IT Staff Security Training for Welfare Sector

MAKE SMART SMARTER

Objectives

- To learn how to control and manage information security
- To learn the routine housekeeping work and monitoring required
- To learn the techniques of detecting vulnerabilities/ security breach, and how to respond when there is a security incident
- To learn up-to-date IT security technology
- To understand resource/ cost impact on IT security measures

Outlines

1. Introduction of Cyber Security
2. Latest Trends of Cyber Attacks
3. Major Security Domains
   - ❖ IT Security Governance
     - Security Policy and Related Documents
     - Information Classification and Handling
     - Risk Management
     - Exercise : Use of “Seven Habits of Cyber Security” to conduct self assessment
   - ❖ Websites and Web Applications
     - Web Security Attack & Defense
     - Exercise: Using OWASP Zed Attack Proxy (ZAP)

Outlines

- Network Security
  - Basic Network Security Concept (DMZ, LAN, WiFi)
  - Exercise : Network Scanner - NMap/Zenmap
- System Security
  - System Hardening
  - Vulnerability Management
  - Exercise: Vulnerability Scanning Tool - Nessus
  - Exercise: IIS Crypto - Nartac
- Cloud Security
  - Best Practice of Cloud Security

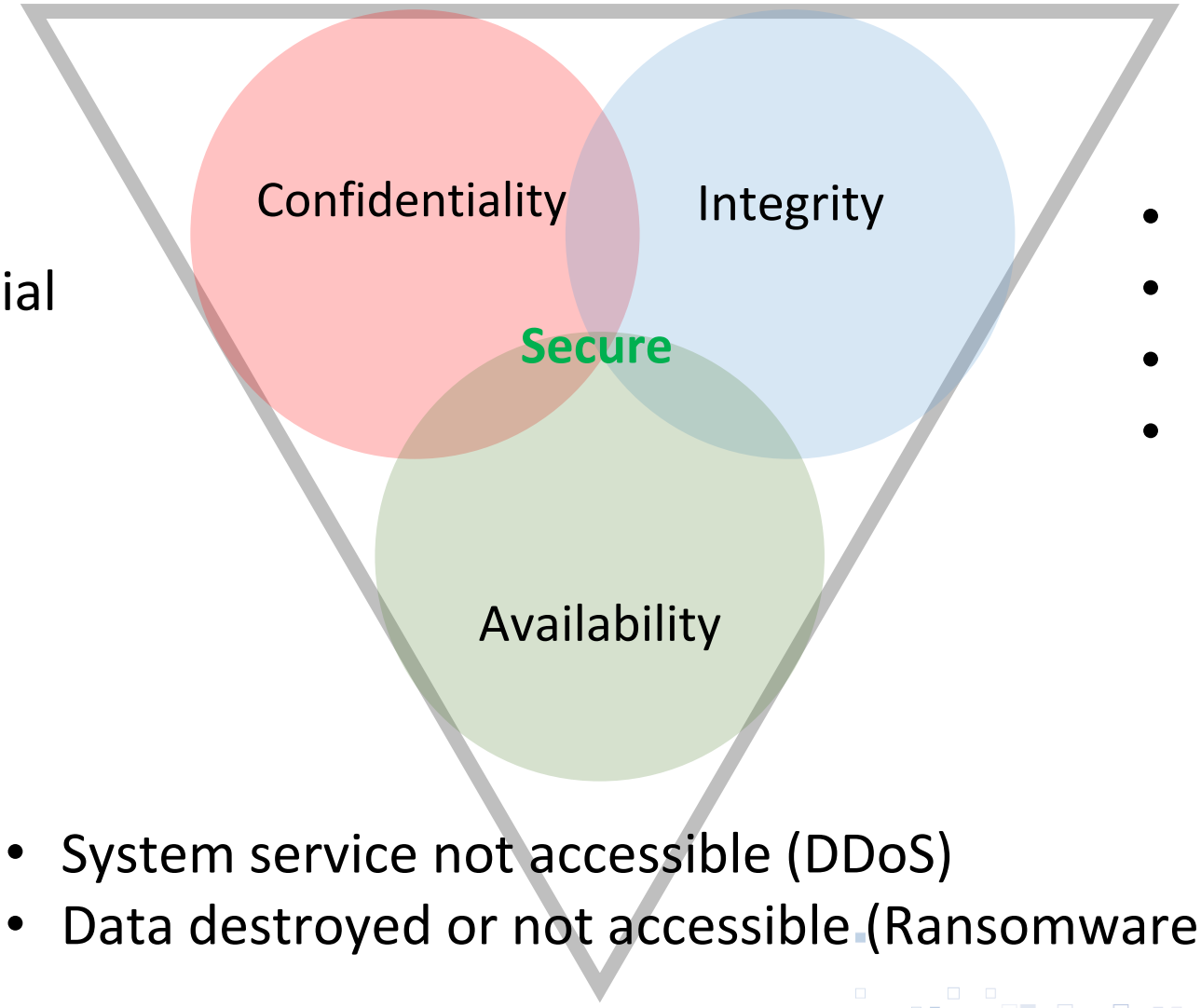
Outlines

- Remote Access/Work from Home
  - Comparison of Remote Access Solutions
  - Best Practice of Remote Work
- Incident Response
  - Methodology of Incident Response
  - Gathering Information of Incident Response
  - Exercise: Gathering Information Techniques
  - Reporting security incidents
  - Exercise: Use of Incident Response Form and Records
- Q&A

Introduction of Cyber Security

MAKE SMART
SMARTER

The CIA Triad



- Leaking confidential data

- Data contaminated
- Forged transaction
- System compromised
- Identity spoofed

- System service not accessible (DDoS)
- Data destroyed or not accessible (Ransomware)

Loss of Confidentiality

Share Tweet Share Pin it + −

The 2018 data breach that exposed the personal information of over 400,000 British Airways customers will cost the company £20 million, in the form of one of the largest GDPR fines to date. The UK ICO's decision found that the travel giant was negligent due to "poor security arrangements" creating a hole in the network that was exploited by attackers for two months before being discovered.

MAKE SMART SMARTER

Source: https://www.cpomagazine.com/data-protection/uk-ico-levies-gdpr-fine-of-20-million-for-british-airways-2018-data-breach-substantially-less-than-the-initial-183-million/

Loss of Integrity

Save the Children charity lost £800,000 to sophisticated BEC scam

December 14, 2018

Well-known U.S.-based charity Save the Children Foundation lost as much as £800,000 to a clever business email compromise scam (BEC) last year after a hacker hacked into an employee's email account and defrauded the charity into sending the funds to a fraudulent entity in Japan.

Source: https://www.teiss.co.uk/save-the-children-bec-scam/

Loss of Availability

Cyber attack shuts major US pipeline system

Assault on Colonial Pipeline underscores vulnerabilities in critical US infrastructure

The Colonial Pipeline is the largest refined products pipeline in the US © AP

Lauren Fedor in Washington, **Myles McCormick** in New York and **Hannah Murphy** in San Francisco MAY 9 2021

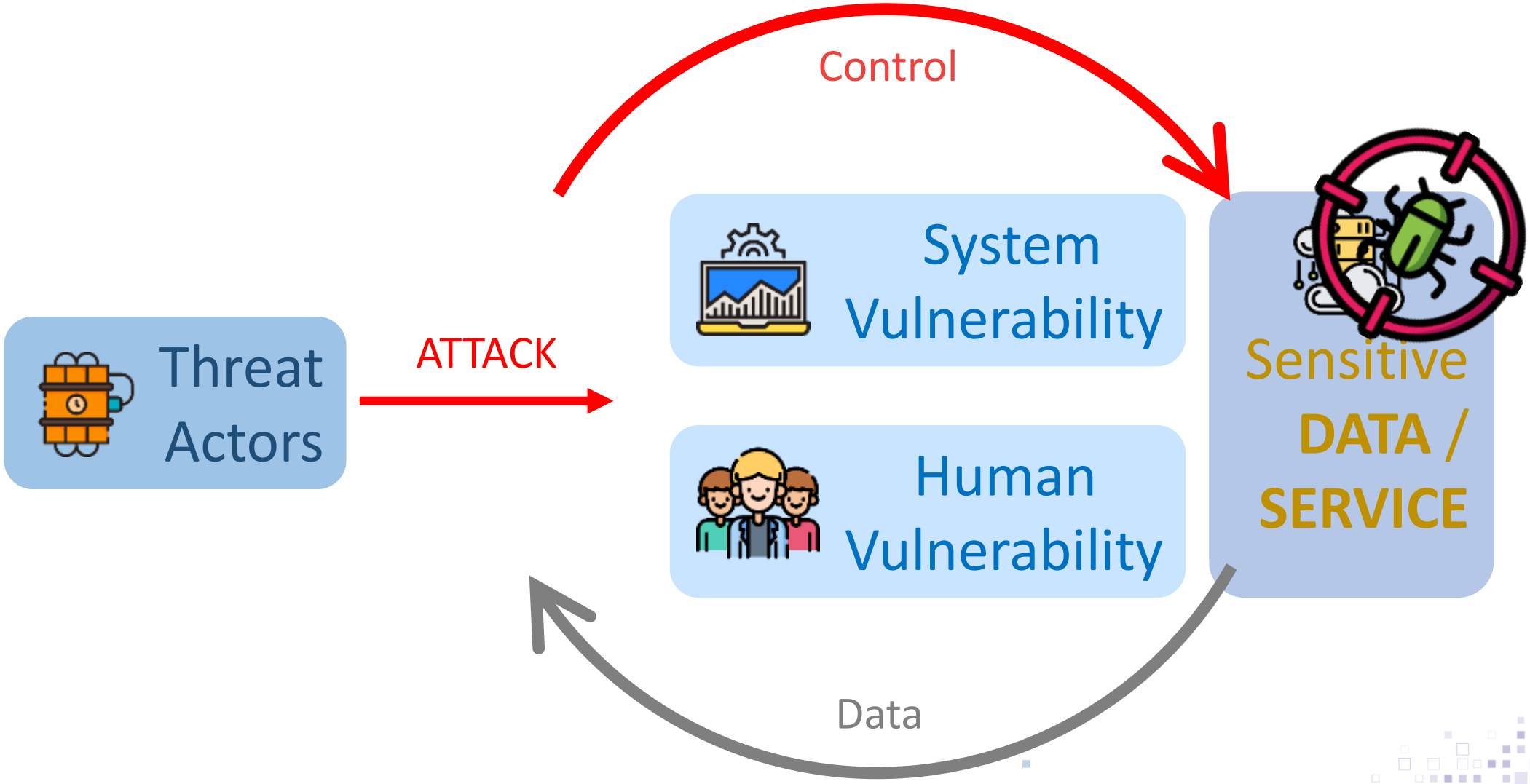
283

A major US fuel pipeline has been shut down after a ransomware attack, in an incident that underscores the vulnerabilities in America's critical infrastructure.

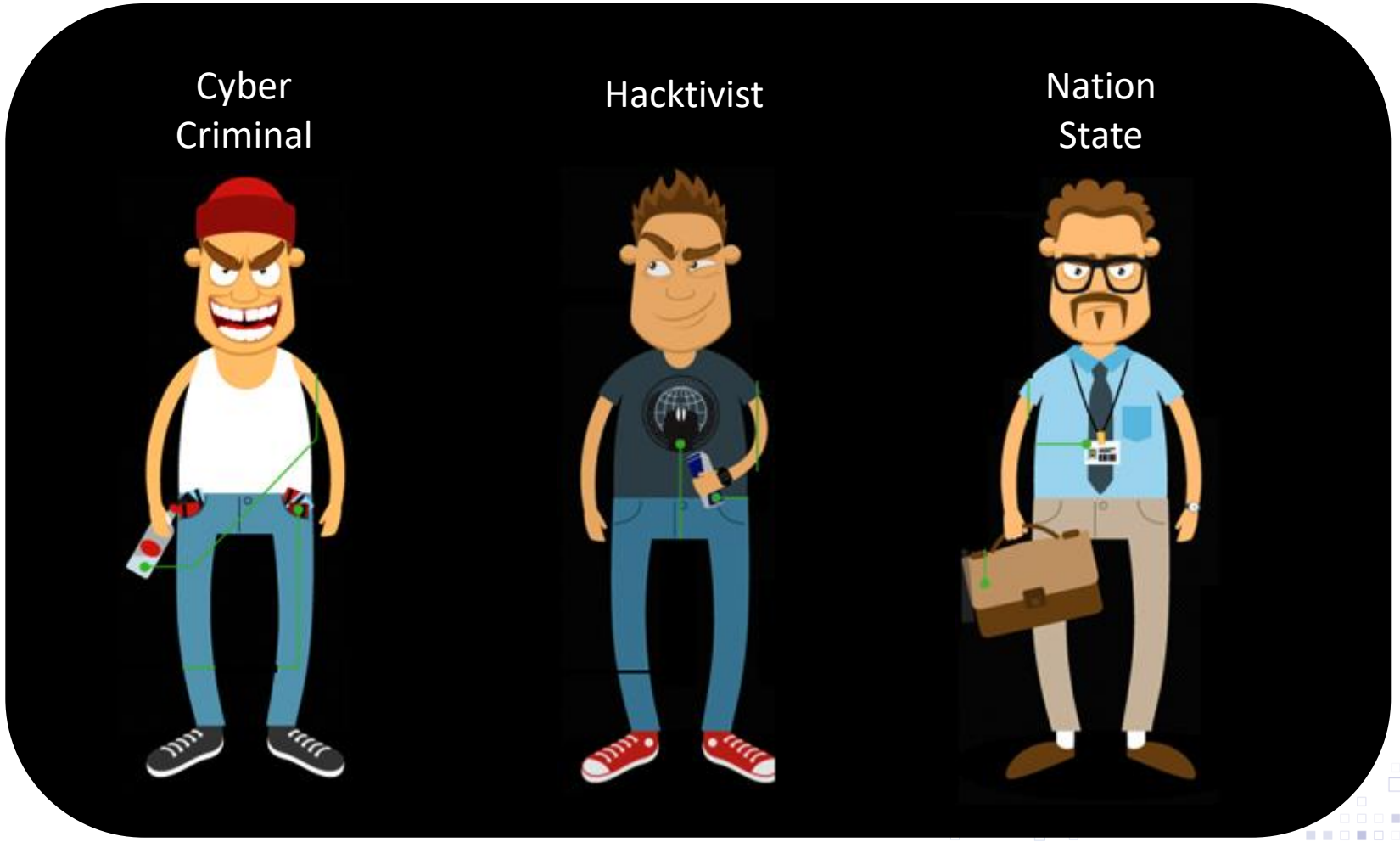
MAKE SMART SMARTER

Source: https://www.ft.com/content/2ce0b1fe-9c3f-439f-9afa-78d77849dd92

Threat, Vulnerability & Attack



Threat Actors



MAKE SMART SMARTER

Threat Actors | *Modern Attackers*

Cyber Criminal

- Motive: **$$$**
  - ✓ Underground Economy
  - ✓ Crime-as-a-Service
- Botnet infrastructure
- Advanced (banking) Trojan
- Moving to mobile and cloud

MAKE SMART SMARTER

Threat Actors | *Modern Attackers*

- Motive:
  Ideological
- High Profile
- Crowdsourcing
- Data leakage: **DDoS**

Hacktivist

MAKE SMART SMARTER

Threat Actors | *Modern Attackers*

- Motive:

  Political / Military
- Targeted:

  Critical Infrastructure, or Espionage
- Low Profile
- Advanced Malware / Attacks

Nation State

MAKE SMART SMARTER

Types of Insider Threats

Compromised Users

Employees that don’t know they are compromised

Careless Users

Employees that leave a computer or terminal unlocked or otherwise violate cyber security best practices

Malicious Users

They usually have legitimate user access to the system and wilfully extract data or Intellectual Property

System Vulnerability

- Unpatched Software
- Misconfiguration
- Missing/Poor Encryption
- Bugs
- Zero-days
- …

Human Vulnerability

- Malicious Insider
- Careless Staff
- Staff vulnerable to social engineering
- Weak Passwords
- …

Financial Loss

The average economic loss in cyber security attack for a mid-sized organization in Hong Kong

US$38,000

- **Business Downtime**
- **Damaged Assets**
- **Recovery Cost**
- **Financial Penalties**

Source: The result is commissioned by Microsoft and carried out by consultancy Frost & Sullivan, surveyed 1,300 business and IT executives in the Asia-Pacific region in 2018.

Damage to Brand Image and Reputation

Data Security by CimTrak. PHOTO: Cybercrime Magazine.

60 Percent Of Small Companies Close Within 6 Months Of Being Hacked

Source: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/

Legal Consequences

General Data Protection Regulation (GRPR)

The Personal Data (Privacy) Ordinance (PDPO)

British Airways fined £20m over GDPR breach

OUT-LAW NEWS | 19 Oct 2020 | 3:52 pm | 4 min. read

British Airways (BA) has been fined £20 million by the UK's data protection authority over data security failings which enabled unauthorised access to be obtained to personal and payment card information relating to more than 400,000 of its customers.

Source: https://www.pinsentmasons.com/out-law/news/british-airways-fined-20m-over-gdpr-breach

Legal Consequences

General Data Protection Regulation (GDPR)

The Personal Data (Privacy) Ordinance (PDPO)

Hong Kong Government Considering Amendments to the PDPO

3 . Sanctioning Powers

- Confer additional powers on the PCPD to impose **administrative fines**
- Maximum level of fine may be **a fixed amount or a percentage of the annual turnover**, whichever is higher
- Administrative fines **credited to the HKSAR Government** and not the coffers of the PCPD

Source: https://www.bakermckenzie.com/en/insight/publications/2020/01/hong-kong-considering-amendments-pdpo

Latest Trends of Cyber Attacks

MAKE SMART
SMARTER

Cybersecurity Trends in 2021

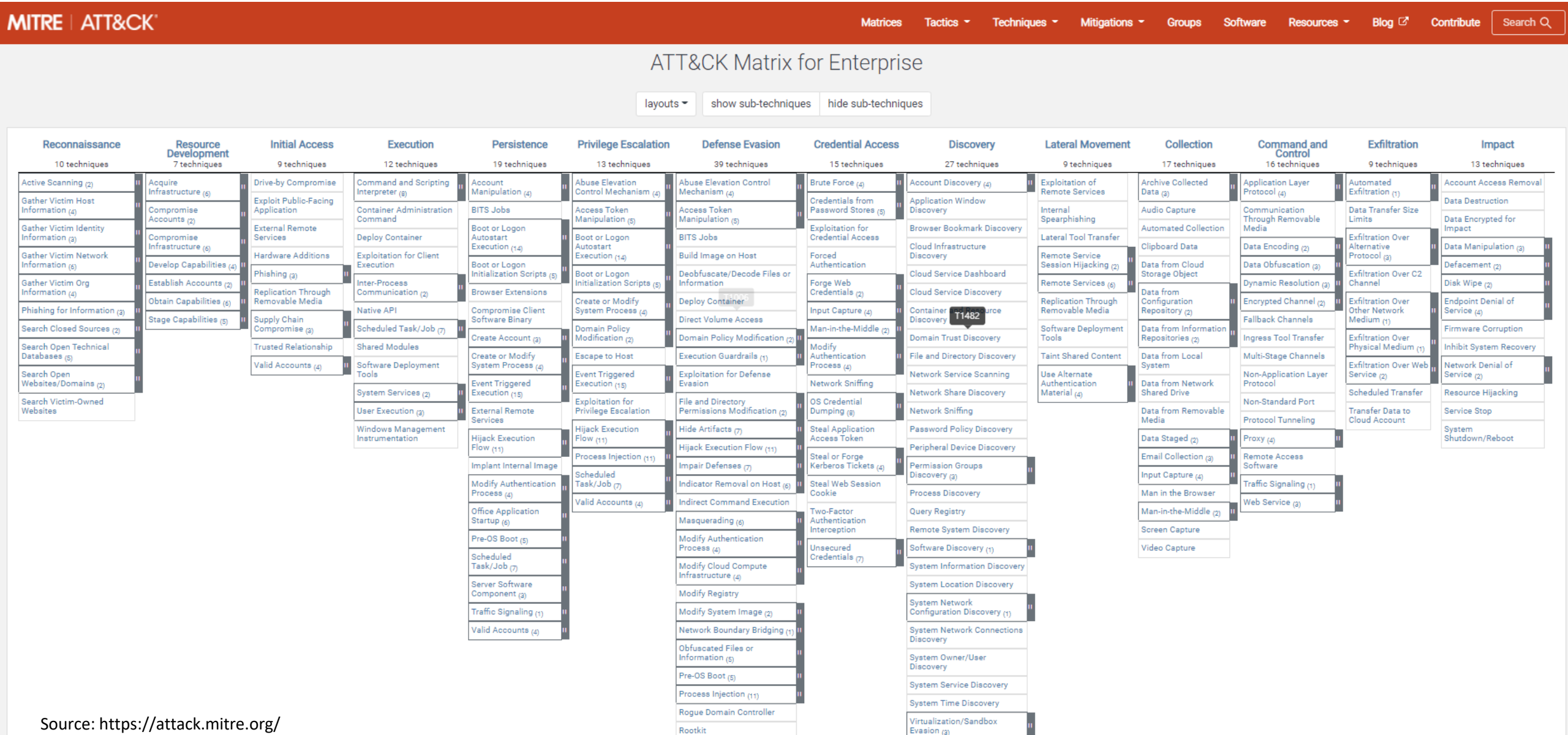
- Remote Service Attacks
- Insider Threats
- Targeted Ransomware
- Spear Phishing Attacks
- Supply Chain Attacks
- Cloud Threats
- Deepfakes
- IOT Security Gap

MAKE SMART SMARTER

Cyber Kill Chain model

Image Credit: Netsurion

ATT&CK Matrix



Source: https://attack.mitre.org/

- Remote Service Attacks
- Insider Threats
- Targeted Ransomware

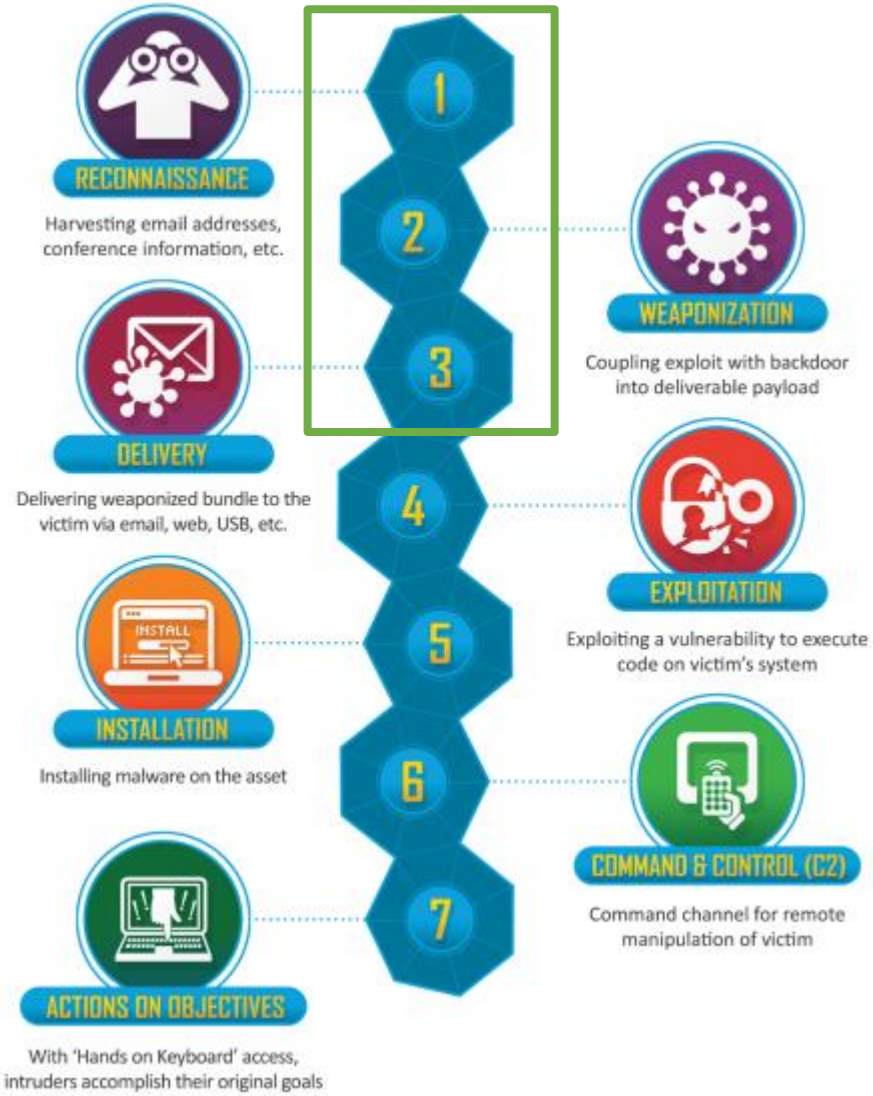
Case Study : Ransomware Attack

A ransomware attack started with a student downloaded a “Free” software

Case Study : Ransomware Attack

Background: A European biomolecular research institute involved in COVID-19 related research was infected Ryuk Ransomware.

