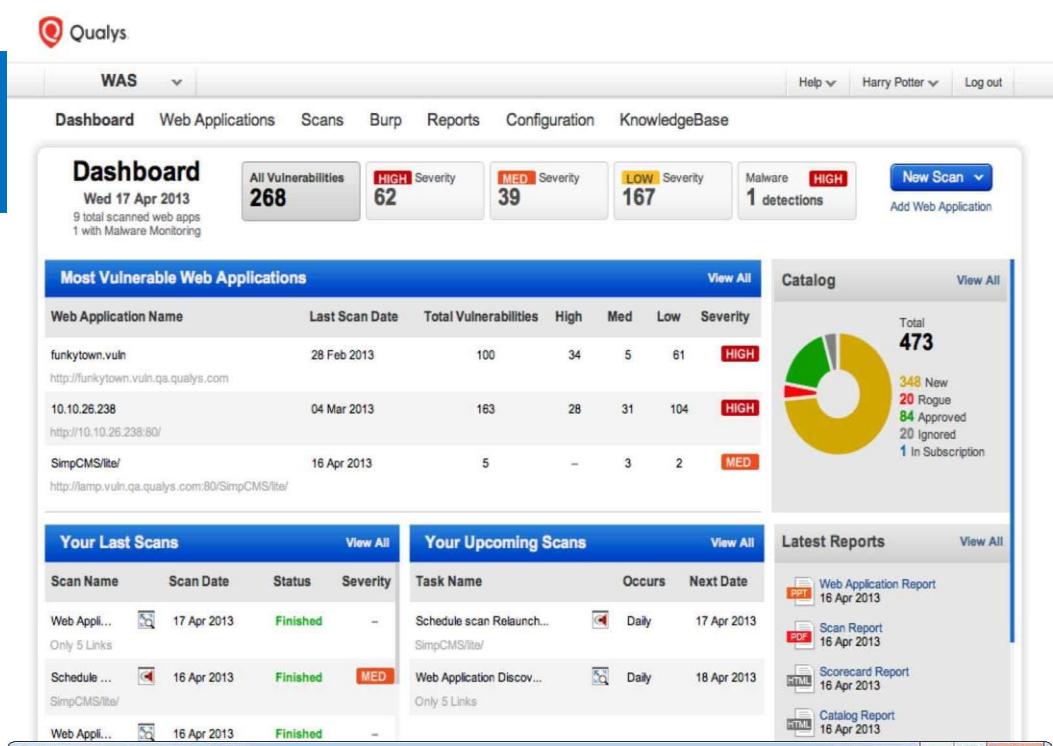


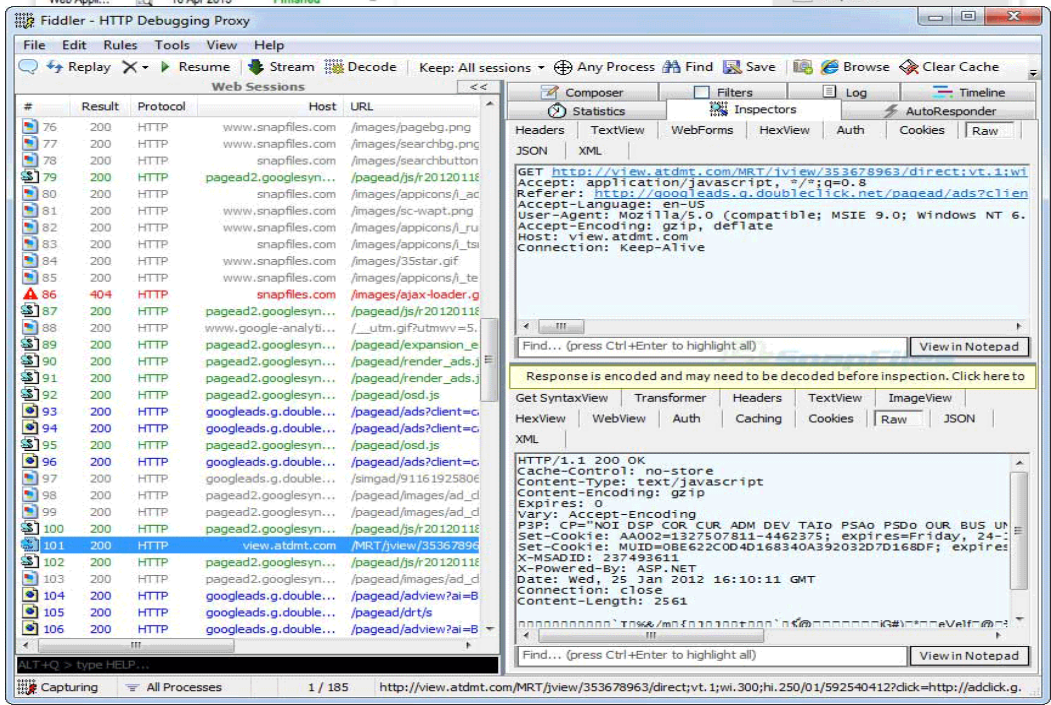
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

University of Victoria

Secure Coding

- different types of scanning and testing
  - netstat
  - tcpdump/snoop
  - port scanning
  - fiddler
  - network vulnerability scanning
  - web app vulnerability scanning
  - static code analysis

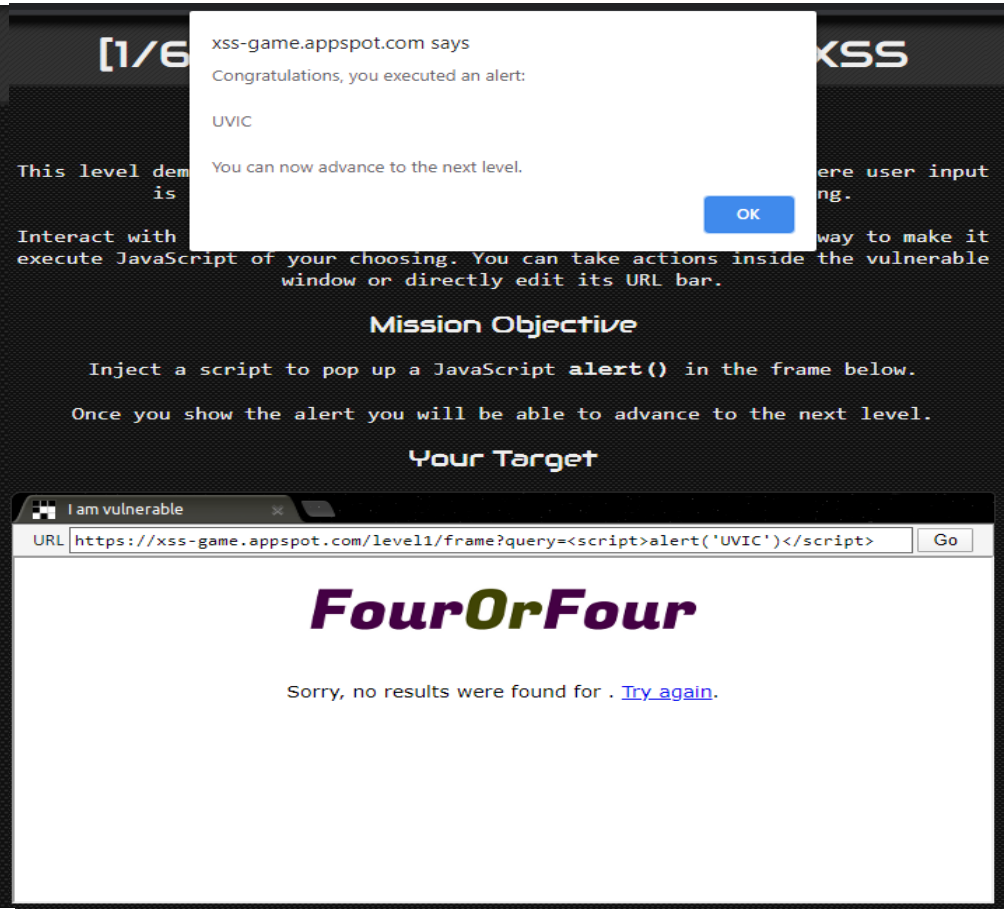




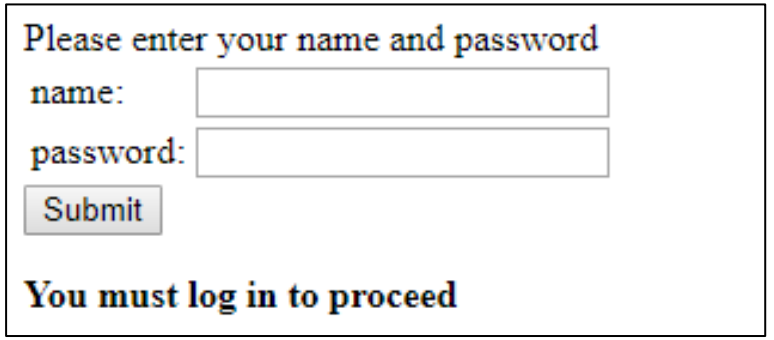
University of Victoria

Cross-site Scripting (XSS)

https://xss-game.appspot.com/



SQL Injection

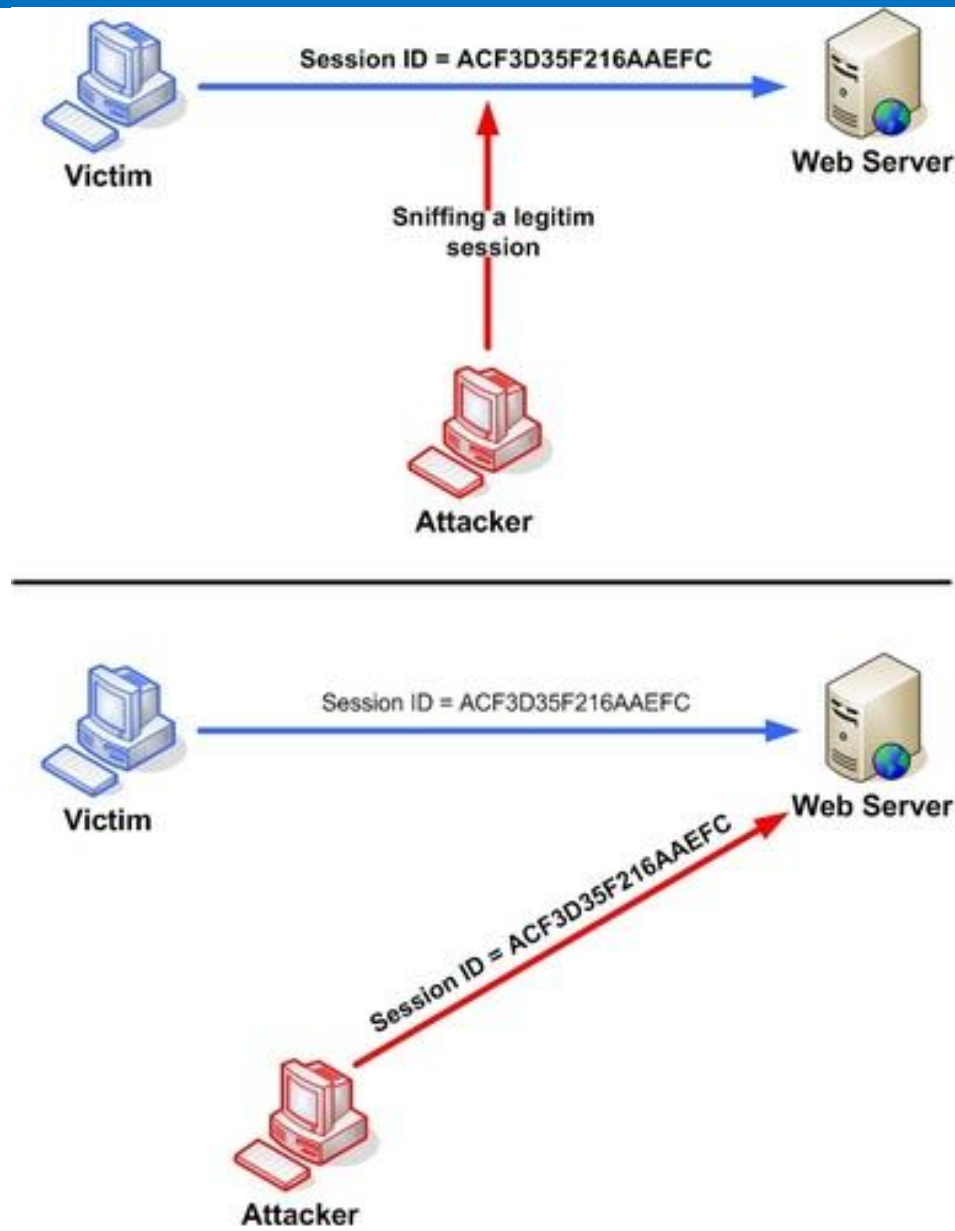


- consider the code used to authenticate users and the database call
- SELECT * FROM users WHERE name='$name' AND password='$password'
- insufficient input validation may allow an attacker to input:
  password' OR '1=1
  resulting in:
  SELECT * FROM users WHERE name='john' AND password='password' OR '1=1'

what about if it was:
password'; DROP TABLE users;

