**BCY233T04 ETHICAL HACKING**

**Common for B.Sc. (CS) / BCA/B.Sc. (Data Science)/B.Sc. (Cyber security)**

**COURSE OBJECTIVES**

· To know the theory and practices of finding the vulnerabilities.

· To find the different attacks and then defining the appropriate security policy.

· To take action to detect or prevent the attacks and thus reduce the damages.

· To understand the concept of Web Server Hacking.

· To understand the concept of Firewalls

**COURSE OUTCOMES:**

· To describe the basics of the ethical hacking.

· Ability to learn technical foundations of hacking.

· Able to perform the foot printing and scanning.

· Demonstrate the techniques for system hacking.

· Characterize the malware and their attacks.

**SYLLABUS**

**UNIT – I INTRODUCTION TO ETHICAL HACKING**

Security Fundamental - Security Testing - Hacker and Cracker – Descriptions - Test Planskeeping it legal - Ethical and Legality- Process - The Ethical Hacker’s Process.

**UNIT – II FOOTPRINTING AND SCANNING**

Information Gathering - Determining the Network Range - Finding Open Ports and Access Points - OS Fingerprinting Services - Mapping the Network Attack Surface.

**UNIT – III MALWARE THREATS AND SESSION HIJACKING**

Viruses and Worms- Trojans - Covert Communication - Keystroke Logging and Spyware – Malware Counter Measures- Sniffers - Session Hijacking - Denial of Service.

**UNIT – IV WEB SERVER HACKING AND ATTACKS**

Web Server Hacking - Web Application Hacking - Database Hacking – Wireless Technologies – Mobile Security and Attacks: Wireless Technologies – Wireless LANs.

**UNIT – V CASE STUDY**

Intrusion Detection Systems - Firewalls - Honeypots - Physical Security - Social Engineering – Case Studies: Intrusion detection Real Secure Tripwire Dragon Snort.

**TEXT BOOKS:**

1. Michael Gregg, “Certified Ethical Hacker”, Pearson IT Certification, 3rd Edition, 2019.

2. Roger Grimes, “Hacking the Hacker”, Wiley, 1st Edition, 2017

**REFERENCES:**

1. Ankit Fadia, “The Unofficial Guide to Ethical Hacking”, Laxmi Publications, 2nd Edition, 2006.

2. Randy Weaver, Dawn Weaver, Dean Farwood, “Guide to Network Defense and Countermeasures”, Cengage Learning, Third edition, 2014

**Notes**

**UNIT – I INTRODUCTION TO ETHICAL HACKING**

Security Fundamental - Security Testing - Hacker and Cracker – Descriptions - Test Planskeeping it legal - Ethical and Legality- Process - The Ethical Hacker’s Process.

No organization can ever be 100 percent secure. There will always be some risk left over, known as residual risk,

**Ethical hacking**, also known as **penetration testing** or **white-hat hacking**, is the practice of intentionally probing computer systems, networks, or applications for security vulnerabilities (weak or flaw in system) by CEH — but with permission and for a good purpose, to find and fix weaknesses before malicious hackers (black-hats) can exploit them.

**Common tasks of Ethical Hacker:**

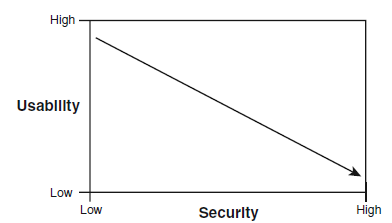
* Scanning for open ports or vulnerabilities
* Testing password strength
* Bypassing authentication mechanisms
* Exploiting vulnerabilities (safely) to demonstrate risks
* Reporting findings with recommendations

**Security Fundamentals:**

One way to secure a system from network attack is to unplug it ☺ and make it a standalone system. Although this system would be relatively secure from Internet-based attackers, its usability would be substantially reduced.

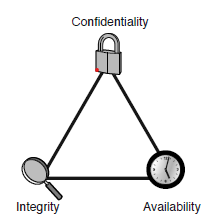
The opposite approach of plugging it in directly to the Internet without any firewall, antivirus, or security patches would make it extremely vulnerable, yet highly accessible.

