Operation security Week7

- What is Operations Security (OPSEC)?
- OPSEC Processes:
  - Identify critical information
  - Analyze threats
  - Discover vulnerabilities
  - Assess risks
  - Develop countermeasures
- Identify threats, vulnerabilities, and risks
- Handling threats

What is OPSEC?

- OPSEC is taking precautions to protect information
- and assets from potential threats.
- Examples:
  - Preventing house break-ins while traveling
  - Avoiding purse or package theft
  - Protecting against credit card fraud

OPSEC Overview

- A security and risk management process
- to classify and protect information.
- Originally a military strategy to prevent adversaries from
- accessing sensitive information.

OPSEC Processes

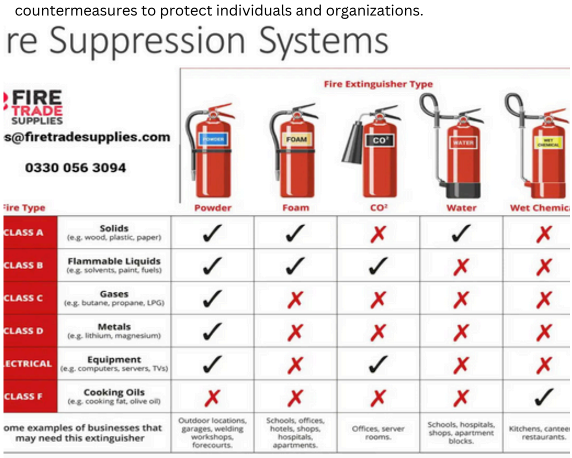
1. Identify Critical Information:
   - Examples: Credit card numbers, passwords, travel dates, etc.
2. Analyze Threats:
   - Examples: Phishing, malware, viruses, etc.
3. Discover Vulnerabilities:
   - Examples: Outdated software, weak passwords, unencrypted data.
4. Assess Risks:
   - Evaluate the impact of losing data and estimate potential loss.
5. Develop Countermeasures:
   - Implement security controls to mitigate risks.

Identifying Threats, Vulnerabilities & Risks

- Threat: Event or person that could harm resources (e.g., natural disasters, intentional attacks).
- Vulnerability: Weaknesses in systems (e.g., unpatched software, viruses).
- Risk: Potential loss or damage when a threat exploits a vulnerability (e.g., financial loss, reputation damage).

How to Handle Threats

- Train employees
- Keep systems updated
- Ensure endpoint protection (devices)
- Install firewalls
- Backup data regularly
- Control access to systems
- Secure Wi-Fi (WPA2, WPA3)
- Manage access to accounts and passwords
- OPSEC is essential for identifying and mitigating risks by recognizing critical information, analyzing potentia
- l threats, addressing vulnerabilities, and developing effective countermeasures to protect individuals and organizations.



re Suppression Systems

FIRE TRADE SUPPLIES
s@firetradesupplies.com
0330 056 3094

Fire Extinguisher Type

ire Type		Powder	Foam	CO²	Water	Wet Chemic
CLASS A	Solids (e.g. wood, plastic, paper)	✓	✓	✗	✓	✗
CLASS B	Flammable Liquids (e.g. solvents, paint, fuels)	✓	✓	✓	✗	✗
CLASS C	Gases (e.g. butane, propane, LPG)	✓	✗	✗	✗	✗
CLASS D	Metals (e.g. lithium, magnesium)	✓	✗	✗	✗	✗
ECTRICAL	Equipment (e.g. computers, servers, TVs)	✓	✗	✓	✗	✗
CLASS F	Cooking Oils (e.g. cooking fat, olive oil)	✗	✗	✗	✗	✓
ome examples of businesses that may need this extinguisher		Outdoor locations, garages, welding workshops, forecourts.	Schools, offices, hotels, shops, hospitals, apartments.	Offices, server rooms.	Schools, hospitals, shops, apartment blocks.	Kitchens, cantee restaurants.

Network security (week 8)

What is "Security"?

- Safety: Freedom from risk or danger.
- Confidence: Freedom from doubt, anxiety, or fear.
- Protective Measures: Actions taken to safeguard a place and ensure only authorized access.
- Data Protection: Ensuring only authorized individuals have access to sensitive computer files.

Why do we need security?

- Protect Vital Information: Safeguard sensitive data like trade secrets, medical records, etc.
- Provide Authentication and Access Control: Ensure only authorized users can access resources.
- Guarantee Resource Availability: Ensure high availability, e.g., 99.999% (5 9's) reliability.

Who is vulnerable?