Session Hijacking

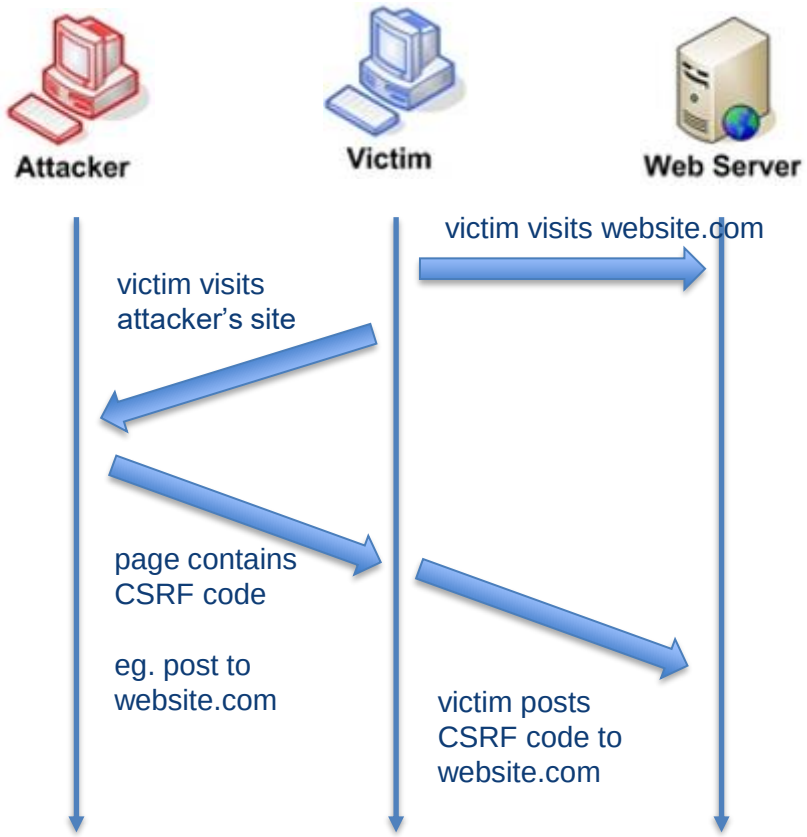
- victim visits website
- attacker sniffs the traffic and captures the session
- attacker replays the session to the webserver and hijacks the session



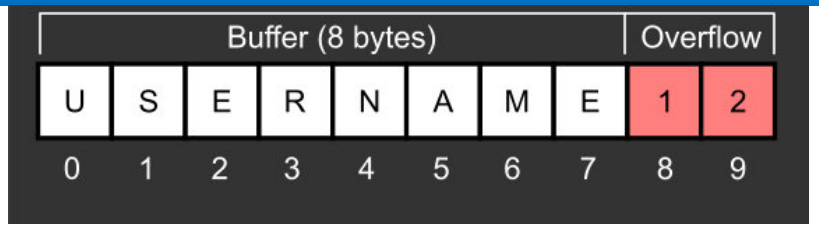
University of Victoria

Cross-Site Request Forgery (CSRF)

- victim visits website
- victim visits attacker's site
- page contains CSRF code
- victim posts CSRF code to website.com



Buffer Overflows



- eg. writing 10 bytes of data to an 8 byte buffer
- program may become unstable, crash, or return corrupt info
- can run other malicious code
- when a max of 8 bytes are expected then limit the amount of data written to the buffer to 8 bytes

Hack the Box

University of Victoria

DISCLAIMER

UNAUTHORIZED USE OF COMPUTER (s.341 CRIMINAL CODE OF CANADA)
/ Definitions / "computer program" / "computer service" / "computer system" / "data" / "electro-magnetic, acoustic, mechanical or other device" / "function" / "intercept" .

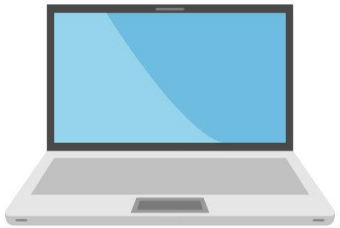
342.1. [1] Every one who, fraudulently and without colour of right,
[a] obtains, directly or indirectly, any computer service,
[b] by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or
[c] uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph [a] or [b] or an offence under section 430 in relation to data or a computer system
is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.
[2] In this section,
"computer program"
means data representing instructions or statements that, when executed in a computer system, causes the computer system to perform a function;
"computer service"
includes data processing and the storage or retrieval of data;
"computer system"
means a device that, or a group of interconnected or related devices one or more of which,
[a] contains computer programs or other data, and
[b] pursuant to computer programs,
[i] performs logic and control, and
[ii] may perform any other function;

"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;
"electro-magnetic, acoustic, or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal hearing of the user to not better than normal hearing;
"function" includes logic, control, arithmetic, deletion, storage and retrieval and communications or telecommunications to, from or within a computer system;
"intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof. [R.S.C. 1985, C.27 [1st Supp.], s.45.]

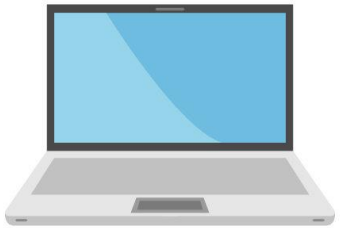
University of Victoria

Rules

students
192.168.10.2-99



targets
192.168.10.100-254



University of Victoria

Rules

- make sure you are connected to the MATRIX network
- do not DDoS or DoS
- do not attack other students, no deauth attempts
- do not erase flags, don’t change passwords
- **make sure you are connected to the MATRIX network**
- do not rob other students of the opportunity
- do not make changes on the systems although you may add a file indicating you were there
- in some cases when a path is occupied, others won’t be able to use it
- **make sure you are connected to the MATRIX network**

University of Victoria

Rules

- no tech support on your machines
- if a system is frozen I can reset it
- if too many problems will have to shut it down
- if any indications of inappropriate behavior will have to shut it down

Make sure you are connected to the MATRIX network!

Password???

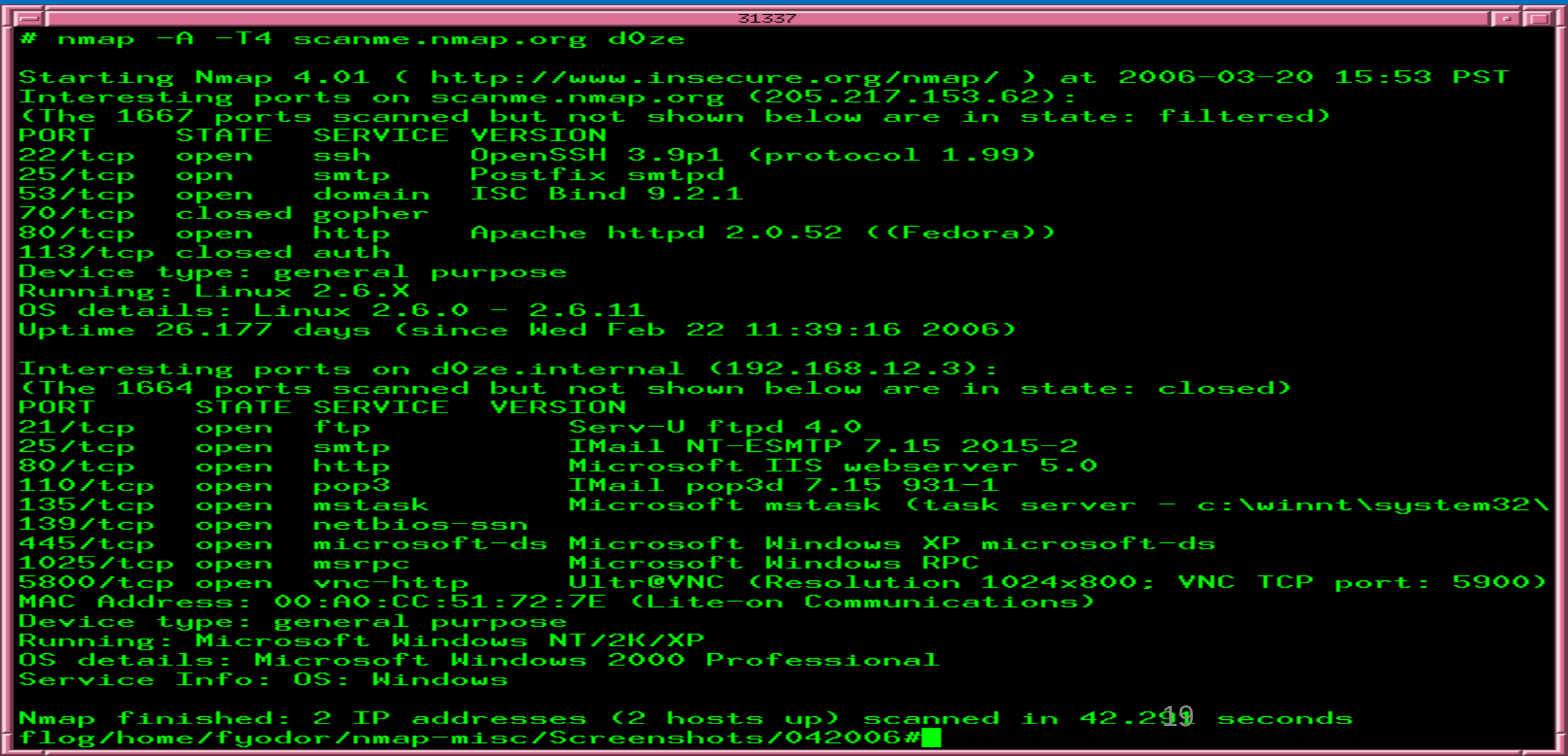
University of Victoria

Recommended Steps

- connect to MATRIX WiFi and check your IP
- ping gateway to ensure connectivity
- scan 192.168.10.100-254 to identify interesting hosts
- scan the hosts more thoroughly
- open ports mean opportunities
- consider OS fingerprinting
- review the services and poke at them
- experiment and gain access
- determine most vulnerable services
- use Metasploit or Armitage to find and exploit them

University of Victoria

nmap – port scanner*



Nmap

- nmap –Pn 192.168.10.100-254
- nmap --top-ports 20 192.168.10.100
- nmap -sV <target> services
- nmap -A -T4 <target> OS detection, version, script, trace, fast
- nmap -Pn --script vuln 192.168.10.100

University of Victoria

Vulnerability Scanning

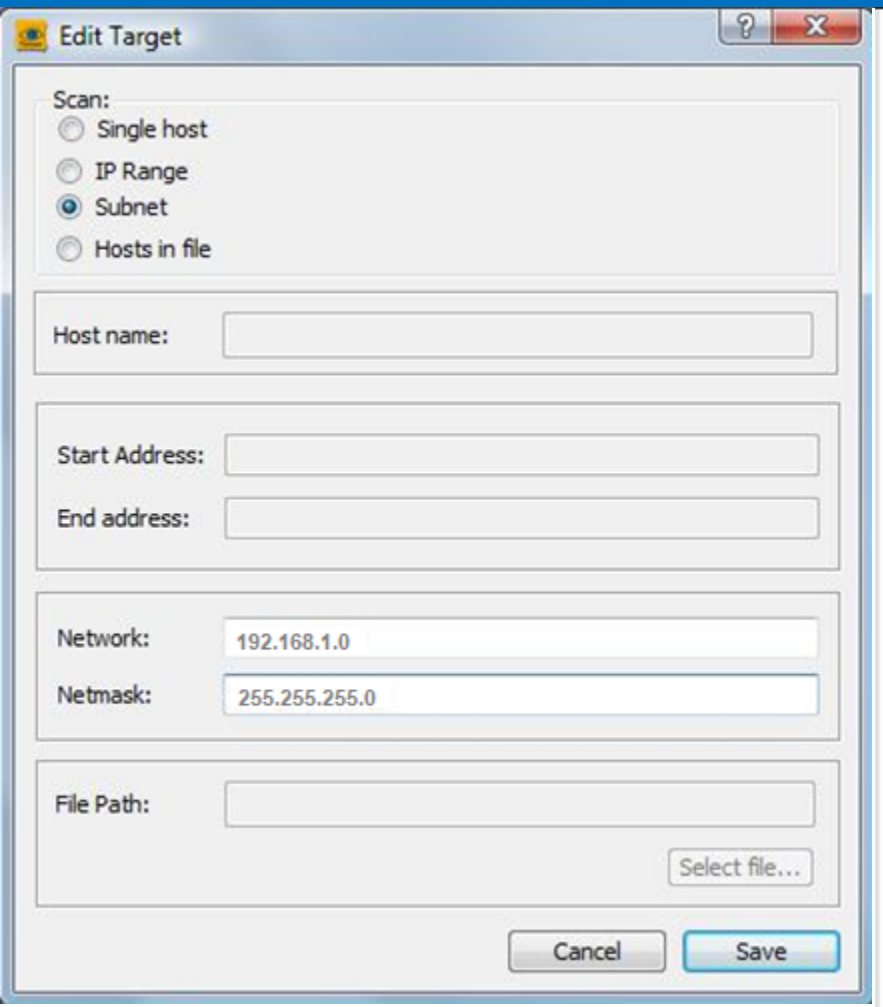
- identify vulnerabilities based on open ports
- maturity:
  - external vulnerability scans
  - internal vulnerability scans
  - credentialed scans
  - databases and network elements
- vulnerabilities exist due to:
  - end of life systems, embedded systems, lack of vendor support, poor coding, improper input/error handling, default configuration, resource exhaustion, etc