So, the job of security professionals is to find a balance somewhere between security and usability.



Security triad of confidentiality, integrity, and availability (CIA) form the basic building blocks of any good security initiative.

* Confidentiality – lakhs of pwd breaches in Yahoo, Dropbox, etc
* Integrity – accuracy of same data across departments, Correctness doesn’t mean that the data is accurate, just that it hasn’t been modified in storage or transit. Integrity in electronic documents and data is much more difficult to protect than in paper ones. Electronic storage can be tightened with Cryptographic, Access control. In transit, same can be controlled with protocols.
* Availability: a legitimate user needs the information, it should be available. If no recent backups are done, there is not point to restore. Backups, SLA, Redundant Array of Inexpensive Disks(RAID), Redundant storage (Hot, Warm, Cold) can control this during Disaster management scenarios for Business Continuity (BCP)



**Risk, Assets, Threats, and Vulnerabilities:**

* Risk is the probability or likelihood of the occurrence or realization of a threat. U.S. federal government has adopted a six step risk management framework (RMF).
* An asset is any item of economic value owned by an individual or corporation like routers, servers, formula, trade secret, xls, processing time, etc.,
* A threat is an event that sets the stage for risk and is any agent, condition, or circumstance that could potentially cause harm, loss, or damage, or compromise an IT asset or data asset and can result in
  + Destruction (Natural disaster)
  + Disclosure (by hackers - An insider or outsider who is unauthorized and purposely attacks an organization’s components,
  + Cyber-attack to systems,
  + Viruses and Malware tool that do data modification, corruption of data
  + Denial of service (DoS) or Distributed DoS: To bring the network or access to a particular

TCP/IP host/server to its knees by flooding it with useless traffic.

* vulnerability is a weakness in the system design, implementation, software, or code, or the lack of a mechanism in OS, Applications, Config Files, Shrinkwrap software (ready-made, off-the-shelf software for huge common audience without custom fixes/features for specific customer. Ex: MS Office, Windows, etc)

**Backups:**

* Full: Takes longer time without excluding any files
* Differential back up: After a full back up, this is periodically done only with modified/created files, restoration done with last full and differential backup
* Incremental back up: After a full back up, this is daily done. Slow in restoration due to large number of incremental backups.

**Exploits:** An *exploit* refers to a piece of software, a tool, a technique, or a process that takes advantage of a vulnerability that leads to access, privilege escalation, loss of integrity, or denial of service on a computer system.

**zero-day exploit:** Sometimes you may not even know the vulnerability exists, and that is known as zero-day exploit.

**Risk Assessment:** is a process to identify potential security hazards and evaluate what would happen if a hazard or unwanted event were to occur.

Approaches to risk assessment:

* Qualitative risk assessment: methods use scenarios to drive a prioritized list of critical concerns and do

not focus on dollar amounts. Example impacts might be identified as critical, high,

medium, or low.

* Quantitative risk assessment: assigns a monetary value to the asset.

**Step 1. Determine the single loss expectancy (SLE):** involves determining the single amount of loss you could incur on an asset if a threat becomes realized or the amount of loss you expect to incur if the asset is

exposed to the threat one time.

Step 2. **Evaluate the annual rate of occurrence (ARO):** The purpose of evaluating the ARO is to determine how often an unwanted event is likely to occur on an annualized basis.

Step 3. **Calculate the annual loss expectancy (ALE):** This final step of the quantitative assessment seeks to combine the potential loss and rate per year to determine the magnitude of the risk. This is expressed as annual

loss expectancy (ALE)

**Security testing** is the primary job of ethical hackers. These tests might be configured in such way that the ethical hackers have no knowledge, full knowledge, or partial knowledge of the target of evaluation (TOE).

