SYLLABUS OF CERTIFICATE COURSE (Attachment-2)

Course Title:	**INFORMATION PROTECTION USING CYBER SECURITY(Level-2)**	
Course Credits:	2	
Course Hours:	30 (10 Hours Theory + 20 Hours Practical)	
Course Duration:	15 Days	
Eligibility:	**INFORMATION PROTECTION USING CYBER SECURITY (Level-1)**	
Course Objective:	To provide advanced level knowledge to the students about cyber security and to protect electronic devices' information from cyber attack	
Expected Outcome:	The students will be able to safeguard computer system and Network using cyber security tools.	
Method of Instruction:	Class work/lectures, group discussion, seminar, case study, self-study, practical.	
Evaluation Method:	Multiple Choice Question (MCQ)/Theory/PracticalExam., Assignments. *Students who scored passing marks will get certificate.*	
	COURSE CONTENT	
		Teaching Hours
Unit-1:	**Law & Security**	**02 Th.**
	1.6 Cyber Law (Offence and Fine/Penalty/Punishment)	2 Th.
	1.7 Security standards, regulations and frameworks	
Unit-2:	**Advanced Network Security**	**03 Th. 05 Pr.**
	2.1 Digital Forensics	2 Th.
	2.2 IP Security	
	2.3 VPN	
	2.4 Intrusion Detection	1 Th.
	2.5 Practical Case study based on Unit-2	5Pr.
Unit-3:	**Web SecurityProtocols**	**03 Th. 05 Pr.**
	3.1 Web Security methods	2 Th.
	3.2 SSL	
	3.3 TLS	1 Th.
	3.4 HTTPS	
	3.5 Practical Case study based on Unit-3	5 Pr.

Unit-4:	**Web Application Tools**	**02 Th. 10 Pr.**
	4.1 Scanning for web vulnerabilities tools: Nikto, W3af etc.	2 Th.
	4.2 HTTP utilities - Curl, OpenSSL, Stunnel etc.	
	4.3 Application Inspection tools – Zed Attack Proxy, Sqlmap, DVWA, Webgoat etc.	
	4.4 Password Cracking and Brute-Force Tools: John the Ripper, L0htcrack, Pwdump, HTC-Hydra etc.	
	4.5 Practical Case study based on Unit-4	10 Pr.
	Total Hours (10 Th. + 20 Pr.)	**30**
Reference Books:	1) James Graham, Richard Howard and Ryan Olson, CYBER SECURITY ESSENTIALS, CRC Press	
	2) Cryptography & Network Security, William Stalling, PHI.	
	3) Web Application Security (Exploitation and Countermeasures for Modern Web Applications), Andrew Hoffman, O'Reilly.	
	4) Network Security Tools, Nitesh Dhanjani & Justin Clarke, O'Reilly.	
	5) Web Application Security, A Beginner's Guide, Bryan Sullivan, Vincent Liu, McGraw Hill LLC	

Suggested Practical Problems:

1) Practical ondigital forensic.
2) Practical on IP security, protection of VPN and detection of intrusions.
3) Practical onvarious methods of web security protocols such as SSL, TLS and HTTPS.
4) Practical using various web application tools as given in the unit- 4.

UNIT-1

Law & Security

1.6 Cyber Law (Offence and Fine/Penalty/Punishment)

Cyber Law also called IT Law is the law regarding Information-technology including computers and the internet. It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

IT law does not consist of a separate area of law rather it encloses aspects of contract, intellectual property, privacy, and data protection laws. Intellectual property is a key element of IT law. The area of software license is controversial and still evolving in Europe and elsewhere.

According to the Ministry of Electronics and Information Technology, Government of India :

Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.

Importance of Cyber Law:

1. It covers all transactions over the internet.
2. It keeps an eye on all activities over the internet.
3. It touches every action and every reaction in cyberspace.

Area of Cyber Law:

Cyber laws contain different types of purposes. Some laws create rules for how individuals and companies may use computers and the internet while some laws protect people from becoming the victims of crime through unscrupulous activities on the internet. The major areas of cyber law include:

Fraud:

Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim. Cyber lawyers work to both defend and prosecute against allegations of fraud using the internet.

Copyright:

The internet has made copyright violations easier. In the early days of online communication, copyright violations were too easy. Both companies and individuals need

lawyers to bring an action to impose copyright protections. Copyright violation is an area of cyber law that protects the rights of individuals and companies to profit from their creative works.

Defamation:

Several personnel use the internet to speak their mind. When people use the internet to say things that are not true, it can cross the line into defamation. Defamation laws are civil laws that save individuals from fake public statements that can harm a business or someone's reputation. When people use the internet to make statements that violate civil laws, that is called Defamation law.

Harassment and Stalking:

Sometimes online statements can violate criminal laws that forbid harassment and stalking. When a person makes threatening statements again and again about someone else online, there is a violation of both civil and criminal laws. Cyber lawyers both prosecute and defend people when stalking occurs using the internet and other forms of electronic communication.

Freedom of Speech:

Freedom of speech is an important area of cyber law. Even though cyber laws forbid certain behaviors online, freedom of speech laws also allow people to speak their minds. Cyber lawyers must advise their clients on the limits of free speech including laws that prohibit obscenity. Cyber lawyers may also defend their clients when there is a debate about whether their actions consist of permissible free speech.

Trade Secrets:

Companies doing business online often depend on cyber laws to protect their trade secrets. For example, Google and other online search engines spend lots of time developing the algorithms that produce search results. They also spend a great deal of time developing other features like maps, intelligent assistance, and flight search services to name a few. Cyber laws help these companies to take legal action as necessary to protect their trade secrets.

Contracts and Employment Law:

Every time you click a button that says you agree to the terms and conditions of using a website, you have used cyber law. There are terms and conditions for every website that are somehow related to privacy concerns.

Advantages of Cyber Law:

Organizations are now able to carry out e-commerce using the legal infrastructure provided by the Act.

Digital signatures have been given legal validity and sanction in the Act.

It has opened the doors for the entry of corporate companies for issuing Digital Signatures Certificates in the business of being Certifying Authorities.

It allows the Government to issue notifications on the web thus heralding e-governance.

It gives authority to the companies or organizations to file any form, application, or any other document with any office, authority, body, or agency owned or controlled by the suitable Government in e-form using such e-form as may be prescribed by the suitable Government.

The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions.

Cyber Law provides both hardware and software security.

Penalty and Compensation under the Information Technology Act, 2000

Section 43 - Penalty and compensation for damage to computer, computer system etc.

if any person introduces any computer contaminant or computer virus to a computer resources without the owner's permission will be liable to pay damages by way of compensation to the person so affected.

Section 43A – Compensation for failure to protect data –

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Section 44 – Penalty for failure to furnish information return, etc.-

If any person who is required under this Act or any rules or regulations made there under to –

(a) Furnish any document, return or report to the Controller or the Certifying Authority, fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;
(b) File any return or furnish any information, books or other documents within the time specified therefore in the regulations, fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues:
(c) Maintain books of account or records, fail to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

Section 45 – Residuary Penalty –

Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided,shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty-five thousand rupees.

Offences and Punishment under the Information Technology Act, 2000

The various offences and the punishment provided under the Information Technology Act 2000 is as under:

Section	Contents	Imprisonment	Fine
65	Tampering with computer source documents	Up to 3 years or	With Fine which may extend to 2 Lakh Rupees
66	Hacking with computer system dishonestly or fraudulently	Up to 3 years or	With fine which may extend to 5 Lakh Rupees
66A*	Punishment for Sending offensive messages through communication device	Up to 3 years and	Fine
66B	Punishment for dishonestly receiving Stolen computer resource or communication device	Up to 3 years or	With fine which may extend to 1 Lakh Rupees
66C	Punishment for Identity Theft - fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person	Up to 3 years and	With fine which may extend to 1 Lakh Rupees
66D	Punishment for cheating by Personation by using computer resource	Up to 3 years and	With fine which may extend to 1 Lakh Rupees
66E	Punishment for Violation of Privacy	Up to 3 years and	With fine which may extend to 1 Lakh Rupees
66F	Punishment for Cyber Terrorism	With Imprisonment which may extend to imprisonment	With fine not exceeding 2 Lakh Rupees
67	Punishment for Publish or transmitting Obscene material in electronic form - First time Second Time or Subsequent conviction	Up to 3 years and Up to 5 years and	With fine which may extend to 5 Lakh Rs. With fine which may extend to 10 Lakh Rs.