1. A student tries to download a "Crack" version of a data visualization software tool
2. A security alert was triggered from Windows Defender
3. The student disabled the Windows Defender and firewall, then download the software again.
4. A malicious info-stealer was downloaded to student's computer

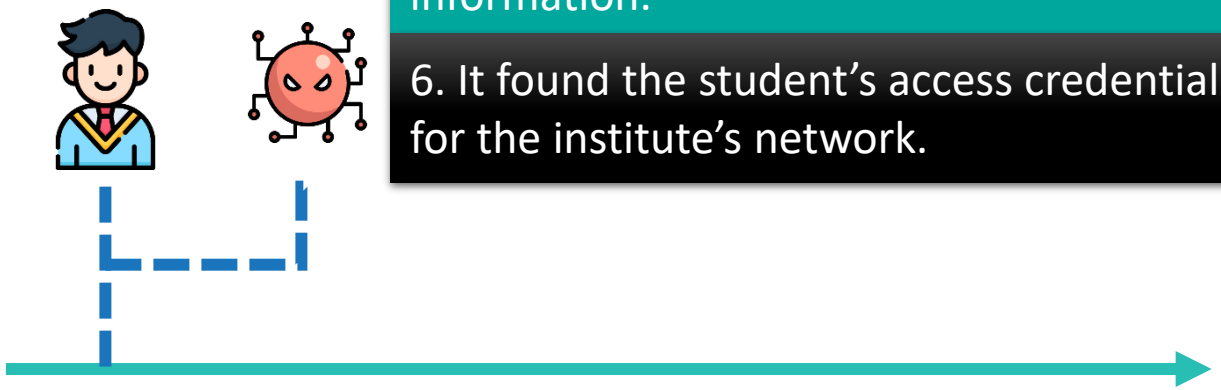


Source: https://news.sophos.com/en-us/2021/05/06/mtr-in-real-time-pirates-pave-way-for-ryuk-ransomware/

Image Credit: Lockheed Martin

Case Study : Ransomware Attack

Background: A European biomolecular research institute involved in COVID-19 related research was infected Ryuk Ransomware.



5. This malware starts to steal the student's information.

6. It found the student's access credentials for the institute's network.

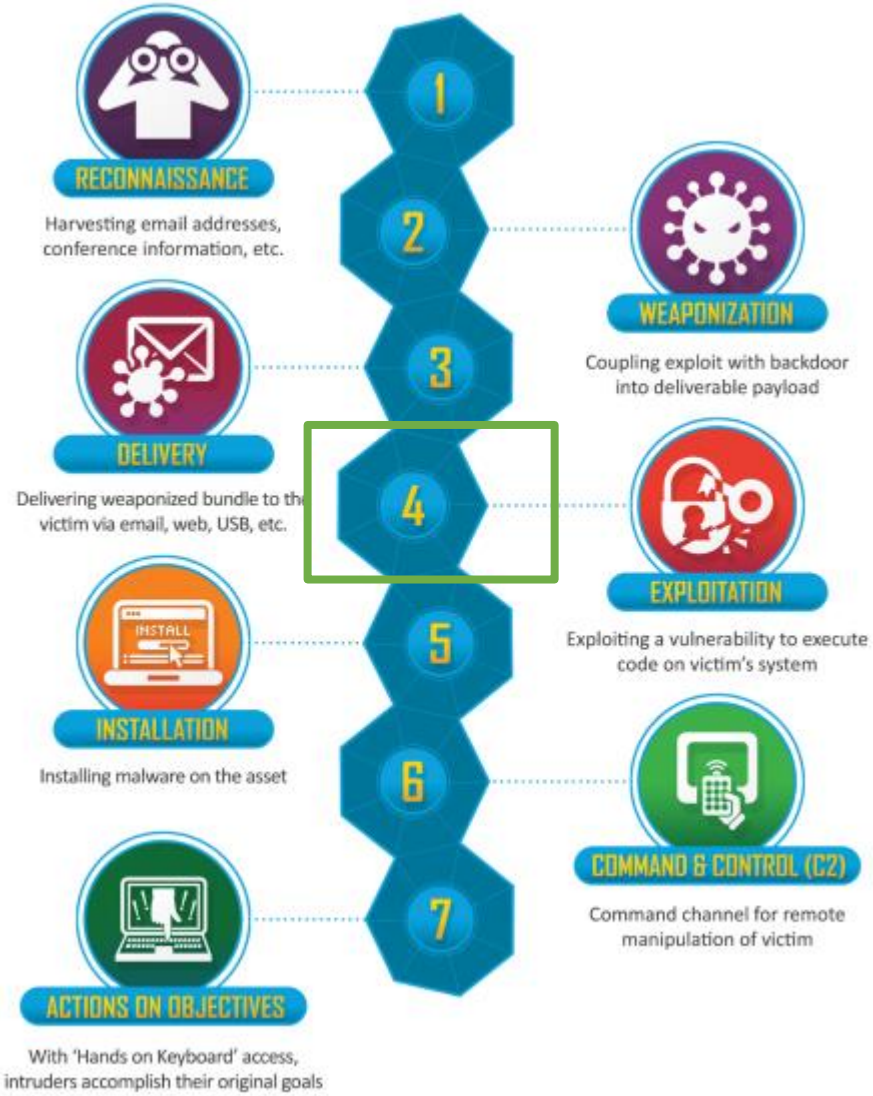
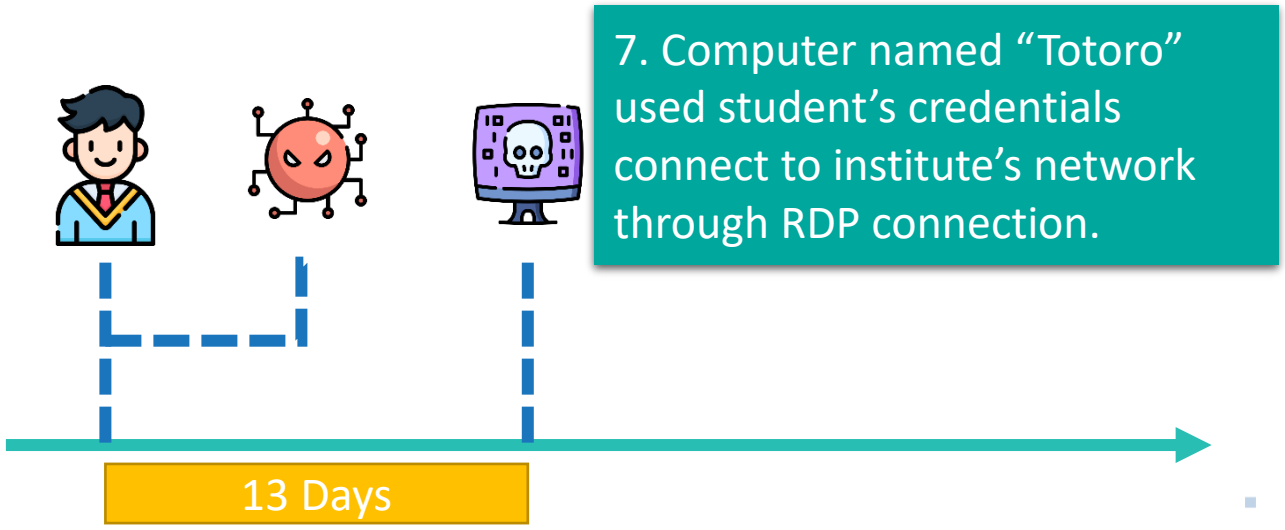


Image source: lockheedmartin

Case Study : Ransomware Attack

Background: A European biomolecular research institute involved in COVID-19 related research was infected Ryuk Ransomware.



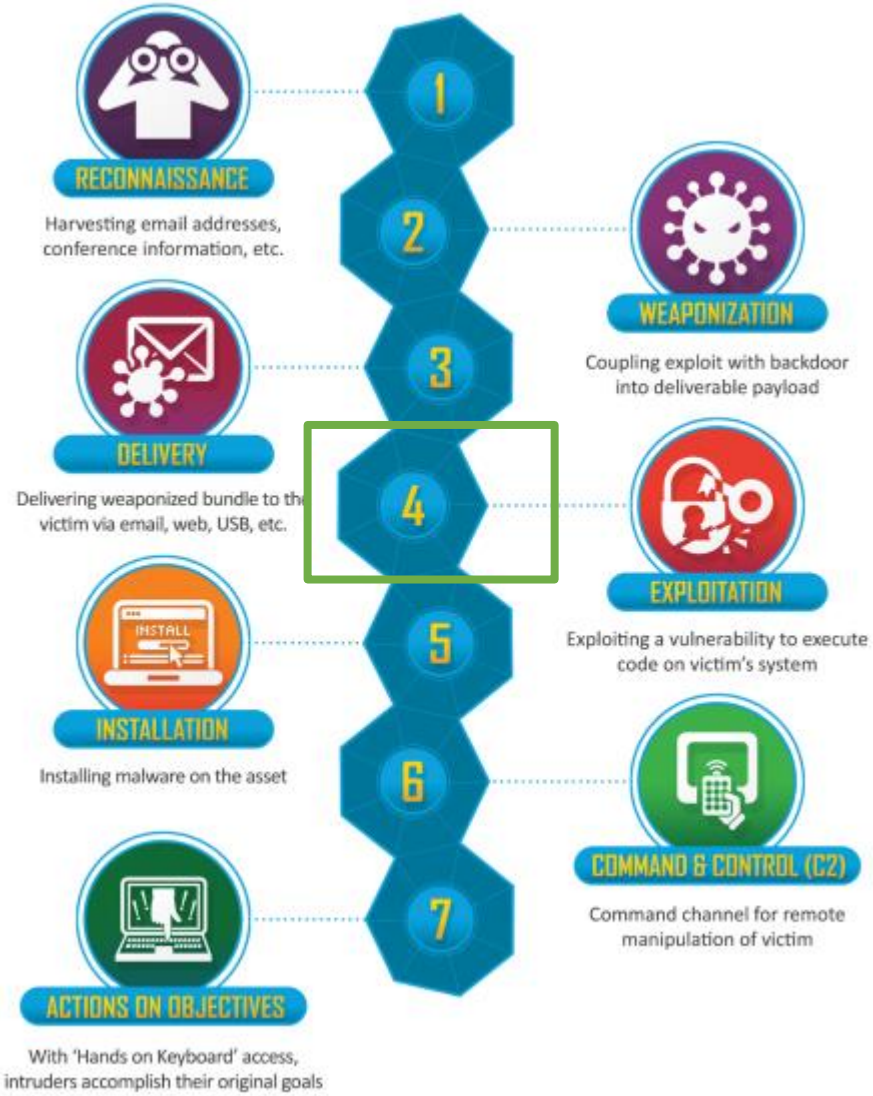
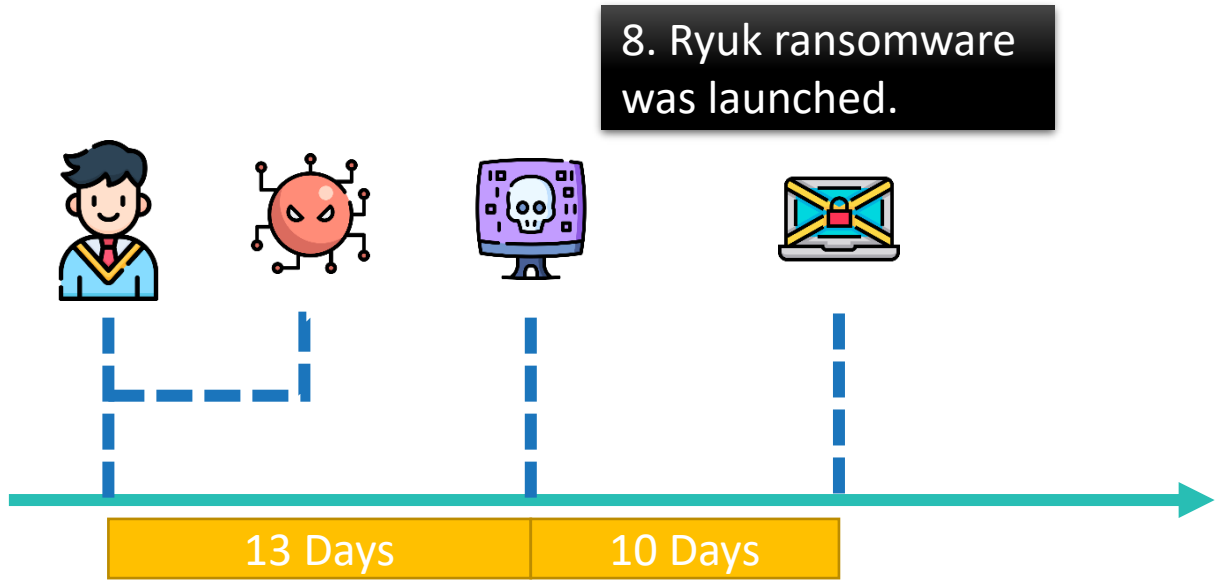


Image source: lockheedmartin

Case Study : Ransomware Attack

Background: A European biomolecular research institute involved in COVID-19 related research was infected Ryuk Ransomware.



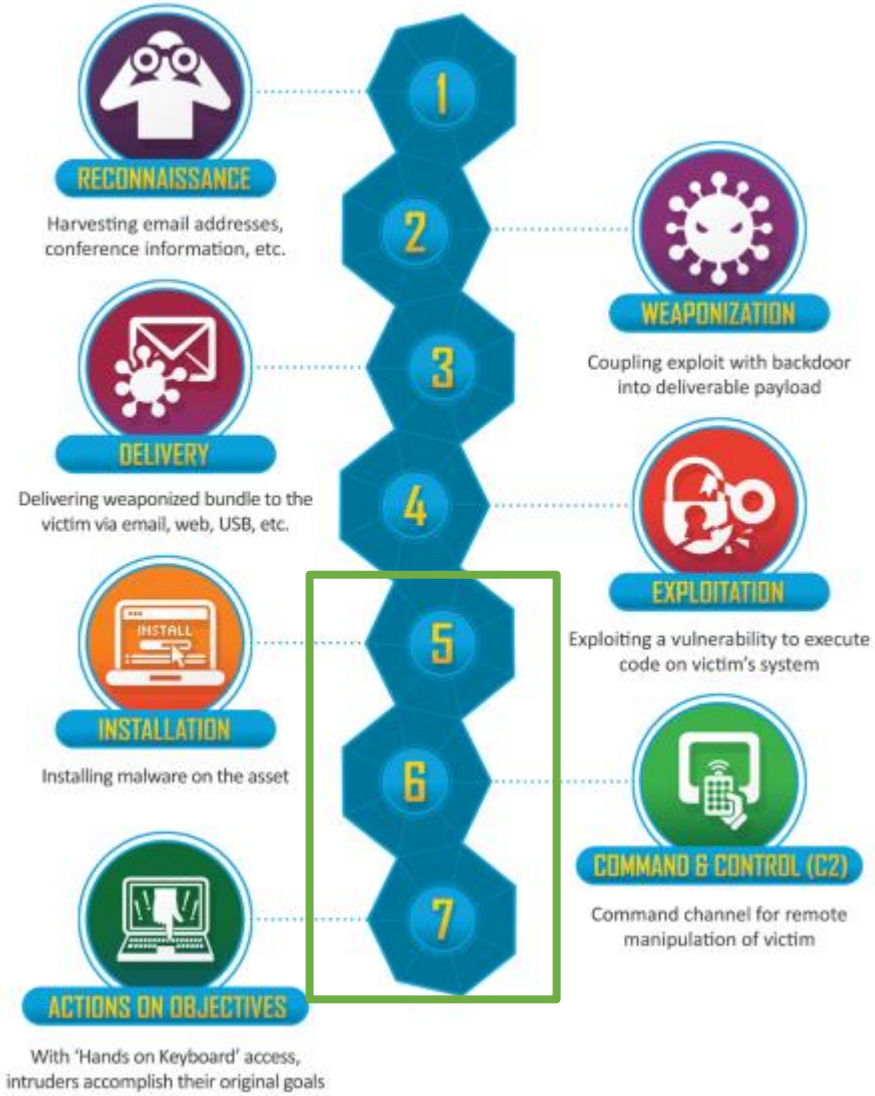


Image source: lockheedmartin

Lesson Learn

1. User awareness is important as a preventive control
2. Apply the least privilege principle
3. Ensure user workstation has patched and installed anti-virus with up-to-date signatures.
4. Enable two-factor authentication (2FA) for remote access
5. Limit the remote access with static Local Area Network (LAN) rules or whitelist IP
6. Implement segregation of network , provide a segregated environment between trusted and untrusted zones
7. Monitor the abnormal remote access and log

Supply Chain Attacks

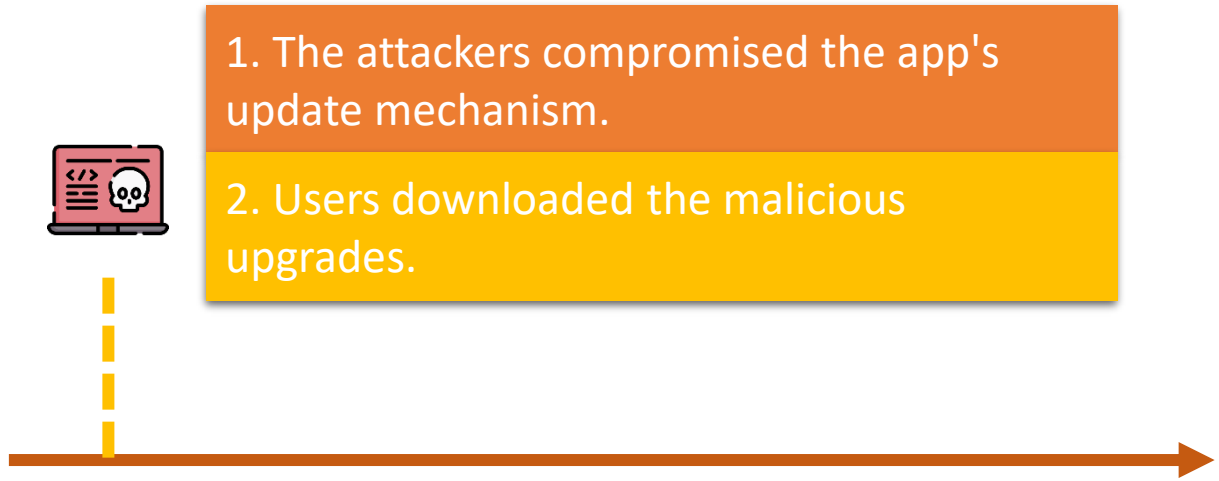
Spear Phishing Attacks

Case Study : Supply Chain Attack

Passwordstate password manager hacked in supply chain attack

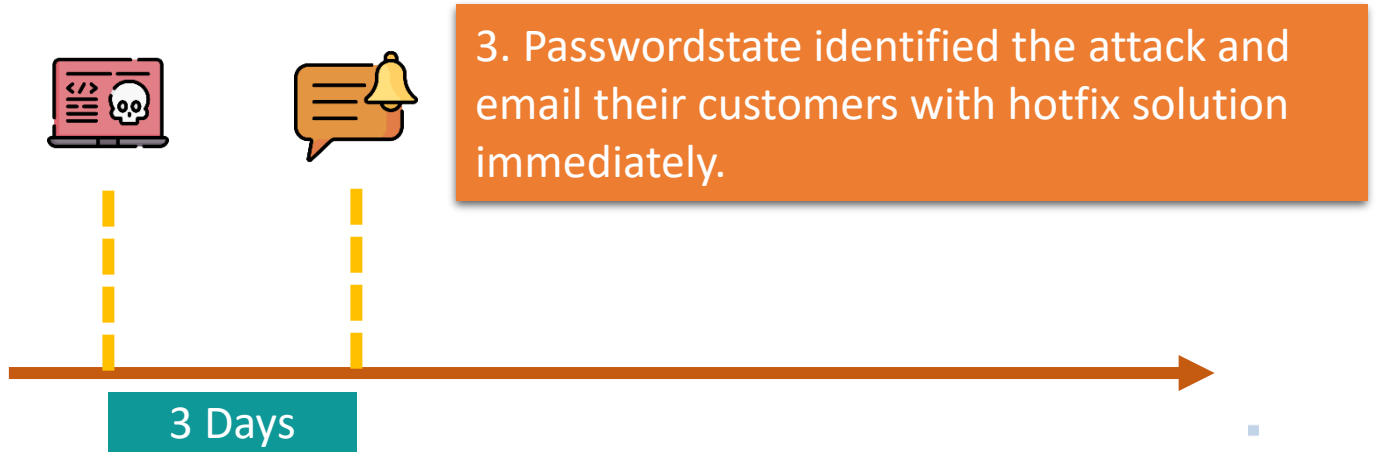
Case Study: Supply Chain Attack

Background: Passwordstate is an on-premises password management solution used by over 370,000 security and IT professionals at 29,000 companies worldwide, was hacked in supply chain attack.



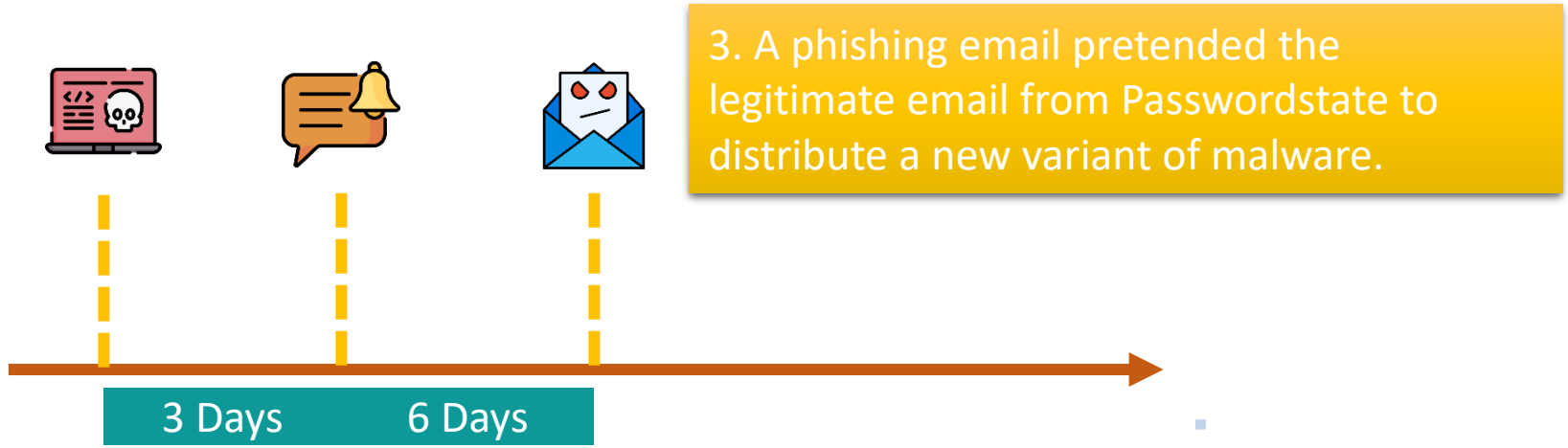
Case Study: Supply Chain Attack

Background: Passwordstate is an on-premises password management solution used by over 370,000 security and IT professionals at 29,000 companies worldwide, was hacked in supply chain attack.



Case Study: Supply Chain Attack

Background: Passwordstate is an on-premises password management solution used by over 370,000 security and IT professionals at 29,000 companies worldwide, was hacked in supply chain attack.



Common Attack Techniques

- Hijacking Updates
- Undermining Codesigning
- Compromising Open-Source Code

Recommendations

1. Establish a formal C-SCRM (Cyber Supply Chain Risk Management) program.
2. Know and manage critical components and suppliers.
3. Understand the organization's supply chain.
4. Closely collaborate with key suppliers.
5. Include key suppliers in resilience and improvement activities
6. Assess and monitor throughout the supplier relationship.
7. Plan for the full lifecycle.