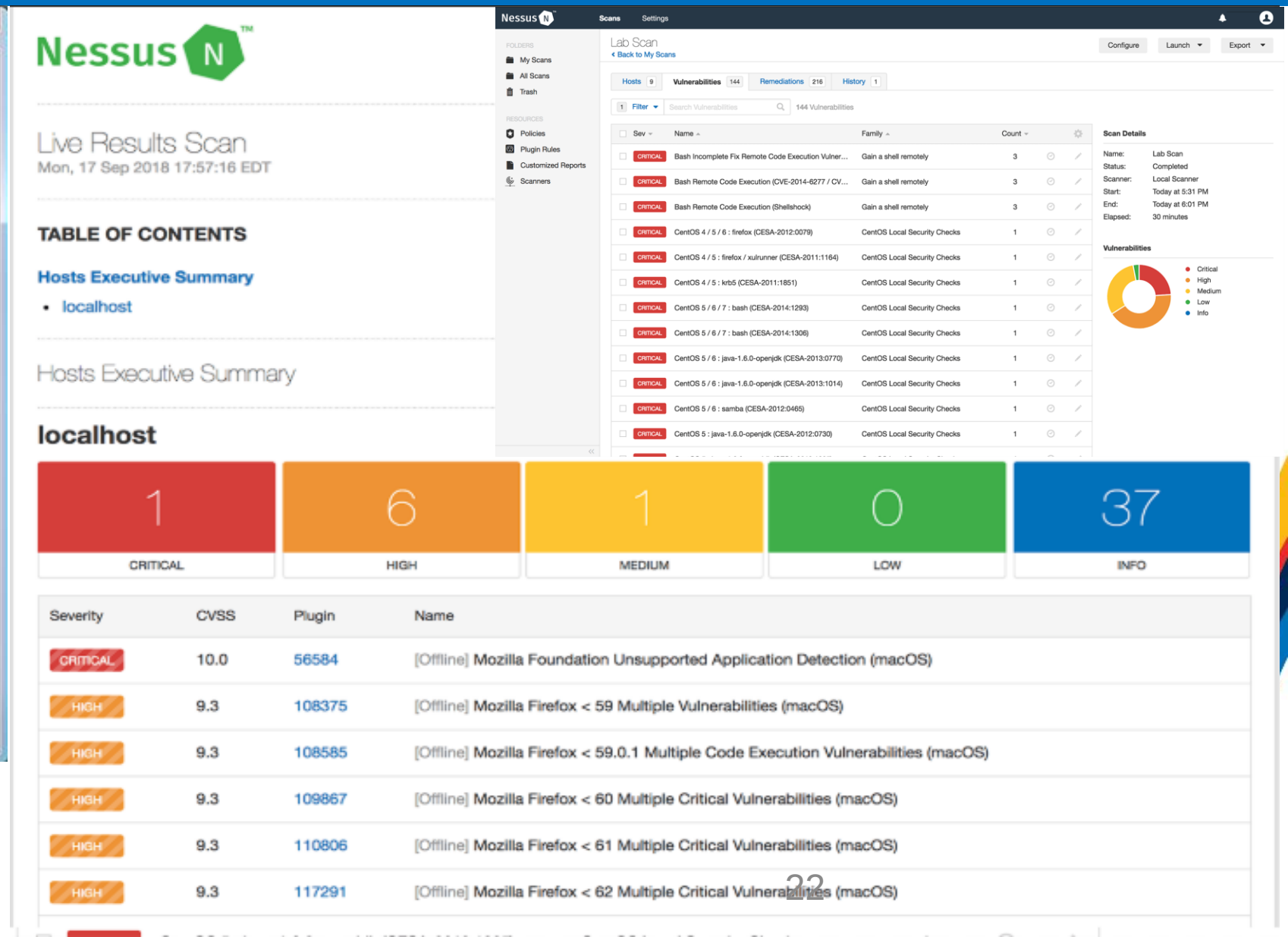
case	result
false positive	identifies something it shouldn't
false negative	doesn't identify something it should
true positive	identifies something it should
true negative	doesn't identify something it shouldn't

University of Victoria

best practice is to scan before and after production launch (and after any changes and periodically)

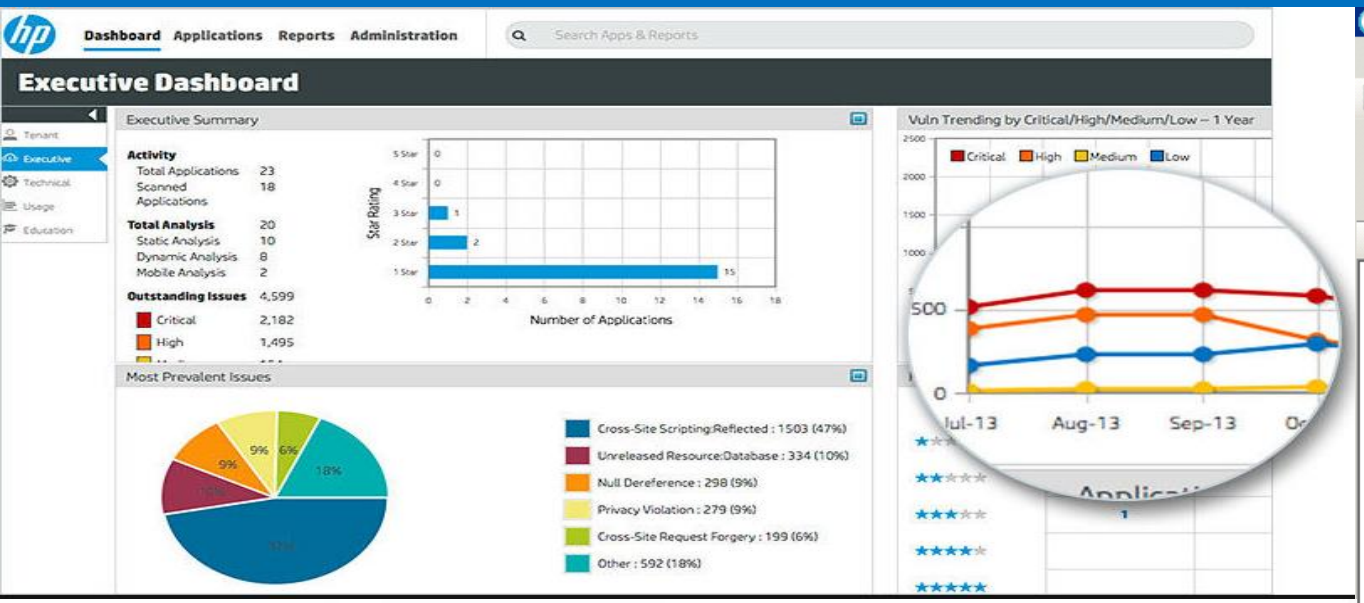
Nessus – network vulnerability scanner

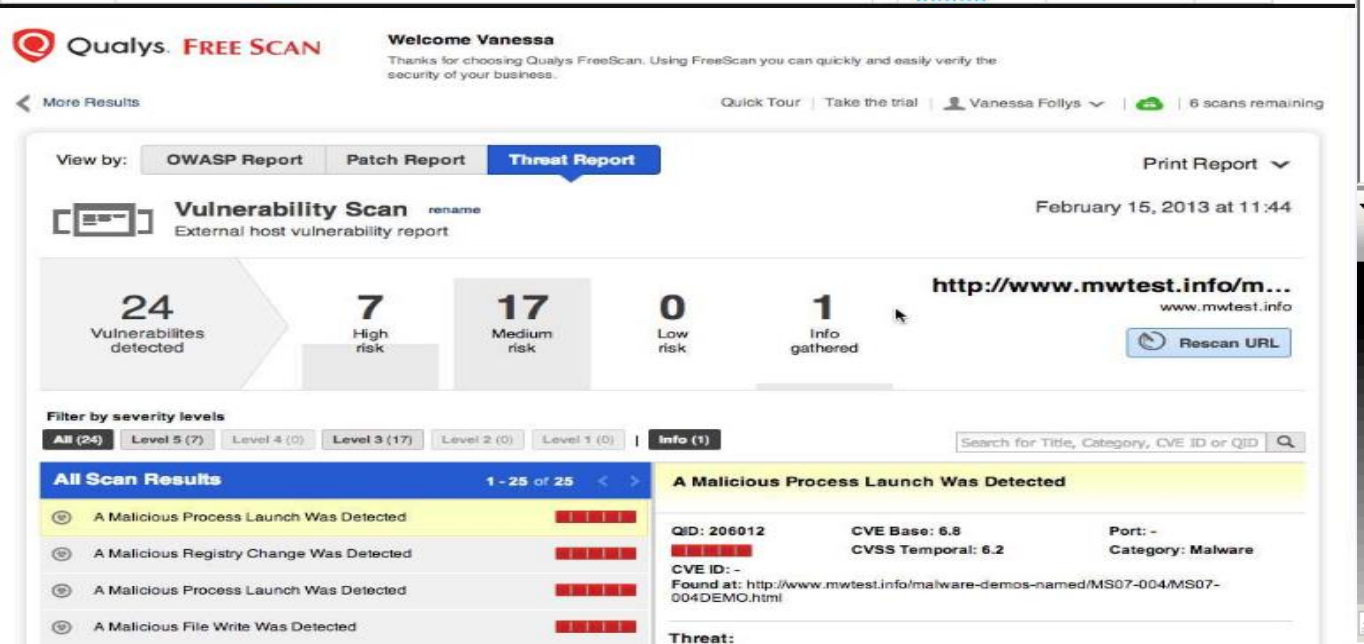


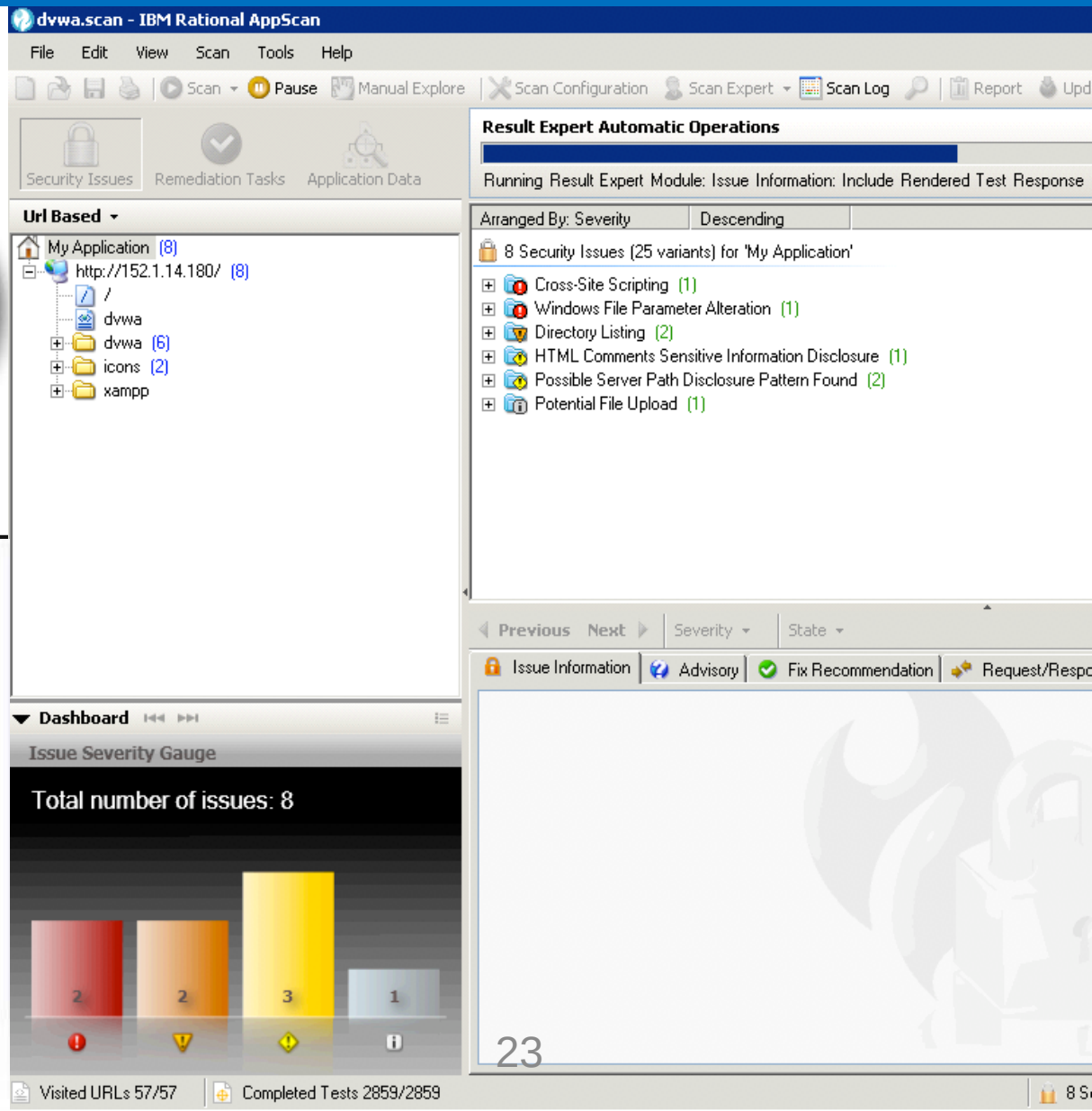


University of Victoria

Web App Scanners (Fortify, App Scan, Qualys)







Qualys SSL and other Scans

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test

SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname: Submit

Do not show the results on the boards

Recently Seen		Recent Best		Recent Worst	
ftd.atenalms.com.br		www.interssl.com	A+	pr.kia.com	T
digitalw8.com		nitter.exonip.de	A+	accounts-cbc.bizagi.com	T
www.google.co.jp		mkpa.inter.mx	A+	www.idbins.com	F
homedu.use.go.kr		geschmack-in-flaschen.de	A	www.shfe.com.cn	T
krishnarp.guru	Err	www.rmcweb.com	A	vault.noonatest.com	T
www.eswan.com.tw		www.neomailbox.com	A	iteams.dshs.texas.gov	F
romantic-chaum.164-92-186-24 ...		gdelices.nc	A	external.gw-em-vpn-fpr-qa-ac ...	T
jbhs.de		fm.mobiletyreshop.com.au	B	www.datacall.net.au	F
econt.nydp.co.kr		greatquestion.co	B	happybirthdoula.co.uk	T
www.yebigun1.mil.kr	Err	voltage-pp-0000.sds.demo.vol ...	B	mail.kostrading.cz	F

SSL Report v2.1.10

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > www.datacall.net.au

SSL Report: www.datacall.net.au (103.225.161.115)

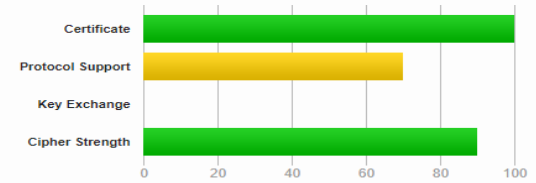
Assessed on: Fri, 18 Mar 2022 00:28:53 UTC | Clear cache

Scan Another »

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server is vulnerable to the DROWN attack. Grade set to F. MORE INFO »

This server supports anonymous (insecure) suites (see below for details). Grade set to F.