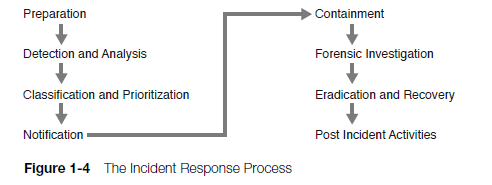
* No-Knowledge Tests (Black Box)
* Full-Knowledge Testing (White Box): tester has full knowledge of the network, systems, and infrastructure.
* Partial-Knowledge Testing (Gray Box)
* Names of Security Tests:
  + Vulnerability testing
  + Network evaluations
  + Red-team exercises
  + Penetration testing
  + Host vulnerability assessment
  + Vulnerability assessment
  + Ethical hacking

Types of Security Tests:

* + **High-level assessment/audit:** Also called a level I assessment, it is a top down look at the organization’s policies, procedures, and guidelines. The purpose of a top-down assessment is to answer three questions:
    - * Do the applicable policies, procedures, and guidelines exist?
      * Are they being followed?
      * Is their content sufficient to guard against potential risk?
  + **Network evaluation:** Also called a level II assessment, it has all the elements specified in a level I assessment, and it includes hands-on activities like scanning, firewall, etc.,
  + **Penetration test:** Unlike assessments and evaluations, penetration tests are adversarial in nature. Penetration tests are also referred to as level III assessments. These events usually take on an adversarial role and look to see what the outsider can access and control. Penetration tests are less concerned with policies and procedures and are more focused on finding low-hanging fruit and seeing what a hacker can accomplish on this network.

Penetration tests are sometimes performed in a double-blind environment. This means that the internal security team has not been informed of the penetration test.

Penetration tests are not effective if an organization does not have the policies and procedures in place to control security. The EC-Council (International Council of E-Commerce Consultants) approach to incident response follows the steps shown below:



SysAdmin, Audit, Network, and Security (SANS), is a widely recognized and respected organization in the cybersecurity field. SANS templates can be used in building security policies.

**Hackers & Crackers**: A hacker is a person who enjoyed understanding the internal workings of a system, computer, and computer network.

Cracker describes individuals who seek to compromise the security of a system without permission from an authorized party.

An ethical hacker is an individual who performs security tests and other vulnerability-assessment activities to help organizations secure their infrastructures.

■ **White hat hackers:** These individuals perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same manner as a criminal hacker to better understand its

vulnerabilities.

■ **Black hat hackers:** These individuals perform illegal activities.

■ **Gray hat hackers:** These individuals usually follow the law but sometimes venture over to the darker side of black hat hacking. It would be unethical to employ these individuals to perform security duties for your organization

because you are never quite clear where they stand. While wanting to use the force of good, he is also drawn to the dark side.

■ **Suicide hackers:** These are individuals that may carry out an attack even if they know there is a high chance that they will get caught and serve a long prison term.

**Hackers methodology:** that includes the following steps:

1. **Reconnaissance and foot printing:** Foot printing focuses on gathering publicly available information to create a profile of the target, like known direct agent, while reconnaissance extends this to active probing and vulnerability identification like spy.

2. **Scanning and enumeration:** Can include the use of port scanning tools and network mappers.

3. **Gaining access:** The entry point into the network, application, or system.

4. **Maintaining access:** Techniques used to maintain control, such as escalation of privilege.

5. **Covering tracks:** Planting rootkits (process of installing malicious software designed to provide unauthorized, persistent access to a computer system while hiding its presence from the user and security software), backdoors, and clearing logs are activities normally performed at this step.

| **Feature** | **Rootkit** | **Backdoor** |
| --- | --- | --- |
| **Purpose** | Stealth and persistence | Unauthorized access |
| **Visibility** | Designed to be hidden | May or may not be hidden |
| **Level of access** | Kernel/user/firmware level | Application/network/system level |
| **Example usage** | Hiding malware, processes, files | Re-entering a system after compromise |
| **Used together?** | Yes, often used together for stealth | Yes, rootkit may hide a backdoor |

**Attackers:**

■ **Phreakers:** The original hackers. These individuals hacked telecommunication and to explore the capabilities and make free phone calls. Their activities include physical theft, stolen calling cards, access to telecommunication

services, reprogramming of telecommunications equipment, and compromising user IDs and passwords to gain unauthorized use of facilities, such as phone systems and voicemail.