- Financial institutions and banks
- Internet service providers
- Government agencies
- Military systems
- Anyone on the network

Common Security Attacks and Their Countermeasures

- Finding a way into the network: Countered by firewalls.
- Exploiting software bugs, buffer overflows: Countered by Intrusion Detection Systems (IDS).
- TCP Hijacking: Countered by IPSec (Internet Protocol Security).
- Packet Sniffing: Countered by encryption.

TCP Hijacking

- Attack: Taking control of a TCP session.
- Countermeasure: Use of IPSec to secure the session.

Denial of Service (DoS) Attacks

- Attack: Overwhelming a system to make it unavailable.
- Countermeasure: Ingress filtering (filtering out malicious traffic).

Social Problems

- Countermeasure: Education and training to prevent social engineering attacks.

SMURF Attack

1. Attacker identifies and steals IP address of the victim: The attacker spoofs the IP address of the target.
2. Attacker sends requests to the server on the network: The attacker sends numerous ICMP (ping) requests to a network's broadcast address.
3. Server replies to the victim: The server replies to the spoofed IP address (victim's address) with responses.
4. Victim is flooded with replies and overloaded: The victim receives a flood of replies, overwhelming its resources and causing a denial of service.

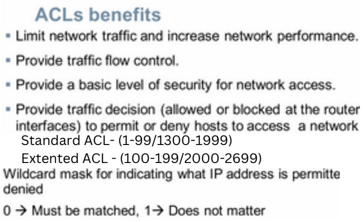
Firewalls

- Problem: Many network applications and protocols have security vulnerabilities.
- Solution: Administrators use firewalls to limit access and control traffic.
- Up-to-date Firewalls: Must be maintained by administrators to remain effective.

Firewalls: Conceptual Comparison

- Castle with a drawbridge: Only one point of access into the system (like a castle) which can be an advantage or disadvantage.
- Types:
  - Hardware: Some routers include firewall functionality.
  - Software: Unix systems, Windows XP, and Mac OS X come with built-in firewalls.

Week- 9



ACLs benefits

- Limit network traffic and increase network performance.
- Provide traffic flow control.
- Provide a basic level of security for network access.
- Provide traffic decision (allowed or blocked at the router interfaces) to permit or deny hosts to access a network

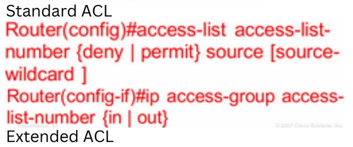
Standard ACL- (1-99/1300-1999)

Extented ACL - (100-199/2000-2699)

Wildcard mask for indicating what IP address is permitte denied

0 → Must be matched, 1→ Does not matter

Standard ACL



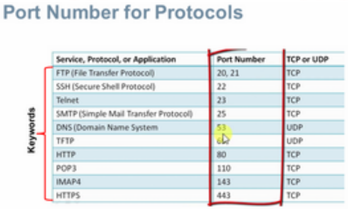
```
Router(config)#access-list access-list-number {deny | permit} source [source-wildcard ]
Router(config-if)#ip access-group access-list-number {in | out}
```

Extended ACL

```
Router(config)#access-list access-list-number {deny | permit} protocol source [source-wildcard] destination [destination-wildcard] [port number](or)[keywords]
```

Access list number → 100 – 199 / 2000 – 2699

```
Router(config)#specific interface
Router(config-if)#ip access-group access-list-number {in | out}
```



Port Number for Protocols

Service, Protocol, or Application	Port Number	TCP or UDP
FTP (File Transfer Protocol)	20, 21	TCP
SSH (Secure Shell Protocol)	22	TCP
Telnet	23	TCP
SMTP (Simple Mail Transfer Protocol)	25	TCP
DNS (Domain Name System	53	UDP
TFTP	69	UDP
HTTP	80	TCP
POP3	110	TCP
IMAP4	143	TCP
HTTPS	443	TCP

VPN Tunneling

1. Set ip address for all the router and pc.
2. Set gateway for pc and server(if exist)
3. Set default routing in routers

(CMD- ip route 0.0.0.0 0.0.0.0 (IP of connection)

4. test between router by pinging

5. Create vpn tunnel in both router

(CMD- interface tunnel 1
ip address (VPN address and subnet)
tunnel source (direction of connection)
tunnel destination (destination of connection)
end

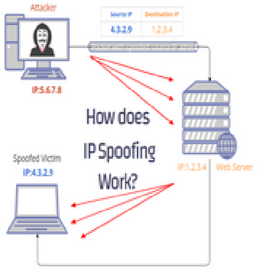
6. check ping in router

(CMD- ping (VPN address)

7.create route for pc to connect over VPN

(CMD - ip route (Pc IP Subnet IP destination VPN IP)

8. Check connection by pinging from pc to another network pc



Application Security (week 11)

Keeping Up with Patches

- Identify the application: Know which applications require patching.
- Follow vendors or developers: Keep track of update releases from the relevant vendors or developers.
- Automatic patching: Some vendors, like Microsoft, offer automatic updates.
- Risk of bad patch: Less risky than delaying patches.
- Patch timing: Worms often spread around patch releases, making timely updates crucial.