Source: https://www.cisa.gov/publication/software-supply-chain-attacks

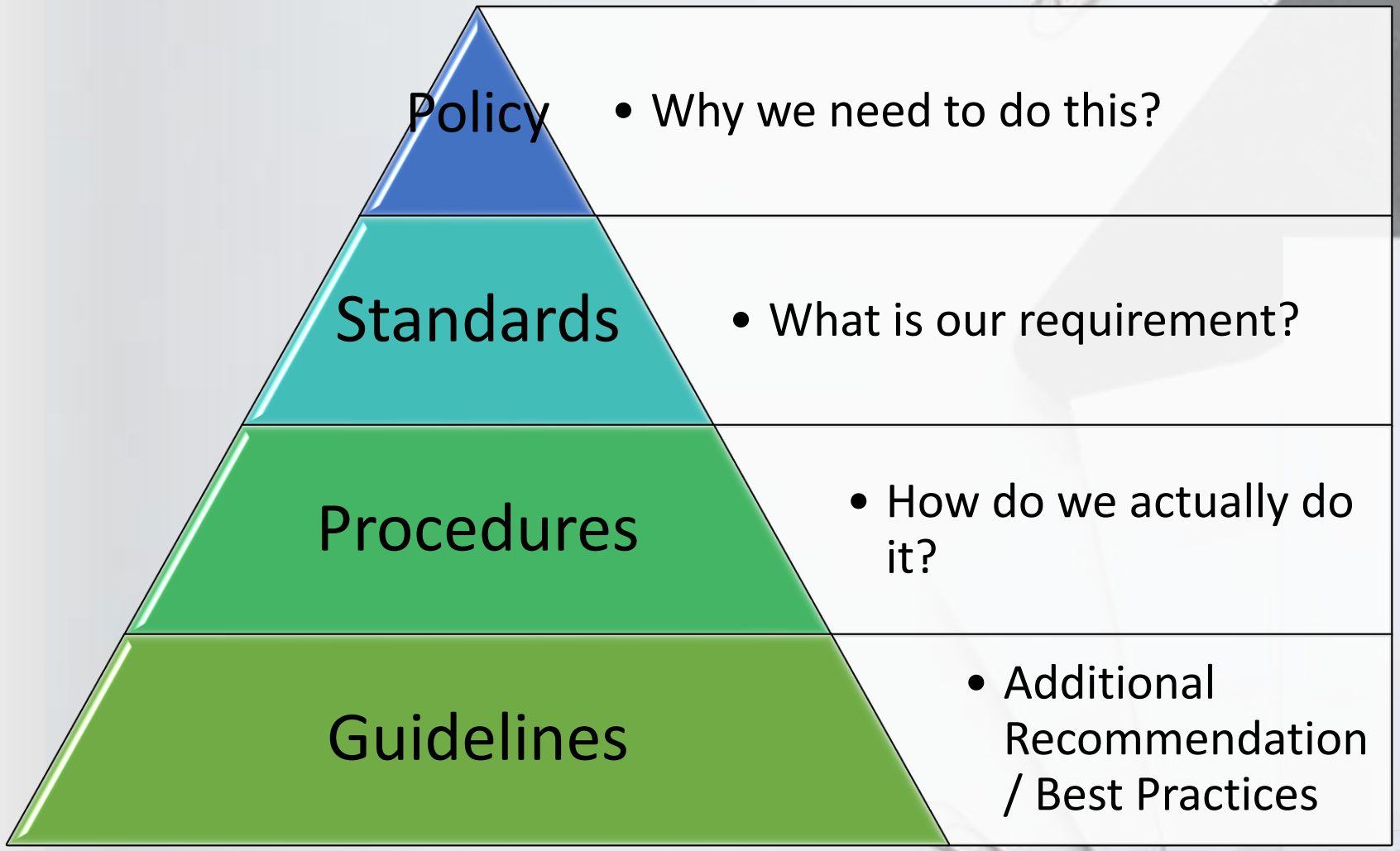
IT Security Governance

MAKE SMART
SMARTER

Security Policy and Related Documents

MAKE SMART
SMARTER

Security Policy and Related Documents



Policy **Mandatory**

A policy is a set of ideas or strategies that are used as a basis for decision making. They are the high-level statements of direction by the management.

Password Policy

1. All system passwords must be changed at least 180 days; while user passwords must be changed at least once per year.
2. Employees must protect their passwords and to secure their accounts.
3. Employees should not share their password with anyone.
4. Passwords should never be written down or stored without encryption.
5. All system and user password must conform to the Password Construction Guidelines.

Standards Mandatory

A standard is a mandatory requirement to be followed in order to protect the cyber environment of a user or organisation.

International Standards

ISO/IEC 27001: ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control.

Industry-specific Standards

PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organisations that handle branded credit cards from the major card schemes.

Procedures **Mandatory**

A procedure is step-by-step guide that help to support the policy objectives. Procedures are low level and specific.

Procedure for creating a new user account on ABC system

1. Receive a new user request form.
2. Verify if the user's manager and IT manager has approved and signed the form.
3. Create the account and set the proper permission.
4. Email the new account information to the user.
5. Inform the user's manager and IT manager that the new account creation has been completed.

Guidelines Discretionary

A guideline provides the information such as examples, suggestions, recommendation and other details for executing the policies and procedures.

Password Construction Guidelines

1. The password should not contain all or part of user account name or login id.
2. The password should between 10 and 30 characters.
3. The password should contain at least three (3) of the following character categories:
   - Uppercase letters (A-Z)
   - Lowercase letters (a-z)
   - Numbers (0-9)
   - Nonalphabetic characters (e.g. !, $, #, %, ?)
4. The three previous passwords should not be re-used.

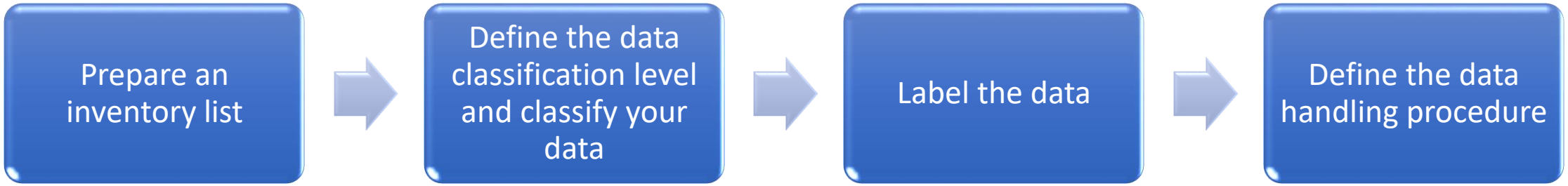
Information Classification and Handling

MAKE SMART
SMARTER

Information Classification and Handling

- Sensitive data should be classified and labelled, treated by different measures.

- 4 Step for classify your data:



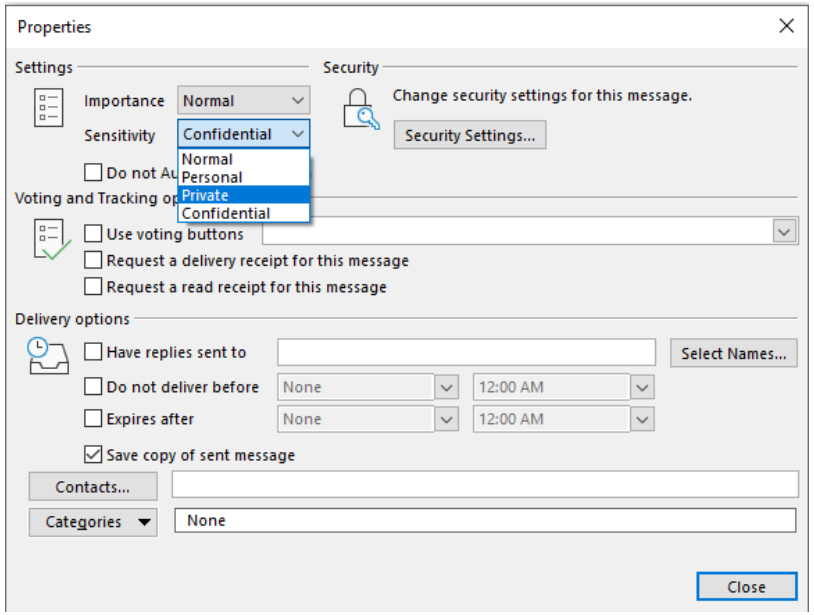
Information Classification

Define the level of classification criteria (see example below):

1) Confidential (top confidentiality level)
2) Restricted (medium confidentiality level)
3) Internal (lowest level of confidentiality)
4) Public (everyone can see the information)

4 Level	3 Level	2 Level
Public	Public	Public
Internal	Internal	Confidential
Restricted	Confidential	Confidential
Confidential	Confidential	Confidential

Information Labelling



MAKE SMART SMARTER

Information Handling

	Confidential	Restricted	Internal
Encryption in storage	Mandatory	Mandatory	Mandatory
Shared Access	Prohibited	Prohibited	Allowed
Shared Access tracking	Audit trail	Audit trial	Recommended
Encryption in data transfer over trusted network	Mandatory, only in isolated LAN	Recommended	Recommended
Encryption in data transfer over trusted network	Data transfer prohibited	Mandatory	Mandatory

Risk Management


Threat
Asset
Vulnerability
Risk

Cyber Risk Assessment

- What are our organization's most important information **assets**?
- What are the relevant **threats** and the threat sources to our organization?
- What are the internal and external **vulnerabilities**?
- What is the **impact** if those vulnerabilities are exploited?
- What is the **likelihood** of exploitation?
- What **cyber attacks**, **cyber threats**, or **security incidents** could impact affect the ability of the business to function?
- What is the **level** of risk my organization is comfortable taking?

Risk Analysis : Qualitative Methods

Subjective

- Importance
- Confidentiality
- Integrity
- Availability

Impact	Critical 5	Low 5x1 = 5	Medium 5x2 = 10	High 5x3 = 15	Critical 5x4 = 20
	High 4	Low 4x1 = 4	Low 4x2 = 8	Medium 4x3 = 12	High 4x4 = 16
	Medium 3	OFI 3x1 = 3	Low 3x2 = 6	Medium 3x3 = 9	Medium 3x4 = 12
	Low 2	OFI 2x1 = 2	Low 2x2 = 4	Low 2x3 = 6	Low 2x4 = 8
	Very Low 1	OFI 1x1 = 1	OFI 1x2 = 2	OFI 1x3 = 3	Low 1x4 = 4
		Very Low 1	Low 2	Medium 3	High 4
		Likelihood			

- ✓ Brainstorming
- ✓ Questionnaire and structured interviews
- ✓ Evaluation for multidisciplinary groups
- ✓ Judgment of specialists and experts

MAKE SMART SMARTER

Risk Analysis : Quantitative Methods

Objectives

Expected Monetary Value = Likelihood x Impact

Asset	Risk	Likelihood	Cost Impact	EMV
Backup Server	Hardware failures	5% / year	$50,000	$2,500 / year
Data Center	Flooding	0.01% / year	$800,000	$80 / year

- ✓ Analysis of likelihood
- ✓ Analysis of consequences
- ✓ Computer simulation

MAKE SMART SMARTER

Risk Analysis : Quantitative Methods

Objectives

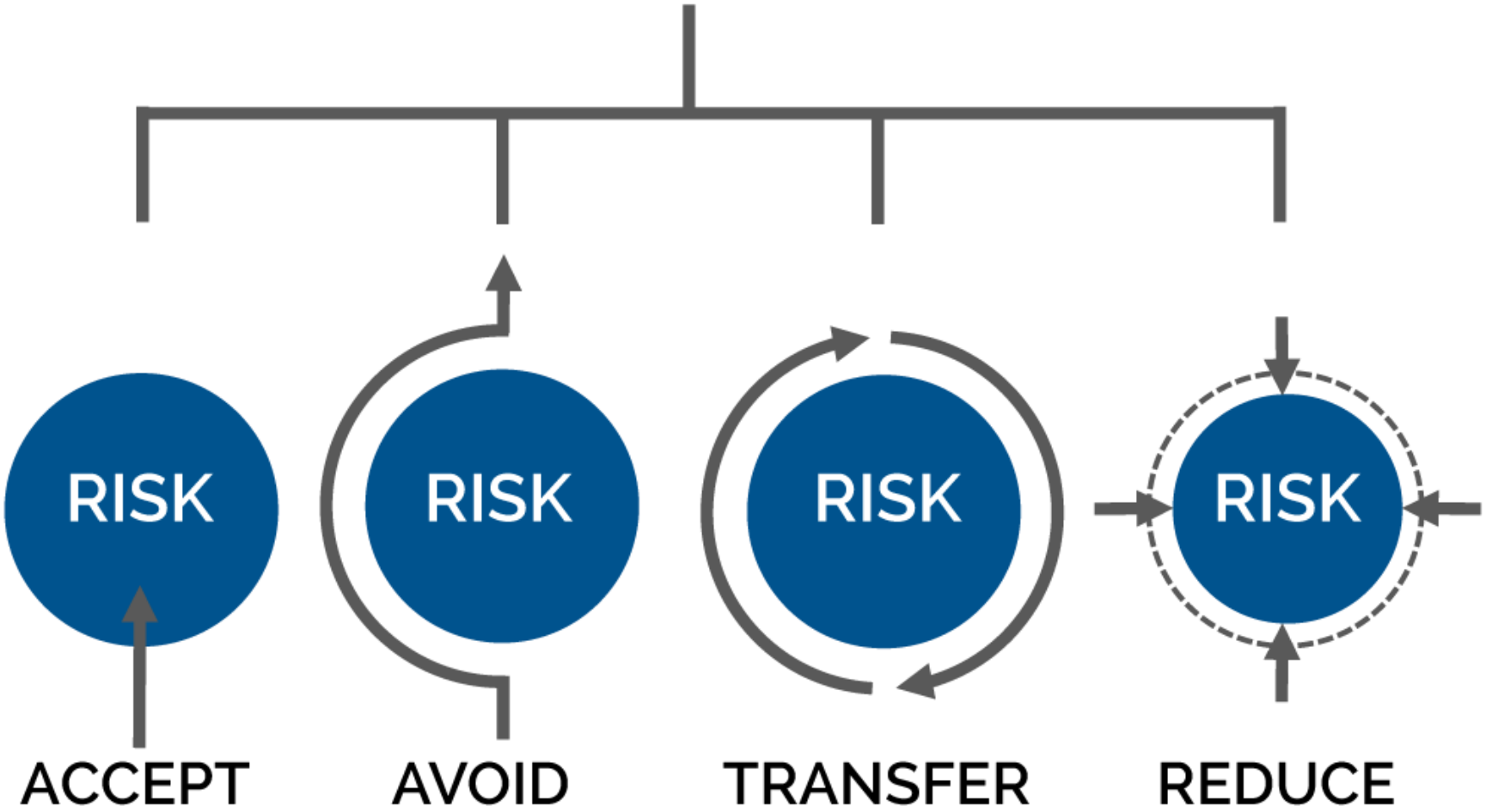
Expected Monetary Value = Likelihood x Impact

Asset	Risk	Likelihood	Cost Impact	EMV
Backup Server	Hardware failures	5% / year	$50,000	$2,500 / year
Hardware Maintenance Fee = $1,000 / year **Mitigate**				
Data Center	Flooding	0.01% / year	$800,000	$80 / year
Warm site as a DR location = $200,000 / year **Accept**				

- ✓ Analysis of likelihood
- ✓ Analysis of consequences
- ✓ Computer simulation

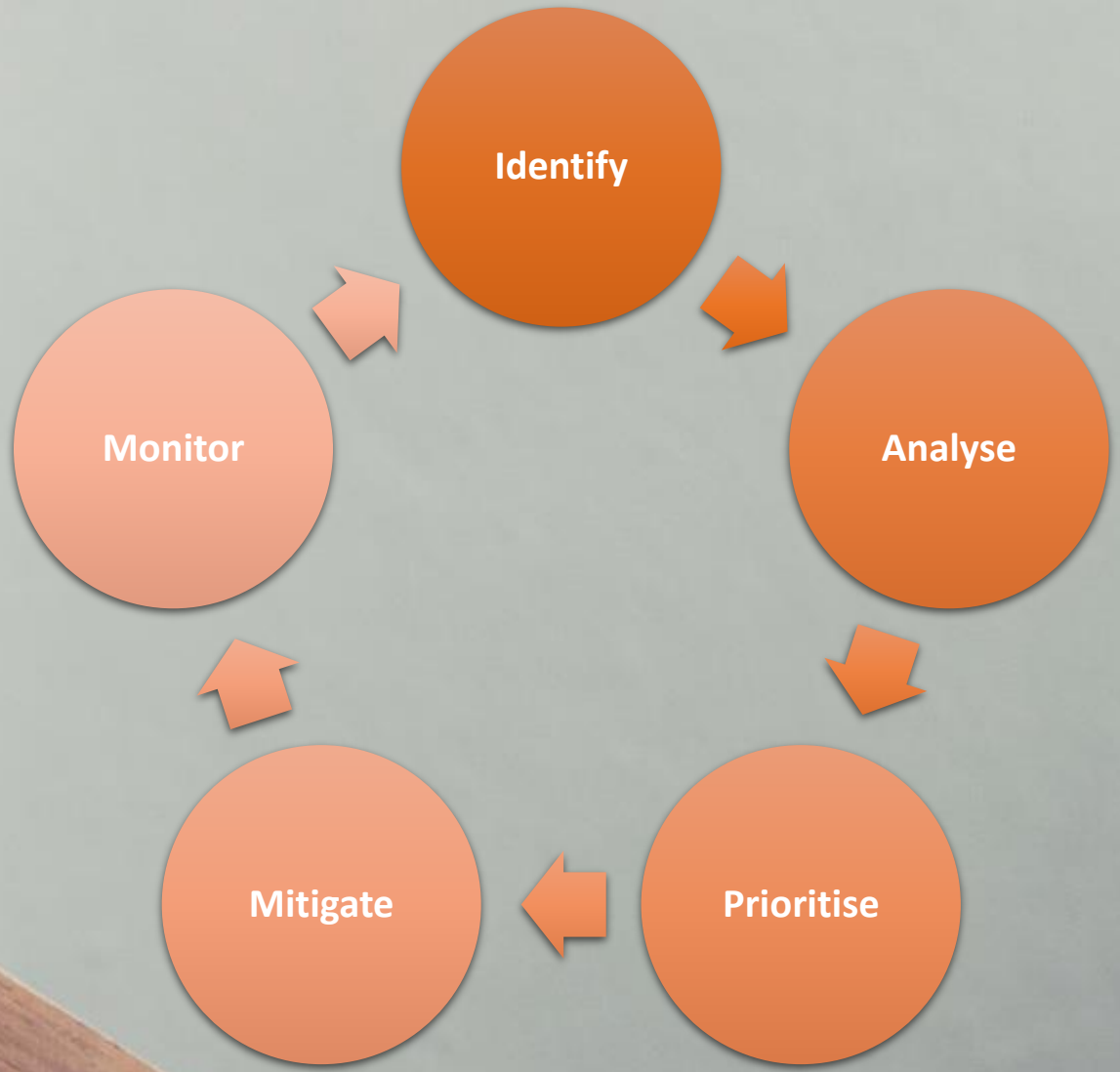
MAKE SMART SMARTER

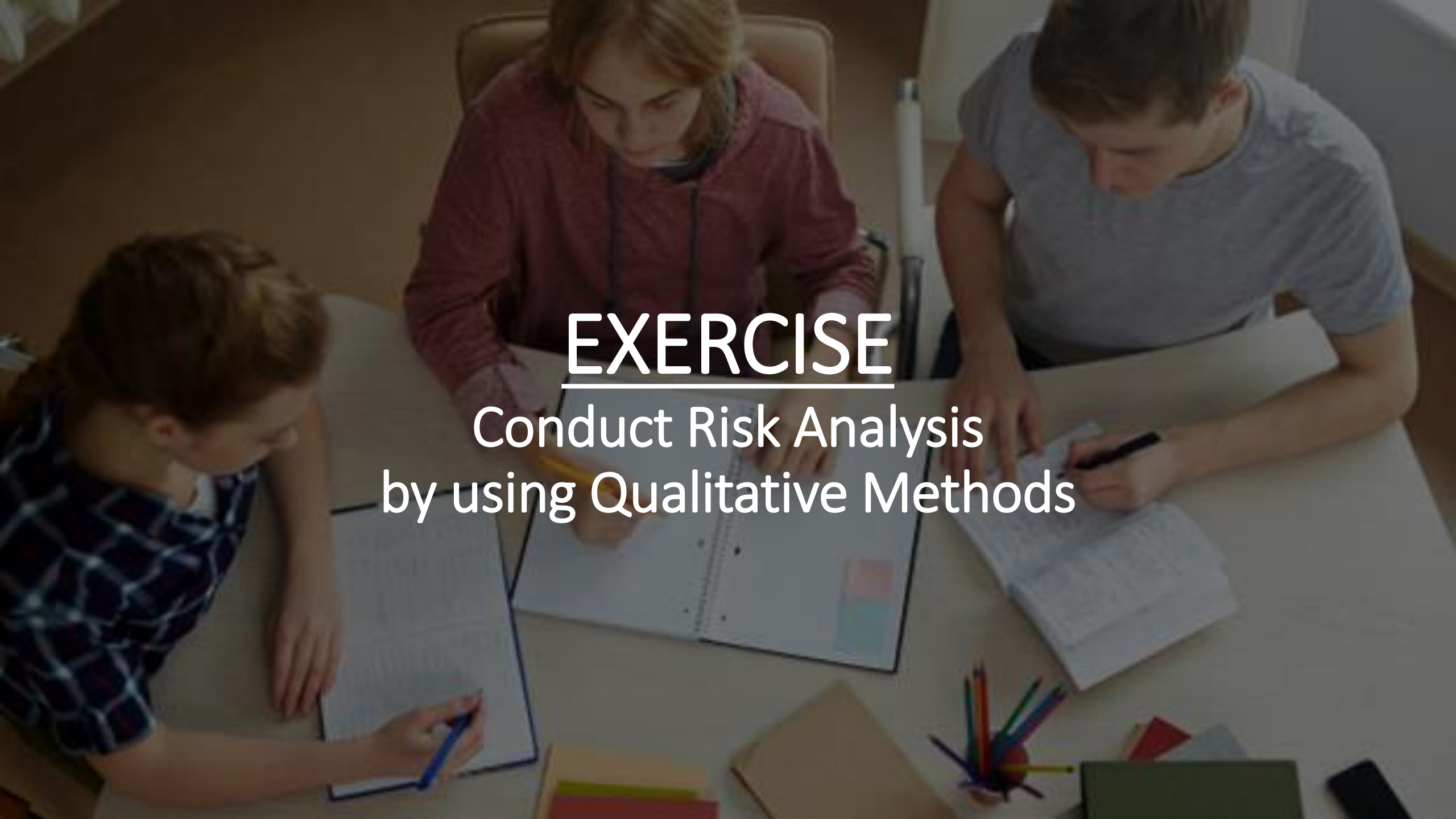
FOUR TYPES OF RISK MITIGATION



Graph Source: https://www.mha-it.com/2013/05/17/four-types-of-risk-mitigation/

Risk Management





EXERCISE

Conduct Risk Analysis
by using Qualitative Methods

Conduct Risk Analysis by using Qualitative Methods

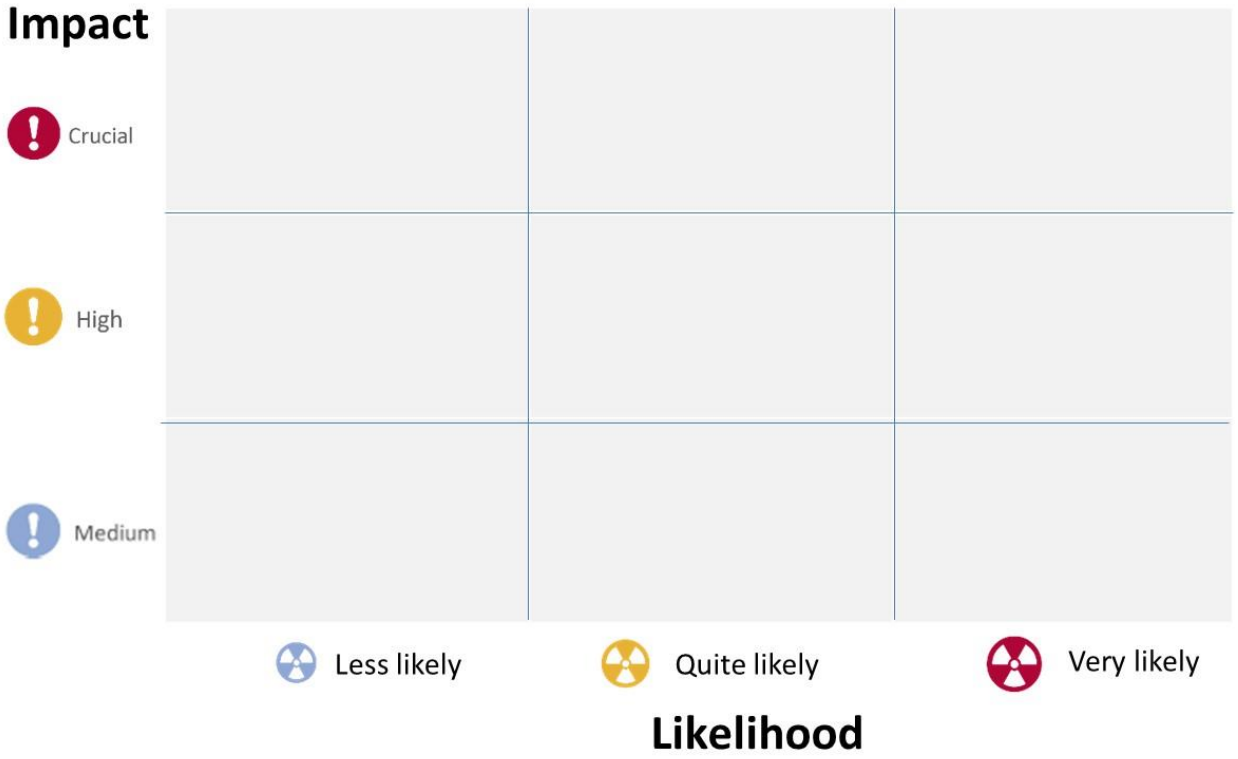
1. Cite one security threat (ransomware, virus, DDoS) in your business operation; and one personnel vulnerability in your business operation.