■ **Script kiddies:** Younger attackers who use widely available freeware vulnerability-assessment tools and hacking tools without much tech knowledge.

■ **Disgruntled employees:** Employees who have lost respect and integrity for the employer.

■ **Software crackers/hackers:** Individuals who have skills in reverse engineering software programs and, in particular, licensing registration keys used by software vendors

■ **Cyberterrorists/cybercriminals: I**ndividuals or groups of individuals who are usually funded to conduct clandestine or espionage activities on governments, corporations, and individuals in an unlawful manner.

■ **System crackers/hackers:** Elite (skilled) hackers who have specific expertise in attacking vulnerabilities of systems and networks by targeting operating systems. Due to the loss/impact of global impact, these individuals get the most attention and media coverage.

**Skills of an Ethical Hacker**:

**- Routers:** Knowledge of routers, routing protocols, and access control lists (ACLs - User, group, or system being granted/denied for an object). Certifications such as Cisco Certified Network Associate (CCNA) and Cisco Certified Internetworking Expert (CCIE) can be helpful.

- **MS**: Microsoft Certified Solutions Associate (MCSA) or Microsoft Certified Solutions Expert (MCSE)

- **Linux**

**- Firewalls**: Knowledge of firewall configuration and the operation of intrusion detection systems (IDS) and intrusion prevention systems (IPS)

- **Programming**

**- Mainframes**

**- Network Protocols**

**- Project management**

**Modes of Ethical Hacking:**

■ **Information gathering:**

■ **External penetration testing:**

■ **Internal penetration testing:**

■ **Network gear testing**: Firewall, IDS, router (across networks), and switches (within network).

■ **DoS testing:**

■ **Wireless network testing:**

■ **Application testing:**

■ **Social engineering:**

| **Type** | **Description** |
| --- | --- |
| **Phishing** | Deceptive emails or messages trick users into clicking malicious links or revealing info (e.g., login credentials). |
| **Spear Phishing** | Targeted phishing aimed at a specific individual or organization, often using personal info. |
| **Vishing** | Voice phishing — attackers call pretending to be a trusted figure (e.g., bank, IT support). |
| **Smishing** | SMS-based phishing messages with malicious links. |
| **Pretexting** | Attacker creates a fake scenario to trick the victim (e.g., pretending to be HR needing sensitive data). |
| **Baiting** | Tempting users with a reward (e.g., free movie download, USB stick with malware). |
| **Tailgating** | Physically following someone into a secure area by exploiting social norms (e.g., holding the door open). |
| **Quid pro quo** | Offering something in return for information (e.g., fake tech support offering help). |

■ **Physical security testing:**

■ **Authentication system testing:**

■ **Database testing:**

■ **Communication system testing:**

■ **Stolen equipment attack:**

**Rules for EH:**

■ **Never exceed the limits of your authorization:**

■ **Protect yourself by setting up damage limitations with NDA:**

■ **Be ethical:**

■ **Maintain confidentiality:**

■ **Do no harm:**

■ **Due diligence (carefulness):**

**Compliance with state, federal, regulatory, or other law or mandate:**

US: Finance Confidentiality - Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and Health Insurance

Portability and Accountability Act (HIPAA)

ISO/IEC 27002: This information security standard was first published in December 2000 by the International Organization for Standardization and the International Electrotechnical Commission. This code of practice for information security management is considered a security standard benchmark and includes the following 14 main elements:

■ Information Security Policies

■ Organization of Information Security

■ Human Resource Security

■ Asset Management

■ Access Control

■ Cryptography

■ Physical and environmental security

■ Operation security

■ Communication security

■ System acquisition, development, and maintenance

■ Supplier relationships

■ Information security incident management

■ Information security aspects of business continuity management

■ Compliance

**Basic questions to help establish the goals and objectives** of the tests, including the following:

*Never* perform tests without written approval.

■ What is the organization’s mission?

■ What specific outcomes does the organization expect?

■ What is the budget?

■ When will tests be performed: during work hours, after hours, on weekends?

■ How much time will the organization commit to completing the security evaluation?

■ Will insiders be notified?

■ Will customers be notified?