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

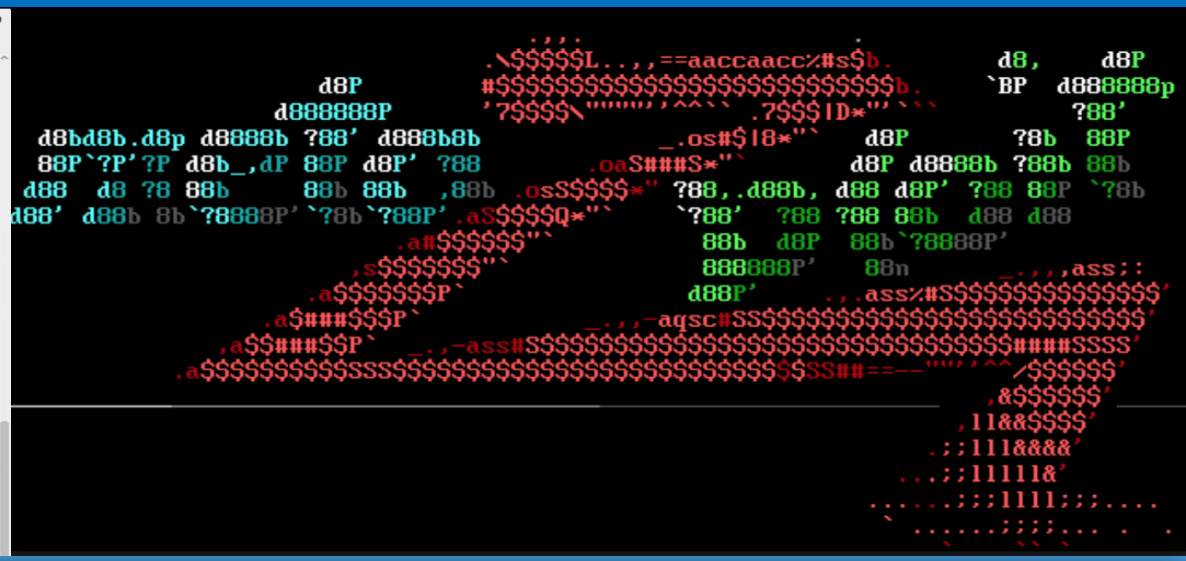
This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. MORE INFO »

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

Metasploit – security tool

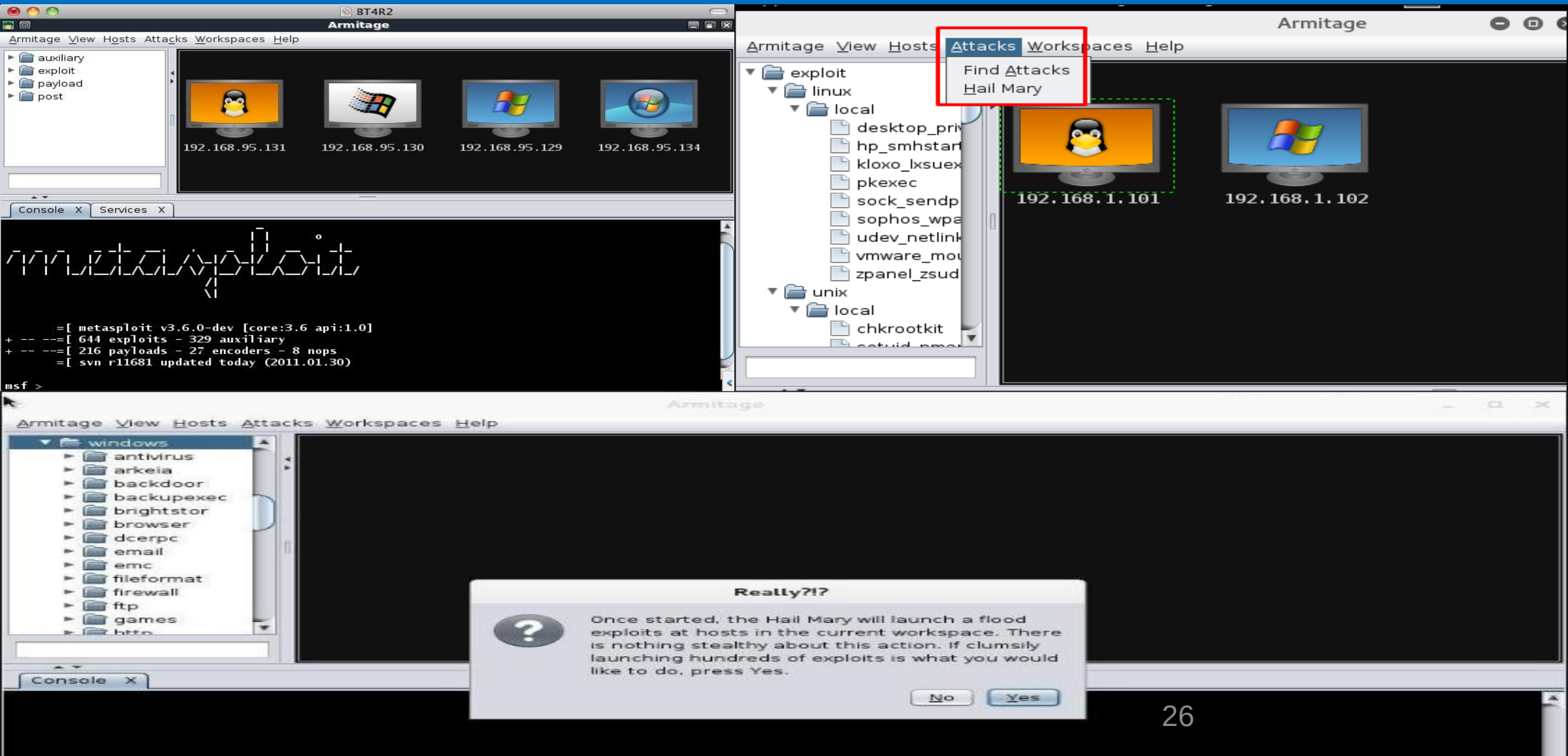
```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# msfconsole -h
Usage: msfconsole [options]

Common options
    -E, --environment ENVIRONMENT    The Rails environment. Will use RAIL_ENV environment variable if that is set.  Defaults to production if
 neither option not RAILS_ENV environment variable is set.

Database options
    -M, --migration-path DIRECTORY   Specify a directory containing additional DB migrations
    -n, --no-database                Disable database support
    -y, --yaml PATH                  Specify a YAML file containing database settings

Framework options
    -c FILE                          Load the specified configuration file
    -v, --version                    Show version

Module options
        --defer-module-loads         Defer module loading unless explicitly asked.
    -m, --module-path DIRECTORY      An additional module path


Console options:
    -a, --ask                        Ask before exiting Metasploit or accept 'exit -y'
    -d, --defanged                   Execute the console as defanged
    -L, --real-readline              Use the system Readline library instead of RbReadline
    -o, --output FILE                Output to the specified file
    -p, --plugin PLUGIN              Load a plugin on startup
    -q, --quiet                      Do not print the banner on startup
    -r, --resource FILE              Execute the specified resource file (- for stdin)
    -x, --execute-command COMMAND    Execute the specified string as console commands (use ; for multiples)
    -h, --help                       Show this message
root@kali:~#
```



C:\Windows\system32\cmd.exe

```
[*] Starting Metasploit Console...
IIIIII    dTb.dTb
  II     4'  v  'B
  II     6.     .P
  II     'T;. .;P'
  II      'T; ;P'
IIIIII     'YvP'

I love shells --egypt


       =[ metasploit v4.15.4-dev                          ]
+ -- --=[ 1680 exploits - 1053 auxiliary - 308 post        ]
+ -- --=[ 489 payloads - 40 encoders - 9 nops              ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Successfully loaded plugin: pro
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter_reverse_http
payload => windows/meterpreter_reverse_http
msf exploit(handler) > set lhost 127.0.0.1
lhost => 127.0.0.1
msf exploit(handler) > exploit
[*] Exploit running as background job.
msf exploit(handler) >
[!] You are binding to a loopback address by setting LHOST to 127.0.0.1. Did you want ReverseListenerBindAddress?
[*] Started HTTP reverse handler on http://127.0.0.1:8080

msf exploit(handler) > _
```

Armitage – security tool & hail mary



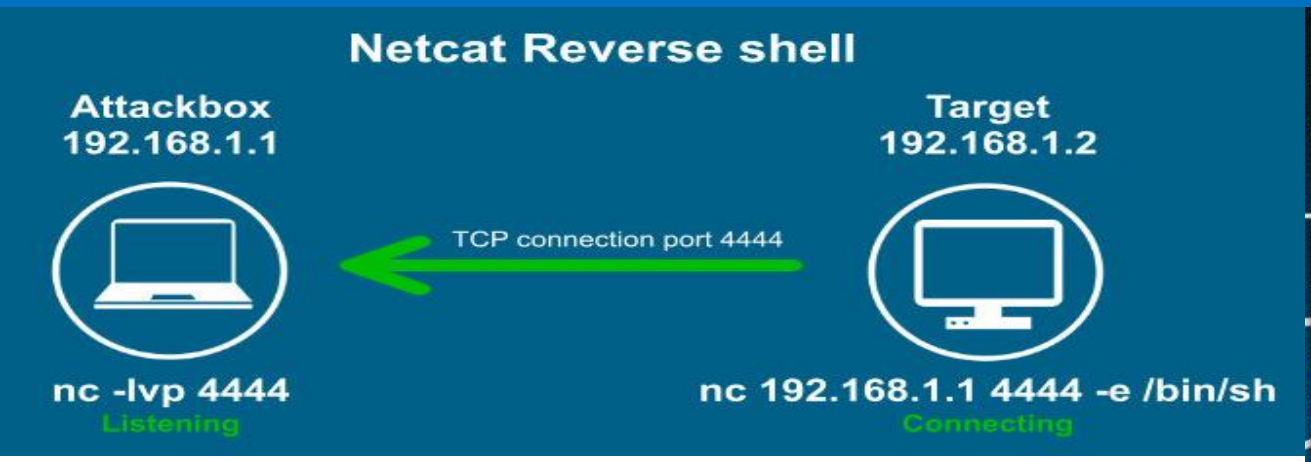
Armitage

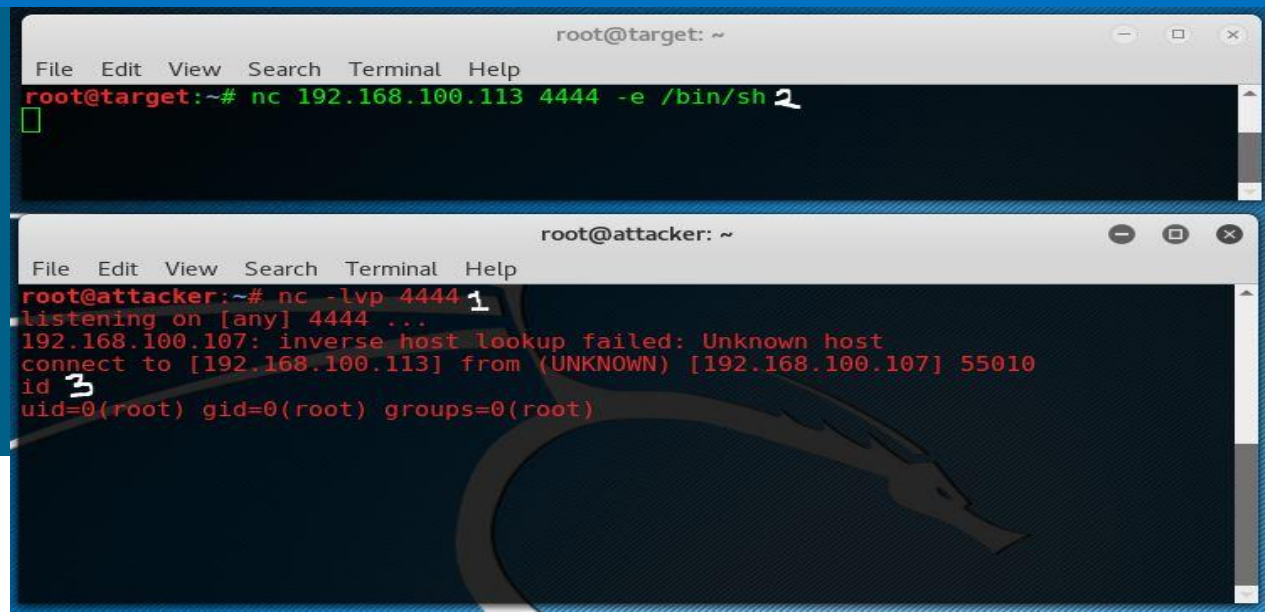
- GUI front-end for Metasploit

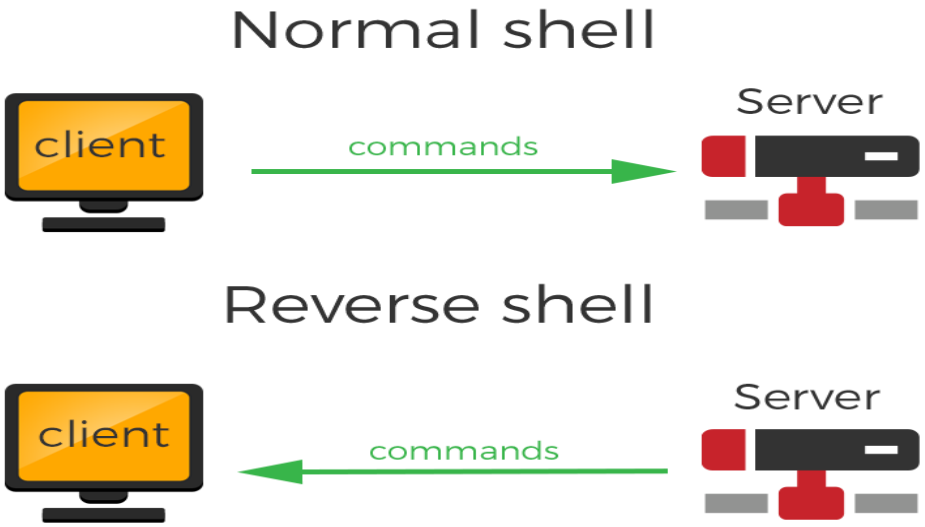
https://www.youtube.com/watch?v=JALmoY4LuT8