Section	Contents	Imprisonment	Fine
67A	Punishment for Publishing or transmitting material containing Sexually Explicit Act etc. in electronic form First time Second time or subsequent conviction	Up to 5 years and Up to 7 years and	With fine which may extend to 10 Lakh Rs With fine which may extend to 10 Lakh Rs
67B	Punishment for Publishing or transmitting material containing Children in Sexually Explicit Act – First time second time or Subsequent conviction	Up to 5 years and Up to 7 years and	With fine which may extend to 10 Lakh Rs With fine which may extend to 10 Lakh Rs
67C	Preservation and retention of information by intermediaries	Up to 3 years and	Shall also be liable to Fine
68	Power of controller to give directions	Up to 2 years or	With fine not exceeding 1 Lakh Rs.
69	Failure to comply with directions for Intercepting, monitoring or decryption of any info transmitted through any computer system/network	Up to 7 Years and	Shall also be liable to Fine
69A	Failure to comply with directions for Blocking for Public Access of any information through any computer resource	Up to 7 years and	Shall also be liable to Fine
69B	Failure to comply with directions to Monitor and Collect Traffic Data or information generated, transmitted, received or stored in any computer resource	Up to 3 years and	Shall also be liable to Fine
70	Protected system. Any unauthorized access to such system	Up to 10 years and	Shall also be liable to Fine
70B	Failure to provide information called for by the Indian Computer Emergency Response Team or comply with directions	Up to 1 year or	With fine which may extend to 1 Lakh Rs
71	Penalty for Misrepresentation or suppressing any material fact	Up to 2 years or	With fine which may extend to 1 Lakh Rs
72	Penalty for breach of confidentiality and privacy of electronic records, books, register, information etc without consent of the person to whom they belong.	Up to 2 years or	With fine which may extend to 1 Lakh Rs
72A	Punishment for Disclosure of information in breach of lawful contract	Up to 3 years or	With fine which may extend to 5 Lakh Rs

Section	Contents	Imprisonment	Fine
73	Penalty for publishing Electronic Signature Certificate False in certain particulars	Up to 2 years or	With fine which may extend to 1 Lakh Rs
74	Publication for Fraudulent purpose	Up to 2 years or	With fine which may extend to 1 Lakh Rs
75	Act to apply for offences or contravention committed outside India if the act or conduct constituting the offence involves a computer, computer system or computer network located in India		
76	Confiscation - Any computer, computer system, floppies, CDs, tape drives or other accessories related thereto in contravention of any provisions of the Act, Rules, Orders or Regulations made there under has been or is being contravened shall be liable to confiscation		
77	Compensation, Penalties or Confiscation not to interfere with other punishment		
77A	Compounding of offences		
77B	Offences with three years imprisonment to be bailable		
78	Power to investigate offences by police officers not below the rank of Dy. Superintendent of Police.		

* On 24/03/2015 the Supreme Court struck down Sec.66A of the Information Technology Act, 2000 in Shreya Singhal vs. Union of India (2015). Hon'ble Supreme Court said that Section 66A of the Information Technology Act, 2000 is struck down in its entirety being violative of Article 19(1)(a) and not saved under Article 19(2).

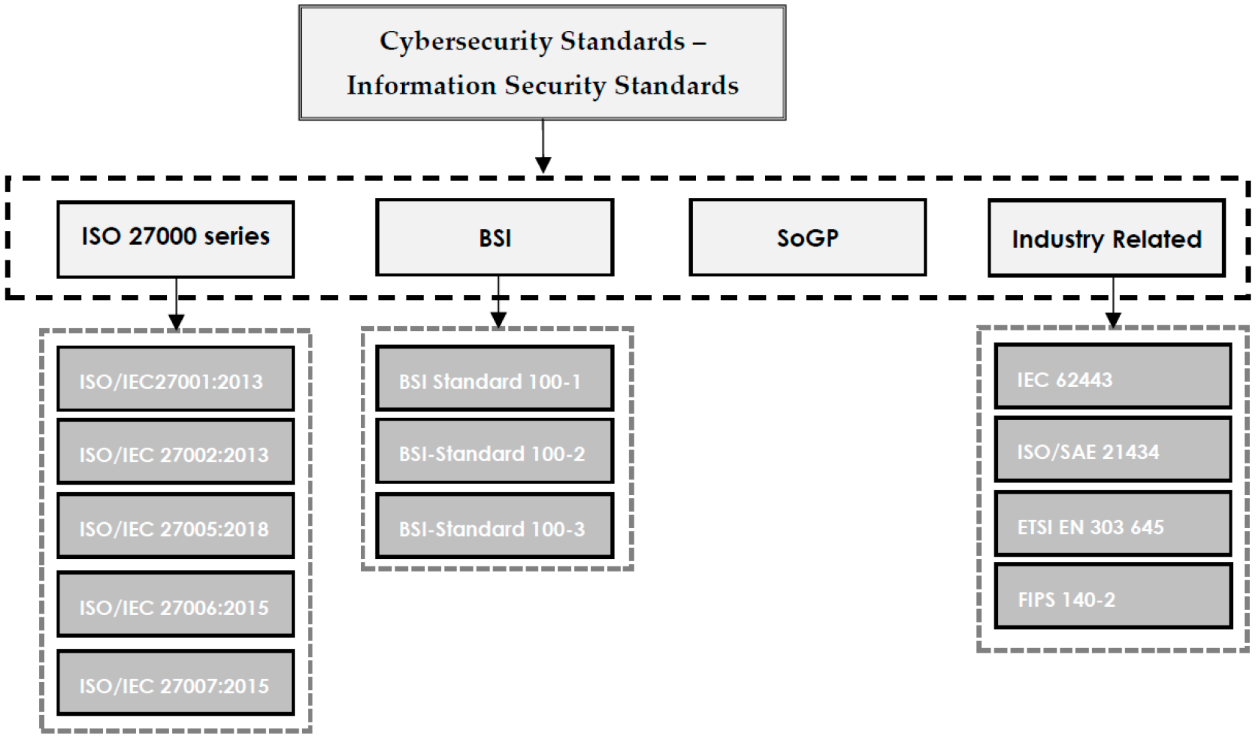
1.7 Security standards, regulations and frameworks

1.7.1 What is a cybersecurity standard?

A cybersecurity standard is a set of guidelines or best practices that organizations can use to improve their cybersecurity posture.

Organizations can use cybersecurity standards to help them identify and implement appropriate measures to protect their systems and data from cyber threats. Standards can also provide guidance on how to respond to and recover from cybersecurity incidents.

Cybersecurity frameworks are generally applicable to all organizations, regardless of their size, industry, or sector. This page details the common cybersecurity compliance standards that form a strong basis for any cybersecurity strategy.



1.7.2 What is a Cyber Security Framework?

Cyber security frameworks are sets of documents describing guidelines, standards, and best practices designed for cyber security risk management. The frameworks exist to reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit.

Cyber security framework provides foundation, structure, and support to an organization's security methodologies and efforts.

1.7.2.1 What Are the Types of Cyber Security Frameworks?

Frameworks break down into three types based on the needed function.

Control Frameworks

- Develops a basic strategy for the organization's cyber security department
- Provides a baseline group of security controls
- Assesses the present state of the infrastructure and technology
- Prioritizes implementation of security controls

Program Frameworks

- Assesses the current state of the organization's security program
- Constructs a complete cybersecurity program
- Measures the program's security and competitive analysis
- Facilitates and simplifies communications between the cyber security team and the managers/executives

Risk Frameworks

- Defines the necessary processes for risk assessment and management
- Structures a security program for risk management
- Identifies, measures, and quantifies the organization's security risks
- Prioritizes appropriate security measures and activities

Top Cyber Security Frameworks

When it comes to picking a cyber security framework, you have an ample selection to choose from. Naturally, your choice depends on your organization's security needs.

1. **The NIST CyberSecurity Framework.**

   The NIST Framework for Improving Critical Infrastructure Cybersecurity, or the "NIST cybersecurity framework" for brevity's sake, was established during the Obama Administration in response to presidential Executive Order 13636. The NIST was designed to protect America's critical infrastructure (e.g., dams, power plants) from cyberattacks.

   NIST is a set of voluntary security standards that private sector companies can use to find, identify, and respond to cyberattacks. The framework also features guidelines to help organizations prevent and recover from cyberattacks. There are five functions or best practices associated with NIST:

   - Identify
   - Protect
   - Detect
   - Respond

- Recover

2. **The Center for Internet Security Critical Security Controls (CIS).**

   If you want your company to start small and gradually work its way up, you must go with CIS. This framework was developed in the late 2000s to protect companies from cyber threats. It's made up of 20 controls regularly updated by security professionals from many fields (academia, government, industrial). The framework begins with basics, moves on to foundational, then finishes with organizational.

   CIS uses benchmarks based on common standards like HIPAA or NIST that map security standards and offer alternative configurations for organizations not subject to mandatory security protocols but want to improve cyber security anyway.

3. **The International Standards Organization (ISO) frameworks ISO/IEC 27001 and 27002.**

   This framework is also called ISO 270K. It is considered the internationally recognized cyber security validation standard for both internal situations and across third parties. ISO 270K operates under the assumption that the organization has an Information Security Management System. ISO/IEC 27001 requires management to exhaustively manage their organization's information security risks, focusing on threats and vulnerabilities.

   ISO 270K is very demanding. The framework recommends 114 different controls, broken into 14 categories. As a result, ISO 270K may not be for everyone, considering the amount of work involved in maintaining the standards. However, if implementing ISO 270K is a selling point for attracting new customers, it's worth it.

4. **The Health Insurance Portability and Accountability Act.**

   Better known as HIPAA, it provides a framework for managing confidential patient and consumer data, particularly privacy issues. This legislation protects electronic healthcare information and is essential for healthcare providers, insurers, and clearinghouses.

   There are many other frameworks to choose from, including:

   - SOC2 (Service Organization Control)
   - NERC-CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)
   - GDPR (General Data Protection Regulation)
   - FISMA (Federal Information Systems Management Act)
   - HITRUST CSF (Health Information Trust Alliance)
   - PCI-DSS (Payment Card Industry Data Security Standards)
   - COBIT (Control Objectives for Information and Related Technologies)
   - COSO (Committee of Sponsoring Organizations)

1.7.2.2 Cyber Security Framework Best Practices

Although every framework is different, certain best practices are applicable across the board. Here, we are expanding on NIST's five functions mentioned previously.

Identify

To manage the security risks to its assets, data, capabilities, and systems, a company must fully understand these environments and identify potential weak spots.

Protect

Companies must create and deploy appropriate safeguards to lessen or limit the effects of potential cyber security breaches and events.