Please be specific when citing the vulnerability / threat, e.g. Guest Wi-Fi with default password (not just write something like ‘software vulnerability’).

MAKE SMART SMARTER

Conduct Risk Analysis by using Qualitative Methods

2. Put them into the following 3x3 risk matrix, state the risk level, and explain the risk level assignment.



3. Suggest risk control measure(s) for one of them.

MAKE SMART
SMARTER

EXERCISE

Use of “Seven Habits of Cyber Security” to conduct self assessment

The Seven Habits of Cyber Security

Security Policy & Management

Endpoint Security

Network Security

System Security

Security Monitoring

Incident Handling

User Awareness

Best Practices + **Self-assessment List**

MAKE SMART SMARTER

https://www.hkcert.org/security-guideline/seven-habits-of-cyber-security-for-smes

Exercise: Self-assessment

- Time: 10 minutes
- Please use “Seven Habits of Cyber Security” checklist to perform self assessment

Security Policy and Management

Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
1. Security Policy and Security Management	Security Policy is an important document in an organization. It dictates security requirements and attitude of senior management with respect to cybersecurity risk management. Senior management should setup a mechanism to maintain and disseminate the requirements of security policy to staff in a regularly basis. • Governance • Accessibility and dissemination of policy • User acknowledge and acceptance	✓ Staff should be given a chance to read through the security policy, understand security requirements of the organization and acknowledge to conform when they onboard. ✓ The policy should be put in somewhere the staff can refer to easily. ✓ Policy should be updated and let the staff to re-acknowledge the policy regularly.	☐ My organization does not have a security policy ☐ My organization has a security policy ☐ The security policy can be easily accessed by staff ☐ Staff needed to acknowledge the security policy when they onboard ☐ Staff needed to re-acknowledge the security policy regularly

MAKE SMART SMARTER

Endpoint Security

Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
2. Endpoint Security	Endpoint refers to personal computers or notebook computers used by staff to access business information during work. Email communication, web browsing, and other business applications are all run on endpoints. Attackers would like to compromise the endpoint since it can be used as an entry point to access valuable information assets of the organization. • Endpoint protection • Signature update • Regular check Relevant Attacks • Malware • Botnet	✓ Endpoint computers should be protected by security software like anti-virus and anti-malware software. ✓ Signatures and security software should be kept up to date to protect the endpoint from most recent threats. ✓ Security patches for endpoint computer operating system should also be kept up to date. ✓ IT staff should monitor the update status of the endpoints as well. ✓ User accounts on endpoint should be non-privileged (not Administrator) ✓ Proxy server used to filter malicious URLs during web browsing	☐ My organization does not have any endpoint protection software installed ☐ My organization has endpoint protection software installed ☐ My organization has endpoint protection software installed and signatures are kept updated regularly ☐ IT staff regularly check the update status of endpoint protection software ☐ Security patches for endpoint computer operating system are updated regularly ☐ Accounts used by user on endpoints are non-privileged ☐ Proxy server(s) is setup to filter malicious URL during web browsing

MAKE SMART SMARTER

Network Security

Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
3. Network Security	Most organizations would make use of Internet to facilitate business information exchange. Internet connection inherits network security risks that external attackers may intrude the organization network from outside. Firewall, Internet facing servers and other network devices should be configured properly to avoid intrusion. • Network access control • Security by default • Minimal privilege • Remote access control • Regular review Relevant Attacks • Hacking • APT	✓ Firewall should be configured properly that minimize network ports of organization network exposing to the Internet. ✓ Default rule on firewall should be "DENY". Only "ALLOW" certain traffic based on business needs ✓ Do not allow ANY from internal network to have access to Internet. Only allow approved IP addresses to have Internet access instead. ✓ Do not allow remote access (e.g. RDP) from Internet to internal servers ✓ Firewall rules should be reviewed regularly	☐ My organization does not have a firewall to protect organization network ☐ My organization has a firewall to protect organization network ☐ Firewall(s) has a default "DENY" rule ☐ Firewall(s) does not allow ANY from internal network to access Internet ☐ Firewall(s) does not allow remote access ☐ Firewall rules are reviewed regularly

System Security

Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
4. System Security	Organizations make use of information systems to process business information. Some systems (e.g. web servers) are open to Internet to provide/collect information to/from the Internet. These systems are target of attackers since the information the systems contained are valuable. System security guidelines and practices should be developed for mission critical systems. • Password • Hardening • Minimal exposure • Regular patching • Encryption for data at rest • Input validation for applications • Regular assessment Relevant Attacks • Malware • Botnet • Password brute force • Application attack • Data theft	✓ Password policy should be configured such that passwords of server should meet minimum length and complexity requirement ✓ Servers should be configured securely (called hardened) with security policies enabled and unused services disabled ✓ System patches should be updated timely to protect from recent threats ✓ Internet facing servers should avoid storing sensitive information. Sensitive information should be masked or encrypted when stored in servers ✓ Input from Internet users (e.g. web server forms) should be filtered properly in application to avoid SQL Injection type of attack ✓ For critical systems serving the public and performing critical missions, periodical penetration test should be performed by professional parties	☐ My organization has server password policy that passwords needed to meet minimum length and complexity requirement ☐ My organization has security guideline for servers that enable security features and disable unused services ☐ My organization has a process that update system patches regularly & timely ☐ Sensitive information is not stored in Internet facing servers. ☐ Sensitive information is masked or encrypted when stored ☐ Application(s) has built-in controls to filter user input to avoid SQL Injection type of attack ☐ Periodical penetration test(s) is performed regularly by professional parties on mission critical systems

Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
5. Security Monitoring	There is no way to ensure 100% security of endpoints, servers and network. Organizations should setup mechanism to monitor and detect if something suspicious is happening in information systems. The earlier a threat is identified, the earlier actions can be taken. The potential damage of the threat can then be minimized. • Audit trail • Log centralisation • Log regular review • Automated alerts • Network traffic monitoring Relevant Attacks • External attack • Compromised network including stealth ones • Internal abuse / mistake • All kinds of attacks	✓ Logging should be enabled in network devices (e.g. firewall) and servers ✓ Logs should be centralized somewhere within the organization for periodical review and monitoring ✓ Review of the logs should be timely such that detected issues are taken care properly ✓ Network traffic (e.g. Internet traffic) should be monitored to detect if any abrupt change in traffic pattern.	☐ Logging is enabled in my organization's firewall(s) and servers ☐ Logs are collected in a centralized log server ☐ Logs are periodically reviewed by IT staff ☐ Mechanisms are setup to notify IT staff if something abnormal is detected ☐ Network traffic pattern is included in monitoring

Security Monitoring

MAKE SMART SMARTER

Security Incident Response

Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
6. Incident Handling	System outages due to system issues or security incidents are not 100% avoidable. Organization should develop incident response plans for different kinds of scenarios including small incidents like malware infections all the way to big incidents that require system restoration. • Incident response plan • Backup plan for system & data • Restore plan and drill Relevant Attacks • External attack including ransomware • Internal abuse / mistake • Partner related incident	✓ Incident response plans (including different kinds of security incidents) are developed according to different scenarios ✓ Systems and data are backup regularly, the backups are taken offline (and even offsite) ✓ Restore procedures are drilled to make sure that the backup can be restored properly	☐ My organization does not have any incident response plans ☐ My organization has incident response plans that handle different kinds of incidents ☐ My organization has backup plan for systems and data ☐ Backup data is kept offline ☐ Drills are done on restore plan regularly to make sure backups are restorable

MAKE SMART SMARTER

User Awareness

Security Aspects	Control Rationale	Best Practices	Self-Assessment (Click all that applicable)
7. User Awareness	Users are the weakest links in cyber security. 95% security incidents involved human as a contributing factor. Organizations should ensure that staff understand their roles and responsibility in protecting information assets of the organization. • Periodical awareness training • Drill test & historic track Relevant Attacks • Phishing • Malware infection • CEO Scan • Other types of attacks	✓ Staff should be reminded their roles and responsibility in protecting information assets of the organization regularly, e.g. by staff awareness training ✓ Drills (e.g. simulated phishing attacks) can be performed to test the readiness of staff against common cyber attack	☐ My organization does not have any security awareness activity for staff ☐ My organization has periodical security awareness training for staff ☐ My organization performs simulated test to assess readiness of staff against common cyber attack

MAKE SMART SMARTER

Exercise: Self-assessment

Self-assessment Score Calculation:

33 Blue Box ✓, 5 Yellow Box ✓

Total Score = number of Blue Box ✓ — number of Yellow Box ✓

Total Score	-5 to 2	3 to 10	11 to 18	19 to 25	26 to 33
Security Level	Most Vulnerable	Vulnerable	Security to be strengthened	Adequate security	Robust and adequate security

MAKE SMART SMARTER

Websites and Web Applications

OWASP Top 10

A1	Injection
A2	Broken Authentication
A3	Sensitive Data Exposure
A4	XML External Entities (XEE)
A5	Broken Access Control
A6	Security Misconfiguration
A7	Cross-Site Scripting
A8	Insecure Deserialization
A9	Using Components With Known Vulnerabilities
A10	Insufficient Logging And Monitoring

A1

Injection

Injection attacks happen when untrusted data is sent to a code interpreter through a form input or some other data submission to a web application.

Username : _____ Password: _____ Send

```
strSQL = "SELECT * FROM users WHERE (name = '" + username + "') and (pw = '"+ password +"');"
```

Username : "1' OR '1'='1" Password: "1' OR '1'='1" Send

```
strSQL = "SELECT * FROM users WHERE (name = '" + 1' OR '1'='1 + "') and (pw = '"+ 1' OR '1'='1 +"');"
```

TURE TURE

MAKE SMART SMARTER

A1

Injection

How To Prevent?

Injection attacks can be prevented by validating and/or sanitizing user-submitted data. (Validation means rejecting suspicious-looking data, while sanitization refers to cleaning up the suspicious-looking parts of the data.) In addition, a database admin can set controls to minimize the amount of information an injection attack can expose.

Example of using Prepare Command:

```
sql = "SELECT * FROM user WHERE name = @name AND pw = @pass
cmd.Parameters.Add("@name", SqlDBType.NVarChar, 50).Value = name
cmd.Parameters.Add("@pass", SqlDBType.NVarChar, 50).Value = pw
```

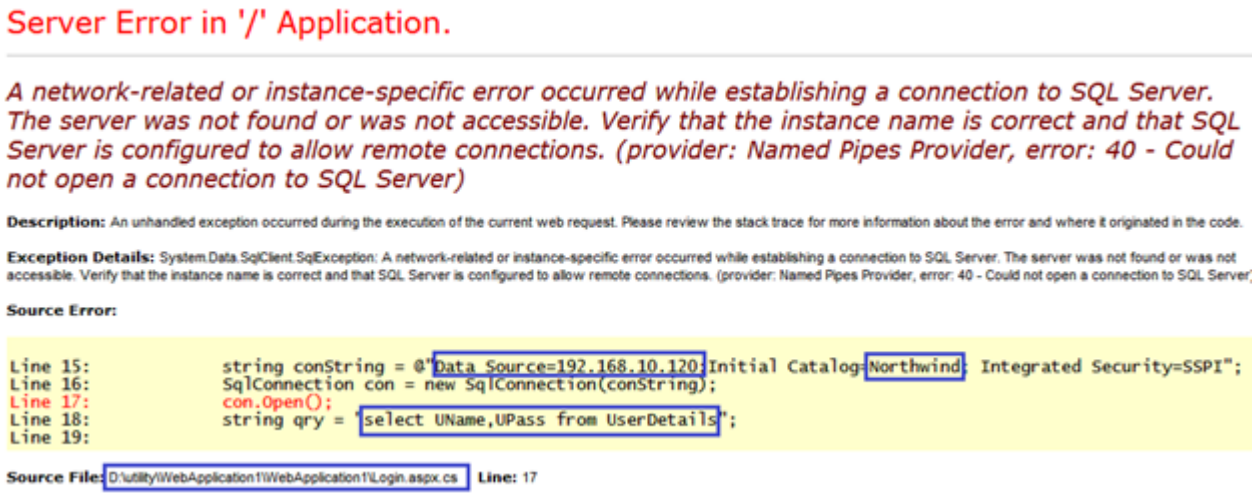
Demo

SQL Injection and Blind SQL Injection

A3

Sensitive Data Exposure

- System Error Message



- Not enforce HTTPS
- Sensitive data in commands
- Store sensitive date without encryption

MAKE SMART SMARTER

A6

Security Misconfiguration

Security misconfiguration is the most common vulnerability on the list, and is often the result of using default configurations or displaying excessively verbose errors.

- Missing appropriate security hardening across any part of the application stack, or improperly configured permissions on cloud services.
- Unnecessary features are enabled or installed (e.g. unnecessary ports, services, pages, accounts, or privileges).
- Default accounts and their passwords still enabled and unchanged.
- The software is out of date or vulnerable

A6

Security Misconfiguration

How To Prevent?

- A repeatable hardening process
- A minimal platform without any unnecessary features, components, documentation, and samples. Remove or do not install unused features and frameworks.
- Review and update the configurations appropriate to all security notes, updates and patches as part of the patch management process. In particular, review cloud storage permissions.

A7

Cross-Site Scripting

Cross-site scripting vulnerabilities occur when web applications **allow users to add custom code into a url path or onto a website that will be seen by other users**. This vulnerability can be exploited to run malicious JavaScript code on a victim's browser.

Example of Cross-Site Scripting

<textarea><textarea>
Attacker Input: *<script>alert('XSS Attack');</script>*
Victim Browser:
<textarea><script>alert('XSS Attack');</script><textarea>

Example of Cross-Site Request Forgery

<textarea><textarea>
Attacker Input: *<img src="http://hacker.com/hacker.php">*
Victim Browser:
<textarea><img src="http://hacker.com/hacker.php"><textarea>

MAKE SMART SMARTER

A7

Cross-Site Scripting

How To Prevent?

Preventing XSS requires separation of untrusted data from active browser content. This can be achieved by:

- Using frameworks that automatically escape XSS by design, such as the latest Ruby on Rails, React JS.
- Escaping untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL) will resolve Reflected and Stored XSS vulnerabilities.
- Enabling a Content Security Policy (CSP) as a defense-in-depth mitigating control against XSS.

A9

Using Components With Known Vulnerabilities

Many modern **web developers use components such as libraries and frameworks** in their web applications.

Some **attackers look for vulnerabilities in these components** which they can then use to orchestrate attacks.

Some of the more popular components are used on hundreds of thousands of websites; an attacker finding a security hole in one of these components could leave hundreds of thousands of sites vulnerable to exploit.

A9

Using Components With Known Vulnerabilities

How To Prevent?

- Remove unused dependencies, unnecessary features, components, files, and documentation.
- Continuously inventory the versions of both client-side and server-side components (e.g. frameworks, libraries) and their dependencies using tools like versions, DependencyCheck, retire.js, etc.
- Only obtain components from official sources over secure links.
- Monitor for libraries and components that are unmaintained or do not create security patches for older versions.

EXERCISE

Using OWASP Zed Attack Proxy (ZAP)

DO NOT scan the web site without authorization

Testing Environment

OWASP Zed Proxy Scanner

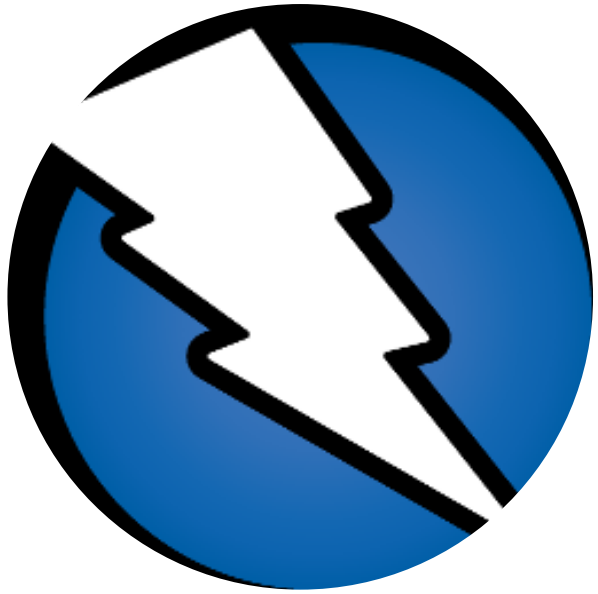
https://www.zaproxy.org/

Apache + MariaDB + PHP + Perl

https://www.apachefriends.org/index.html

Damn Vulnerable Web Application

https://dvwa.co.uk/



Exercise 1: Using OWASP ZAP

1. Launch XAMPP
2. Start Apache and MySQL
3. Launch ZAP
4. Open Browser with ZAP Proxy
5. Go to testing web site (http://127.0.0.1:5080/test)

How many findings identified? (HINTS: Alerts)

Exercise 2: Active Scan

1. Login
2. Set DVWA Security Level to **LOW**
3. Click SQL Injection
4. Input a number (1 – 5) and see the result
5. Back to ZAP
6. Click Sites -> http://127.0.0.1:5080 -> test -> vulnerabilities -> sqli -> GET:/(Submit,id)
7. Active Scan (Right Click -> Attack -> Active Scan)

How many High Risk identified? What is it?

Exercise 3: Result Analysis and Report Generation

1. Explore SQL Injection
2. Type below text in the text field

```
%' and 1=0 union select null,
concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from
users #
```

What is the output?

3. Generate Report by clicking Report on the menu

EXERCISE

Using Online Free Tools to Scan Website Security Vulnerabilities & Malware

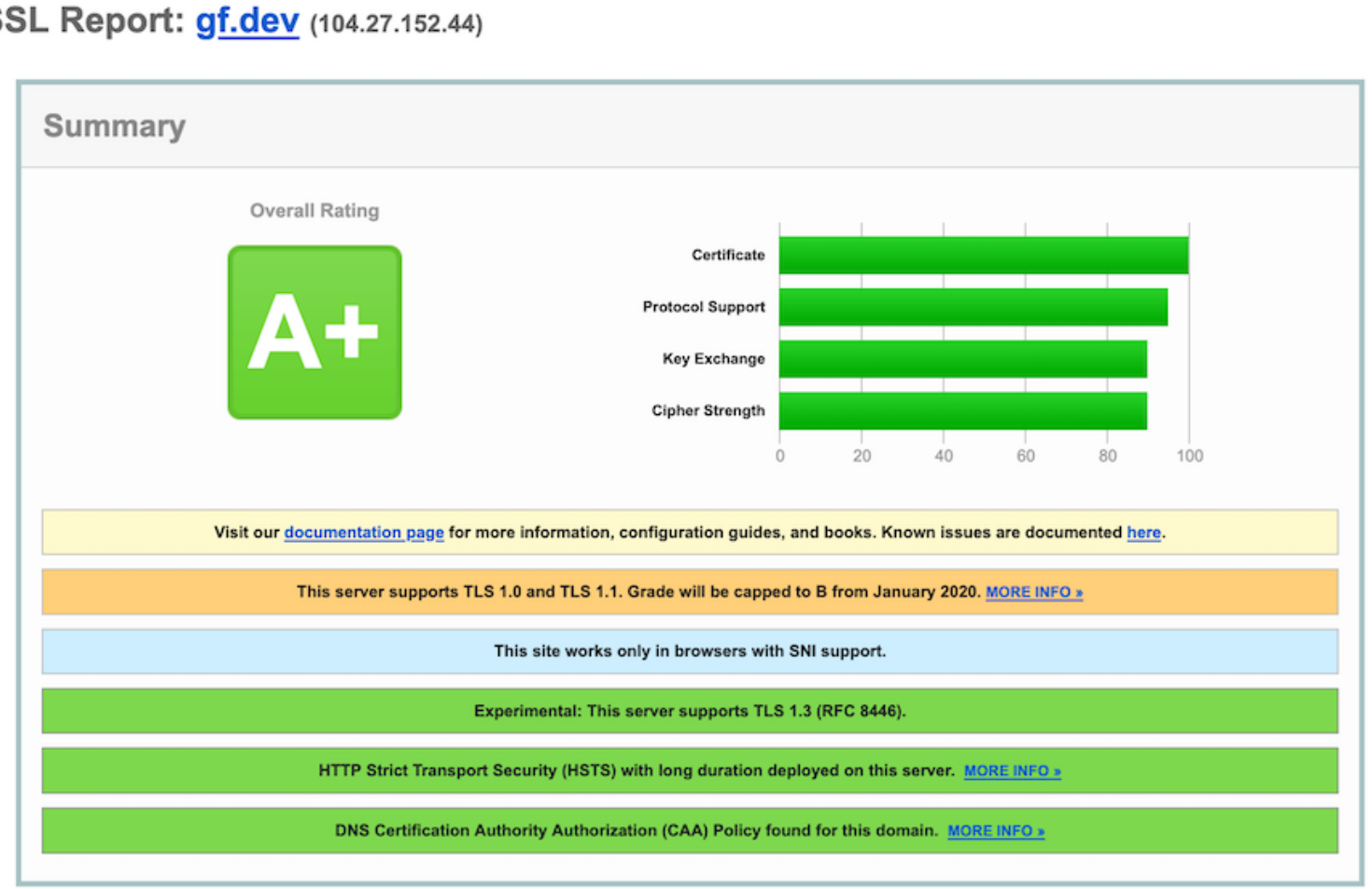
Online Free Tools – Qualys SSL Labs

Qualys. SSL Labs

https://www.ssllabs.com/ssltest/

Scan the website for SSL/TLS misconfiguration and vulnerabilities.

Analysis of https:// URL including expiry day, overall rating, cipher, SSL/TLS version, handshake simulation, protocol details, BEAST, and much more.