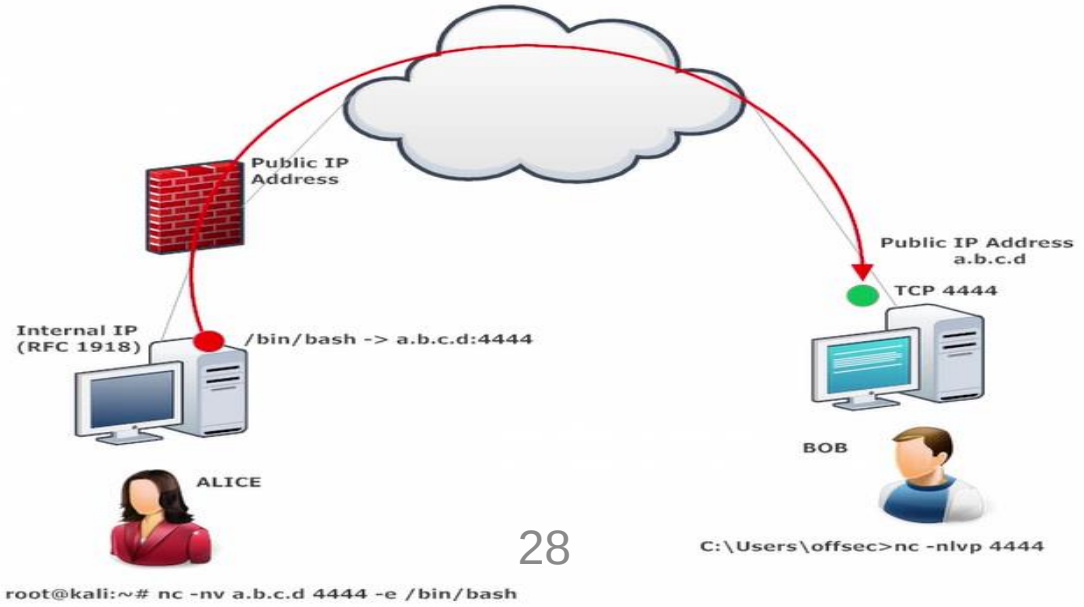
feel free to view on your own

Netcat – reverse shells (persistence)





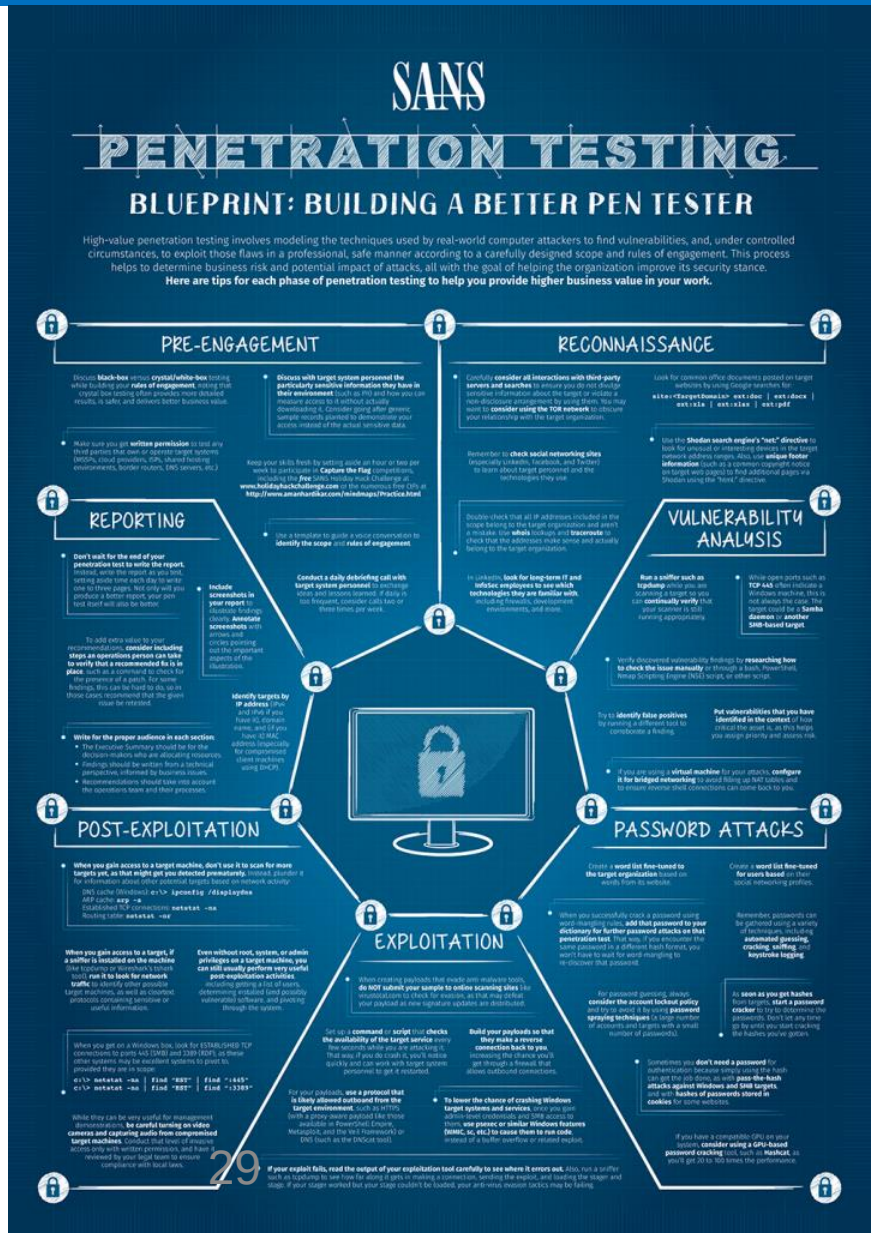




University of Victoria

Penetration Testing

- pre-engagement (permission, scope)
- reconnaissance (passive, active)
- vulnerability analysis
- password attacks
- exploitation
- post-exploitation
- reporting



University of Victoria

Penetration Testing

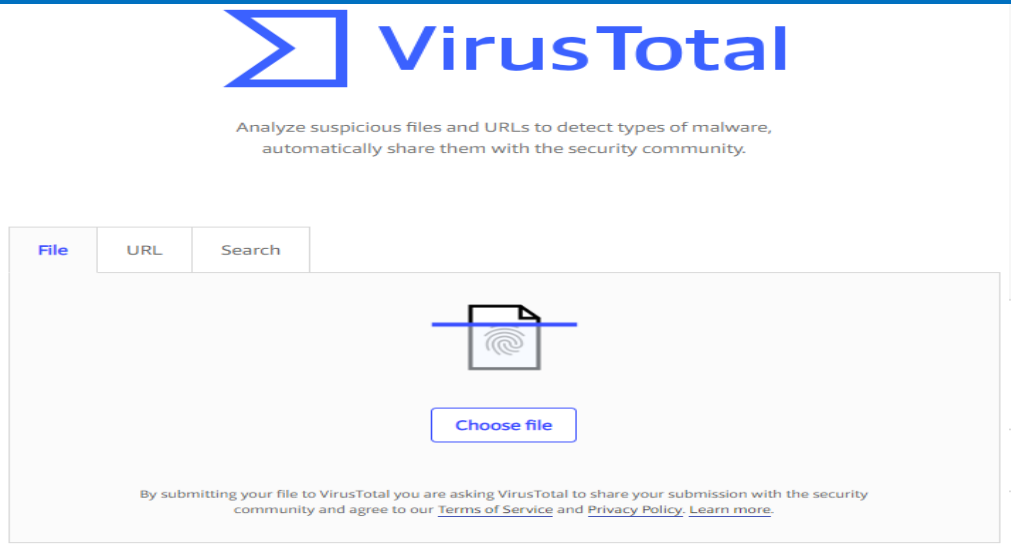
- **penetration testing:** aka pen testing, ethical hacking - attempts to **exploit** vulnerabilities
- **external**: targets external infrastructure to see how far outside attacker would get
- **internal**: mimics inside attack behind firewall with standard user access
- **blind testing**: pentesters only given company name, takes longer, $$$
- **double-blind test**: blind testing and only a few people know
- **blackbox testing**: pentester gets no information
- **whitebox testing**: pentester gets information
- future terms? zero knowledge, partial knowledge, full knowledge

Terms

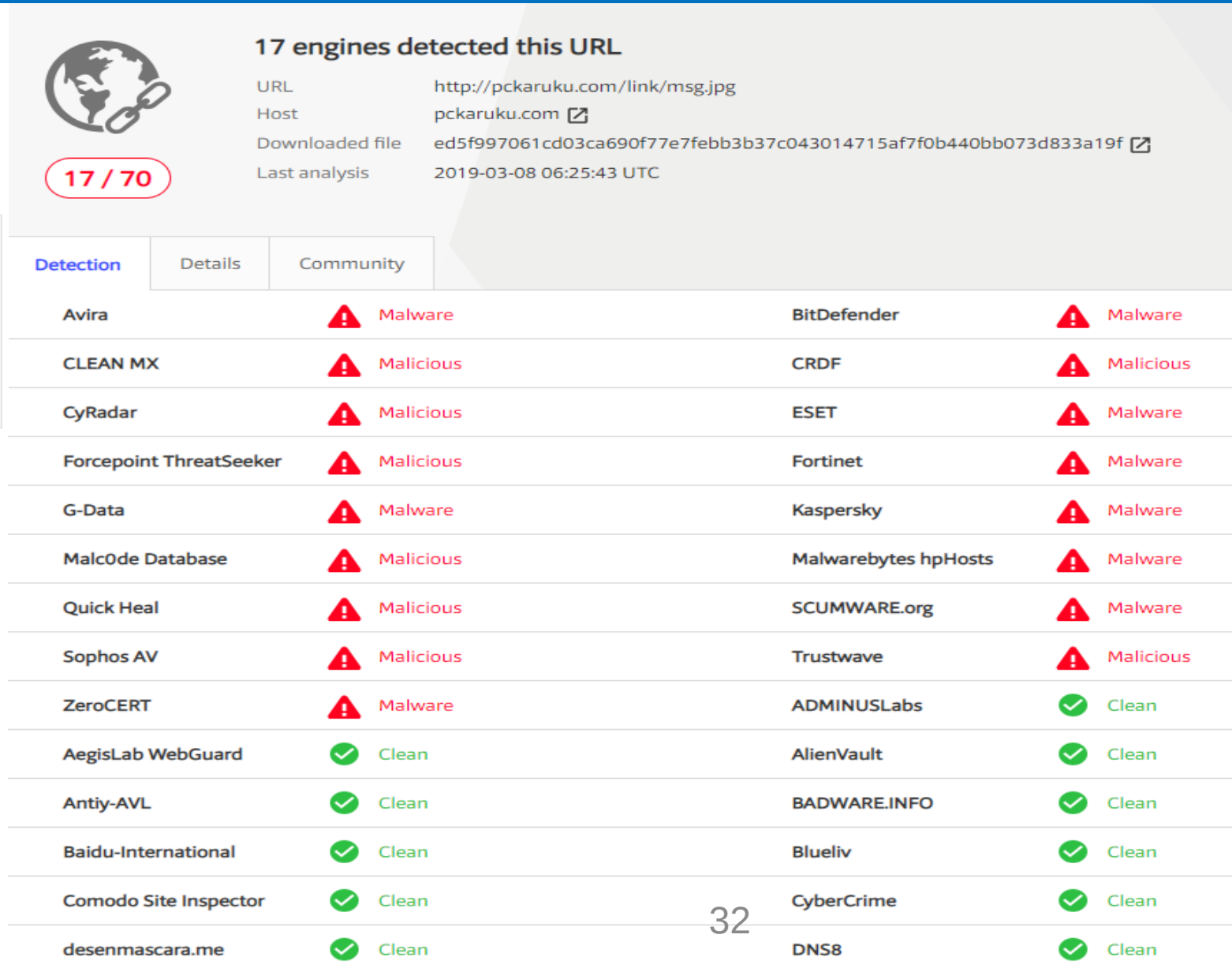
- **white hat**: does not have any malicious intent
- **black hat**: has malicious intent
- **grey hat**: somewhere between white and black

Updated terms in the future?