■ How far will the test proceed? Root the box, gain a prompt, or attempt to retrieve another prize, such as the CEO’s password?

■ Whom do you contact should something go wrong?

■ What are the deliverables?

■ What outcome is management seeking from these tests?

**EH Report to include below with appropriate data classification like private & confidential, etc., :**

■ Introduction

■ Statement of work performed

■ Results and conclusions

■ Recommendations

**EH to be up to date:**

■ **National Vulnerability Database:** http://nvd.nist.gov/

■ **Security Tracker:** http://securitytracker.com/

■ **HackerWatch:** http://www.hackerwatch.org/

■ **Dark Reading:** http://www.darkreading.com/

■ **Exploit Database:** http://www.exploit-db.com/

■ **HackerStorm:** http://hackerstorm.co.uk/

■ **SANS Reading Room:** http://www.sans.org/reading\_room/

■ **SecurityFocus:** http://www.securityfocus.com/

Some examples of IT organizations that have codes of ethics include

■ **EC-Council:** https://www.eccouncil.org/code-of-ethics

■ **(ISC)2:** https://www.isc2.org/ethics/default.aspx

■ **ISACA:** http://www.isaca.org/Certification/Code-of-Professional-Ethics/Pages/default.aspx

**Overview of U.S. Federal Laws**

■ Section 1029, Fraud and related activity with access devices:

■ Section 1030, Fraud and related activity in connection with computers:

■ Electronic Communication Privacy Act:

■ Computer Fraud and Abuse Act of 1984:

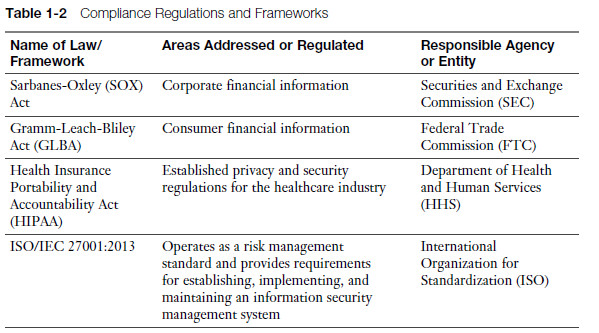
■ The Cyber Security Enhancement Act of 2002:

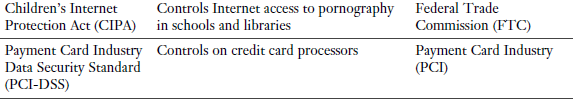
■ The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001:

■ The Federal Information Security Management Act (FISMA):

■ Federal Sentencing Guidelines of 1991:

■ Economic Espionage Act of 1996:

****

****

**Payment Card Industry Data Security Standard (PCI-DSS)**

The requirements follow security best practices and are aligned across six goals:

■ Build and maintain a secure network that is PCI compliant

■ Protect cardholder data

■ Maintain a vulnerability management program

■ Implement strong access control measures

■ Regularly monitor and test networks

■ Maintain an information security policy

**UNIT – II FOOTPRINTING AND SCANNING**

Information Gathering - Determining the Network Range - Finding Open Ports and Access

Points - OS Fingerprinting Services - Mapping the Network Attack Surface.

The hacking methodology contains the following progressive steps:

1. Information Gathering

2. Penetration (drilling, insights, intelligence)

3. Optional: Guaranteeing Future Easier Access

4. Internal Reconnaissance(preliminary survey, exploration, investigation on other available resources/ways once entered)

5. Optional: Movement

6. Intended Action Execution

7. Optional: Covering Tracks

**Information Gathering:**

- Hackers usually have a destination target in mind, accessible IP addresses, email addresses, and domain names, OS with version names, IIS or Apache web server like application server, mail server, db server versions, patches, weak configuration files, employee names for social engineering, what mergers or divestitures are happening.

- good hacker starts to gather all the software and services hosted on each of target/partner sites, a process generally known as **fingerprinting/footprinting**

**Penetration**: Success of this step makes or breaks the entire cycle. If by chance all the software and devices are perfectly secured, then you can attack the human element. Here are the different techniques a hacker can use to break into a target:

■■ Zero-days: an undiscovered flaw in an application or operating system, a gap in security for which there is no defense or patch.