MAKE SMART SMARTER

Online Free Tools - SUCURI

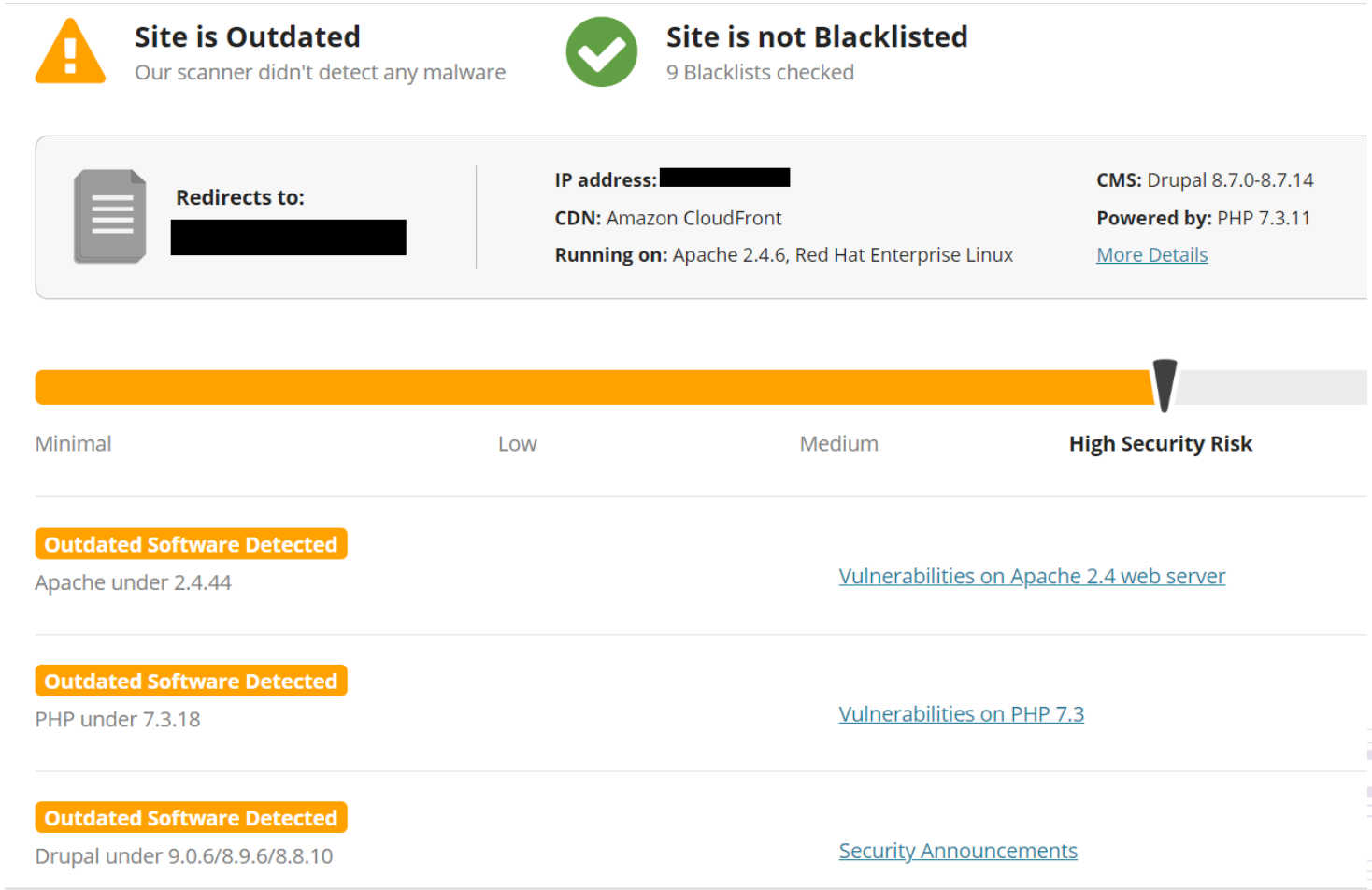
https://sitecheck.sucuri.net/

Site Details Information: IP Address, CDN, Web Server Version, OS, Language, TLS Certificate, Web Application Info,…

Website Malware & Security: Malware, Spam, Defacement, Internal Server Error,…

Website Blacklist Status

Website Firewall



MAKE SMART SMARTER

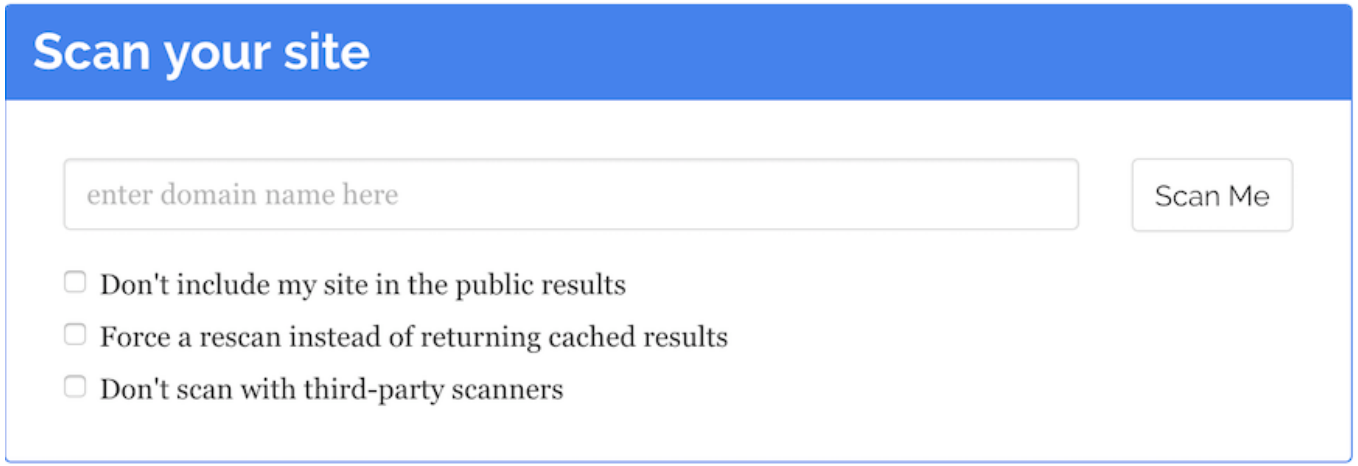
Online Free Tools - Observatory

Observatory
moz://a

https://observatory.mozilla.org/

Check various security elements. It validates against OWASP header security, TLS best practices, and performs third-party tests from SSL Labs, High-Tech Bridge, Security Headers, HSTS Preload, etc.

.



MAKE SMART SMARTER

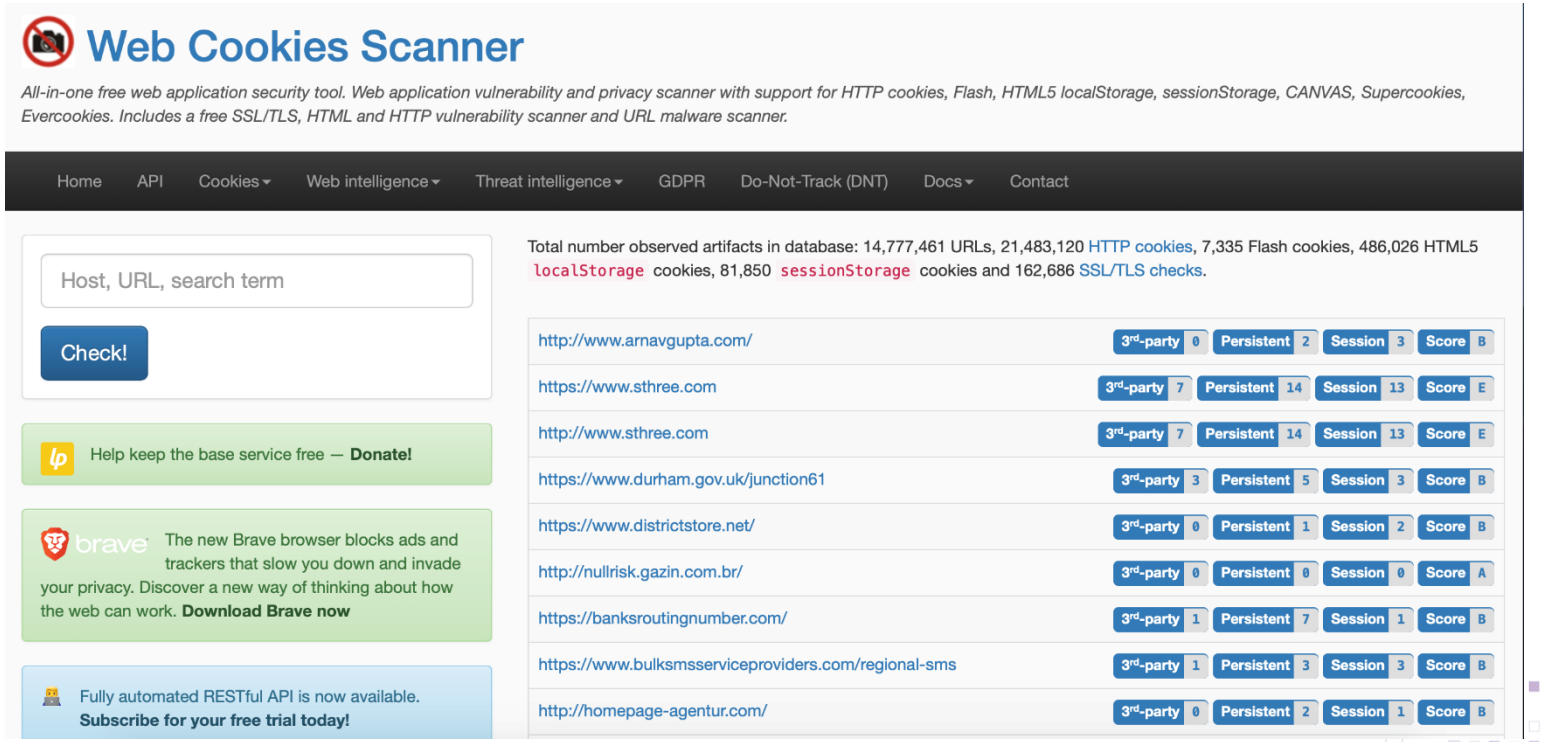
Online Free Tools – Web Cookies Scanner

Web Cookies Scanner

https://webcookies.org/

search for vulnerabilities and privacy issues on HTTP cookies, Flash applets, HTML5 localStorage, sessionStorage, Supercookies, and Evercookies. The tool also offers a free URL malware scanner and an HTTP, HTML, and SSL/TLS vulnerability scanner

.



MAKE SMART SMARTER

Network Security

MAKE SMART
SMARTER

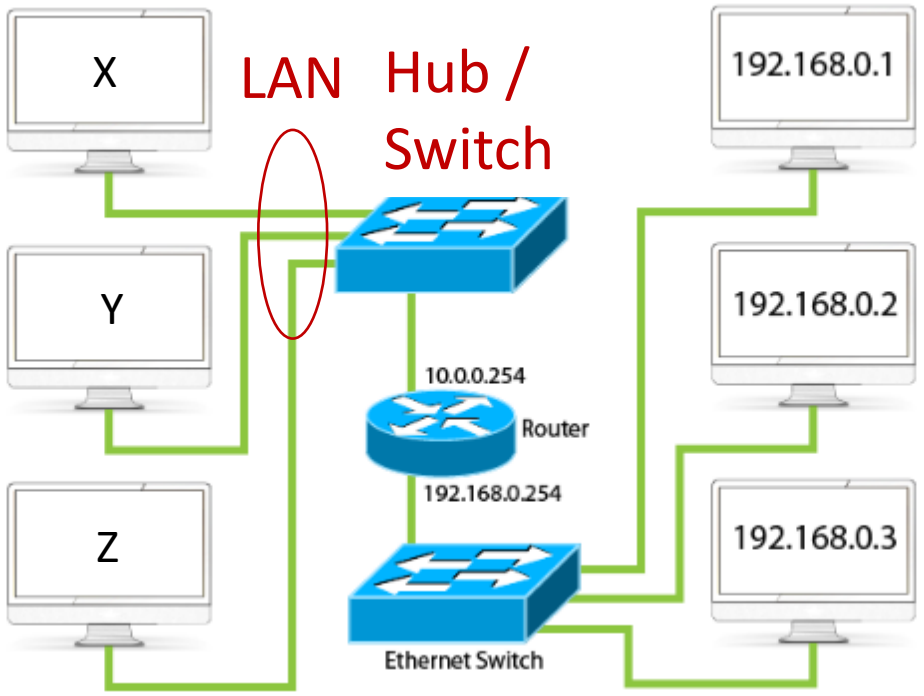
Local Area Network (LAN)

Each computer on the LAN has a unique MAC address

Computers in the **same LAN** can talk to each other using MAC addresses

Hub / Switch

- Hardware connecting computers on the same LAN
- Hub can be sniffed; Switch can segregate machine-to-machine traffic



MAC Address (hexa-decimal)

X: 00-e0-aa-aa-aa-aa
Y: 00-e0-bb-bb-bb-bb
Z: 00-e0-cc-cc-cc-cc

MAKE SMART SMARTER

IP network (Multiple LANs)

Each computer has a unique IP address

Each LAN has a unique network number

Switch

connects computers on the same LAN only (i.e. not routable)

SW A: 10.0.0.0 (LAN 1)

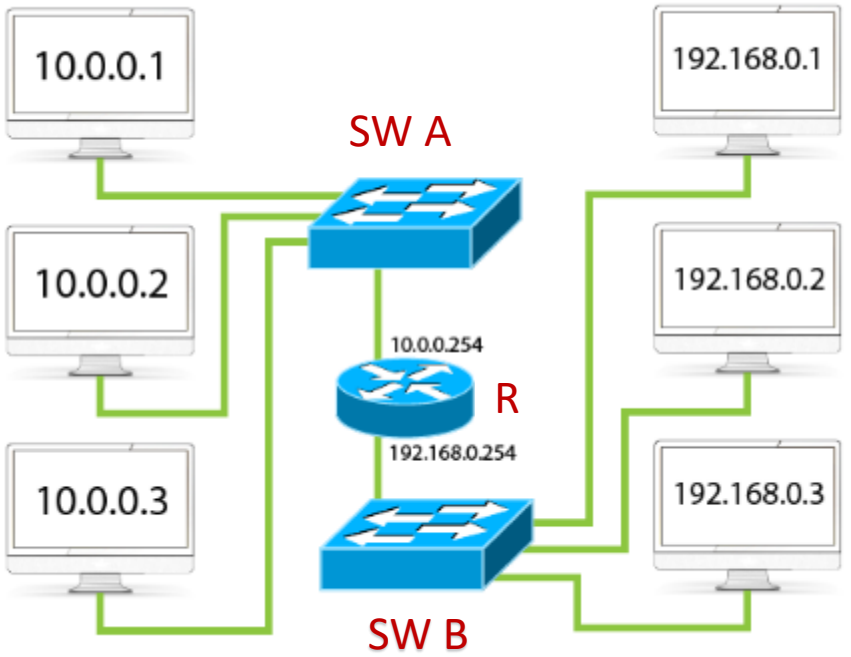
SW B: 192.168.0.0 (LAN 2)

Router (R)

connects different LANs via different network interfaces

10.0.0.254

192.168.0.254

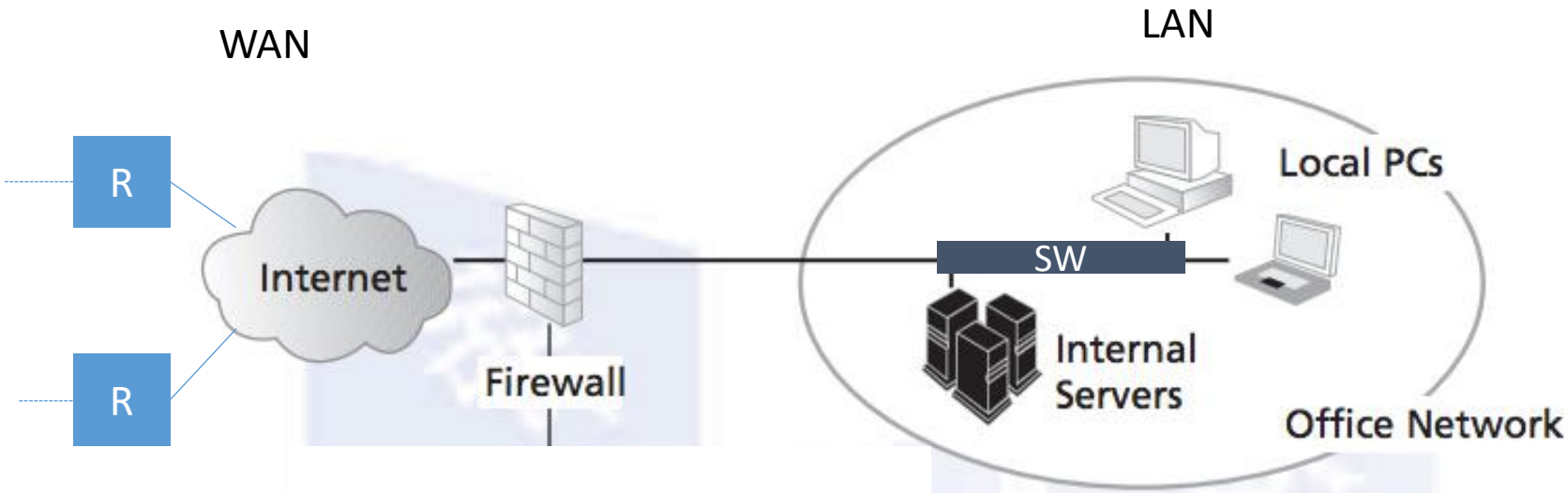


LAN 1
10.0.0.0

LAN 2
192.168.0.0

MAKE SMART SMARTER

Network Components

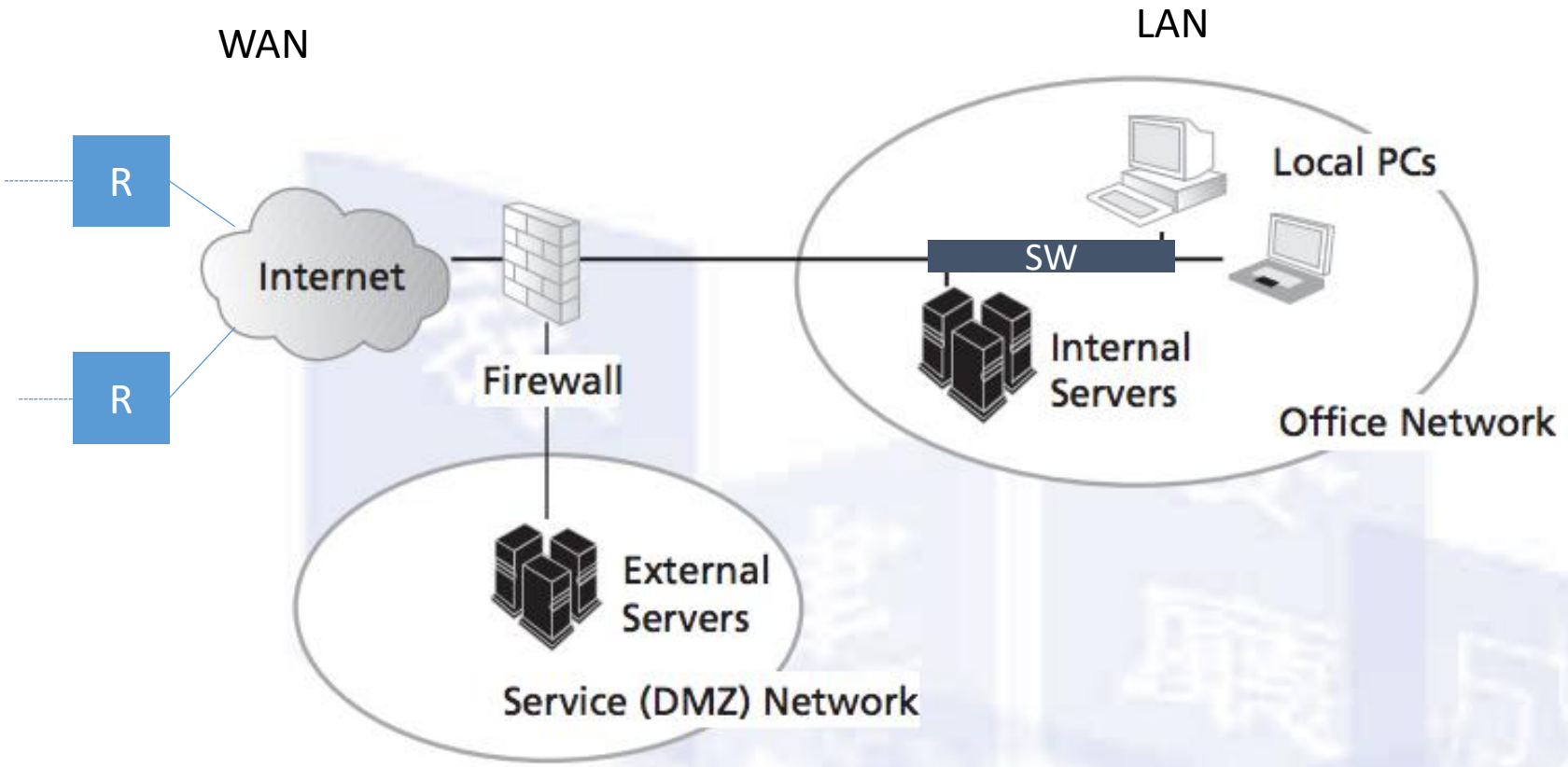


SW: switch
R: router

WAN (wide area network) – external network

Firewall – a router with (traffic) access control policy

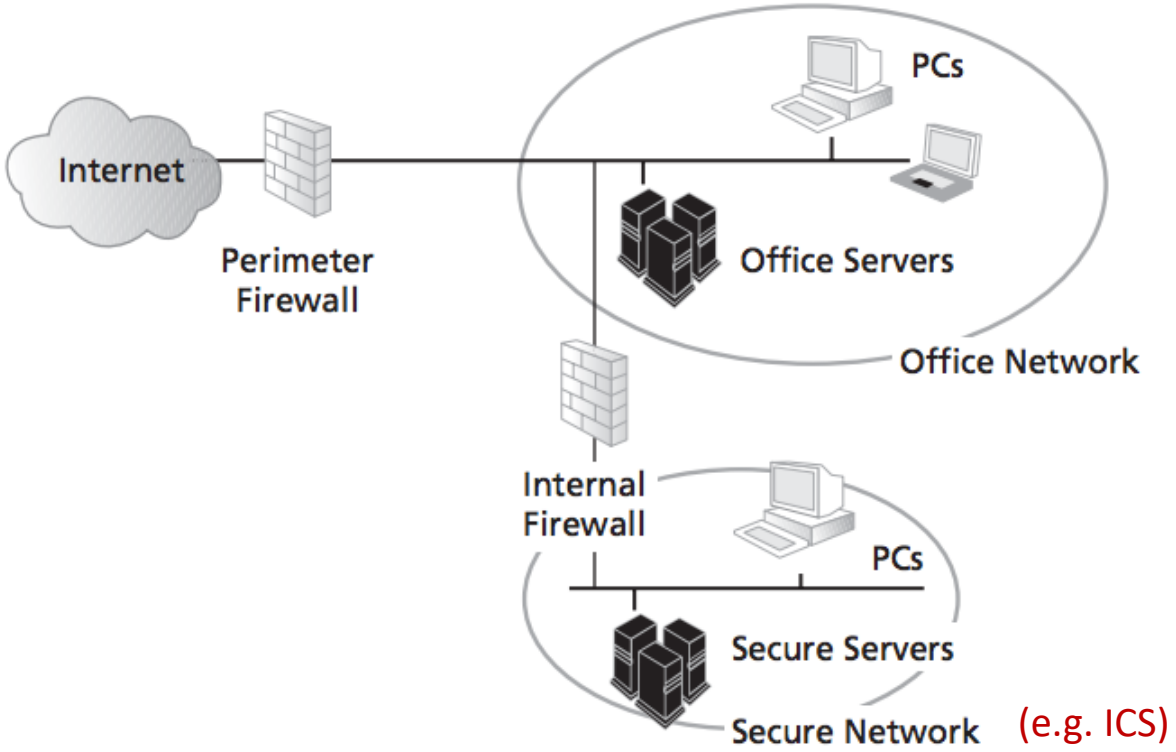
Network Components



DMZ (demilitarized zone) – a network for placing servers for external access

Firewall policy allows WAN users visits DMZ but not the LAN

Network Components

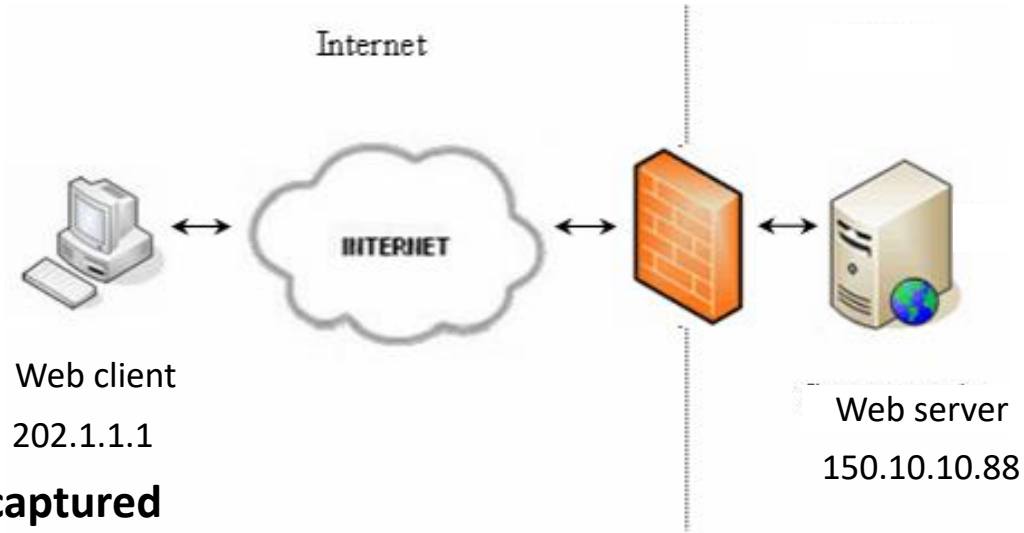


Perimeter firewall – control external access to internal resources

Internal firewall – control different groups of internal users accessing internal resources, e.g. SCADA / ICS network