VirusTotal



- files
- URLs



University of Victoria

Other Tools

- Security Onion
  - Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management. It includes Elasticsearch, Logstash, Kibana, Snort, Suricata, Bro, Wazuh, Sguil, Squert, CyberChef, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!
- Bro (Zeek) network analysis, NIDS
- Rita real intelligence threat analytics
- Suricata open source IDS
- pfSense open source firewall
- wireshark, tcpdump, snoop, ettercap – packet capture

Physical Security

University of Victoria

Example 1 – Vancouver Riot

Millions in Costs from Vancouver Riot of 2011

Listen now
02:33 Powered by Trinity Audio

Almost five years later, details have been released on the financial damage caused by the Vancouver Stanley Cup Riot in 2011.

On June 15 of that year, fans rioted in the streets for five hours after the home team, the Vancouver Canucks, lost to the Boston Bruins.

In the course of that time, rioters set cars on fire, vandalized and stole from local businesses, and confronted police. Numerous people were assaulted.

Photo Credit: Skeezix1000, Wiki Commons.
A car pushed over and set on fire on the street during the riot

It took 928 police officers to finally get the situation under control. They were also assisted by Vancouver Fire and Rescue and BC Ambulance.

Once it was over, the investigation began.

This included pouring over surveillance video, emails, and social media posts.

Investigators created a website for the public to assist in the identification of rioters, with photos and videos posted for recognition.

They found 112 businesses were damaged, along with 122 vehicles, and at least 52 assaults took place. There were at least 26 arsons and the same number of break and enters. There were almost 200 other crimes where suspects have been charged with mischief.

During business hours, 316 people broke in to London Drugs on Granville Street and looted. In total, the business suffered almost $1,000,000 in damage and losses.

The Hudson Bay was also on the victim list. Rioters broke through windows and looted, setting a fire outside, forcing employees to evacuate into the riot. This damage totalled almost $1.5 million.

The total financial loss from the event is estimated at $3.78 million, with $2.7 million in damage to businesses, a $540,000 cost to people involved and $525,000 to the City of Vancouver, BC Ambulance Services, and St. Paul's Hospital.

In total, nearly $5 million was spent on prosecution of those involved.

Less than 20 per cent of those charged in the Vancouver riot had a previous criminal record, which appears to be a unique situation compared to similar incidents in other parts of the world.

Example 1 – Vancouver Riot

Four hours of violent rioting in Vancouver's downtown core following the Canucks' Game 7 loss caused millions of dollars in damage to dozens of local businesses, not to mention the black eye it gave to the city's reputation.

Charles Gauthier of the Downtown Vancouver Business Improvement Association said its members are "shocked and dismayed" by the actions of angry rioters who turned the downtown core into complete bedlam following the game.

Related Links

- B.C. premier vows to hunt down rioters
- 'Criminals, anarchists, thugs' behind post-Cup riot
- From bad to brutal: Timeline of a riot
- Looting breaks out as riots intensify in Vancouver
- 'Despicable' riots make worldwide headlines
- Strangers come together to clean up Vancouver

Gauthier said 50 businesses suffered various degrees of damage during the post-Cup riot, including broken windows and doors and tens of thousands of dollars of merchandise stolen during looting.

He's encouraging business owners to forward any videos and footage of rioters to police so the people behind the riots can be brought to justice.

One of the stores that suffered the most damage was the London Drugs at the corner of Granville and Georgia streets, where managers closed the doors two hours early because of the angry mob growing outside.

The store's front doors withstood about two hours of pounding before the rioters finally crashed through the double layer of laminated glass and security gates at 10 p.m.

Sweeping through the empty store on Thursday, Clint Mahlman, senior VP of London Drugs, said the 20 staff members still in the store ran for cover when an estimated 200 looters stormed into the store and grabbed anything and everything they could get their hands on.

People stole big screen TVs, expensive SLR cameras, makeup and crates of potato chips.

Down the street, coffee shop owner Minnie Dun said she was forced to barricade herself and three staff members in a storage room when rioters started rampaging through her business.

"The whole place is demolished," she said, choking back tears. "The whole place is gone, there's nothing left."

Four staff members also barricaded themselves into a small back room at a Blenz coffee shop when rioters began roaming the streets looking for trouble.

Staff members say stones and shopping carts were thrown against their store windows before they finally broke down.

Next door at Black and Lee Tuxedos the shelves were completely empty after hooligans busted store windows and fled with mannequins and merchandise.

Managers estimate at least $10,000 in clothing was stolen.

Construction superintendent John Revington said damage to just one of his downtown sites was up to $20,000.

"Here's a message to the people out there who did this: You're a bunch of morons," he said.

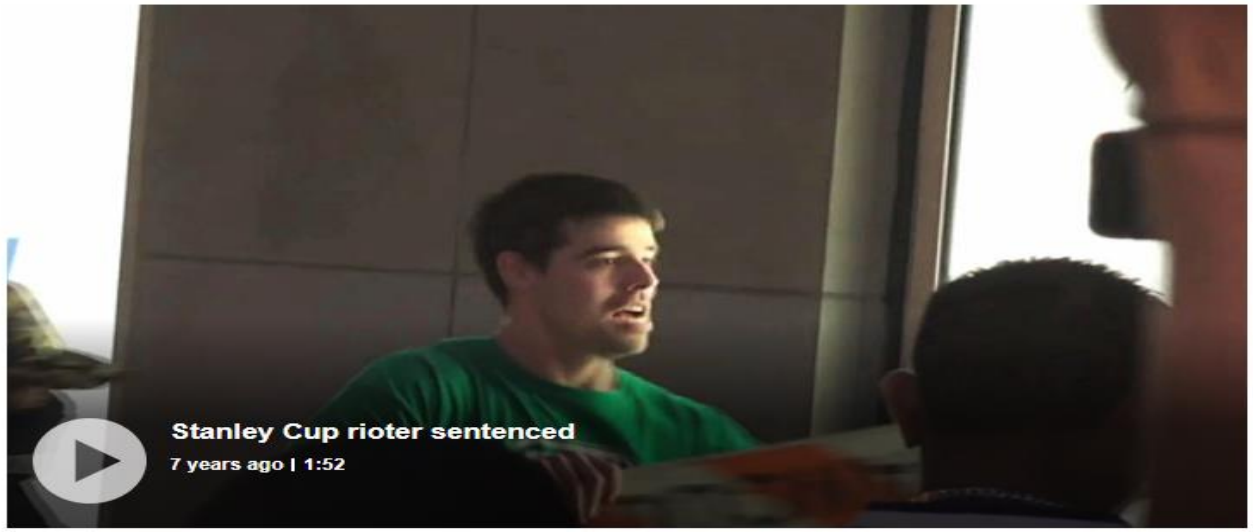
"We'll get the businesses open but who's going to pay for this, the morons who did this last night? I don't think so. Come on down and give me a cheque for the damage you did to my building when you were drunk and high on violence."

Example 1 – Vancouver Riot

Drunk Stanley Cup rioter gets conditional sentence

Spencer Kirkwood, 26, convicted of mischief and participating in a riot

CBC News · Posted: Jun 05, 2013 10:14 AM PT | Last Updated: June 5, 2013



Spencer Kirkwood was drunk, smashed windows, escaped jail time 1:52

The Stanley Cup rioter who argued he was too drunk to be held responsible for his actions has been handed a 30-day conditional sentence with no jail time.

At a sentencing hearing in Vancouver on Wednesday, Spencer Kirkwood, 26, was also sentenced to two years probation, with a ban on drinking alcohol.

Kirkwood was convicted in April on charges of mischief and participating in a riot after he was caught on tape smashing the windows of a Telus building in downtown Vancouver during the Stanley Cup riot in June 2011.

Vancouver is still scared to hold big city events even 8 years after Stanley Cup Riot

Kenneth Chan | Jun 14 2019, 5:59 pm

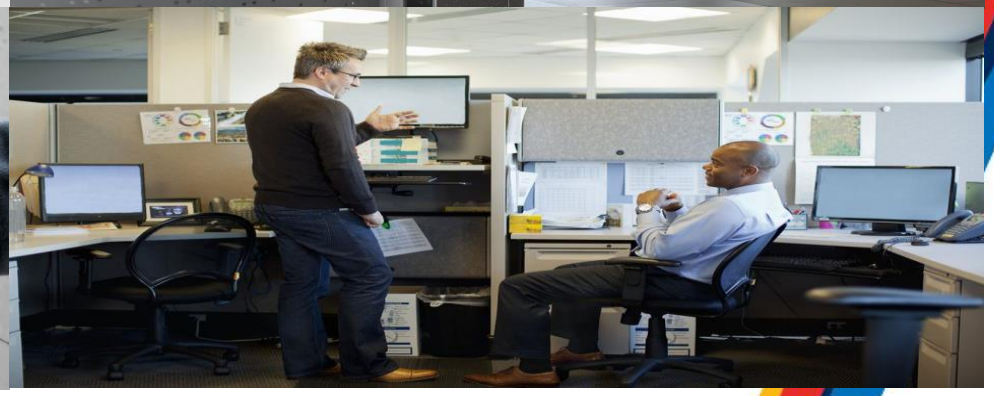
Example 2 – Call Centre/Social Engineering



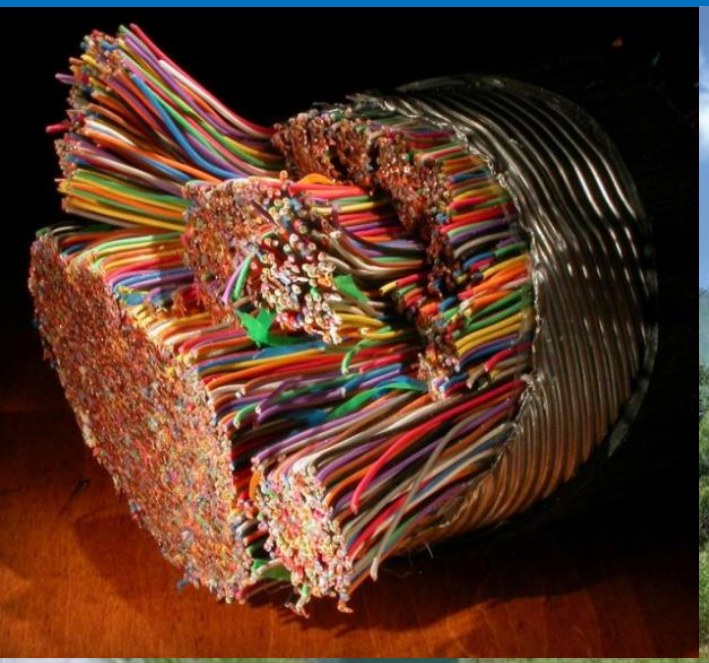








Example 3 – Copper Theft



Physical Security

- **tailgating:** gaining unauthorized access to a facility by following someone in that has access (aka piggybacking)
- **dumpster diving:** looking through garbage for valuable information
- **shoulder surfing:** when someone watches over your shoulder what you're doing on your computer

University of Victoria

Personnel Security

- RUN. HIDE. FIGHT.

Surviving an Active Shooter Event

https://www.youtube.com/watch?v=5VcSwejU2D0 (5:55)

University of Victoria

Physical Security

- physical security encompasses a set of threats, vulnerabilities, and risks
- includes design and layout, environmental components, emergency response readiness*, training, access control, intrusion detection, and power and fire protection
- protect people, data, equipment, systems, facilities, assets

Physical Security

- similarities in language between physical and logical security

- consider convergence between physical and logical
  - access controls, access badges
  - proximity cards for building access shifting to smart cards enabling PC login and multi-factor authentication

- network security does not mean physical security is obsolete or legacy – **you need both**!
  - consider cases where attacker has physical access or steals your gear

Physical Security

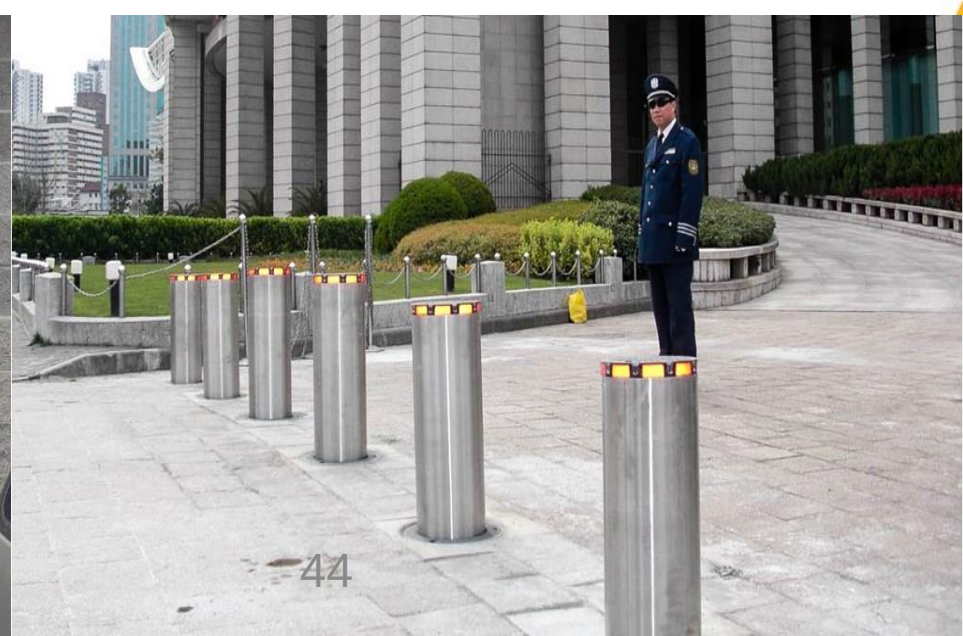
- guards, fences, gates, cages (eg. shipping example)
- locks, safes, secure cabinets, signs
- walls, barriers, barricades/bollards, astragals
- lighting, CCTV
- access controls
- air gaps, man traps
- prevention/deterrent,

  detection, response

tailgating
fences,
gates

astragal

bollards



University of Victoria

Threat Categories

- natural environment threats
  - floods, earthquakes, storms and tornadoes, fires, extreme temperature
- supply system threats
  - power distribution outages, communications, interruptions, and interruption of other resources such as water, gas, air filtration
- manmade threats
  - unauthorized access (both internal and external), explosions, employee errors and accidents, vandalism, fraud, theft, collusion
- politically motivated threats
  - strikes, riots, civil disobedience, terrorism, bombings