Detect

Organizations should put in motion the necessary procedures to identify cyber security incidents as soon as possible.

Respond

Companies must be capable of developing appropriate response plans to contain the impacts of any cyber security events.

Recover

Companies must create and implement effective procedures that restore any capabilities and services damaged by cyber security events.

UNIT - 2

Advanced Network Security

2.1 Digital Forensics

Forensic Science

Forensic science is the use of scientific methods or expertise to investigate crimes or examine evidence that might be presented in a court of law. Forensic science comprises a diverse array of disciplines, from fingerprint and DNA analysis to anthropology and wildlife forensics. Though they represent varied disciplines, all forensic scientists face a common set of challenges. How do you ensure that forensic methods produce reliable results? How do you communicate findings to a jury or other non-experts in a way that is accurate and understandable? How do you keep up with new technology without falling behind on casework? Meeting these and other challenges is critical to ensuring that forensic science remains a powerful force in support of justice and public safety.

Digital Forensics

Digital forensics is the process of storing, analyzing, retrieving, and preserving electronic data that may be useful in an investigation. It includes data from hard drives in computers, mobile phones, smart appliances, vehicle navigation systems, electronic door locks, and other digital devices. The process's goal of digital forensics is to collect, analyze, and preserve evidence.

Steps of Digital Forensics

- **Identification**

  This is the initial stage in which the individuals or devices to be analyzed are identified as likely sources of significant evidence.

- **Preservation**

  It focuses on safeguarding relevant electronically stored information (ESI) by capturing and preserving the crime scene, documenting relevant information such as visual images, and how it was obtained.

- **Analysis**

  It is a methodical examination of the evidence of the information gathered. This examination produces data objects, including system and user-generated files, and seeks specific answers and points of departure for conclusions.

- **Documentation**

  These are tried-and-true procedures for documenting the analysis's conclusions, and they must allow other competent examiners to read through and duplicate the results.

- **Presentation**

  The collection of digital information, which may entail removing electronic devices from the crime/incident scene and copying or printing the device(s), is critical to the investigation.

Objectives of Digital Forensics

Knowing the primary objectives of using digital forensics is essential for a complete understanding of what is digital forensics:

- It aids in the recovery, analysis, and preservation of computers and related materials for the investigating agency to present them as evidence in a court of law
- It aids in determining the motive for the crime and the identity of the primary perpetrator
- Creating procedures at a suspected crime scene to help ensure that the digital evidence obtained is not tainted
- Data acquisition and duplication: The process of recovering deleted files and partitions from digital media in order to extract and validate evidence
- Assists you in quickly identifying evidence and estimating the potential impact of malicious activity on the victim
- Creating a computer forensic report that provides comprehensive information on the investigation process
- Keeping the evidence safe by adhering to the chain of custody

Types of Digital Forensics

As digital data forensics evolves, several sub-disciplines emerge, some of which are listed below:

Computer Forensics

It analyzes digital evidence obtained from laptops, computers, and storage media to support ongoing investigations and legal proceedings.

Mobile Device Forensics

It entails obtaining evidence from small electronic devices such as personal digital assistants, mobile phones, tablets, sim cards, and gaming consoles.

Network Forensics

Network or cyber forensics depends on the data obtained from monitoring and analyzing cyber network activities such as attacks, breaches, or system collapse caused by malicious software and abnormal network traffic.

Digital Image Forensics

This sub-specialty focuses on the extraction and analysis of digital images to verify authenticity and metadata and determine the history and information surrounding them.

Digital Video/Audio Forensics

This field examines audio-visual evidence to determine its authenticity or any additional information you can extract, such as location and time intervals.

Memory Forensics

It refers to the recovery of information from a running computer's RAM and is also known as live acquisition.

2.2 IP Security

IP Sec (Internet Protocol Security) is an Internet Engineering Task Force (IETF) standard suite of protocols between two communication points across the IP network that provide data authentication, integrity, and confidentiality. It also defines the encrypted, decrypted, and authenticated packets. The protocols needed for secure key exchange and key management are defined in it.

Uses of IP Security

IPsec can be used to do the following things:

- To encrypt application layer data.
- To provide security for routers sending routing data across the public internet.
- To provide authentication without encryption, like to authenticate that the data originates from a known sender.
- To protect network data by setting up circuits using IPsec tunneling in which all data being sent between the two endpoints is encrypted, as with a Virtual Private Network(VPN) connection.

Components of IP Security

It has the following components:

1. Encapsulating Security Payload (ESP)
2. Authentication Header (AH)
3. Internet Key Exchange (IKE)

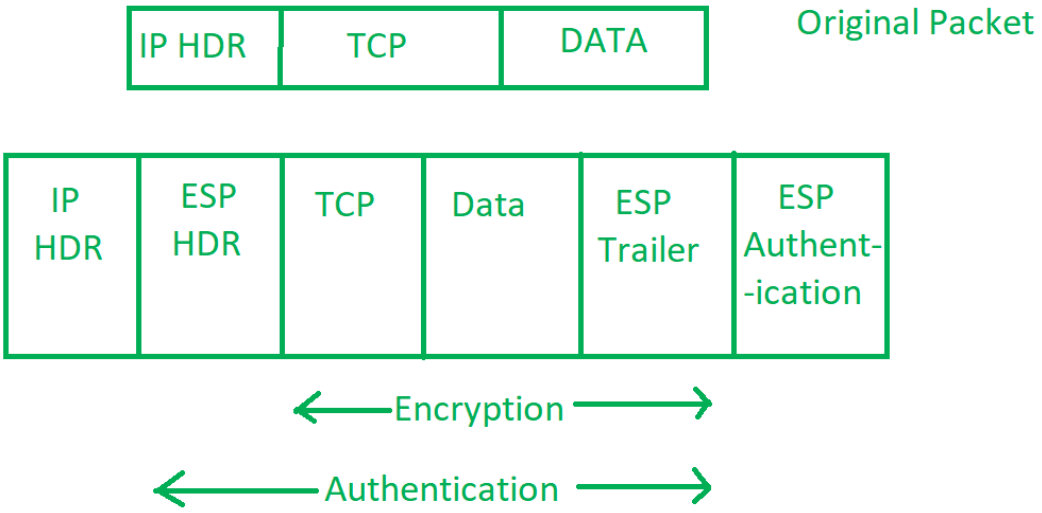
1. **Encapsulating Security Payload (ESP):** It provides data integrity, encryption, authentication, and anti-replay. It also provides authentication for payload.
2. **Authentication Header (AH):** It also provides data integrity, authentication, and anti-replay and it does not provide encryption. The anti-replay protection protects against the unauthorized transmission of packets. It does not protect data confidentiality.

3. **Internet Key Exchange (IKE):** It is a network security protocol designed to dynamically exchange encryption keys and find a way over Security Association (SA) between 2 devices. The Security Association (SA) establishes shared security attributes between 2 network entities to support secure communication.

   The Key Management Protocol (ISAKMP) and Internet Security Association provides a framework for authentication and key exchange. ISAKMP tells how the setup of the Security Associations (SAs) and how direct connections between two hosts are using IPsec.

   Internet Key Exchange (IKE) provides message content protection and also an open frame for implementing standard algorithms such as SHA and MD5.

   The algorithm's IP sec users produce a unique identifier for each packet. This identifier then allows a device to determine whether a packet has been correct or not. Packets that are not authorized are discarded and not given to the receiver.



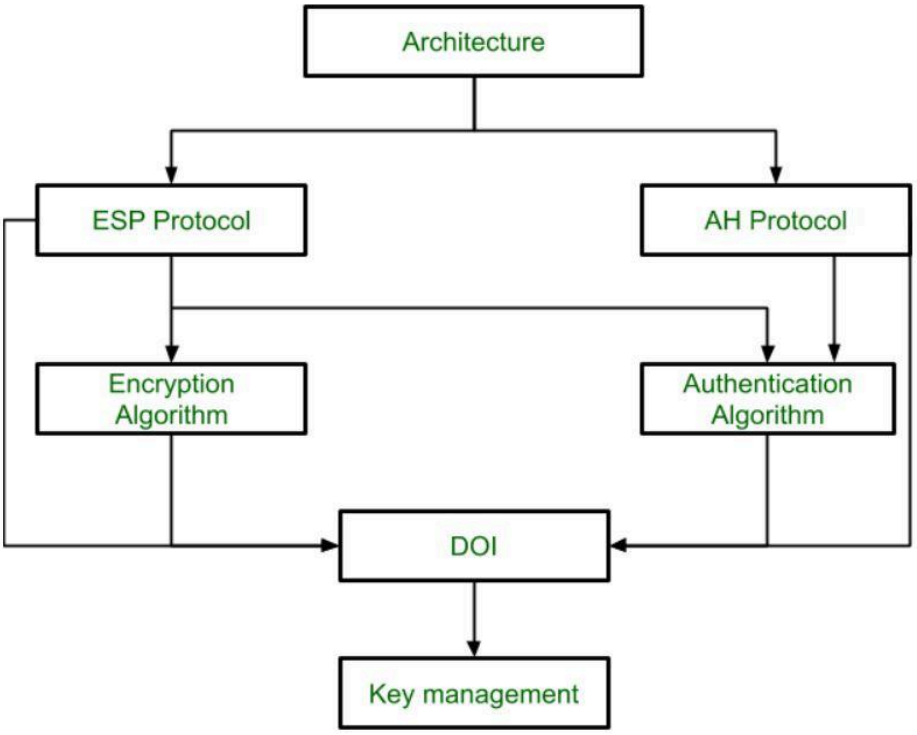
IP Security Architecture

IPSec (IP Security) architecture uses two protocols to secure the traffic or data flow. These protocols are ESP (Encapsulation Security Payload) and AH (Authentication Header). IPSec Architecture includes protocols, algorithms, DOI, and Key Management. All these components are very important in order to provide the three main services:

Confidentiality

Authenticity

Integrity



Working on IP Security

- The host checks if the packet should be transmitted using IPsec or not. This packet traffic triggers the security policy for itself. This is done when the system sending the packet applies appropriate encryption. The incoming packets are also checked by the host that they are encrypted properly or not.
- Then IKE Phase 1 starts in which the 2 hosts(using IPsec) authenticate themselves to each other to start a secure channel. It has 2 modes. The Main mode provides greater security and the Aggressive mode which enables the host to establish an IPsec circuit more quickly.
- The channel created in the last step is then used to securely negotiate the way the IP circuit will encrypt data across the IP circuit.
- Now, the IKE Phase 2 is conducted over the secure channel in which the two hosts negotiate the type of cryptographic algorithms to use on the session and agree on secret keying material to be used with those algorithms.
- Then the data is exchanged across the newly created IPsec encrypted tunnel. These packets are encrypted and decrypted by the hosts using IPsec SAs.
- When the communication between the hosts is completed or the session times out then the IPsec tunnel is terminated by discarding the keys by both hosts.