■■ Unpatched software: Most vendors do a fairly good job of patching their software in a timely manner, especially after a vulnerability becomes publicly known. Unfortunately, customers are notoriously slow in applying those patches.

■■ Malware: Malicious programs like viruses, Trojan horse programs, and worms. When a new exploit method is discovered, defenders know that malware writers will use automated malware to spread the exploit faster in a process known as “weaponization.”

| **Feature** | **Virus** | **Trojan Horse** | **Worm** |
| --- | --- | --- | --- |
| Requires human action | Yes (attached to files) | Yes (user clicks on some offer links, etc) | No |
| Self-replicates | Sometimes | No | Yes |
| Hidden/Disguised | No | Yes | No |
| Main threat | Data corruption | Data theft/backdoor | Network disruption |

■■ Social engineering: It can be an email that tricks an end-user into clicking on a malicious web link or running a rogue file attachment, can be accomplished many ways, including over a computer, using a phone call, in-person, or using traditional postal mail. A common social engineering target is to capture a user’s logon credentials, called phishing. The most common phishing ploy (plan) is to send an email purporting (appear to be true) to be from a web site administrator claiming that the user’s password must be verified or else their access to the site will be cut off.

■■ Password issues

■■ Eavesdropping/MitM: Eavesdropping and “man-in-the-middle” (MitM) attacks compromise a legitimate network connection to gain access to or Hacker maliciously participate in the communications.

■■ Data leaks: data classifications

■■ Misconfiguration

■■ Denial of service: with overloaded requests to a server. The attacker uses a **network of infected computers** (called a **botnet**) to send an overwhelming number of requests to the target. These requests can **crash** the target system or make it **unable to respond to legitimate users**.

■■ Insider/partner/consultant/vendor/third party

■■ User error

■■ Physical access

■■ Privilege escalation

**UNIT – III MALWARE THREATS AND SESSION HIJACKING**

Viruses and Worms- Trojans - Covert Communication - Keystroke Logging and Spyware –

Malware Counter Measures- Sniffers - Session Hijacking - Denial of Service.

**DDoS Types:**

**Direct Do**S: A direct DOS attack is one in which all the maliciously created traffic is being generated by the single host sending it. The attacker may (randomly) change the originating IP address in an attempt to hide, but in direct attacks, there is only one sender crafting the traffic that then heads directly to the target without any intermediate hosts used.

**Reflection** attacks are when the attack uses one or more intermediate hosts to generate DDoS attacks. Most of the time there are thousands of DDoS “bot” malware programs waiting for commands from originating “Command-and-Control(C&C) Server to be instructed to attack a particular host.

**Amplified** DDoS attacks use “noisy” protocols, which respond with more than one packet when receiving a single packet (thus the amplification), against the intended targets

DoS/DDoS attacks can be accomplished along **every layer of the OSI model** (Physical, Data-Link, Network, Session, Transport, Presentation, and Application).

**Escalating** Attacks: The attacker often uses the application layer, faking traffic that initially looks like legitimate customers, Then they switch attack layers, moving up through the OSI model, and add even more traffic.

**Upstream and Downsteam Attacks**

**UNIT – IV WEB SERVER HACKING AND ATTACKS**

Web Server Hacking - Web Application Hacking - Database Hacking - Wireless

Technologies – Mobile Security and Attacks: Wireless Technologies – Wireless LANs.

Eavesdropping is unauthorized viewing and/or recording of an otherwise intended private conversation.

**Wireless Hacking:** even though the wired world is faster and more secure, It is a wireless world—a world that hackers are constantly attacking. It’s a rarity that anyone plugs in a network cable to their desktop or laptop computer, cell phones and other computing devices.

“wireless” encompasses a huge swath of the electromagnetic spectrum, which includes X-rays, light, radio, and other forms of wireless energy like magnetism, light, satellite, terrestrial radio, Bluetooth, Near Field Communications (NFC), RFID, and microwave.