University of Victoria

Physical Security - Examples

- store examples
  - greetings on entry, rulers on doors of stores
  - too many posters on exterior windows
- controlling vegetation and bushes – obstructing signs, lights, doors
  - tailgating examples
- locked door may not be sufficient
  - consider the motivation
- example
  - financial organization doesn't have a secure recycling bin/shredder

Physical Security

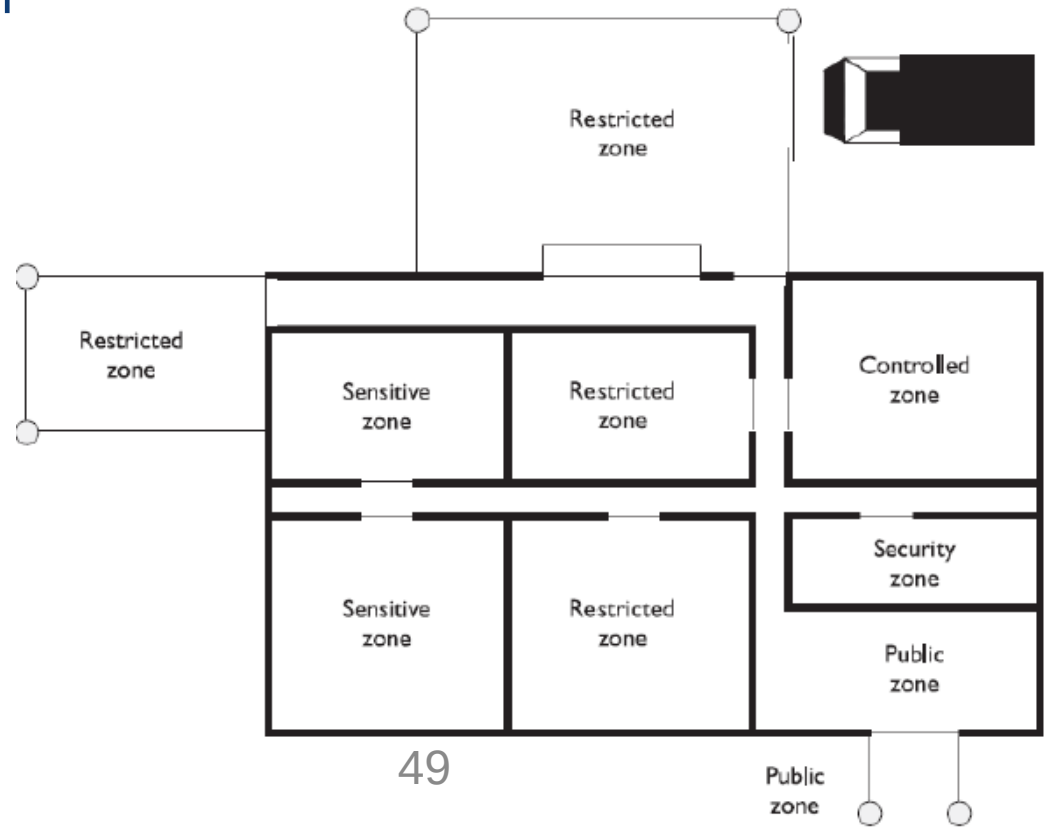
- device security
  - docking station, cable locks, screen filters
- environmental controls
  - HVAC, hot/cold aisles, fire suppression
- environmental design
  - CPTED: crime prevention through environmental design
  - physical environment can reduce crime by affecting human behavior
  - three main strategies: **natural access control, natural surveillance, natural territorial reinforcement**

Design Goals

1) deter criminal activity (layout and policies)
2) delay intruders (add impediments – locks/fences/barriers, slow and monitor people)
3) detect intruders (allow criminal activity to be detected)
4) assess situation (actions to be taken when event occurs)
5) respond to intrusions and disruptions (appropriate responses to intruders and disruptions)

Design

- natural access control
  - follow the flow of people
  - consider placement of doors, lights, fences and landscaping to satisfy security goals in least obtrusive and most appealing manner
  - consider security zones with different classifications



University of Victoria

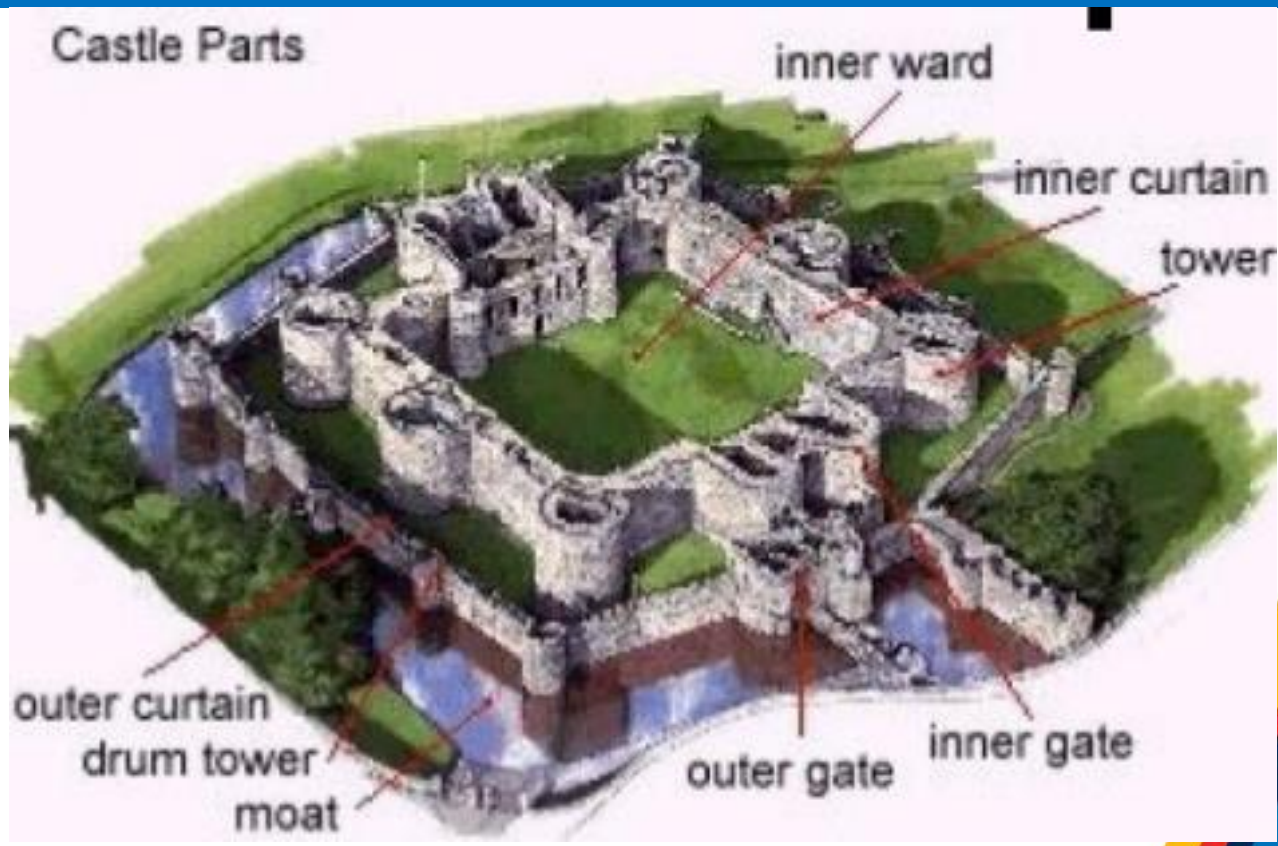
Physical Security

- natural surveillance
  - visibility of all areas to discourage crime
  - organized (security guards), mechanical (CCTV), large windows, open benches

- natural territorial reinforcement
  - promotes feeling of community in the area and extends sense of ownership to the employees
  - eg. parks, courts, fields

Layered Defence

- shouldn't rely on any single physical security concept but on use of multiple approaches that support one another



University of Victoria

Physical Security

- assessment
  - construction materials of wall and ceilings
  - power distribution systems
  - communication paths and types
  - surrounding hazardous materials
  - regulations and legal issues
  - exterior components (proximity to airports, highways, railroads, electromagnetic interference, vehicle activity, neighbours)
  - eg. external warehouse door

Physical Security

- selection criteria
  - **visibility** – desired visibility depends on organization and processes being carried out
  - **surrounding area and external entities** – consider nature of operations of surrounding businesses
  - **accessibility** – ease with which employees and responders can access facility
  - **natural disaster** – likelihood of floods, tornadoes, earthquakes, hurricanes, etc.

Physical Security NOT TESTED

- selection criteria

- **Walls**
  - Combustibility of material (wood, steel, concrete)
  - Fire rating
  - Reinforcements for secured areas
- **Doors**
  - Combustibility of material (wood, pressed board, aluminum)
  - Fire rating
- **Ceilings**
  - Combustibility of material (wood, steel, concrete)
  - Fire rating
- **Windows**
  - Translucent or opaque requirements
  - Alarms

Flooring

Weight-bearing rating
Combustibility of material (wood, steel, concrete)

- **Heating, ventilation, and air conditioning**
  - Positive air pressure
  - Protected intake vents
  - Dedicated power lines
  - Emergency shutoff valves and switches
- **Electric power supplies**
  - Backup and alternate power supplies
- **Water and gas lines**
  - Shutoff valves—labeled and brightly painted for visibility
  - Placement—properly located and labeled
- **Fire detection and suppression**
  - Placement of sensors and detectors
  - Placement of suppression systems

Physical Security

- fences
  - 3-4 ft: deter casual intruders
  - 6-7 ft: too tall to climb easily
  - 8+ ft: deter more determined intruders esp. with razor wire

TESTED

- gates
  - class 1: residential use
  - class 2: commercial use
  - class 3: industrial use
  - class 4: restricted area

NOT TESTED

Physical Security NOT TESTED

- lighting systems
  - continuous array of lights, even lighting
  - standby only certain times or schedule
  - movable repositioned as needed
  - emergency when power is out
- types of lighting
  - fluorescent, mercury vapor, sodium vapor, quartz lamps
- levels of lighting
  - recommended 10 to 12 foot-candles over parked cars and 15 to 20 foot-candles in walking and driving aisles

University of Victoria

foot-candle is one lumen per square foot
lumen is measure of quantity of visible light emitted by source per unit of time

Physical Security NOT TESTED

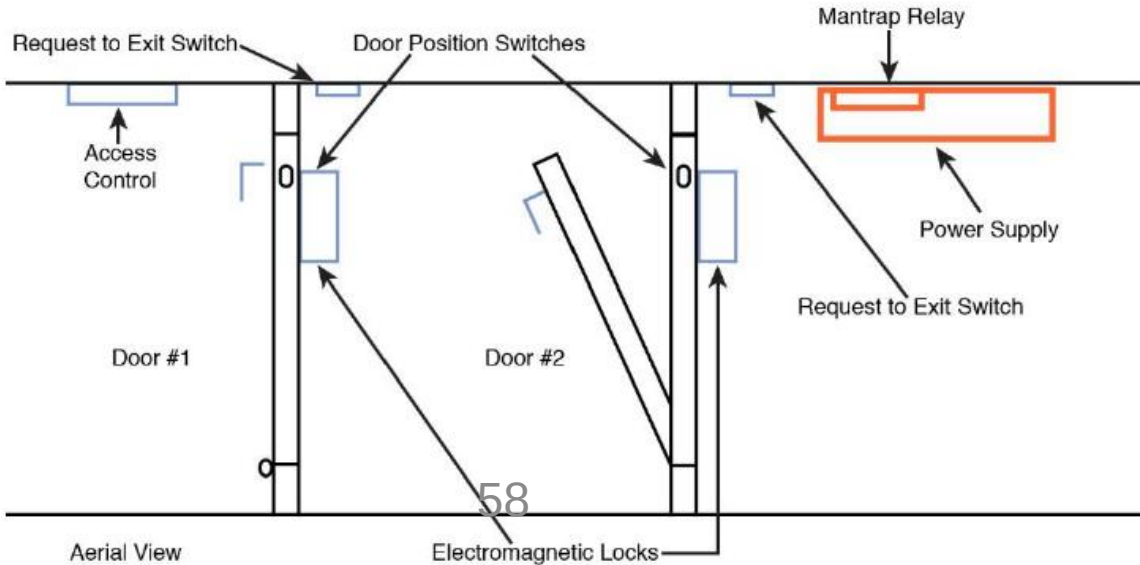
- intrusion detection
  - infrared
  - electromechanical — detecting break in system
  - photometric / photoelectric — changes in light; windowless areas
  - acoustical systems — based on sound
  - wave motion — detect motion that disturbs wave pattern
  - capacitance — magnetic field
  - CCTV — monitored in real time, video analytics, or viewed as needed later

Physical Security

- guards
  - **‘observe and report’**
  - visitors sign into “guest book” - who/when/where/why
  - escorted access (accompanying visitors into, around, and out of facility), knowing where they are at all times