MAKE SMART SMARTER

TCPIP (IP and service port)



Network traffic captured

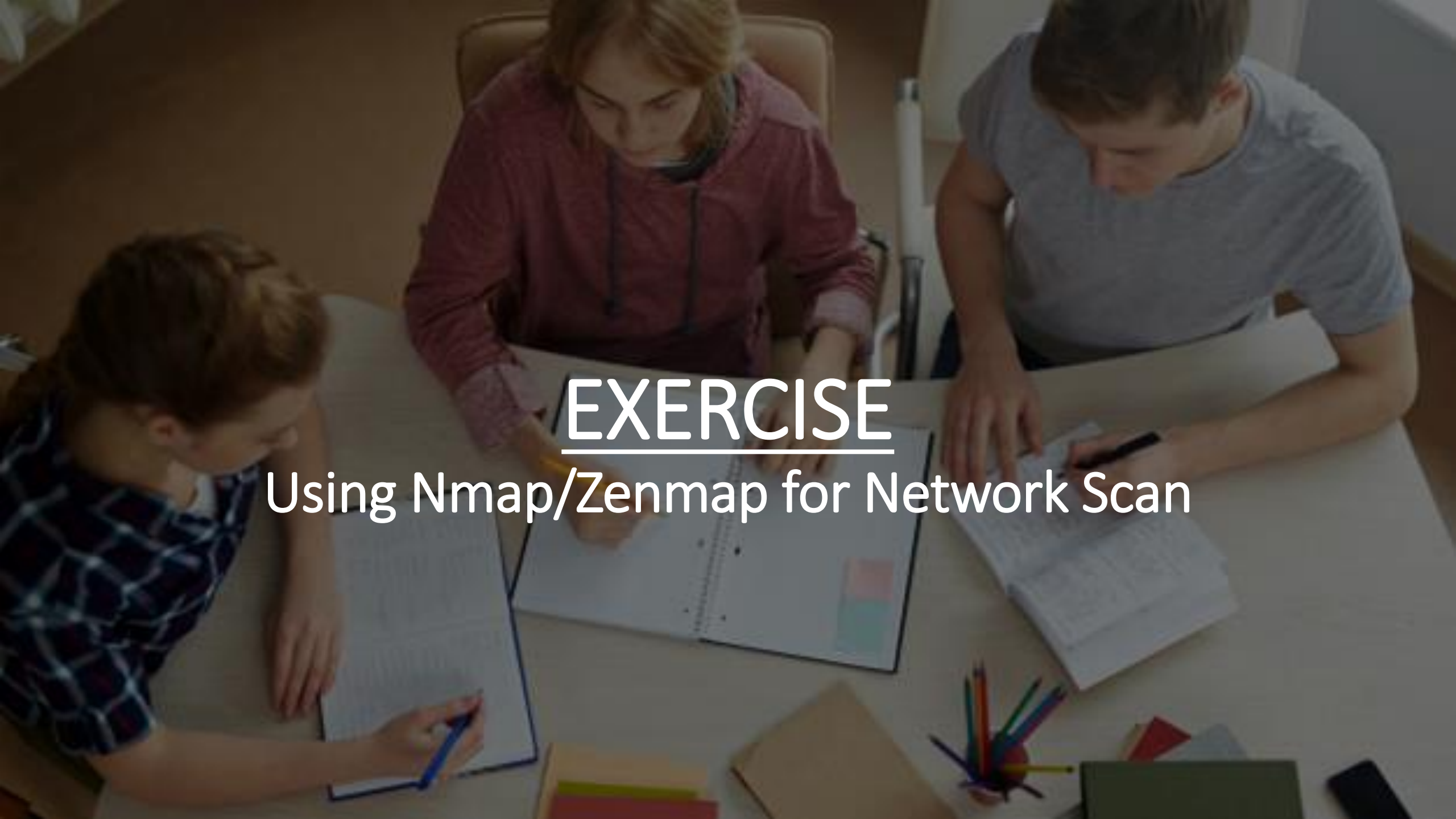
Src IP	Src Port	Dst IP	Dst Port	URL	Remark
202.1.1.1	10234	150.10.10.88	80	/	Web client uses a dummy available port to make a request to web server home page (port 80)
150.10.10.88	80	202.1.1.1	10234	[home page data]	Web server reply and send the data back to web client
202.1.1.1	10234	150.10.10.88	80	/images/logo.jpg	Web client requests an image from web server
150.10.10.88	80	202.1.1.1	10234	[logo graphics]	Web server returns the logo image

Firewall ruleset sample

You have a web server and a mail server for public access.

These servers need to query ISP's DNS server directory.

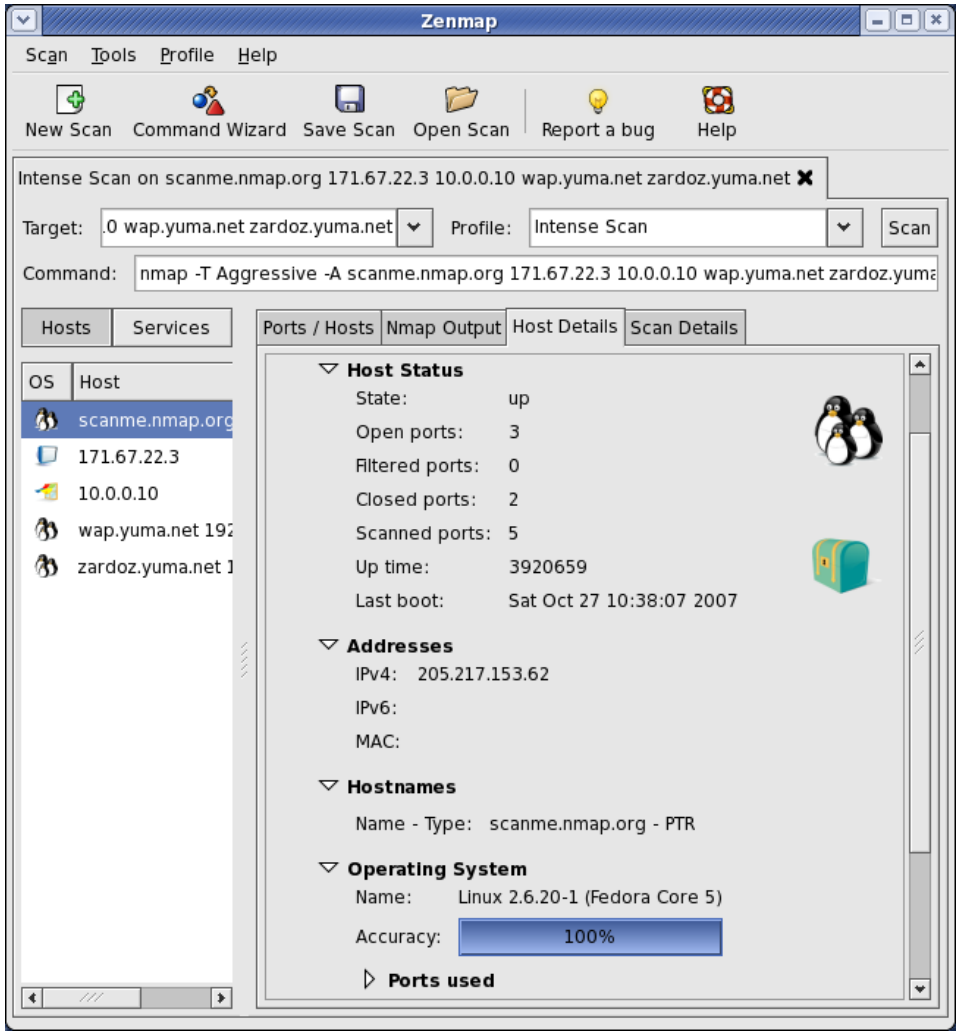
Src IP	Src Port	Dst IP	Dst Port	In / Out	Action	Remark
Any	Any	150.10.10.88	TCP:80	Incoming	Allow	Allow any external IP to access web server (150.10.10.88)
Any	Any	150.10.10.99	TCP:25 TCP:465	Incoming	Allow	Allow any external IP to access mail server (150.10.10.99) using SMTP or SMTPS (encrypted)
Any	Any	20.20.20.20	UDP:53	Outgoing	Allow	Allow any internal IP to query the DNS server (UDP:53) of the ISP (20.20.20.20)
Any	Any	Any	Any	Any	Deny	Deny all other traffics



EXERCISE

Using Nmap/Zenmap for Network Scan

Nmap / Zenmap



MAKE SMART SMARTER

Nmap / Zenmap

Nmap is widely used by network administrators to scan for:

- Open ports and services
- Discover services along with their versions
- Guess the operating system running on a target machine
- Get accurate packet routes till the target machine
- Monitoring hosts

https://nmap.org/

Nmap Scan Types

TCP SCAN	UDP SCAN	SYN SCAN
ACK SCAN	IDLE SCAN	FIN SCAN
XMAS SCAN	RPC SCAN	NULL SCAN

Scenario 1: Basic Nmap Scan against IP or host

Scan by IP

```
nmap 127.0.0.1
```

Scan by host

```
nmap cloudflare.com
```

Scenario 2: Ping Scan

Ping Scan

```
nmap -sp 192.168.5.0/24
```

Usage:
Detect hosts on any network

Drawback:
Remote hosts often block IP-based ping packets for this ICMP-only type of scan.

Scenario 3: Scan specific ports and multiple IP

Scan all 65535 ports

```
nmap -p 1-65535 localhost
```

Scan specific ports

```
nmap -p 80,443 localhost
```

Scan multiple IP

```
nmap 192.168.1.2 192.168.1.3
```

```
nmap 192.168.1.2,3,4
```

=>

```
nmap 192.168.1.2 192.168.1.3 192.168.1.4
```

MAKE SMART SMARTER

Scenario 4: Scan IP Range

Scan IP Range

```
nmap -p 8.8.8.0/28
```

This will scan 14 consecutive IP ranges, from 8.8.8.1 to 8.8.8.14.

=>

```
nmap -p 8.8.8.1-14
```

Scan entire C Class IP range

```
nmap 8.8.8.*
```

This will scan 256 IP addresses from 8.8.8.1 to 8.8.8.256.

Exclude certain IP(s)

```
nmap 8.8.8.* --exclude 8.8.8.1
```

Scenario 5: Scan the most popular ports

Scan the top 20 most common ports for that host

```
nmap --top-ports 20 192.168.1.106
```

```
PORT STATE SERVICE
21/tcp closed ftp
22/tcp closed ssh
23/tcp closed telnet
25/tcp closed smtp
53/tcp closed domain
80/tcp filtered http
110/tcp closed pop3
111/tcp closed rpcbind
135/tcp closed msrpc
139/tcp closed netbios-ssn
143/tcp closed imap
443/tcp filtered https
445/tcp closed microsoft-ds
993/tcp closed imaps
995/tcp closed pop3s
1723/tcp closed pptp
3306/tcp closed mysql
3389/tcp closed ms-wbt-server
5900/tcp closed vnc
8080/tcp closed http-proxy
```

Scenario 6: Scan hosts/IP addresses reading from a text file and save scan results

<<list.txt>>

```
192.168.1.106
cloudflare.com
microsoft.com
securitytrails.com
```

```
nmap -iL list.txt
```

Output to text file

```
nmap -oN output.txt localhost
```

Output to xml file

```
nmap -oX output.xml localhost
```

Scenario 7: Scan + OS and service detection

Scan + OS and service detection

nmap -A -T4 cloudflare.com

-T4 for faster execution

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Cloudflare nginx
| http-server-header:
|   cloudflare
|_  cloudflare-nginx
|_http-title: Did not follow redirect to https://www.cloudflare.com/
443/tcp  open  ssl/https     cloudflare
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 403 Forbidden
|     Server: cloudflare
|     Date: Mon, 01 Oct 2018 11:58:15 GMT
|     Content-Type: text/html
|     Content-Length: 167
|     Connection: close
|     CF-RAY: 462ec1a4696267c1-EZE
|     <html>
|     <head><title>403 Forbidden</title></head>
|     <body bgcolor="white">
|     <center><h1>403 Forbidden</h1></center>
|     <hr><center>cloudflare</center>
|     </body>
|     </html>
```

Scenario 8: Detect service/daemon version

Detect service/daemon version

```
nmap -sV localhost
```

```
PORT STATE SERVICE VERSION
111/tcp open rpcbind 2-4 (RPC #100000)
631/tcp open ipp CUPS 2.2
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
```

Scenario 9: TCP/UDP protocol

Scan TCP

nmap -sT localhost

```
PORT STATE SERVICE
80/tcp open http
1900/tcp open upnp
20005/tcp open btx
49152/tcp open unknown
49153/tcp open unknown
```

Scan UDP

nmap -sU localhost

```
PORT STATE SERVICE
68/udp open|filtered dhcpc
111/udp open rpcbind
5353/udp open|filtered zeroconf
```

Scenario 10: Scan SSL Ciphers

nmap -sV --script ssl-enum-ciphers -p 443 localhost