Advantages of IPSec

1. **Strong security:** IPSec provides strong cryptographic security services that help protect sensitive data and ensure network privacy and integrity.
2. **Wide compatibility:** IPSec is an open standard protocol that is widely supported by vendors and can be used in heterogeneous environments.
3. **Flexibility:** IPSec can be configured to provide security for a wide range of network topologies, including point-to-point, site-to-site, and remote access connections.
4. **Scalability:** IPSec can be used to secure large-scale networks and can be scaled up or down as needed.
5. **Improved network performance:** IPSec can help improve network performance by reducing network congestion and improving network efficiency.

Disadvantages of IPSec

1. **Configuration complexity:** IPSec can be complex to configure and requires specialized knowledge and skills.
2. **Compatibility issues:** IPSec can have compatibility issues with some network devices and applications, which can lead to interoperability problems.
3. **Performance impact:** IPSec can impact network performance due to the overhead of encryption and decryption of IP packets.
4. **Key management:** IPSec requires effective key management to ensure the security of the cryptographic keys used for encryption and authentication.
5. **Limited protection:** IPSec only provides protection for IP traffic, and other protocols such as ICMP, DNS, and routing protocols may still be vulnerable to attacks.

2.3 VPN

VPN stands for the Virtual Private Network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the Internet.

A Virtual Private Network is a way to extend a private network using a public network such as the Internet. The name only suggests that it is a "Virtual Private Network", i.e. a user can be part of a local network sitting at a remote location. It makes use of tunnelling protocols to establish a secure connection.

How does a VPN work?

Let us understand VPN with an example:

Think of a situation where the corporate office of a bank is situated in Washington, USA. This office has a local network consisting of say 100 computers. Suppose other branches of the bank are in Mumbai, India, and Tokyo, Japan.

The traditional method of establishing a secure connection between the head office and the branch was to have a leased line between the branches and head office which was a very costly as well as troublesome job.

VPN lets us effectively overcome this issue.

The situation is described below:

- All 100 hundred computers of the corporate office in Washington are connected to the VPN server(which is a well-configured server containing a public IP address and a switch to connect all computers present in the local network i.e. in the US head office).
- The person sitting in the Mumbai office connects to The VPN server using a dial-up window and the VPN server returns an IP address that belongs to the series of IP addresses belonging to a local network of the corporate office.
- Thus a person from the Mumbai branch becomes local to the head office and information can be shared securely over the public internet.
- So this is the intuitive way of extending the local network even across the geographical borders of the country.

What is VPN used for?

Do you need help determining when you should use a VPN? Let us shed some light on the subject and show you how the best VPNs can revolutionize your online activities.

- **For Unlimited Streaming:** Love streaming your favourite shows and sports games? A VPN is your ultimate companion for unlocking streaming services like Netflix or Hulu. Access all the content you desire and never miss a moment of your beloved NFL games.
- **For elevating your Gaming Experience:** Unleash your gaming potential with the added layer of security and convenience provided by a VPN. Defend yourself against vengeful competitors aiming to disrupt your gameplay while improving your ping for smoother, lag-free sessions. Additionally, gain access to exclusive games that may be restricted in your region, opening up a world of endless gaming possibilities.
- **For Anonymous Torrenting:** When it comes to downloading copyrighted content through torrenting, it's essential to keep your IP address hidden. A VPN can mask your identity and avoid potential exposure, ensuring a safe and private torrenting experience.
- **For supercharging your Internet Speed:** Are you tired of your Internet speed slowing down when downloading large files? Your Internet Service Provider (ISP) might be intentionally throttling your bandwidth. Thankfully, a VPN can rescue you

by keeping your online activities anonymous, effectively preventing ISP throttling. Say goodbye to sluggish connections and embrace blazing-fast speeds.

- **Securing Public Wi-Fi:** VPNs are essential for maintaining security when using public Wi-Fi networks, such as those in coffee shops, airports, or hotels. These networks are often vulnerable to cyberattacks, and using a VPN encrypts your internet connection, protecting your data from potential hackers and eavesdroppers when you connect to untrusted Wi-Fi hotspots.

Are VPNs legal or illegal?

Using a VPN is legal in most countries. The legality of using a VPN service depends on the country and its geopolitical relations with another country as well.

A reliable and secure VPN is always legal if you do not intend to use it for any illegal activities like committing fraud online, cyber theft, or in some countries downloading copyrighted content.

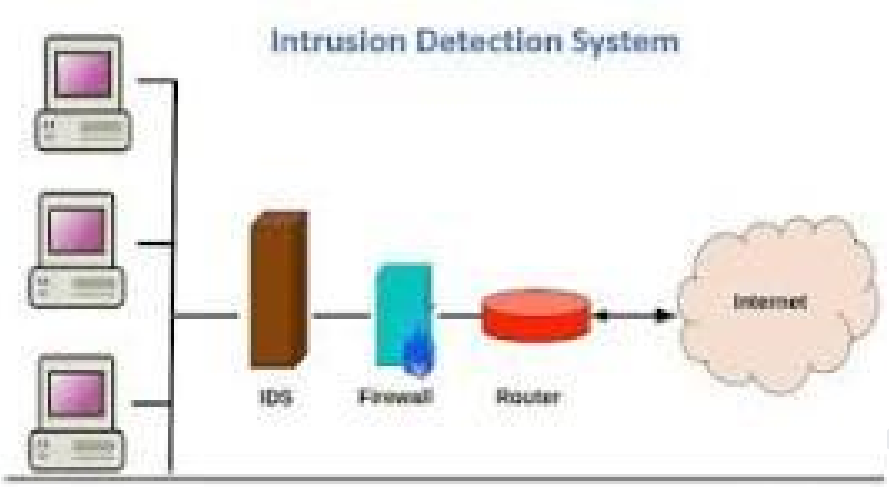
China has decided to block all VPNs (Virtual private network) by next year, as per the report of Bloomberg. Many Chinese Internet users use VPNs to privately access websites that are blocked under China's so-called "great firewall". This is done to avoid any information leakage to rival countries and to tighten the information security.

2.3 Instruction Detection

A system called an intrusion detection system (IDS) observes network traffic for malicious transactions and sends immediate alerts when it is observed. It is software that checks a network or system for malicious activities or policy violations.

Each illegal activity or violation is often recorded either centrally using a SIEM(Security information and event management) system or notified to an administration. IDS monitors a network or system for malicious activity and protects a computer network from unauthorized access from users, including perhaps insiders.

The intrusion detector learning task is to build a predictive model (i.e. a classifier) capable of distinguishing between 'bad connections' (intrusion/attacks) and 'good (normal) connections'.



How does an IDS work?

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Benefits of IDS

1. **Detects malicious activity:** IDS can detect any suspicious activities and alert the system administrator before any significant damage is done.
2. **Improves network performance:** IDS can identify any performance issues on the network, which can be addressed to improve network performance.
3. **Compliance requirements:** IDS can help in meeting compliance requirements by monitoring network activity and generating reports.
4. **Provides insights:** IDS generates valuable insights into network traffic, which can be used to identify any weaknesses and improve network security.

Snort : Intrusion Prevention System (IPS)

- Snort is an open source Network Intrusion Detection System (NIDS) which is available free of cost. NIDS is the type of Intrusion Detection System (IDS) that is used for scanning data flowing on the network.
- It can perform real time traffic analysis and packet-logging on IP networks.
- Also perform protocol analysis, content searching/matching.
- It can be used to detect a variety of attacks, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts, and much more.
- Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level.

There are two types of IDS : Network IDS and Host IDS.

A **Network IDS** is an intrusion detection system that tries to identify malicious action such as denial of service attacks; port scans or even attempts to crack into computers by monitoring network traffic. Network intrusion detection systems gain access to network traffic by connecting to a hub/switch configured for port mirroring, or a network tap.

A **host-based IDS** is an intrusion detection system that monitors and analyzes the internals of a computing system rather than the network packets on its external interfaces. It consists of an agent on a host that identifies intrusions by analyzing system calls, application logs, file-system modifications.

Snort can be configured to run in three modes:

Sniffer mode, which simply reads the packets off of the network and displays them on the screen.