**Types:**  Hackers can directly attack the **Access Points (**AP) to compromise the wireless communications. They can crack the AP’s admin password, change its operations, conduct eavesdropping, or trick the victim into connecting to a rogue AP.

**DoS** with Jamming/flooding

**Try until you succeed:** Rarely APs lock out devices after a set number of incorrect guesses.

**Session Hijacking:** Using logged in credentials (when they forgot to logout, stored pwd in browser, etc in an internet cafe) and mimic you to steal data like cookies, credit card, PII, etc., .

| **Method** | **Description** |
| --- | --- |
| **Session Sniffing** | Capturing session IDs from unencrypted traffic (e.g. public Wi-Fi without HTTPS) |
| **Cross-Site Scripting (XSS)** | Injecting malicious scripts to steal session cookies |
| **Man-in-the-Middle (MitM)** | Intercepting traffic between user and server to grab session info |
| **Session Fixation** | Forcing a user to use a session ID the attacker already knows |
| **Brute Force / Guessing** | Trying different session IDs until one works (possible if IDs are weak) |

**Protection:**

**Frequency Hopping** (short for **Frequency Hopping Spread Spectrum**, or **FHSS**) is a wireless communication technique where the signal **rapidly switches** between different frequencies within a certain range, according to a specific pattern.

only allow predefined clients to connect with IP/MAC addresses, certificates.

**Strong Protocols:**

**WiFi Protected Access (WPA)** Features:

* Stronger encryption (SAE = Simultaneous Authentication of Equals)
* Individualized encryption for each session
* Forward secrecy (past data remains secure even if password is compromised)
* Resists brute-force attacks

| **Protocol** | **Year Introduced** | **Encryption Type** | **Security Strength** | **Still Secure in 2025?** |
| --- | --- | --- | --- | --- |
| **WPA3** | 2018 | SAE, 192-bit | ⭐⭐⭐⭐⭐ Strongest | ✅ Yes (Recommended) |
| **WPA2** | 2004 | AES | ⭐⭐⭐⭐ Strong | ⚠️ Yes (if AES is used) |
| **WEP** | 1997 | RC4 | ❌ Weak | ❌ No (Obsolete) |

**Domain Isolation** means creating a secure border between authorized and unauthorized network traffic. This can be accomplished using a variety of tools and methods, including firewalls (both network-based and host-based), virtual private network connections, IPSEC, routers, software-defined networks, and other types of switching fabrics.

**Virtual Private Networks (VPN)**

**IoT hacking:** by mimic the flow, manual intervention, etc.,

**UNIT – V CASE STUDY**

Intrusion Detection Systems - Firewalls - Honeypots - Physical Security - Social Engineering

– Case Studies: Intrusion detection Real Secure Tripwire Dragon Snort.

Intrusion detection/prevention (IDS/IPS) is the art of detecting unauthorized activity. Intrusion detection is part of an event-logging system. Most attackers (70% to 80%) are in the system for long periods of time (months) before discovering a flaw, then initial compromise in minutes or a day.

The end result is that most security event logs are very “noisy,” meaning full of more useless information than useful. Good computer security event message should have these traits:

■■ Low noise

■■ indicates true maliciousness

■■ Readily understood description of event

■■ As much surrounding detail as can be captured and useful to investigators

■■ Generation of the event always triggers an incident response investigation

Advanced persistent threats (APTs) attacks are conducted by professional, criminal groups and have been responsible for compromising a large majority of businesses, military systems, and other entities over the last decade.

■ They intend to remain permanently engaged after the initial compromise.

■■ They do not “run” when discovered.

■ They have dozens to hundreds of compromises and exploits they can use, including zero-days.

■■ They always get total ownership of the environment.

■■ Their objective is often stealing the victim's intellectual property (IP) over the long-term.