```
PORT    STATE SERVICE REASON
443/tcp open  https   syn-ack
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (secp256r1) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp256r1) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (secp256r1) - C
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_ECDSA_WITH_RC4_128_SHA (secp256r1) - C
|       TLS_ECDHE_RSA_WITH_RC4_128_SHA (secp256r1) - C
|       TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
|       TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|       Broken cipher RC4 is deprecated by RFC 7465
|       Ciphersuite uses MD5 for message integrity
|       Weak certificate signature: SHA1
|   TLSv1.2:
|     ciphers:
.....................................
```

MAKE SMART SMARTER

System Security

MAKE SMART
SMARTER

System Hardening

EXERCISE

Vulnerability Scanning Tool – Nessus

My First Scan

Exercise 1: My First Scan

1. Launch Nessus Web Client
2. Login Nessus
3. New Scan
4. Click Advanced Scan
5. Type “Exercise1” in Name
6. Type 127.0.0.1 in Targets
7. Add Windows Credential in “Credentials” Tab
8. Click option “Start the Remote Registry service during the scan”
9. Click save and Start scan by clicking “Launch”

How many findings? What is it?

System Hardening

- **System Hardening** is the process of securing a system's configuration and settings to **reduce IT vulnerability and the possibility of being compromised**. This can be done by reducing the attack surface and attack vectors which attackers continuously try to exploit for purpose of malicious activity.

System Hardening
Standard Operating Environments

SOEs are used for workstations and servers.

SOEs provided by third parties are scanned for malicious content and configurations before being used.

SOEs are reviewed and updated at least annually.

MAKE SMART SMARTER

System Hardening
OS Configuration

Hardening Guidance

Assist in hardening the configuration of OS.

Default OS accounts

Disabled, renamed or have their passphrase changed.

Removed Unneeded

Unneeded operating system accounts, software, components, services and functionality are removed or disabled.

Standard Users

Prevented from bypassing, disabling or modifying security functionality of operating and running script execution engines include Windows Script Host (cscript.exe and wscript.exe), PowerShell, cmd.exe, wmic.exe, mshta.exe, etc.

MAKE SMART SMARTER

System Hardening
Local Administrator Account

Local administrator accounts are disabled; alternatively, passphrases that are random and unique for each device's local administrator account are used.

Unique domain accounts with local administrative privileges, but without domain administrative privileges, are used for workstation and server management.

MAKE SMART SMARTER

System Hardening
Application / Software Firewall / Antivirus

Users do not have the ability to install unapproved software or uninstall or disable approved software.

A software firewall is implemented on workstations and servers to limit both inbound and outbound network connections.

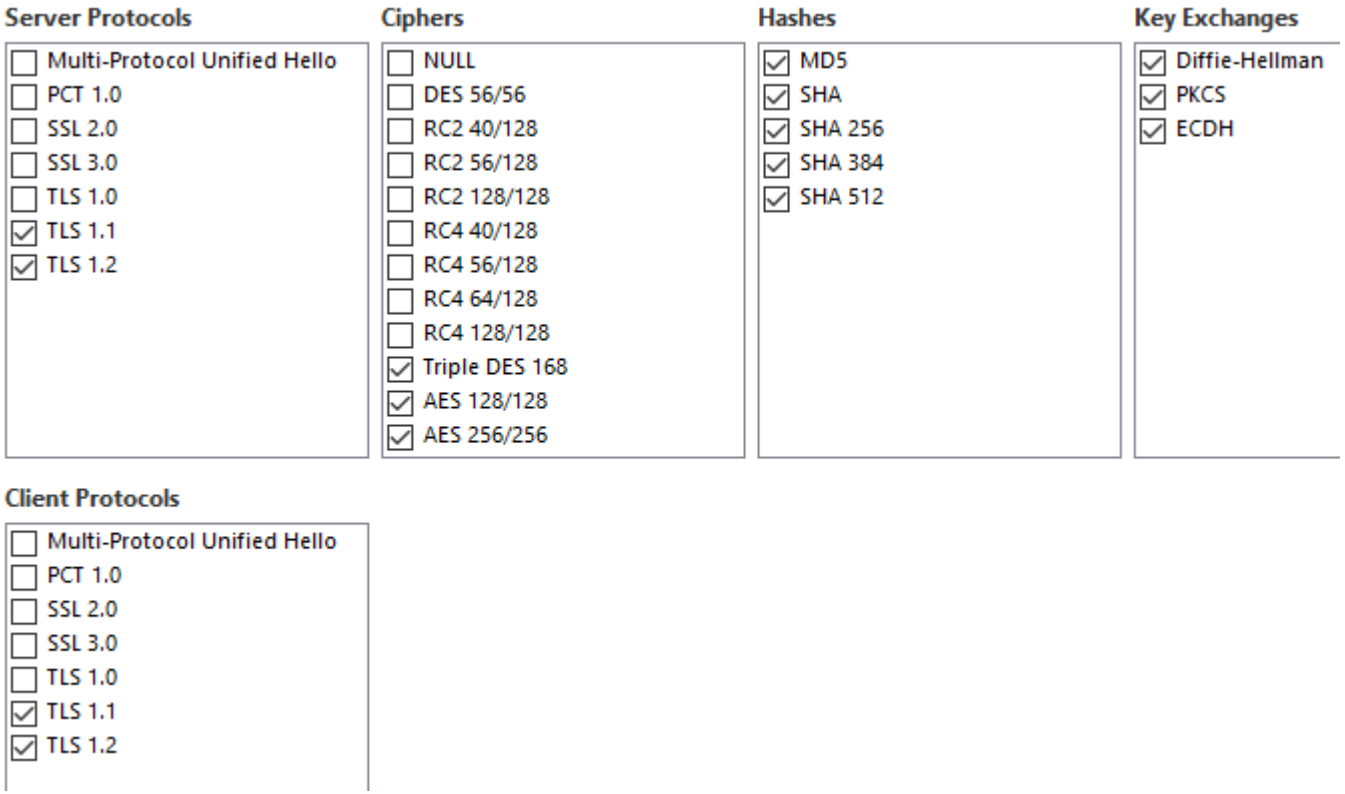
Antivirus software is implemented on workstations and servers.

EXERCISE

Using IISCryto

Exercise 2: Using IISCryto to fix issues

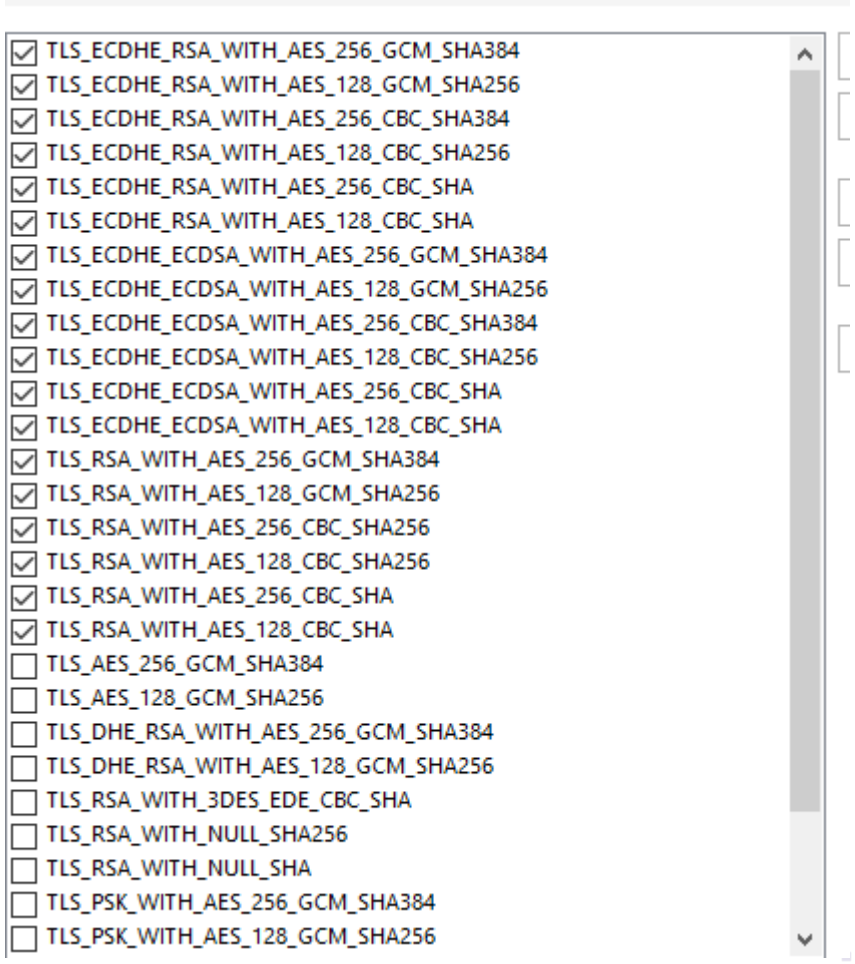
1. Launch IISCryto
2. Disable options as below



Exercise 2: Using IISCryto to fix issues (Cont')

3. For Cipher Suites
4. Click "Reboot" and apply
5. Create new scan and scan again
   (same as Exercise 1)

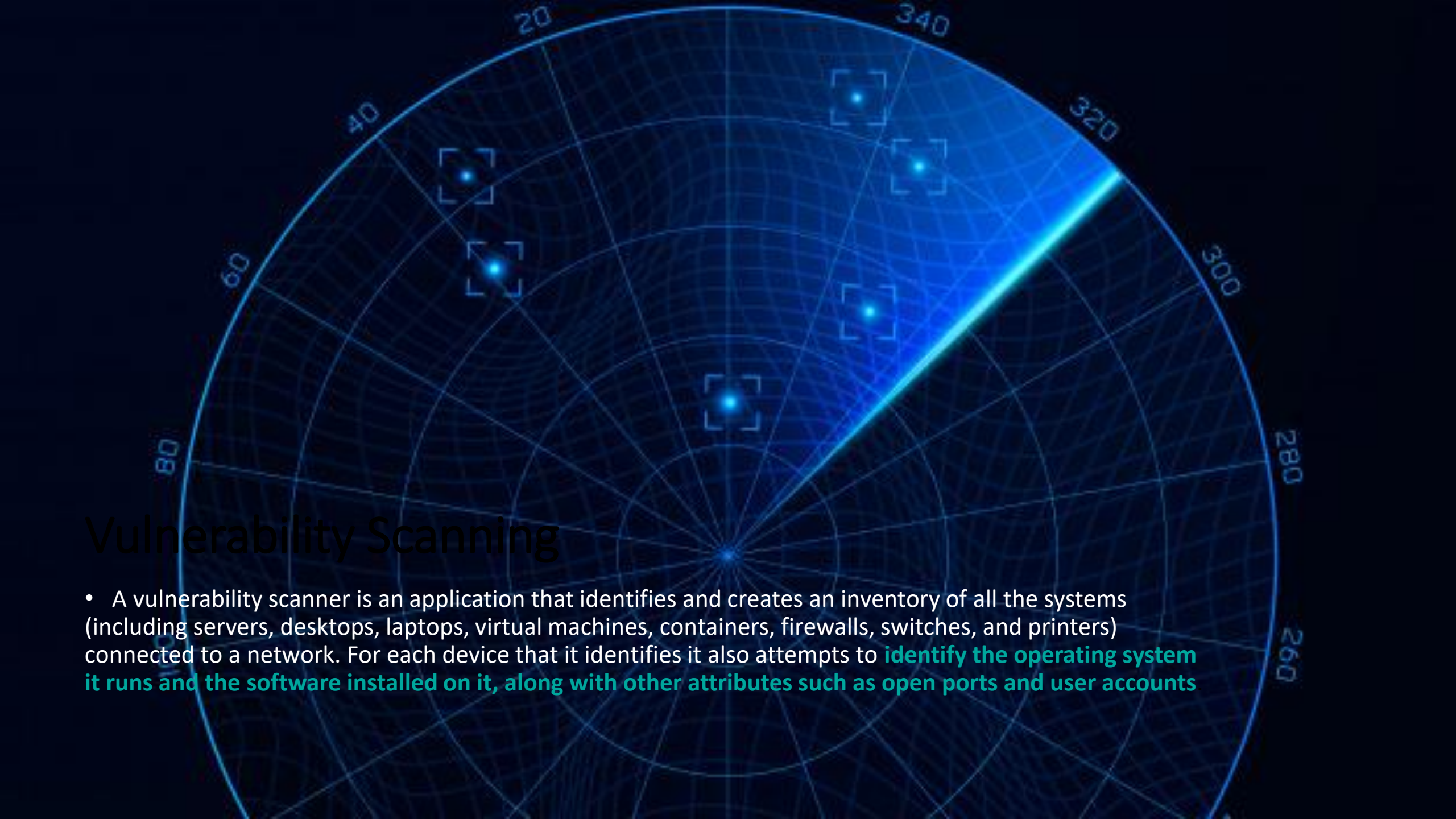
Is the issue fixed?



Vulnerability Management

Vulnerability Management

Vulnerability management is a key responsibility of any IT security team or managed security service provider, and it involves assessing, mitigating (if necessary) and reporting on any security vulnerabilities that exist in an organization's systems and software. But **vulnerabilities can be managed only if they have been discovered and identified**, and the way to achieve this is through a comprehensive vulnerability scanning program.



Vulnerability Scanning

- A vulnerability scanner is an application that identifies and creates an inventory of all the systems (including servers, desktops, laptops, virtual machines, containers, firewalls, switches, and printers) connected to a network. For each device that it identifies it also attempts to **identify the operating system it runs and the software installed on it, along with other attributes such as open ports and user accounts**

Vulnerability Management Process

1. Identification of vulnerabilities
2. Evaluation of the risk posed by any vulnerabilities identified
3. Treatment of any identified vulnerabilities
4. Reporting on vulnerabilities and how they have been handled

MAKE SMART SMARTER

EXERCISE

Generate Scanning Results Report

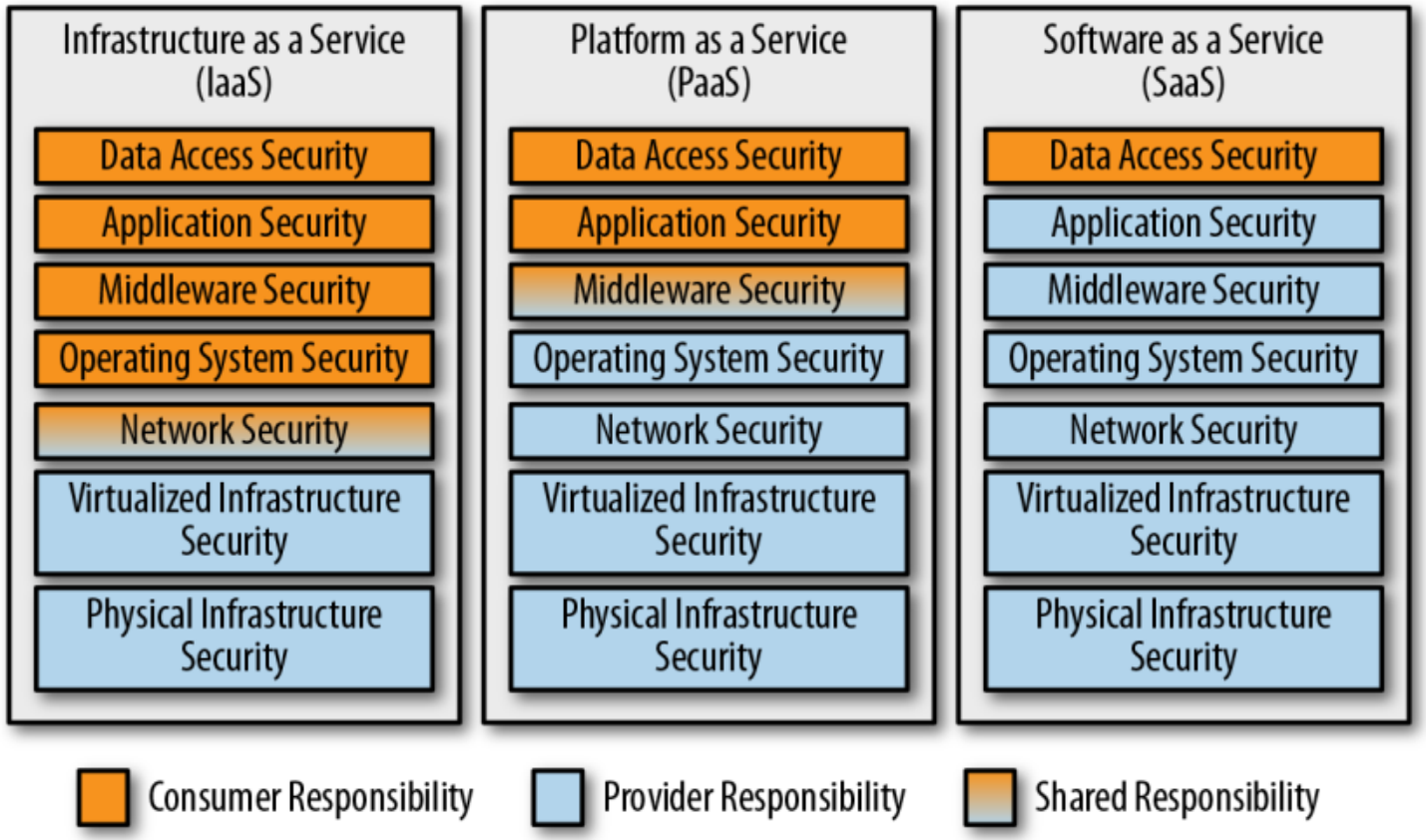
Exercise 3: Scanning Report

1. Click the completed scanning result
2. Click Report
3. Choose HTML
4. Choose Executive Summary and Click Generate Report
5. Generate another report with “Custom” to see the difference

Cloud Security

MAKE SMART
SMARTER

Cloud Security
Shared Responsibility Mode



Cloud Security
Role and Responsibilities

Roles and Responsibilities table of the cloud architecture should be clearly defined and implemented.

Components	CSP	PaaS Provider	Managed Service Provider	Cloud User
User Identity Security		Provide	Define, Provide	Define, Use
Data Access Security		Provide	Define	Use
Application Security		Provide		
Middleware Security	Provide	Define		
Data Storage Security	Provide	Define		
Operation System and Infrastructure Security	Provide	Define		
Network Security	Provide	Define		
Virtualization Security				
Physical Infrastructure Security				

Roles and Responsibilities table of the typical PaaS service model and managed service provider. The red color square shows the shared responsibilities in SaaS service model.

Cloud Security

Access and Authentication

Necessary user account management controls should be enforced.

Privileged User Account should be tightly controlled.

Data should only be accessed and used by appropriate user.

Cloud Security

Storage Security and Encryption

Data at rest encryption should be enforced at all the data storage.

Data encryption key should be securely stored outside the data storage.

Cloud Security

Network Security

Data in transition encryption should be enforced

Application and System should only be accessed from authorized source location.

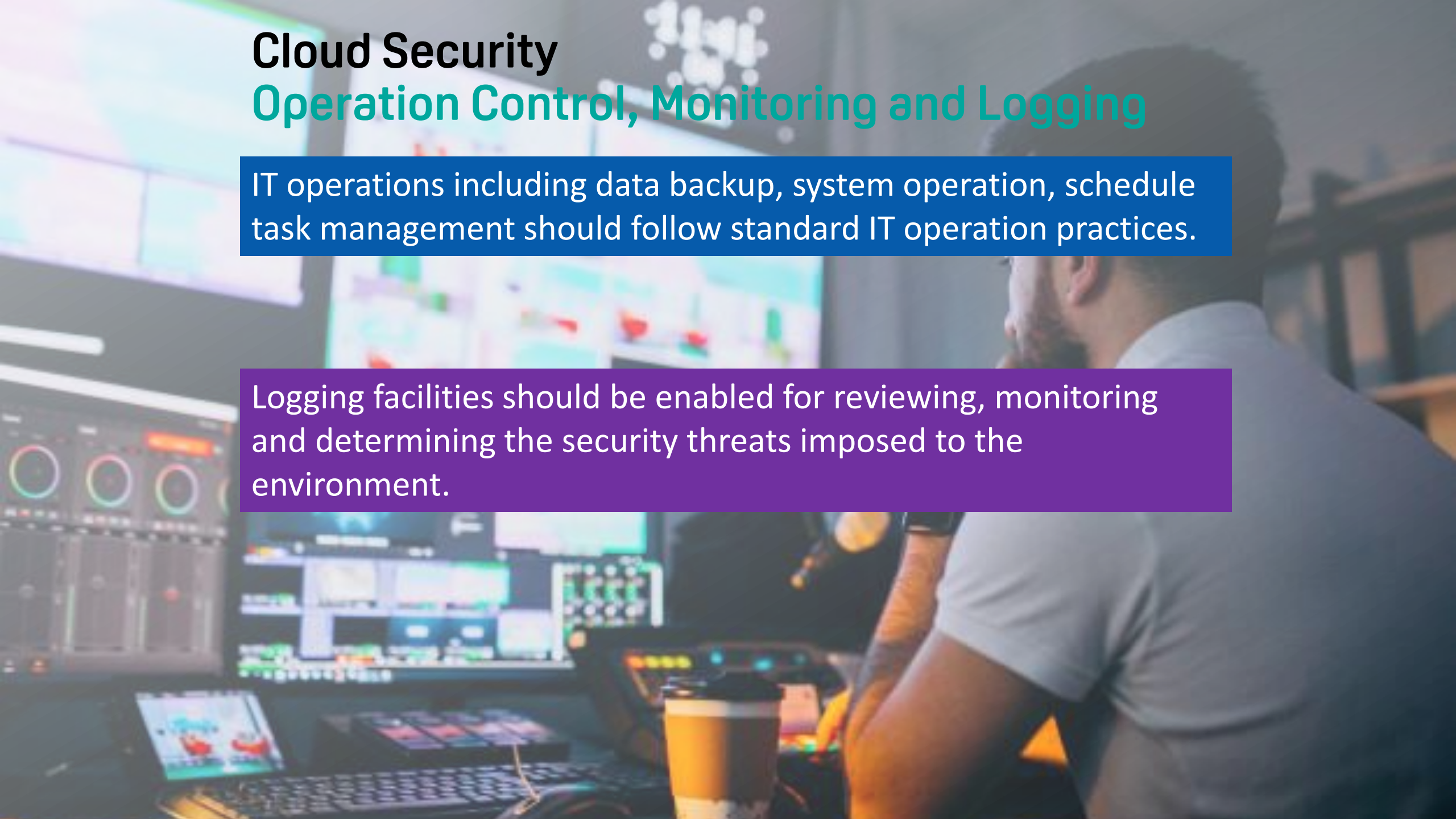
Network should be isolated to prevent unforeseeable multitenant access of data.

Cloud Security

Operation Control, Monitoring and Logging

IT operations including data backup, system operation, schedule task management should follow standard IT operation practices.

Logging facilities should be enabled for reviewing, monitoring and determining the security threats imposed to the environment.



Remote Access/Work from Home

MAKE SMART
SMARTER

Types of Remote Access Technology

1. Remote Desktop Control (**RDC**)

2. Virtual Private Network (**VPN**)

3. Virtual Desktop Infrastructure (**VDI**)

What's the Difference?

RDC

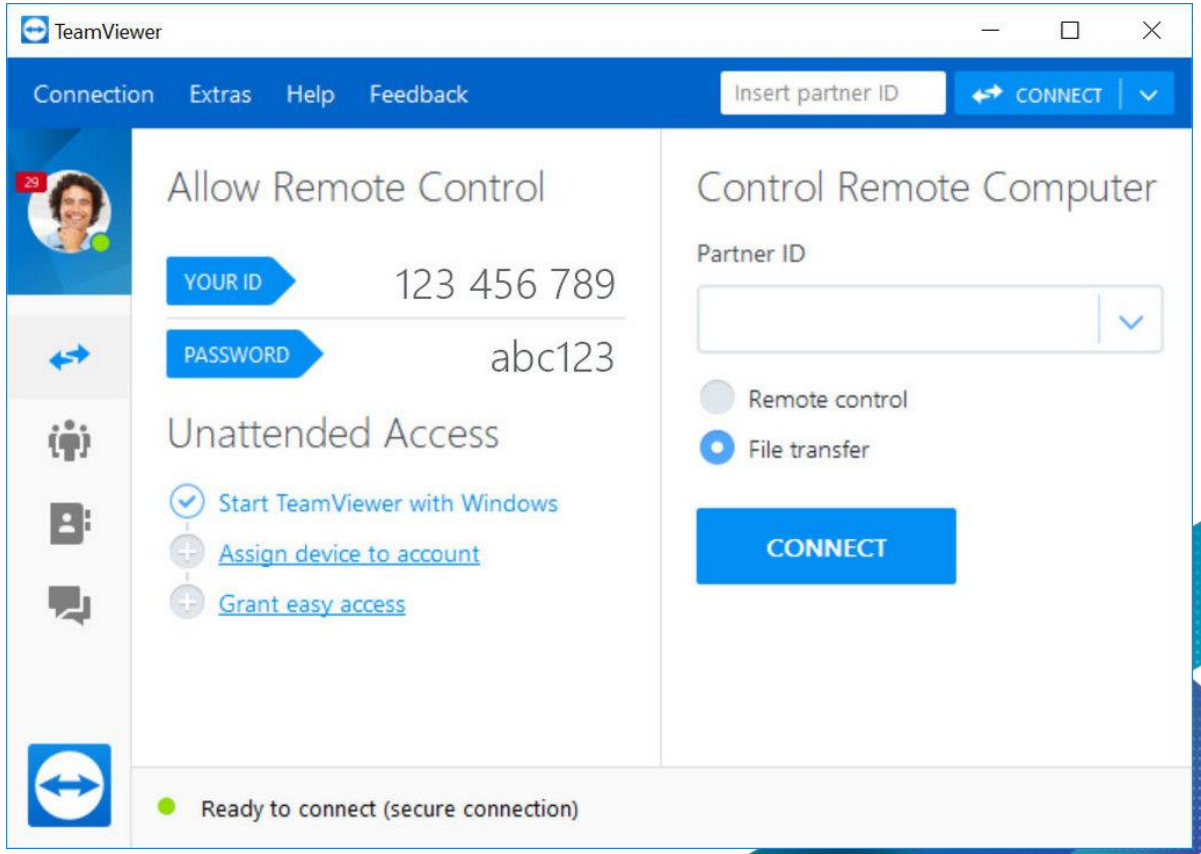
GoToMyPC

TeamViewer

Google Remote Desktop

Microsoft Remote Desktop

Remote Desktop Control is the opening of a corporate PC in internal network to the Internet, allowing the remote users to take control of it from almost anywhere. Its attraction is low cost, convenience and easy-to-use.



***Graph Source**: TeamViewer*

What's the Difference?

VPN

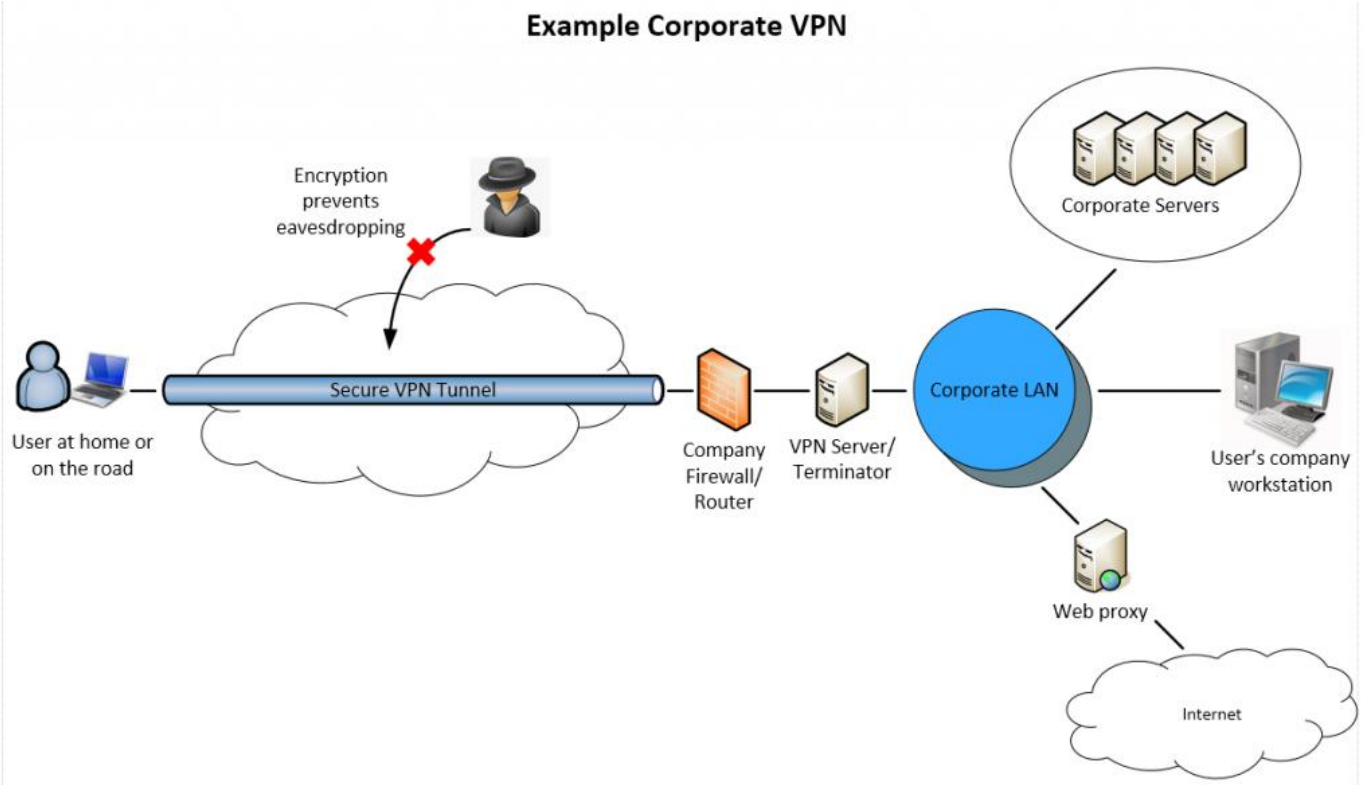
Cisco

Fortinet

Palo Alto

Sangfor

Virtual Private Network is a technology for users to securely access corporate network services through public network as if their computing devices are directly connected to the private network. This technology gives users secure access to corporate network resource such as central storage and printer, but the processing is still done on client machine.



***Graph Source**: securityelements*

What's the Difference?

VDI

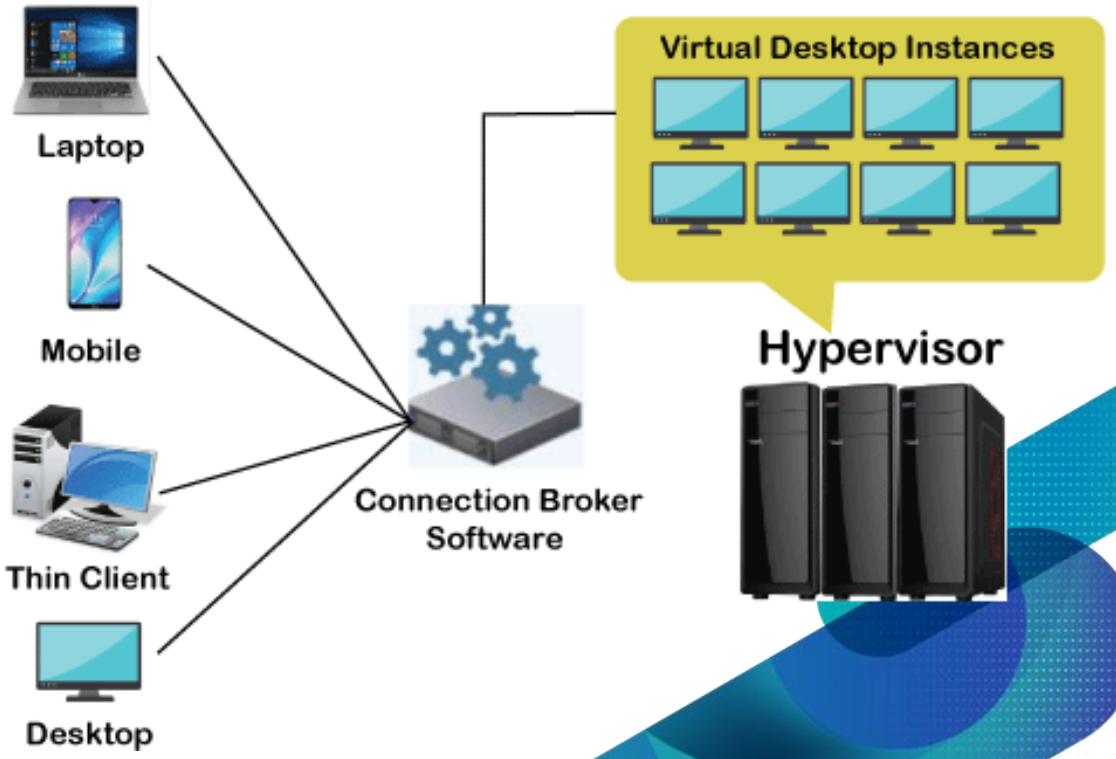
Citrix

Huawei

Microsoft

VMware

Virtual Desktop Infrastructure is the technology for providing and managing virtual desktops. VDI hosts desktop environments on a centralized server and deploys them to end clients on request. These virtualized desktops are created by a virtual machine controlled by a hypervisor. All computing activity on the virtual desktop occurs on the centralized server.



***Graph Source**: javatpoint*

What's the Difference? | COST

RDC

VPN

VDI

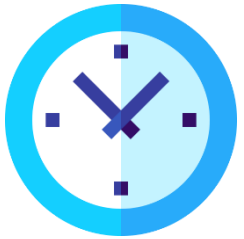
SMARTER

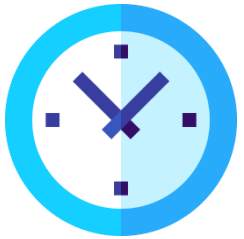
What's the Difference? | PREPARATION TIME

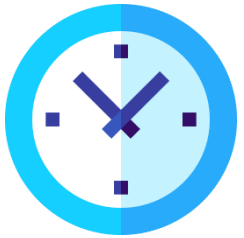
RDC

VPN

VDI







SMARTER

What's the Difference? | PROs

RDC

- *FREE – w/ basic remote control functionality*
- *Additional function - Chargeable*
- *Easy to set up*
- *Good user experience*

VPN

- *Better control (e.g. password strength, 2FA/MFA) and visibility on the network access / activities*
- *Flexible control on the resource(s) that the user is allowed to access*

VDI

- *Flexible to customise or standardise the configuration of the infrastructure*
- *Better visibility on the overall performances and activities*

SMARTER

What's the Difference? | CONs

RDC

- *Suitable for remote support / helpdesk only*
- *Weak on password control*
- *Usually doesn't have 2FA/MFA*
- *Less /no control on the connection*

VPN

- *Infected (personal) may caused risk to corporate network.*

VDI

- *Additional hardware, software and licenses*
- *Maintenance time, IT technical skillset and cost is high*

SMARTER

What's the Difference? | Security Advice

RDC

- *Keep Update the remote control software*
- *Use Strong Password*
- *Enable 2FA/MFA (if available)*

VPN

- *Ensure protection mechanism is enabled to secure the employees' device*
- *Use Strong Password*
- *Enable 2FA/MFA (if available)*

VDI

- *Ensure the OS or application in virtual machines have been patched and updated.*
- *Have full inventory list of all resource*
- *Use Strong Password*
- *Enable 2FA/MFA (if available)*

SMARTER

Increase in exposure during COVID-19.....

and also Cyber Attacks!

EXPLOITS AND VULNERABILITIES | WEB THREATS

Brute force attacks increase due to more open RDP ports

Posted: October 20, 2020 by Pieter Arntz
Last updated: April 14, 2021

While leaving your back door open while you are working from home may be something you do without giving it a second thought, having unnecessary ports open on your computer is a security risk that is sometimes underestimated. That's because an open port can be subject to brute force attacks.

Figure 1. Trend of RDP attack attempts against unique clients (per day), detected by ESET technologies

Source: https://blog.malwarebytes.com/exploits-and-vulnerabilities/2020/10/brute-force-attacks-increasing/
https://www.bankinfosecurity.com/brute-force-attacks-targeting-rdp-on-rise-a-14531

DON'T Rush to Set Up Infrastructure

DO Adopt Secure Design Principles

Security Advices for Organisation

1.Provide Remote Access Security Policy

Ensure all staff fully understand the rules of using the relevant services

2.Review the Security Configuration Regularly

Ensure the software is updated and security configurations are tightened

3.Review User List & the Access Right Regularly

Ensure each employee can only access the systems resources required for their work

4.Set Up Log Monitoring & Alert Mechanism

Any abnormal logs or suspicious traffic should trigger alert and notify relevant staff immediately. Incident investigation should be conducted.

5.Enable 2-Factor Authentication / Multi-Factors Authentication

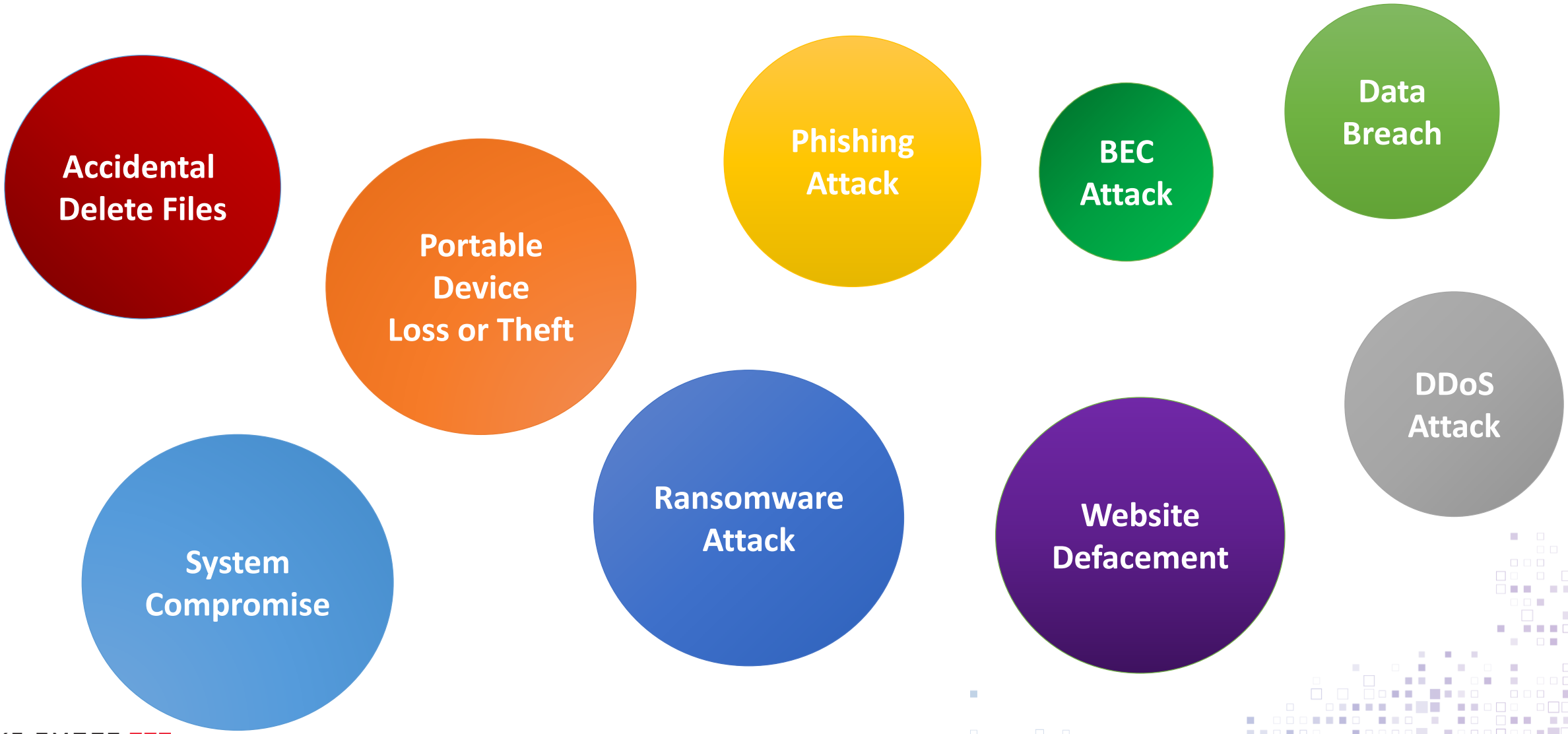
For all privileged and non-privileged accounts

6.Consider DDoS Protection Solution

Protect against DDoS to ensure systems availability

Incident Response

Common Types of Cyber Security Incident



MAKE SMART SMARTER

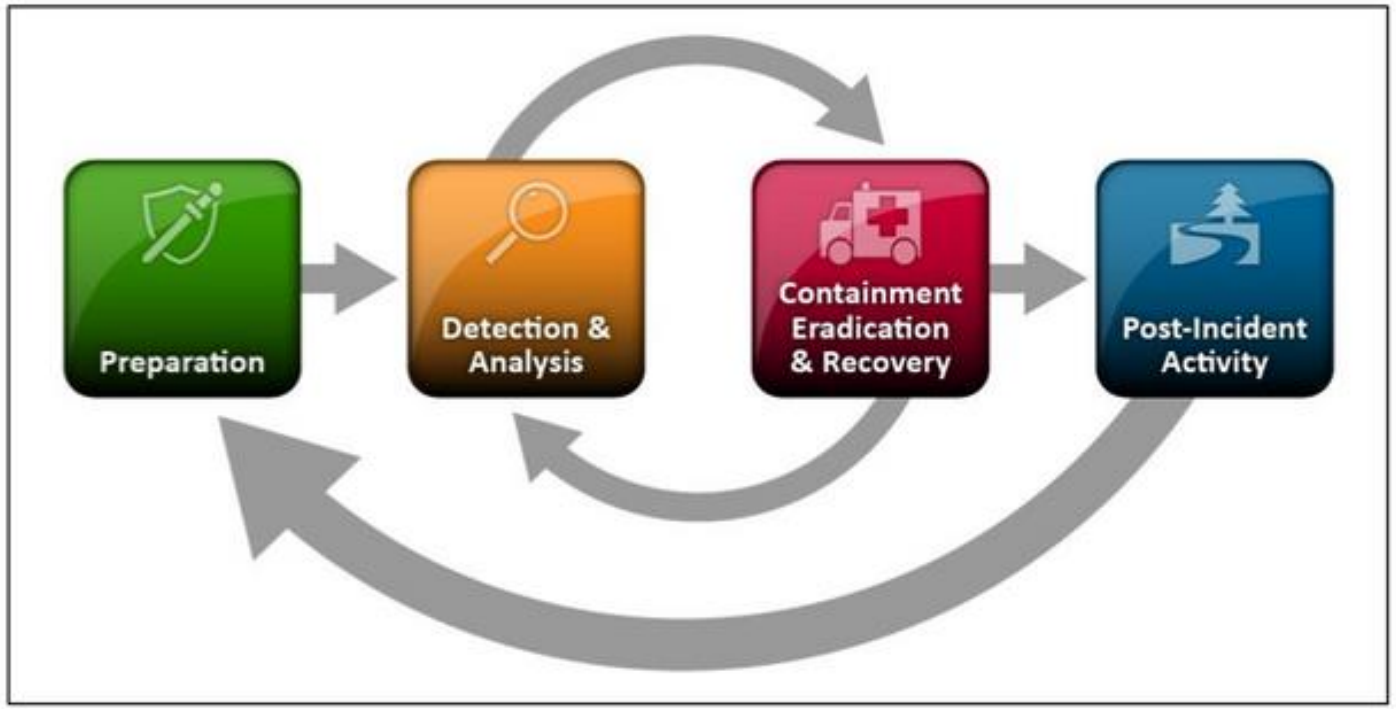
Goals of Incident Response

- Minimise the **possible impact** of the incident
- **Prevent further** attacks and damages
- Protect your organisation's **reputation and assets**
- Ensure that all the responsible parties have clear understanding about the tasks they should perform during an incident by following **predefined procedures**
- Ensure that the **response is systematic and efficient** and that there is **prompt recovery** for the compromised system
- **Educate** senior management and general staff
- Deal with related **legal issues**

Methodology of Incident Response

MAKE SMART SMARTER

Methodology of Incident Response



***Graph Source**: NIST 800-61 Cyber Security Incident Handling Guide*

Source: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Methodology of Incident Response

Preparation

- Establish **Incident Response Polices and Procedures**
- Build up the **Incident Response Team** and define staff roles and responsibilities in incident handling process
- Establish security **monitoring** and **alerts**
- Develop and maintain **emergency contact list**
- Develop and maintain good **backup strategy**
- Provide staff **training** on the knowledge and skills of incident response

The preparation phase includes steps taken **before** an incident occurs.

Methodology of Incident Response

Preparation

Emergency Contact List

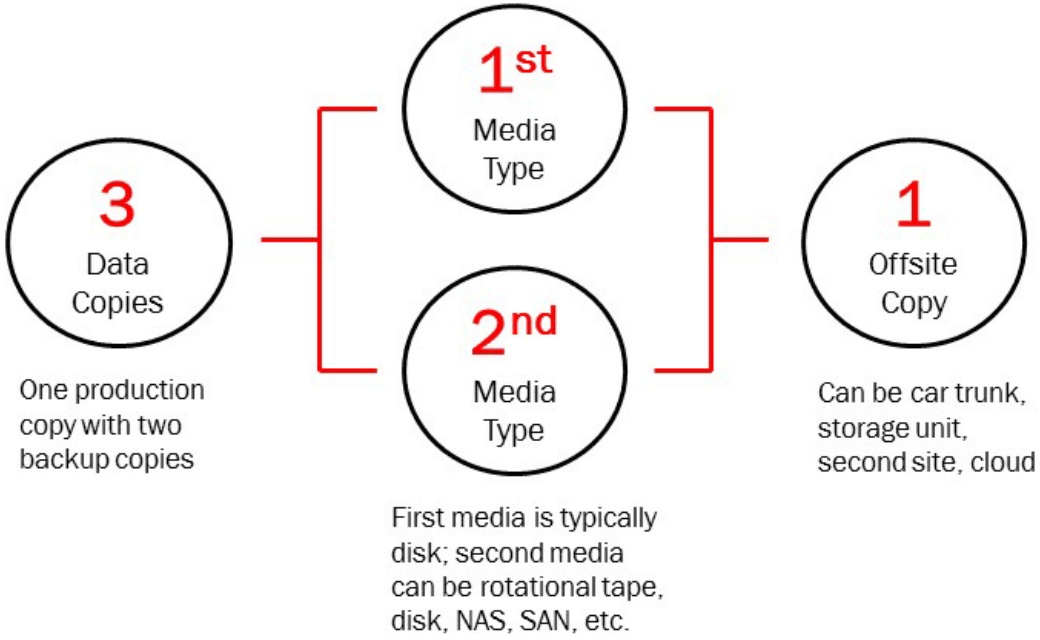
- ✓ IR Team members
- ✓ Project owner, System owner, Asset owner
- ✓ Vendor, Service Supplier
- ✓ Law enforcement
- ✓ Other CERT Team

MAKE SMART SMARTER

Methodology of Incident Response

Preparation

3 -2 - 1 Backup Strategy



- ✓ Backup restoration tests should be conducted regularly.
- ✓ The purposes of the restoration test include:
  1) the backup process is effective, and data can be restored successfully;
  2) practising the restoration process.

MAKE SMART SMARTER

***Graph Source**: unitrends*

Sources of Indicators

Methodology of Incident Response

Detection & Analysis

Alerts

- IDS/IPS
- Antivirus Software
- SIEM
- Data Loss Prevention
- Other monitoring tools

Logs

- OS logs
- Application logs
- Network flows

People

- Staff
- External Consultants, experts

OSINT

- CVE
- CERT information
- Other OSINT databases

MAKE SMART SMARTER

Gathering Information of Incident Response

MAKE SMART
SMARTER

Gathering Information for Incident Response

Objective

- Gather basic information about the threat actors
- Categorise the security incident
- Perform initial analysis with online tools
- Correlate information for further investigation
- Identify related contact information for abuse reporting

Gathering Information - Technique 1

- Check Domain and IP Address information
  - Check geolocation
  - Check registrar
  - Check ISP / ASN
  - Check if suspicious domain name e.g. xyz.top / xyz.info
  - Check abuse reporting contact

- Tools

  Hurricane Electric Internet Services (https://bgp.he.net/)
  APNIC Whois (https://wq.apnic.net/static/search.html)
  Maxmind GeoIP (https://www.maxmind.com/en/geoip-demo)
  CERT.at geolocate (https://contacts.cert.at/cgi-bin/abuse-nationalcert.pl)

Gathering Information - Technique 1

Hurricane Electric Internet Services (https://bgp.he.net/)

DNS Info | Website Info | IP Info | Whois