Check Vendor and Security Websites

- Update distribution: Vendors distribute updates via websites and search engines like Google.
- Widely used vendors:
  - Google Chrome
  - Mozilla Firefox
  - Microsoft
  - Dell
  - HP

Subscribe to Security Mailing Lists

- Security mailing lists: Most vendors have mailing lists for security issues and updates.
- Microsoft’s notifications: For example, Microsoft has a Technical Security Notifications center.
- Search with Google: Many security mailing lists can be easily found through searches.

Minimal Software Footprint

- Avoid unnecessary software: Only install software that you need.
- Restrict server features: Turn off or restrict unused features to reduce risk.
- Reduce insecurity: The fewer programs running, the lower the risk of insecure code.

Select Secure Software

- Vendor security track record: Some vendors are more reliable when it comes to security.
- Review security mailing lists:
  - Does the vendor release patches before vulnerabilities are publicly disclosed?
  - Do they release patches quickly?
  - Do they provide clear information about risks?

Homegrown Applications

- Security advantages:
  - Fewer attackers targeting the software.
  - Security through obscurity.
- Security disadvantages:
  - Time and cost investment.
  - Responsible for your own patches.
  - Less likelihood that others will disclose flaws they find.

Seven Major Sources of Physical Loss

- Physical Security: Security measures to deny unauthorized access to physical resources.
- Temperature Extremes: High or low temperatures that can damage equipment or infrastructure.
- Gases: Harmful gases that can cause damage or impact the functioning of systems.
- Liquids: Water or other liquids that can lead to damage, especially to electronic equipment.
- Living Organisms: Threats from viruses, bacteria, animals, insects, and people.
- Projectiles: Physical objects that could be thrown or dropped, potentially causing harm.
- Movement: Events such as shaking, vibrations, or structural collapse.

Energy Anomalies

- Power Failure: Loss of electrical power that can disrupt operations and damage systems.

Access Controls

- Biometrics: Use of personal physical characteristics (fingerprints, iris scans) for access.
- Smart Cards: Cards with embedded chips used for authentication.
- Wireless Enabled Keycards: Wireless cards that provide access to secure areas.

Secure Facility

- Secure Facility: Physical location with engineered controls (e.g., fences, gates) to minimize attacks from physical threats.
- Protection Controls: Includes fences, gates, walls, guards, and alarms for protecting the facility.

Controls for Protecting the Secure Facility

- Walls, Fencing, and Gates: Physical barriers to prevent unauthorized entry.
- Guards: Personnel to monitor and control access to facilities.
- Dogs: Used for detection and physical deterrence.
- ID Cards and Badges: Provides physical access control via identification.
- Locks and Keys: Traditional methods to secure access points.
- Mantraps: A controlled space with an entry and exit point that verifies access.
- Electronic Monitoring: Video surveillance and recording of events.
- Alarms and Alarm Systems: Systems that detect and notify fire, intrusion, or environmental disturbances.

Computer Rooms and Wiring Closets

- Computer Rooms: Require special attention to prevent unauthorized access.
- Wiring Closets: Also need extra physical security to prevent damage or tampering.
- Custodial Staff: Often overlooked, but their unsupervised access to these areas poses a risk.

ID Cards and Badges

- Visible/Concealed: Name badges visible; ID cards often concealed.
- Risks: Can be easily duplicated or stolen.
- Tailgating: When unauthorized people follow authorized individuals into restricted areas.

Locks and Keys

- Types of Locks: Mechanical, electro-mechanical, and biometric.
- Failure of Locks: Facilities should have alternatives for lock failures (fail-safe and fail-secure).
  - Fail-safe Lock: Unlocks during power failure for safety.
  - Fail-secure Lock: Remains locked during power failure for security.

Mantraps

- Two-Step Process: Requires entering a controlled area, verifying identity, and then being allowed entry or denied access.

Electronic Monitoring

- Surveillance: Cameras record areas where physical controls may not be feasible.
- Limitations: Only records events; doesn't actively prevent them.