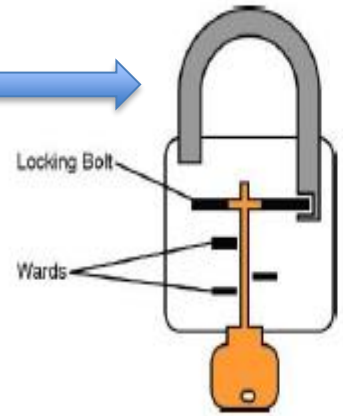
avoid tailgating or piggybacking

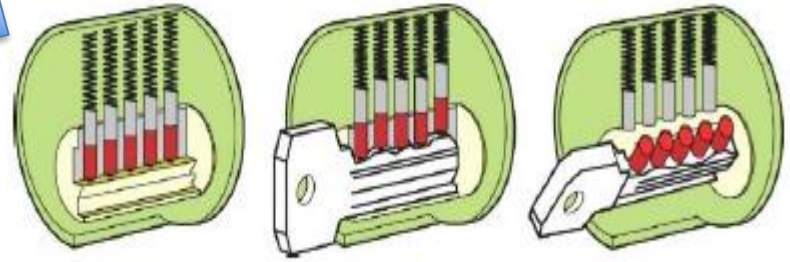
- door types
  - vault doors, personnel doors, industrial doors
  - vehicle access doors, bullet-resistant, turnstile, mantraps

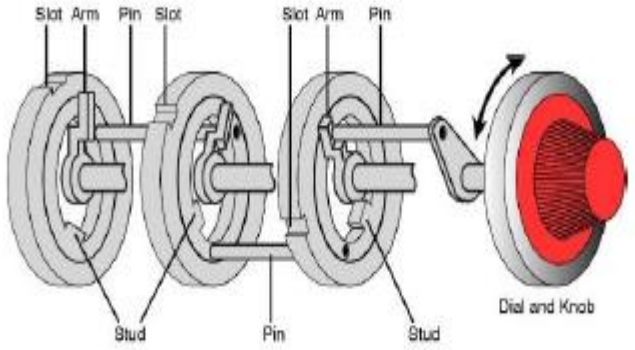


Locks

- warded locks
- tumbler locks
- combination locks
- electronic locks
- proximity cards
- biometrics







University of Victoria

Glass NOT TESTED

- standard
- tempered heated in the process – extra strength
- acrylic stronger but toxic if burned
- laminated multiple layers – extra strength

University of Victoria

Fire Suppression

- wet pipe
  - water in the pipes
- dry pipe
  - water in a tank not in the pipes
- preaction
  - springhead has thermal fusible link
- deluge
  - large amounts of water
- halon gas
  - works by chemically reacting with fuel, oxygen, ignition src
  - myth that Halon takes O2 out of air
  - debatable whether it kills people

University of Victoria

certification: also gas suppression Aero-K, fm 200

Fire Extinguishers

- Class A = (Stand for Ash): Wood and Paper
  - extinguish with water and soda
- Class B = (Stand for Boil): Liquid, Flammable Gases
  - extinguish with gas and soda acid
- Class C = (Stand for Current): Electrical Current
  - extinguish with non-conductive like gas
- Class D = (Stand for Dilute): Combustible Metals
  - extinguish with dry powder

Power Outages NOT TESTED

- types
  - surge — prolonged high voltage
  - brownout — prolonged drop in power
  - fault — momentary power outage
  - blackout — prolonged power outage
  - sags — momentary reduction in level of power
- static electricity: mats, write bands, control humidity
- maintain power: generator, UPS

University of Victoria

Assigned Reading

- no reading
- optional lab on HTML


University
of Victoria

Business Continuity & Disaster Recovery

Business Continuity Plan (BCP)

- plans and framework to ensure business can continue in an emergency
- minimize cost associated with disruptive event and mitigate risk
- 4 elements:
  1) scope and plan initiation
  2) business impact assessment (BIA)
  3) business continuity plan development
  4) plan approval and implementation

  …..maintenance

University of Victoria

Business Impact Assessment (BIA)

- identify the impact of a disruptive event on the business (quantitative – eg. financial or qualitative – eg. brand)

- 3 goals of BIA:
  1) criticality prioritization
  2) maximum tolerable downtime estimation
  3) resource requirements

- identify which business units are critical to maintaining operations

- catalog of important business processes and criticality

University of Victoria

Business Impact Assessment (BIA)

- loss impact analysis quantitative and qualitative

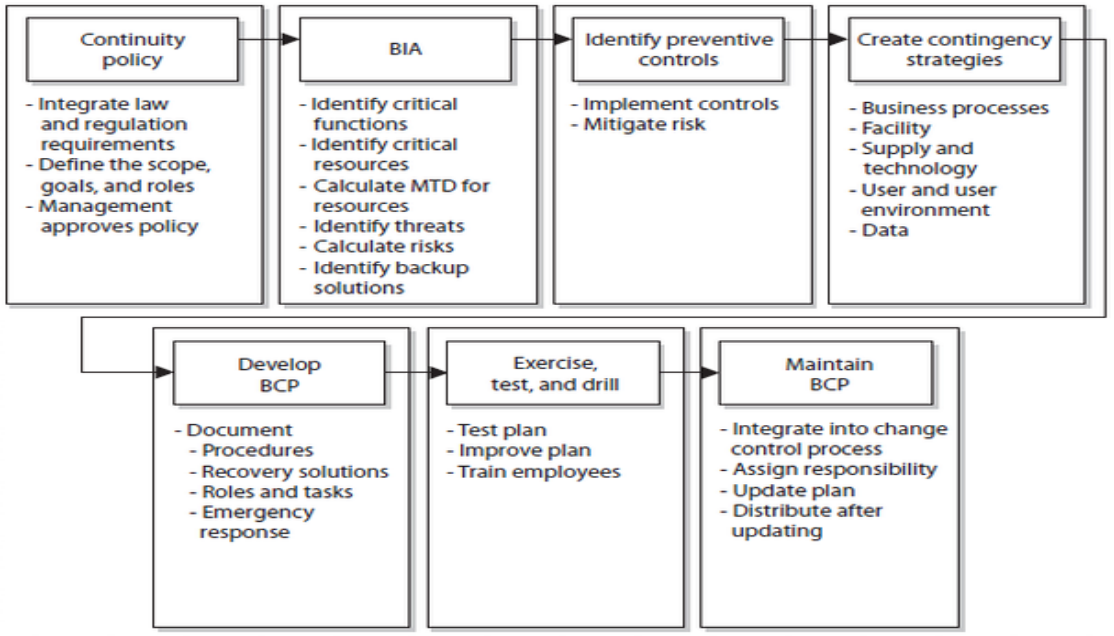
- Steps:
  1) information gathering
  2) risk analysis and threat assessment
  3) determine key metrics (maximum tolerable downtimes, recovery time objective, recovery point objective)
  4) develop impact statements

- ensure remember to establish criticality levels to assist with prioritization

Business Continuity Plan Development

1) identify the business areas
2) engage the stakeholders
3) develop and populate the plan
4) communicate and educate on the plan
5) test the plan
6) review and update on a regular basis

different approaches



1) Identify critical functions and priorities for restoration.
2) Identify support systems needed by critical functions.
3) Estimate potential outages and calculate the minimum resources needed to recover from the catastrophe.
4) Select recovery strategies and determine what vital personnel, systems, and equipment will be needed to accomplish the recovery.
5) Determine who will manage the restoration and testing process.
6) Calculate what type of funding and fiscal management is needed to accomplish these goals.

Business Continuity Plan (BCP)

- proactive
- provide procedures for sustaining essential business operations while recovering from a significant disruption
- continuation of critical business processes in an organization using different people, equipment, facilities
- long term planning of ensuing business can continue if emergency happens

University of Victoria

Differences between BCP & DRP

BCP	DRP
• activities required to ensure continuation of critical business processes in an organization	• assessment, salvage, repair, and restoration of damaged facilities and systems
• alternate personnel, equipment, and facilities	• often focuses on IT systems
• often includes non-IT aspects of business	

Backup Strategies

- **Full**
  - all files are backed up modified or not (archive bit is reset)
- **Incremental**
  - archive data that has changed since the last full or incremental backup (archive bit is reset)
- **Differential**
  - archive data that changed since the last full backup only (archive bit isn’t reset)

Business Continuity Plan (BCP)

- **Business Impact Analysis**
  - A detailed and documented process designed to identify and prioritize business functions and workflow, including establishing Recovery Time Objectives by assessing impacts over time that might result if an organization was to experience a disruptive event.

- **Business Priority Service**
  - Business function or process that is not mission critical, but, should it not be performed, could lead to the loss of a major government service.

- **Critical Services**
  - General term that collectively refers to Business Priority and Mission Critical services.

University of Victoria

Business Continuity Plan (BCP)

- **Recovery Point Objectives (RPO)**
  - The point in time, relative to pre-disaster, at which available data from backup can be restored – max amount of data loss or work loss for a given process (eg. weekly backups RPO = 1 week)

- **Recovery Time Objectives (RTO)**
  - Amount of time that a business function can withstand an interruption before a negative or unacceptable consequence occurs.
  - Time allowed to recover systems – max amount of time process or system will be unavailable.

Business Continuity Plan (BCP)

- **Mean Time Between Failures (MTBF)**
  - how frequent are failures
- **Mean Time to Repair (MTTR)**
  - how long to repair equipment on average
- **Availability Formula**
  - MTBF / (MTBF + MTTR) = availability

525,600 – 6 = 525,594
525,594/525,600 * 100 = 99.99885%

University of Victoria

Business Continuity Plan (BCP)

Availability %	Downtime per year[note 1]	Downtime per month	Downtime per week	Downtime per day
55.5555555% ("nine fives")	162.33 days	13.53 days	74.92 hours	10.67 hours
90% ("one nine")	36.53 days	73.05 hours	16.80 hours	2.40 hours
95% ("one nine five")	18.26 days	36.53 hours	8.40 hours	1.20 hours
97%	10.96 days	21.92 hours	5.04 hours	43.20 minutes
98%	7.31 days	14.61 hours	3.36 hours	28.80 minutes
99% ("two nines")	3.65 days	7.31 hours	1.68 hours	14.40 minutes
99.5% ("two nines five")	1.83 days	3.65 hours	50.40 minutes	7.20 minutes
99.8%	17.53 hours	87.66 minutes	20.16 minutes	2.88 minutes
99.9% ("three nines")	8.77 hours	43.83 minutes	10.08 minutes	1.44 minutes
99.95% ("three nines five")	4.38 hours	21.92 minutes	5.04 minutes	43.20 seconds
99.99% ("four nines")	52.60 minutes	4.38 minutes	1.01 minutes	8.64 seconds
99.995% ("four nines five")	26.30 minutes	2.19 minutes	30.24 seconds	4.32 seconds
99.999% ("five nines")	5.26 minutes	26.30 seconds	6.05 seconds	864.00 milliseconds
99.9999% ("six nines")	31.56 seconds	2.63 seconds	604.80 milliseconds	86.40 milliseconds
99.99999% ("seven nines")	3.16 seconds	262.98 milliseconds	60.48 milliseconds	8.64 milliseconds
99.999999% ("eight nines")	315.58 milliseconds	26.30 milliseconds	6.05 milliseconds	864.00 microseconds
99.9999999% ("nine nines")	31.56 milliseconds	2.63 milliseconds	604.80 microseconds	86.40 microseconds

525600 minutes in a year

Wikipedia – High Availability

Business Continuity Plan (BCP)

- **Work Recovery Time (WRT)**
  - time required to configure systems
- **Minimum Operating Requirements (MOR)**
- **Maximum Tolerable Downtime (MTD) formula:**
  - MTD = RTO + WRT
- period of time after which the organization would suffer considerable pain if the process were unavailable

Disaster Recovery

- **Disaster Recovery**
  - refers to Information Technology (IT) recovery
  - Disaster Recovery Plans (DRPs) document process to recover and restore technology (computer processing, applications and data) needed to support critical business functions

- **Mission Critical Services**
  - functions and processes that, should they not be performed, could lead to loss of life or injury, personal hardship to citizens, major damage to the environment, or significant loss of revenue or assets

Disaster Recovery Plan (DRP)

- reactive – when an IT disaster strikes (DRP heavily IT focused)
- **management approved plan** that addresses operational processes for the recovery of a damaged facility
- what actions need to be taken to restore IT operations as quickly as possible
- assessment, salvage, repair, and eventual restoration of damaged facilities and systems
- **DRP is the effort to recover IT system and applications whereas BCP is effort to recover business processes**
- **detailed procedures** to facilitate recovery of capabilities at an alternate site

Disaster Recovery Plan (DRP)

- recover from emergency with minimum impact on business
- plan for before, during, and after the event
- objective is to move critical processes to an alternate site and return primary site and normal processing within a timeframe that minimizes loss
- **people are the number one priority**

Disaster Recovery Plan (DRP)

- **Hot site:**
  - fully configured computer facility with electrical power, heating, ventilation, and air conditioning (HVAC and **functioning** file/print servers and workstations – has all hardware and critical app data mirrored in real time (resume operations in < 1 hr)

- **Warm site:**
  - computer facility available with electrical power, heating, ventilation, and air conditioning (HVAC), limited file/print servers and workstations – data may not be in real time, backups may be required – MTD between 1 and 3 days with 24-48 hr recovery time

- **Cold site:**
  - computer facility available with electrical power, heating, ventilation and air conditioning (HVAC) – no computer hardware (long MTD required)

Disaster Recovery Plan (DRP)

- Data Centre alternatives
  - **Electronic Vaulting**
    - transfer of backup data to offsite location (transfer occurs over connectivity)
  - **Remote Journaling**
    - parallel processing of transactions to alternate site (transfer occurs live) – provide redundancy for transactions
  - **Database Shadowing**
    - uses live processing of remote journaling but creates more redundancy by duplicating database sets to multiple servers