Packet Logger mode, which logs the packets to disk.

Network Intrusion Detection System (NIDS) mode,

- Performs detection and analysis on network traffic.
- The program will monitor network traffic and analyze it against a rule set defined by the user.
- The program will then perform a specific action based on what has been identified.

UNIT - 3

Web Security Protocols

3.1 Web Security Methods

Website Security is a way of protecting the websites and web application from being hacked or any unauthorized access, done by creating an extra layer of a protection measure and protocol that helps in mitigating the attacks. It is not a simple task, and to secure websites and applications then security comprises a lot of factors that go into web security and web protection, like up to date regarding new threats and how to mitigate them and monitor the traffic.

Protecting a website from malicious hackers requires protecting every way a bad actor can harm your website. Depending on the size and scope of your website, this might include cloud security, web application security, virtual private network (VPN) protection, locking down your web provider account, or having a disaster recovery plan.

What is the best security for websites?

The best security for a website is a collection of strong passwords, encrypted data through SSL certificates, constant monitoring, automated backups, and frequent vulnerability assessments.

Common website security threats

Website security threats

1. Data breach
2. Denial of service (DoS)
3. Loss of website availability
4. Ransomware
5. Cross-site scripting (XSS)
6. SQL and code injections
7. Stolen passwords

Data breach

A data breach happens when someone exposes confidential information. Data breaches can happen by accident, but cyber thieves also target websites and web applications to steal data that they can sell on the black market or use to break deeper into the company's network. Financial and medical data are common targets, but hackers can also sell student data, private correspondence and photos, and customer contact information.

Data breaches are costly, and not just in terms of lost income. Customers can sue if their private data is stolen and they can show that your company was negligent. National governments are becoming more aggressive in protecting their citizens' data, so large fines and legal sanctions are also a possibility. Data breaches can also destroy a business's reputation and the public's perception of its trustworthiness.

Denial of service (DoS) and Loss of website availability

A Denial of Service (DoS) attack is an attempt to crash a website by overloading its servers. A similar attack is a distributed denial of service (DDoS). In a distributed attack, the traffic is coming from multiple resources. This makes it more difficult to stop. You can block one source from flooding your web server, but it is much more difficult to keep hundreds, especially if the list is constantly changing.

Ransomware

Ransomware is a malicious code that blocks access to your website until you pay a ransom. Ransomware is becoming more frequent for small businesses and government municipalities. A criminal encrypts your computer files and user data, then offers to sell you a decryption key in return for cash (often Bitcoin or another cryptocurrency). This is a highly profitable crime because it costs less to pay the ransom than to regain access to business files any other way.

Cross-site scripting (XSS)

Cross-site scripting (XSS) happens when a malicious actor injects executable scripts into a website's code. When this is successful, the hacker is able to gain access to and control the website to impersonate people who have legitimate access to its website code.

SQL and code injections

SQL injections (SQLi) use SQL code to manipulate the databases connected to a website. SQL stands for scripted query language. It is used by database administrators to control the data in a database. An SQL injection bypasses the webpage to access the database directly. Once hackers access the database, they can destroy the sensitive information or copy it to sell on the dark web.

Stolen passwords

Most websites are secured by passwords. Passwords can be broken by software programs that try different combinations until they find one that works. Or in many cases, web developers use the default passwords that come with their web administrator account. If a hacker has the username and password to a website, they can do any amount of mischief or malicious activity, from defacing the webpage to making the files irrecoverable.

3.2 SSL (Secure Socket Layer)

Secure Socket Layer (SSL) provides security to the data that is transferred between web browser and server. SSL encrypts the link between a web server and a browser which ensures that all data passed between them remains private and free from attack.

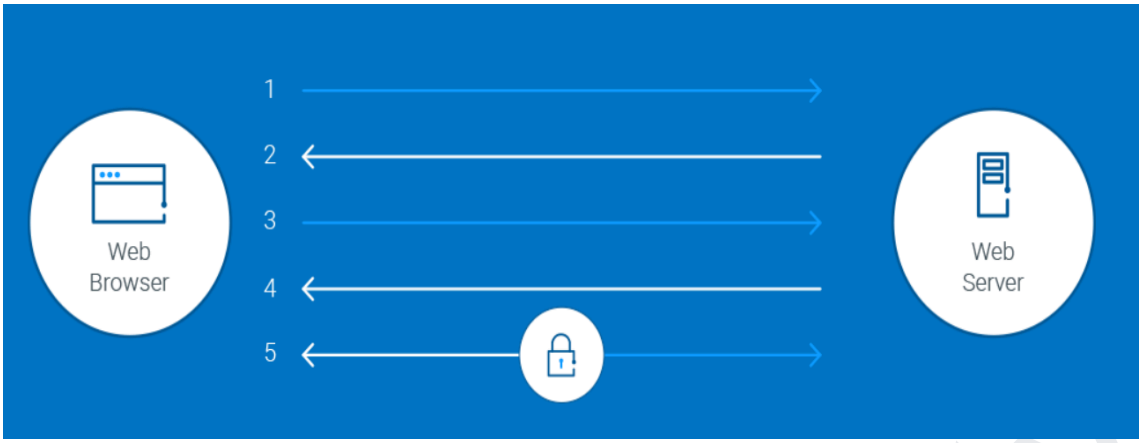
SSL allows sensitive information such as credit card numbers, social security numbers, and login credentials to be transmitted securely. Normally, data sent between browsers and web servers is sent in plain text—leaving you vulnerable to eavesdropping. If an attacker is able to intercept all data being sent between a browser and a web server, they can see and use that information.

How Does the SSL Certificate Create a Secure Connection?

When a browser attempts to access a website that is secured by SSL, the browser and the web server establish an SSL connection using a process called an "SSL Handshake" (see diagram below). Note that the SSL Handshake is invisible to the user and happens instantaneously.

Essentially, three keys are used to set up the SSL connection: the public, private, and session keys. Anything encrypted with the public key can only be decrypted with the private key, and vice versa.

Because encrypting and decrypting with private and public keys takes a lot of processing power, they are only used during the SSL Handshake to create a symmetric session key. After the secure connection is made, the session key is used to encrypt all transmitted data.



1. **Browser** connects to a web server (website) secured with SSL (https). Browser requests that the server identify itself.
2. **Server** sends a copy of its SSL Certificate, including the server's public key.
3. **Browser** checks the certificate root against a list of trusted CAs and that the certificate is unexpired, unrevoked, and that its common name is valid for the website that it is connecting to. If the browser trusts the certificate, it creates, encrypts, and sends back a symmetric session key using the server's public key.
4. **Server** decrypts the symmetric session key using its private key and sends back an acknowledgement encrypted with the session key to start the encrypted session.
5. **Server** and Browser now encrypt all transmitted data with the session key.

3.3 TLS (Transport Layer Security)

Transport Layer Security, or TLS, is a widely adopted security protocol designed to facilitate privacy and data security for communications over the Internet. A primary use case of TLS is encrypting the communication between web applications and servers, such as web browsers loading a website. TLS can also be used to encrypt other communications such as email, messaging, and voice over IP (VoIP). In this article we will focus on the role of TLS in web application security.

TLS was proposed by the Internet Engineering Task Force (IETF), an international standards organization, and the first version of the protocol was published in 1999. The most recent version is TLS 1.3, which was published in 2018.

What is the difference between TLS and SSL?

TLS evolved from a previous encryption protocol called Secure Sockets Layer (SSL), which was developed by Netscape. TLS version 1.0 actually began development as SSL version 3.1, but the name of the protocol was changed before publication in order to indicate that it was no longer associated with Netscape. Because of this history, the terms TLS and SSL are sometimes used interchangeably.

What is the difference between TLS and HTTPS?

HTTPS is an implementation of TLS encryption on top of the HTTP protocol, which is used by all websites as well as some other web services. Any website that uses HTTPS is therefore employing TLS encryption.

Why should businesses and web applications use the TLS protocol?

TLS encryption can help protect web applications from data breaches and other attacks. Today, TLS-protected HTTPS is a standard practice for websites.

The Google Chrome browser gradually cracked down on non-HTTPS sites, and other browsers have followed suit. Everyday Internet users are more wary of websites that do not feature the HTTPS padlock icon.

What does TLS do?

There are three main components to what the TLS protocol accomplishes: Encryption, Authentication, and Integrity.

Encryption: hides the data being transferred from third parties.

Authentication: ensures that the parties exchanging information are who they claim to be.

Integrity: verifies that the data has not been forged or tampered with.

What is a TLS certificate?

For a website or application to use TLS, it must have a TLS certificate installed on its origin server (the certificate is also known as an "SSL certificate" because of the naming confusion described above). A TLS certificate is issued by a certificate authority to the person or business that owns a domain. The certificate contains important information about who owns the domain, along with the server's public key, both of which are important for validating the server's identity.

How does TLS work?

A TLS connection is initiated using a sequence known as the TLS handshake. When a user navigates to a website that uses TLS, the TLS handshake begins between the user's device (also known as the client device) and the web server.