Alarms and Alarm Systems

- Event Notification: Detects and alerts fire, intrusion, or environmental changes using sensors.
  - Sensors: Include motion detectors, smoke detectors, thermal detectors, and glass break sensors.

Fire Safety

- Fire: The most serious physical threat; strong measures needed to detect and respond to fires.
  - Detection Systems: Manual or automatic detection using thermal, smoke, or flame detectors.
  - Fire Suppression Systems: Devices that extinguish or suppress fires, such as water, carbon dioxide, or gas-based systems.

Fire Suppression Systems

- Portable Extinguishers: Rated by fire types (e.g., water-based or gaseous systems).
- Sprinkler Systems: Traditional water systems or newer water mist systems.
- Gaseous Emission Systems: Alternatives like FM-200 or Inergen, which suppress fires without residue.

Failure of Supporting Utilities

- Impact on Operations: Utilities like HVAC, power, and water are essential for continued operation and security.
- Extreme Conditions: Temperature, humidity, and power fluctuations can introduce vulnerabilities.

Heating, Ventilation, and Air Conditioning (HVAC)

- HVAC Risks: Extreme temperatures and static electricity can damage sensitive systems.
- Optimal Conditions: Temperature between 70-74°F and humidity at 40-60%.

Emergency Shutoff

- Power Management: Immediate shutdown capability in case of human or machine risk.

Water Problems

- Lack of Water: Affects fire suppression and air conditioning systems.
- Excess Water: Can pose a significant threat if undetected.

Structural Collapse

- Risk: Failure of building structures, especially when overloaded, can cause loss of life or injury.
- Inspections: Regular checks by civil engineers help identify potential issues.

Testing Facility Systems

- Documentation and Evaluation: Regular testing identifies security weaknesses and improvement areas.

Interception of Data

- Methods: Direct observation, signal interception, or data transmission.
  - TEMPEST: A countermeasure for signal interception.

Mobile and Portable Systems

- Security: Mobile devices like laptops and handhelds require higher security due to portability.
  - CompuTrace: A hardware-based tracking system for lost devices.
  - PC Card Alarms: Motion detector alarms for portable devices.

Special Considerations for Physical Security Threats

- In-house vs. Outsourcing: Decision between developing security internally or outsourcing to professionals.
- Social Engineering: Manipulating individuals to gain access or information.

Here are the learning outcomes in bullet points with explanations for each:

1. What is an Incident?
   - Explanation: An incident is an adverse event or series of events that can negatively affect a computer system, such as security breaches, system failures, or data loss. Examples include compromises to confidentiality, integrity, and availability of resources, as well as misuse or hoaxes.
2. What is Incident Handling?
   - Explanation: Incident handling involves actions taken to protect and restore the normal operation of computer systems after an adverse event. The goal is to mitigate the damage and restore services as quickly as possible.
3. Incident Response Lifecycle
   - Explanation: The incident response lifecycle consists of six stages:
     a. Preparation – Training and planning for incidents.
     b. Detection and Analysis – Identifying and analyzing the incident.
     c. Containment – Limiting the spread of the incident.
     d. Eradication – Eliminating the root cause of the incident.
     e. Recovery – Restoring normal system operations.
     f. Follow-up – Reviewing the incident to improve future responses.
4. Incident Response Team
   - Explanation: A team of professionals responsible for responding to security incidents. Roles include team leader, lead investigator, analysts, and communicators. They must be skilled and well-coordinated, with clear communication and team morale.
5. Incident Management
   - Explanation: Incident management involves overseeing the entire process of responding to an incident. This includes detection, analysis, containment, eradication, recovery, and learning from the incident. The focus is on minimizing impact and ensuring continuity.
6. Procedure of Incident Management
   - Explanation: Incident management procedures involve communication across departments (e.g., IT, business units, legal, public affairs, human resources), ensuring that the right actions are taken to contain and resolve incidents efficiently.

access-list

Static Route Command

```
Router1(Config)#ip route 20.0.0.0 255.0.0.0 192.168.0.2
Router2(Config)#ip route 10.0.0.0 255.0.0.0 192.168.0.1
```

Default Route Command

```
Router1(Config)#ip route 0.0.0.0 0.0.0.0 192.168.0.2
Router2(Config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1Presentation_ID
```

Standard ACLs (For Deny)

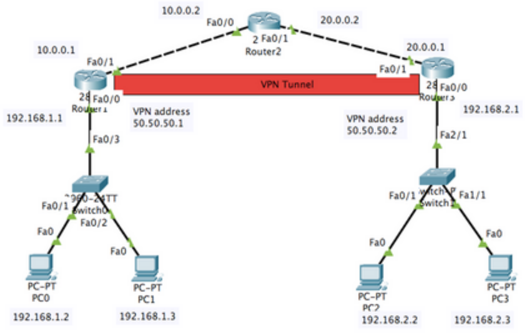
```
Router2( config)# access-list 10 deny host 10.0.0.2
Router2( config)# int fa0/ 1
Router2( config-if)# ip access-group 10 in
Router2( config-if)# exit
```

To permit PC2 10.0.0.3, type the following command in Router 2.