■■ Their origination is often a “safe harbor” country that will never prosecute them for their activities. (Indeed, they are often state-sponsored and celebrated.)

types of intrusion detection: behavior-based: Ex: a file trying to copy itself into another file, a program trying to perfidiously (violation of a promise or loyalty) redirect a browser away from its user-intended URL, an unexpected connection to a honeypot (network set up to mimic real systems that attackers might target. ), or a person copying all the contents of an authentication database. Flags activity that **deviates** from this normal behavior as **potentially malicious**. Can detect unknown attacks. Higher chance of **false positives** and Needs a **learning period.**

Signature based Intrusion detection:

| **Feature** | **Signature-Based IDS** | **Behavioral-Based IDS** |
| --- | --- | --- |
| Detection method | Matches known attack patterns | Detects deviations from normal |
| Detects known threats | ✅ Yes | ✅ Yes |
| Detects unknown threats | ❌ No | ✅ Yes |
| False positives | 🔽 Low | 🔼 High |
| Maintenance | Requires regular updates | Requires learning and tuning |
| Speed | Fast (pattern matching) | Slower (analysis-based) |

IDS/IPS is further classified as being a host-based IDS/IPS (HIDS/HIPS) or a network-based IDS/IPS (NIDS/NIPS), depending on whether the defense protects an individual host system or analyzes packets running across the network for maliciousness.

A firewall (the packet filter) is a software or hardware component designed to prevent unauthorized access between two or more security boundaries. Accomplished by a protocol name or port number and usually at the network level using packet filtering. Many firewalls can also allow or deny traffic based on user names, device names, group membership, and information found in the upper levels of the application traffic and high-level packet analysis, intrusion detection/prevention, malware detection, and VPN services.

Firewall can be kept at network level or host itself.

A “honeypot” is any system set up for the expressed purpose of being a “fake” system to detect unauthorized activity. A honeypot can be a computer system, a device, a network router, a wireless access point, a printer—anything the honeypot administrator wishes to deploy. A “honeynet” is a collection of honeypots. A honeypot can be created by deploying a real but otherwise unused system or by deploying specialized honeypot software that emulates systems.

A “low-interaction” honeypot only mimics very simplistic port connections and logs them. A “medium interaction” honeypot allows the user to log on and tries to offer up a moderate but realistic experience. “High-interaction” honeypots mimic a real production system to the point that a hacker interacting with it should not be able to tell the difference between it and a real production asset.

| **Feature** | **Authentication** | **Authorization** |
| --- | --- | --- |
| Purpose | Verify identity | Determine access rights |
| Happens when? | Before authorization | After successful authentication |
| Based on | Credentials (e.g., password, ID) | Policies, roles, or access control |
| Determines what? | Who the user is | What the user is allowed to do |
| Example | Logging in to Gmail | Viewing only your own emails |

A **password** can be any acceptable set of characters that the authentication system accepts.

**Hashed Passwords:** passwords get converted into a cryptographic hash. The hash can be used in the authentication sequence itself or simply stored for later authentication purposes. Common password hashes on Windows systems are LANManager (LM), NTLANManager (NT), and PBKDF2 for local password cache storage. Linux systems often use MD5, Blowfish, SHA-256, or SHA-512. The best hashes create and use a random value (called the “salt”) during the creation and storage of the password hash. This makes it harder for a hacker obtaining the password hash to convert it back to its plaintext original value.

**Authentication Factors** Because passwords can easily be stolen (and sometimes guessed), authentication systems are increasingly asking for additional “factors” for a subject to prove ownership of a logon label. There are three basic types of factors: something you know (such as a password, PIN, passphrase, or screen pattern), something you have (such as a security token, cell phone, or smart card), or something you are (such as a biometric identity, like a finger print, retina print, or hand geometry).

1. Use Long Passwords

2. Avoid Common Passwords (123456, password, qwerty, Your name, birthdate, or pet’s name)

3. Use a Password Manager: Tools like Bitwarden, 1Password, or KeePass create and store strong passwords for you.

4. Enable Two-Factor Authentication (2FA)

5. Don't Reuse Passwords/between applications

6. Use Passphrases (Combine random words: Example: CorrectHorseBatteryStaple!)

7. Avoid Typing Passwords on Public Devices

8. Update Passwords if Compromised

9. Don’t Save Passwords in Browsers

10. Be Wary of Phishing Attacks(Never enter your password on suspicious links or pop-ups.)