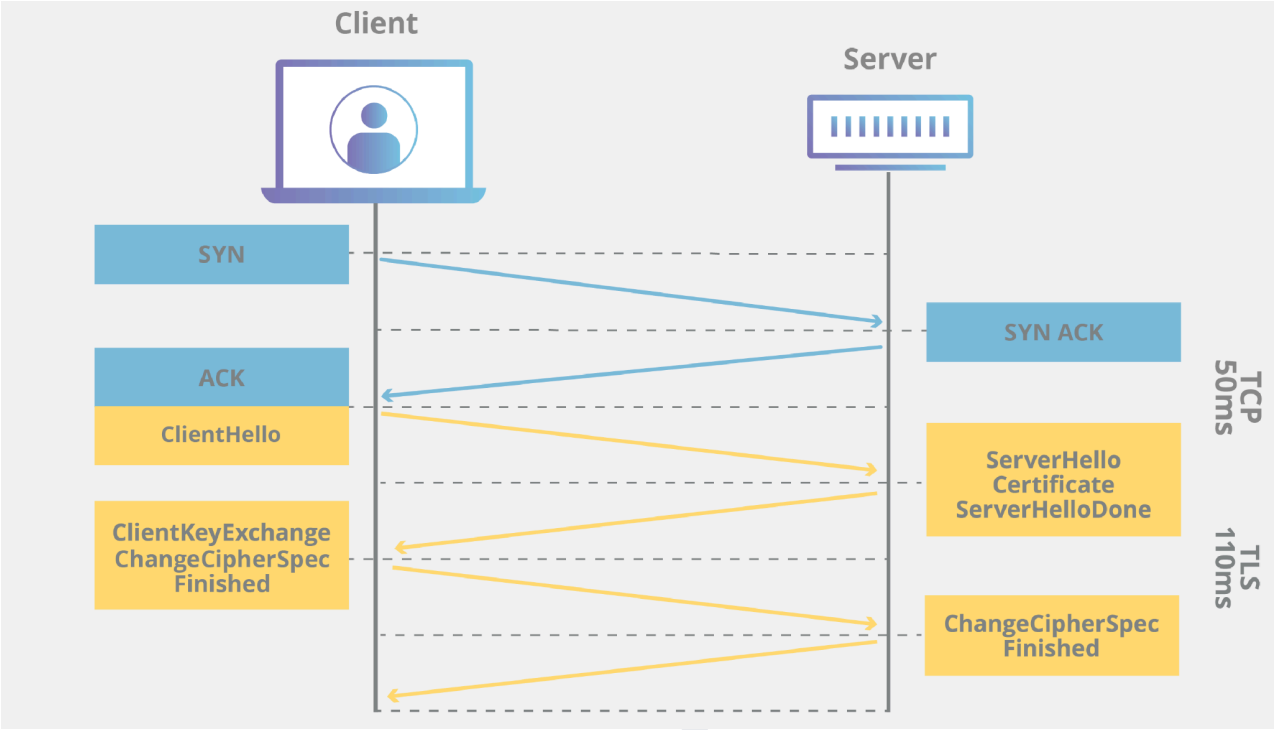
During the TLS handshake, the user's device and the web server:

- Specify which version of TLS (TLS 1.0, 1.2, 1.3, etc.) they will use
- Decide on which cipher suites (see below) they will use
- Authenticate the identity of the server using the server's TLS certificate
- Generate session keys for encrypting messages between them after the handshake is complete

The TLS handshake establishes a cipher suite for each communication session. The cipher suite is a set of algorithms that specifies details such as which shared encryption keys, or session keys, will be used for that particular session. TLS is able to set the matching session keys over an unencrypted channel thanks to a technology known as public key cryptography.

The handshake also handles authentication, which usually consists of the server proving its identity to the client. This is done using public keys. Public keys are encryption keys that use one-way encryption, meaning that anyone with the public key can unscramble the data encrypted with the server's private key to ensure its authenticity, but only the original sender can encrypt data with the private key. The server's public key is part of its TLS certificate.

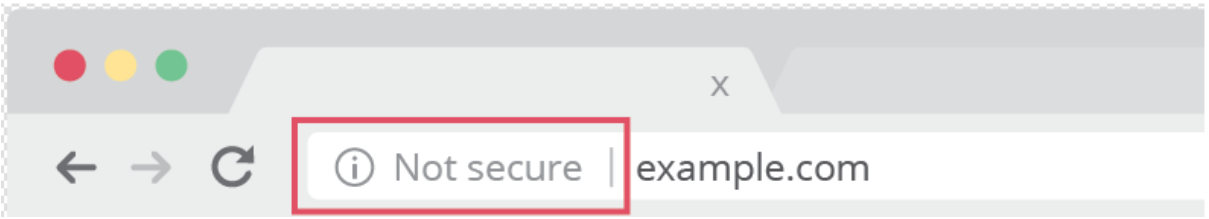
Once data is encrypted and authenticated, it is then signed with a message authentication code (MAC). The recipient can then verify the MAC to ensure the integrity of the data. This is kind of like the tamper-proof foil found on a bottle of aspirin; the consumer knows no one has tampered with their medicine because the foil is intact when they purchase it.



3.4 HTTPS (Hypertext Transfer Protocol Secure)

Hypertext transfer protocol secure (HTTPS) is the secure version of HTTP, which is the primary protocol used to send data between a web browser and a website. HTTPS is encrypted in order to increase security of data transfer. This is particularly important when users transmit sensitive data, such as by logging into a bank account, email service, or health insurance provider.

Any website, especially those that require login credentials, should use HTTPS. In modern web browsers such as Chrome, websites that do not use HTTPS are marked differently than those that are. Look for a padlock in the URL bar to signify the webpage is secure. Web browsers take HTTPS seriously; Google Chrome and other browsers flag all non-HTTPS websites as not secure.



How does HTTPS work?

HTTPS uses an encryption protocol to encrypt communications. The protocol is called Transport Layer Security (TLS), although formerly it was known as Secure Sockets Layer (SSL). This protocol secures communications by using what's known as an asymmetric public key infrastructure. This type of security system uses two different keys to encrypt communications between two parties:

1. The private key - this key is controlled by the owner of a website and it's kept, as the reader may have speculated, private. This key lives on a web server and is used to decrypt information encrypted by the public key.
2. The public key - this key is available to everyone who wants to interact with the server in a way that's secure. Information that's encrypted by the public key can only be decrypted by the private key.

Why is HTTPS important? What happens if a website doesn't have HTTPS?

HTTPS prevents websites from having their information broadcast in a way that's easily viewed by anyone snooping on the network. When information is sent over regular HTTP, the information is broken into packets of data that can be easily "sniffed" using free software. This makes communication over an unsecure medium, such as public Wi-Fi, highly vulnerable to interception. In fact, all communications that occur over HTTP occur in plain text, making them highly accessible to anyone with the correct tools, and vulnerable to on-path attacks.

With HTTPS, traffic is encrypted such that even if the packets are sniffed or otherwise intercepted, they will come across as nonsensical characters.

What port does HTTPS use?

HTTPS uses port 443. This differentiates HTTPS from HTTP, which uses port 80.

(In networking, a port is a virtual software-based point where network connections start and end. All network-connected computers expose a number of ports to enable them to receive traffic. Each port is associated with a specific process or service, and different protocols use different ports.)

How else is HTTPS different from HTTP?

Technically speaking, HTTPS is not a separate protocol from HTTP. It is simply using TLS/SSL encryption over the HTTP protocol. HTTPS occurs based upon the transmission of TLS/SSL certificates, which verify that a particular provider is who they say they are.

When a user connects to a webpage, the webpage will send over its SSL certificate which contains the public key necessary to start the secure session. The two computers, the client and the server, then go through a process called an SSL/TLS handshake, which is a series of back-and-forth communications used to establish a secure connection. To take a deeper dive into encryption and the SSL/TLS handshake, read about what happens in a TLS handshake.

How does a website start using HTTPS?

Many website hosting providers and other services will offer TLS/SSL certificates for a fee. These certificates will often be shared amongst many customers. More expensive certificates are available which can be individually registered to particular web properties.

Practical – 1

Aim: Study Digital Forensics and list different tools used for forensic investigation. Prepare a document that contains the following information about the tools. 1. Description 2.Key Features 3.Snapshot of software.

Digital Forensics:

Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting on data stored electronically.

Digital Forensics helps the forensic team to analyze, inspect, identify and preserve the digital evidence residing on various types of electronic devices.

Process of Digital forensics

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation

Digital forensics tools:

1. Image creation: FTK imager

FTK Imager is a forensic toolkit developed by AccessData that can be used to get evidence. It can create copies of data without making changes to the original evidence. This tool allows you to specify criteria, like file size, pixel size, and data type, to reduce the amount of irrelevant data.

AccessData FTK Imager is a forensics tool whose main purpose is to preview recoverable data from a disk of any kind. It can also create perfect copies, called forensic images, of that data. Furthermore, it is completely free.

This powerful tool can create forensic images of local hard drives, floppy disks, Zip disks, CDs, and DVDs, entire folders, or even of individual files from various places within the media storage device.

Features:

- It provides a wizard-driven approach to detect cybercrime.
- This program offers better visualization of data using a chart.
- You can recover passwords from more than 100 applications.
- It has an advanced and automated data analysis facility.

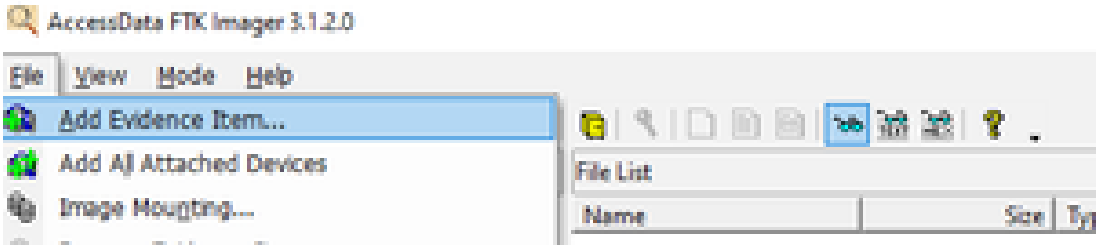
FTK Imager:

FTK Imager is a tool for creating disk images and is absolutely free to use. It was developed by The Access Data Group. It is a tool that helps to preview data and for imaging.