Router2(config)# access-list 10 permit host 10.0.0.3 (or) permit any

Delete ACL in Router2

```
Router2( config)# no access-list 10 deny host 10.0.0.2
```



Step 5: Create VPN tunnel

Router1:

```
Router#config t
Router(config)#interface tunnel 1
Router(config-if)#ip address 50.50.50.1 255.255.255.0
Router0(config-if)#tunnel source fa0/1
Router0(conig-if)#tunnel destination 20.0.0.1
Router0(config-if)#end
```

Router3:

```
Router#config t
Router(config)#interface tunnel 1
Router1(config-if)#ip address 50.50.50.2 255.255.255.0
Router1(config-if)#tunnel source fa0/1
Router1(config-if)#tunnel destination 10.0.0.1
Router1(config-if)#end
```

Step 7: Create routing for PCs to connect over VPN

Router1:

```
 Router(config)#ip route 192.168.2.0    255.255.255.0 50.50.50.2
```

Router3:

```
Router(config)#ip route 192.168.1.0     255.255.255.0 50.50.50.1
```

extented access-list

Static Route Command

```
Router1(Config)#ip route 20.0.0.0 255.0.0.0 192.168.0.2
Router2(Config)#ip route 10.0.0.0 255.0.0.0 192.168.0.1
```

Default Route Command

```
Router1(Config)#ip route 0.0.0.0 0.0.0.0 192.168.0.2
Router2(Config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1
```

Extended ACLs (For Deny)

```
Router2( config)# access-list 100 deny ip host 10.0.0.2 host 20.0.0.2
Router2( config)# int fa0/ 1 (Check again in the interface of your network)
Router2( config-if)# ip access-group 100 in
Router2( config-if)# exit
Router2( config)# exit
```

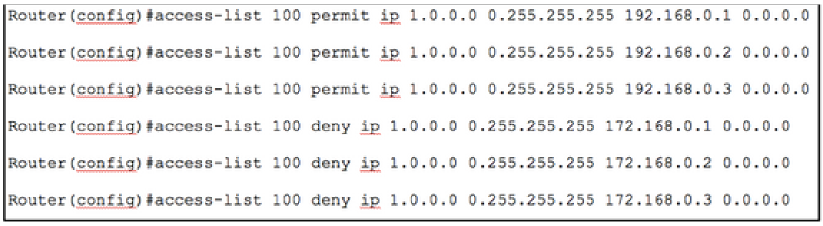
To permit PC2 10.0.0.3, type the following command in Router 2.

Router2(config)# access-list 100 permit ip host 10.0.0.3 host 20.0.0.2 (or) permit ip any any

Extended ACLs (For Permit)

```
Router2( config)# access-list 100 permit ip host 10.0.0.3 host 20.0.0.2
Router2( config)# int fa0/1 (Check again in the interface of your network)
Router2( config-if)# ip access-group 100 in
Router2( config-if)# exit
Router2( config)# exit
```

1. Normally, router has only two interfaces. But in this network, router has three interfaces. To have three interfaces, click the router, click physical, switch off power, drag WIC-1ENET to the right slot as shown in the below picture, and switch on power.



```
Router(config)#access-list 100 permit ip 1.0.0.0 0.255.255.255 192.168.0.1 0.0.0.0
Router(config)#access-list 100 permit ip 1.0.0.0 0.255.255.255 192.168.0.2 0.0.0.0
Router(config)#access-list 100 permit ip 1.0.0.0 0.255.255.255 192.168.0.3 0.0.0.0
Router(config)#access-list 100 deny ip 1.0.0.0 0.255.255.255 172.168.0.1 0.0.0.0
Router(config)#access-list 100 deny ip 1.0.0.0 0.255.255.255 172.168.0.2 0.0.0.0
Router(config)#access-list 100 deny ip 1.0.0.0 0.255.255.255 172.168.0.3 0.0.0.0
```