```
Domain Name: HKCERT.ORG
Registry Domain ID: D82191547-LROR
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.whois.godaddy.com
Updated Date: 2019-06-12T04:16:31Z
Creation Date: 2002-01-09T11:19:20Z
Registry Expiry Date: 2023-01-09T11:19:20Z
Registrar Registration Expiration Date:
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: Hong Kong Productivity Council
Registrant State/Province:
Registrant Country: HK
Name Server: DORTHY.NS.CLOUDFLARE.COM
Name Server: JOEL.NS.CLOUDFLARE.COM
DNSSEC: signedDelegation
URL of the ICANN Whois Inaccuracy Complaint Form https://www.icann.org/wicf/)
>>> Last update of WHOIS database: 2019-08-06T07:27:13Z <<<
```

Registrar Info.

Geolocation

MAKE SMART SMARTER

Gathering Information - Technique 1

IP Address

AS Number

DNS Info | Website Info | IP Info | Whois

104.26.9.124	104.26.0.0/20	AS13335	Cloudflare, Inc.
104.26.9.124	104.16.0.0/12	AS13335	Cloudflare, Inc.
104.26.8.124	104.26.0.0/20	AS13335	Cloudflare, Inc.
104.26.8.124	104.16.0.0/12	AS13335	Cloudflare, Inc.
172.67.72.42	172.67.64.0/20	AS13335	Cloudflare, Inc.
2606:4700:20::ac43:482a	2606:4700:20::/44	AS13335	Cloudflare, Inc.
2606:4700:20::ac43:482a	2606:4700::/36	AS13335	Cloudflare, Inc.
2606:4700:20::681a:97c	2606:4700:20::/44	AS13335	Cloudflare, Inc.
2606:4700:20::681a:97c	2606:4700::/36	AS13335	Cloudflare, Inc.
2606:4700:20::681a:87c	2606:4700:20::/44	AS13335	Cloudflare, Inc.
2606:4700:20::681a:87c	2606:4700::/36	AS13335	Cloudflare, Inc.

ISP

```
ip          countrycode     certname        email
104.26.9.124    US          US-CERT soc@us-cert.gov
```

CERT.at geolocate (https://contacts.cert.at/cgi-bin/abuse-nationalcert.pl)

MAKE SMART SMARTER

Gathering Information - Technique 2

Check HTTP header information

Purpose

- Check if redirection (Status 301)

Tools

- CURL command

```
curl -I <URL>
```

- CURL online tool (https://helloacm.com/curl/)

Gathering Information - Technique 2

http://yahoo.com

Request HTTP Header

```
----Found in Cache----
HTTP/1.1 301 Moved Permanently
Date: Wed, 12 May 2021 01:42:49 GMT
Connection: keep-alive
Server: ATS
Cache-Control: no-store, no-cache
Content-Type: text/html
Content-Language: en
X-Frame-Options: SAMEORIGIN
Location: https://yahoo.com/
Content-Length: 8
----URL Redirected to https://yahoo.com/----
HTTP/2 301
date: Wed, 12 May 2021 01:42:49 GMT
strict-transport-security: max-age=31536000
server: ATS
cache-control: no-store, no-cache
content-type: text/html
content-language: en
x-frame-options: SAMEORIGIN
expect-ct: max-age=31536000, report-uri="http://csp.yahoo.com/beacon/csp?src=yahoocom-expect-ct-report-only"
referrer-policy: no-referrer-when-downgrade
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
location: https://www.yahoo.com/
content-length: 8
----URL Redirected to https://www.yahoo.com/----
```

HTTP Status Code

Redirected to URL

Gathering Information - Technique 3

Check for virus / malware / Phishing

Purpose

- Check if the URL or file contains virus
- Check if the URL in the TI database
- Check HTTP behaviour
- Review SSL Certificate

Tools

- Virustotal (https://www.virustotal.com/)
- URLScan (https://urlscan.io)
- PhishingTank (https://phishtank.com/)

Gathering Information - Technique 3

apple-id-iphone-us.vip

118.107.13.18 Malicious Activity! Private scan

Lookup | Go To | Report | Rescan

Submitted URL: https://apple-id-iphone-us.vip/us
Effective URL: https://apple-id-iphone-us.vip/usIn9BZ?language=CN&Auth%2Flogin.html
Submission: On May 12 via manual (May 12th 2021, 1:55:48 am) from HK

Summary | HTTP 25 | Redirects | Links 23 | Behaviour | Indicators | Similar 684 | DOM | Content | API

Summary

IP information

This website contacted **2 IPs** in **2 countries** across **2 domains** to perform **25 HTTP transactions**.
The main IP is 118.107.13.18, located in **Singapore** and belongs to BCPL-SG BGPNET Global ASN, SG. The main domain is apple-id-iphone-us.vip.
TLS certificate: Issued by *TrustAsia TLS RSA CA* on May 1st 2021. Valid for: a year.

This is the only time *apple-id-iphone-us.vip* was scanned on urlscan.io!

684 similar pages on different IPs, domains and ASNs found — Show Scans 684

urlscan.io Verdict: Potentially Malicious

Targeting these brands: Apple (Online)

Phishing Target Brand

Live information

Google Safe Browsing: Malicious for *apple-id-iphone-us.vip*
Current DNS A record: 118.107.13.18 (AS64050 - BCPL-SG BGPNET Global ASN, SG)

Screenshot

Live screenshot | Full Image

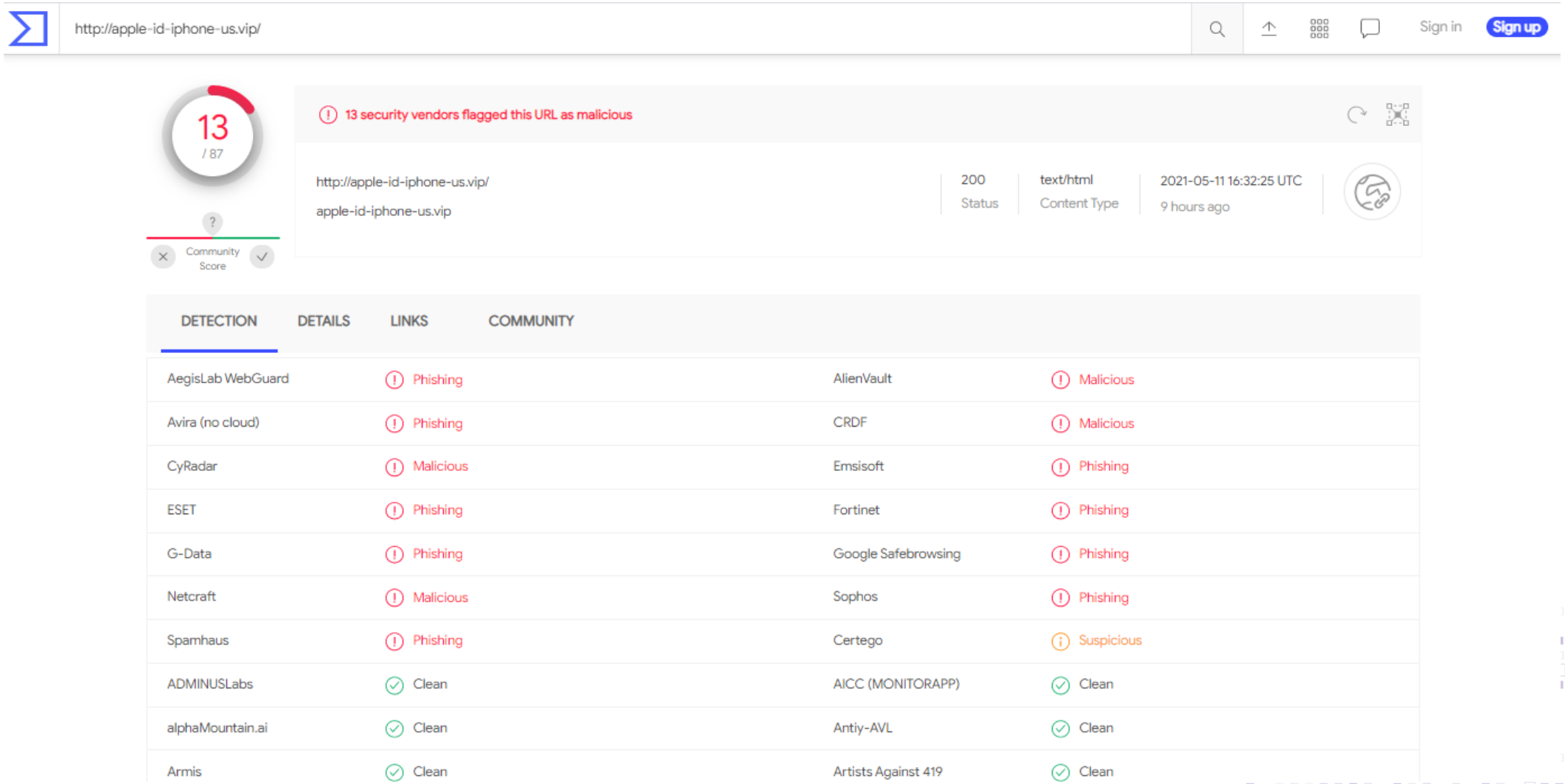
Page URL History

Show full URLs

1. https://apple-id-iphone-us.vip/us HTTP 302
   https://apple-id-iphone-us.vip/usIn9BZ?language=CN&Auth%2Flogin.html Page URL

MAKE SMART SMARTER

Gathering Information - Technique 3



Gathering Information - Technique 4

Check Email header information

Purpose

Check email sender & related information

Tools

Email reader tool (https://mha.azurewebsites.net/)

EXERCISE

Gathering Information

Exercise - Gathering Information

Time: 10 minutes

Your role: Security Analyst

Scenario: A user reported suspected phishing emails that contains suspicious URLs **(Cautions: Do not access the link directly in browser)**

http[:]//findin-appleios[.]cn

Task

Use the techniques to gather basic information about the suspicious URLs

Questions

What is the domain registrant organisation, country, name of registrar?

What is the geolocation of the IP Address?

Any URL redirection?

Any finding on virus / malware?

What is the contact for abuse reporting?

What is the contact of corresponding CERT?

Gathering Information Tool Lists

Hurricane Electric Internet Services (https://bgp.he.net/)

APNIC Whois (https://wq.apnic.net/static/search.html)

Maxmind GeoIP (https://www.maxmind.com/en/geoip-demo)

CERT.at geolocate (https://contacts.cert.at/cgi-bin/abuse-nationalcert.pl)

Virustotal (https://www.virustotal.com/)

URLScan (https://urlscan.io)

PhishingTank (https://phishtank.com/)

Methodology of Incident Response

Containment
Eradication &
Recovery

Containment: The actions required to prevent the incident or event from spreading across the network

Eradication: The actions that are required to completely wipe the threat from the network or system

Recovery: The actions required to bring back the network or system to its former functionality and use

Reporting security incidents

MAKE SMART
SMARTER

Answer 6 W's about the security incidents

Incident Reporting Basics

- **What:**
  - What actually happened?
  - What the incident might mean for the organization?
  - What is the impact?
  - What system affected?
  - What service affected?
  - What actions had been taken?
  - etc.

- **Who:**
  - Threat actor / IP address
  - Attack source
  - Hacking group
  - Attack target
  - Owner of targeted system
  - Owner of involved business function
  - Customers affected
  - Parties involved
    - Internal
    - External
  - etc.

Incident Reporting Basics

- **When:**
  - When the incident happened?
  - When the incident being detected?
  - Incident duration
  - Incident timeline
    - Actions
    - Decisions
    - Information collected
  - etc.

- **Where:**
  - Where is the attacks originated from?
  - Attack paths
  - Lateral movement
  - Logical
    - Network zone
  - Physical
    - Cloud
    - On-premises
  - etc.

Incident Reporting Basics

- **How:**
  - How does it happened?
  - How the systems infected?
  - What vulnerabilities exploited?
  - Attack method
  - Intrusion method
  - Command and control
  - Evade detection
  - Obfuscation
  - etc.

- **Why:**
  - Why does it happened?
  - Root cause
  - etc.


Q & A

Evaluation Form

https://bit.ly/35vdqw8

Thank you

Hong Kong Productivity Council
香港生產力促進局
HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 5678 www.hkpc.org

MAKE SMART
SMARTER