Step 1: Download and install the FTK imager on your machine.

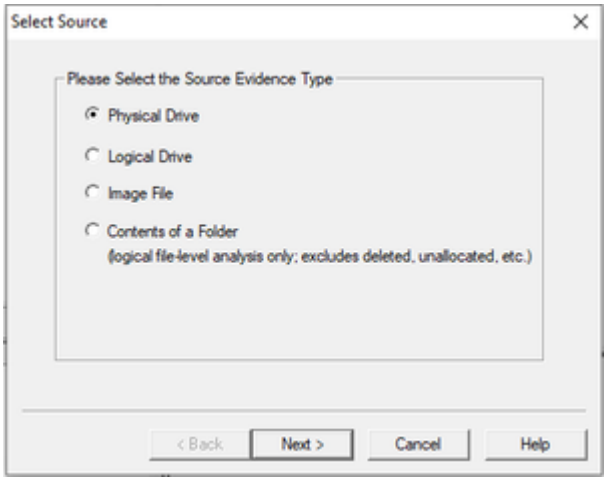
Step 2: Click and open the FTK Imager, once it is installed. You should be greeted with the FTK Imager dashboard.

Step 3: In the menu navigation bar, you need to click on the File tab which will give you a drop- down, like given in the image below, just click on the first one that says, Add Evidence Item.



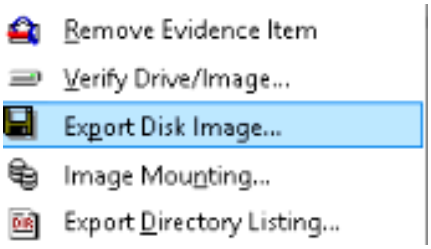
Step 4: After that, there will be a pop-up window that will ask you to Select the Source of the Evidence. If you have connected a physical hard drive to the laptop/computer you are using to make the forensic image, then you will select the Physical Drive here. Click on Next. Now, Select the Physical Drive that you would like to use. Please make

sure that you are selecting the right drive, or you will waste your time exporting a forensic image of your own OS drive.



Step 5: Now, we will export the forensic images.

Right-click on the Physical Drive that you would like to export in the FTK Imager window. Select Export Disk Image here.



- Click the Add button for the Image Destination.
- Select the Type of Forensic Image you would like to export. Select .E01 and Click Next.
- After that, you will have to enter information regarding the case now. You can either leave them blank or keep it general, this part is totally upon you.
- Next, you will need to Choose the Destination that you would like to export the forensic image and Name the Image.

Lastly, you will need to wait for the Forensic Image to be created and then verified. The speed of creating the forensic image will vary based on your hardware. Once both have occurred, you have your forensic images ready.

2. Disk analysis: Autopsy/the Sleuth Kit

Autopsy and the Sleuth Kit are likely the most well-known forensics toolkits in existence. The Sleuth Kit is a command-line tool that performs forensic analysis of forensic images of hard drives and smartphones. Autopsy is a GUI-based system that uses The Sleuth Kit behind the scenes.

Features:

- You can identify activity using a graphical interface effectively.
- This application provides analysis for emails.
- You can group files by their type to find all documents or images.
- It displays a thumbnail of images to quickly view pictures.

3. Network analysis: Wireshark

Wireshark is a tool that analyzes a network packet. It can be used for network testing and troubleshooting. This tool helps you to check different traffic going through your computer system.

Features:

- It provides rich VoIP (Voice over Internet Protocol) analysis.
- Capture files compressed with gzip can be decompressed easily.
- Output can be exported to XML (Extensible Markup Language), CSV (Comma Separated Values) file, or plain text.
- Live data can be read from the network, blue-tooth, ATM, USB, etc.

4. Email Forensics: Email Tracer

This is a free service to trace the email path from the sender's location to recipient's mail server using IP addresses in the email header.

Features:

- Detailed reports and email analytics.
- Real-time alerts on mobile and desktop for all events.
- Automatic email categorization.
- Personalized mail merge campaigns

Sign: _____

Practical – 2:The Sleuth Kit

The sleuth kit is a collection of command line tools and a C library that allows you to analyze disk images and recover files from them. It is used behind the scenes in Autopsy and many other open source and commercial forensics tools.

The Sleuth Kit, also known as TSK, is a collection of UNIX-based command line file and volume system forensic analysis tools. The filesystem tools allow you to examine filesystems of a suspect computer in a non-intrusive fashion. Because the tools do not rely on the operating system to process the filesystems, deleted and hidden content is shown.

The volume system (media management) tools allow you to examine the layout of disks and other media. You can also recover deleted files, get information stored in slack spaces, examine file systems journals, see partitions layout on disks or images etc. But it is very important to clarify that the TSK acts over the current filesystem only.

The Sleuth Kit supports DOS partitions, BSD partitions (disk labels), Mac partitions, Sun slices (Volume Table of Contents), and GPT disks. With these tools, you can identify where partitions are located and extract them so that they can be analyzed with file system analysis tools.

Currently, TSK supports several filesystems, such as NTFS, FAT, exFAT, HFS+, Ext3, Ext4, UFS and YAFFS2.

This package contains the set of command line tools in The Sleuth Kit.

Guymager is a fast and user-friendly forensic imager.

How to install guymager on Ubuntu :

sudo apt-get update

sudo apt-get install guymager

Display Guymager Acquisition File :

cat Filename.info

The **md5sum** is designed to verify data integrity using MD5 (Message Digest Algorithm 5).

MD5 is 128-bit cryptographic hash and if used properly it can be used to verify file authenticity and integrity.

The **md5sum** command displays the file's hash value alongside the filename. The syntax is:

md5sum [filename]

Note: While **md5sum** is a reliable method for testing whether the file you received has been compromised, it is useful only if you know that the website you downloaded it from is secure. If hackers gain access to the website, they can change both the file and its checksum, making it appear as if the file you are downloading is safe.

Read in Binary Mode

To read the file in binary mode, use the -b option (–binary):

md5sum -b [filename]

Read in Text Mode

Use the -t option (–text) to read the file in text mode:

md5sum -t [filename]

Create a BSD-Style Checksum

Using the –tag option outputs the hash value in the BSD-style format:

md5sum --tag [filename]

Validate md5 Checksum with a File

How to install:

sudo apt-get install sleuthkit

To Check version of sleuthkit

mmls -V

Image File Tools

This layer contains tools for the image file format. For example, if the image format is a split image or a compressed image.

img_stat: tool will show the details of the image format

img_cat: This tool will show the raw contents of an image file.

Volume System Tools

These tools take a disk (or other media) image as input and analyze its partition structures. Examples include DOS partitions, BSD disk labels, and the Sun Volume Table of Contents (VTOC). These can be used to find hidden data between partitions and to identify the file system offset for The Sleuth Kit tools.

The media management tools support DOS partitions, BSD disk labels, Sun VTOC, and Mac partitions.

mmls: Displays the layout of a disk, including the unallocated spaces.

mmstat: Display details about a volume system (typically only the type).

mmcat: Extracts the contents of a specific volume to STDOUT.

File System Layer Tools

These file system tools process general file system data, such as the layout, allocation structures, and boot blocks

fsstat: Shows file system details and statistics including layout, sizes, and labels.

File Name Layer Tools

These file system tools process the file name structures, which are typically located in the parent directory.

ffind: Finds allocated and unallocated file names that point to a given meta data structure.

fls: Lists allocated and deleted file names in a directory.

Metadata Layer Tools

These file system tools process the meta data structures, which store the details about a file. Examples of this structure include directory entries in FAT, MFT entries in NTFS, and inodes in ExtX and UFS.

icat: Extracts the data units of a file, which is specified by its meta data address (instead of the file name).

ifind: Finds the meta data structure that has a given file name pointing to it or the metadata structure that points to a given data unit.

Data Unit Layer Tools

These file system tools process the data_units where file content is stored. Examples of this layer include clusters in FAT and NTFS and blocks and fragments in ExtX and UFS.

blkcat: Extracts the contents of a given data unit.

blkls: Lists the details about data units and can extract the unallocated space of the file system.

blkstat: Displays the statistics about a given data unit in an easy to read format.

blkcalc: Calculates where data in the unallocated space image (from blkls) exists in the original image. This is used when evidence is found in unallocated space.

MMLS - Media Management Tools

mmls – displays the layout of the disk

Sign: _____

UNIT - 4

Web Application Tools

4.1 Scanning for web vulnerabilities tools

A vulnerability scanner is a computer program designed to assess computer system,

network or application for weaknesses.

- A web application security scanner is a program which communicates with a web application in order to identify potential security vulnerabilities. It performs a black-box test.
- Unlike source code scanners, web application scanners don't have access to the source code and therefore detect vulnerabilities by actually performing attacks.
- Web applications are highly popular to give an interactive experience on the Internet for users. Provides not only static web pages but is able to create personal accounts, add content, query databases and complete transactions.
- In the process of providing an interactive experience web applications frequently collect, store and use sensitive personal data to deliver their service.
- OpenVAS and Metasploit, which are scanners that check for the presence of known vulnerabilities in web sites in addition to vulns in network devices and operating systems.

4.1.1 Nikto

- The increase in web applications on the internet today raises a security concern because in some cases, security is haphazardly considered during development. As a result we often end up having vulnerable web apps that attackers might exploit user information.
- Nikto is a web application scanner that penetration testers, malicious hackers and web application developers use to identify security issues on web apps.
- Nikto was originally written and maintained by Sullo, CIRT, Inc. it is currently maintained by david lodge, though other contributors have been involved in the project as well.

- It is built to run on any platform which has a perl environment and has been incorporated within the kali linux penetration testing distribution.
- It is an open source tool, supporting ssl, proxies, host authentication, IDS evasion and more, it can be updated automatically from the command - line and supports the optional submission of updated version data back to the maintainers.
- Before installing nikto, you must install basic perl, perl modules, and open ssl on your machine.
- Nikto is completely open source and is written in perl. It runs at the command line without any graphical user interface.

Features of nikto web scanner is as follows:

1. It supports a secure socket layer and HTTP proxy server.
2. It supports text documents , HTML, XML documents.
3. It scans for multiple ports.
4. It can be also scanned on multiple servers by taking inputs from files like nmap output.
5. It is capable enough to identify installed software with header files.

The basic nikto scan requires a simple host to target since port 80 is assumed if none is specified. The host can either be an IP or a host name of a machine and is specified using the -h(-host) option. This will scan the IP 192.168.0.1 on TCP port 80

nikto -h 192.168.0.1 -p 80

nikto -h 192.168.0.1 -p 80 -o results -F txt

4.1.2 W3af - Web Application Attack and Audit Framework

- The web application attack and audit framework (w3af) is an open source framework for auditing and exploitation of web applications.
- You can use w3af to identify over 200 vulnerabilities to reduce your site's risk exposure. The framework is "proudly developed using python and is easy to use and extend", The w3af framework is divided into three main sections.
- The core which coordinates the whole process and provides libraries for using plugins.

- The user interfaces which allow the user to configure and start scans.
- The plugins, which find links and vulnerabilities.
- Black box web application scanning, if we abstract from the details is a simple process:
- Identify all links, forms, query string parameters.
- Send specially crafted strings to each input and analyze the output.
- Generate a report with the findings.

Steps for w3af:

1. w3af
2. w3af_gui

4.2 HTTP utilities

- cURL
- openSSL and stunnel

4.2.1 cURL

- cURL is a computer software project providing a library (Libcurl) and command line tool (cURL) for transferring data using various network protocols which was first released in 1997.
- cURL is a command line tool for getting and sending data including files using URL syntax. cURL supports HTTPS and performs SSL certificate verification by default when a secure protocol is specified such as HTTPS.
- cURL is used in command lines or scripts to transfer data. It is also used in cars, television sets, routers, printers, audio equipment, mobile phones, tablets, setu boxes, media players and is the internet transfer backbone for thousands of software applications affecting billions of humans daily.
- Basic use of cURL involves simply typing curl at the command line, followed by the url of the output to retrieve:
    1. curl --help
    2. man curl
    3. curl www.example.com

4.2.2 openSSL

- openSSL is an open source implementation of the SSL and the TLS protocol.
- The primary goal of the secure socket layer protocol and its successor transport layer security protocol is to provide privacy and reliability between two communicating applications. SSL uses TCP/IP on behalf of the higher level protocols.
- SSL includes two sub protocols : The SSL record protocol and the SSL handshake protocol.
- SSL record protocol defines the format used to transmit data. SSL handshake protocol exchanged messages between SSl server and SSL client.
- openSSL is often used to encrypt authentication of mail clients and to secure web based transactions such as credit card payments. OpenSSL library is the most commonly used open source library for establishing encrypted connections.
- OpenSSL is used for :-
    a. Creating a key for RSA, DSA
    b. Creating X.509 certificate
    c. Message digest calculation
    d. Handling of S/MIME signed
    e. SSL/TLS client and server test
    f. Encryption and decryption with cipher

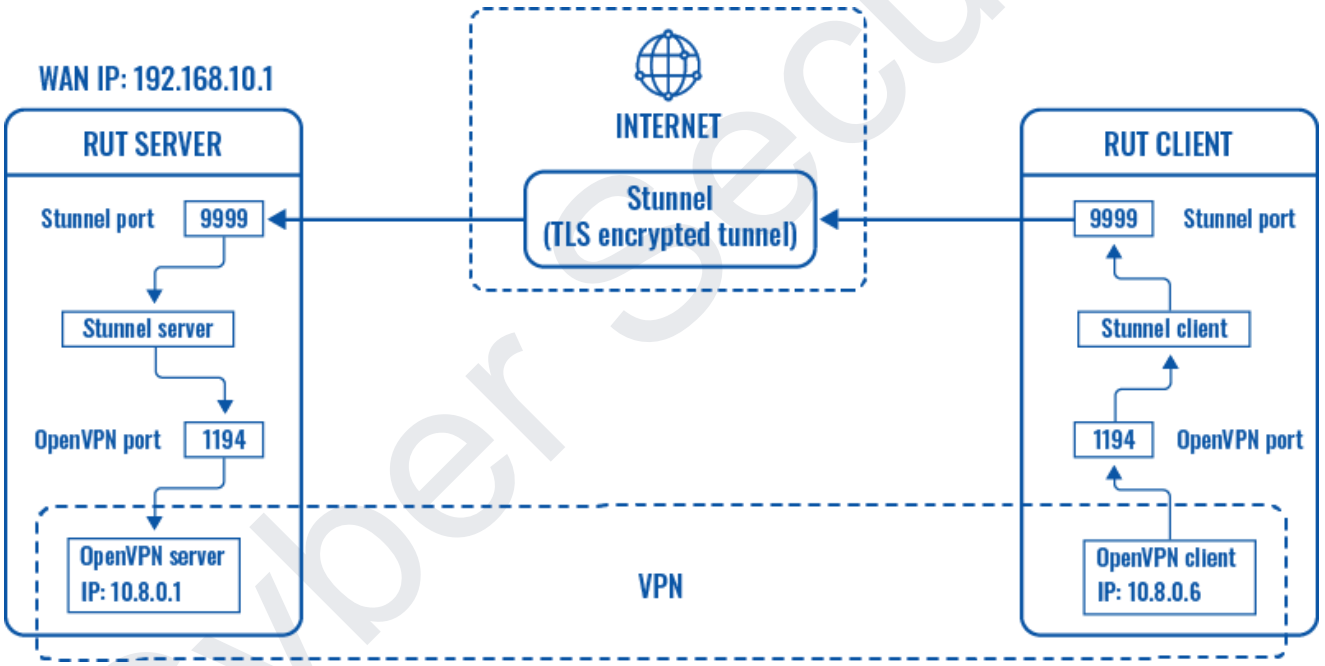
OpenSSL command syntax :

- openSSL command [command_opts][command_args]

Sr.no	Commands	Remarks
1.	ca	Management of certificate authority
2.	cipher	Cipher suite description determination
3.	crl	Certificate revocation list management
4.	dgst	Message digest calculation
5.	dh	Deffie hellman data management
6.	dsa	DSA data management
7.	enc	Encoding with cipher
8.	rsa	RSA data management
9.	passwd	Generation of hashed password

4.2.3 Stunnel

- Stunnel is an open source multi - platform application used to provide a universal TLS/SSL tunneling service. Stunnel can be used to provide secure encrypted connection for clients or servers.
- Stunnel means secure tunnel between TCP applications. The stunnel program is designed to work as an SSL encryption wrapper between remote clients and local or remote server. The concept is that having non-SSL demons running on your system you can easily set them up to communicate with clients over secure SSL channels.
- Stunnel is for managing the connection of internet message access protocol to provide encrypted email access.



- Stunnel is installed on server and client machines using the following command.
    - $ apt-get install stunnel
- The configuration file is held /etc/stunnel under the name of stunnel.config file. There is no graphical user interface for configuration stunnel; all configuration must be done with the stunnel.config configuration file. After installation, you must create a certificate. A default certificate is provided with a stunnel.
    - $openssl req -new-key server.key - out server.csr

- Keep the server.key secret.send the server.crs to your certificate authority. Two things are important when generating certificate-key pairs for a stunnel.
- The private key cannot be encrypted, because the server has no way to obtain the password from the user. To produce an encrypted key add the nodes option when running req command from the openSSL.
- Command to startup stunnel : $ rct Command to startup stunnel :
- Command to p stunnel at boot time : chkconfig stunnel on
- The most common use of stunnel is to listen on a network port and establish communication with either a new port via the connect option or a new program via exec option.

4.3 ApplicaHTTP utilitiestion inspection tools

- Zed Attack Proxy
- SQLMAP

4.3.1 Zed Attack Proxy

- Zed attack proxy is an open source security software written in java programming language and released in 2010.
- It is used to scan web applications and find vulnerability in it. It was started as a small project by open web application security project (OWASP) and now it is the most active project maintained by thousands of individuals around the globe.
- It is available for linux, windows and mac in 29 languages. It can also be used as a proxy server like burp suite to manipulate the request including the https request.
- ZAP provides a basic port scanner which shows ports are open on the target sides. It also provides an application programming interface (API) which allows you to interact with zap programmatically. The API is available in json, HTML and XML formats.
- **Features** :-
    - Passive scanner
    - Automated scanner

    - Proxy server
    - Port identification
    - Directory searching
    - Brute force attack
    - Web crawler
- Why do we use the Zed Attack proxy?
- Zed attack proxy is used to detect vulnerabilities present on any web server and try to remove them. Here are some big vulnerabilities that could be present in the web server.
    - SQL Injection
    - Cross - site scripting (XSS)
    - Broken access control
    - Security - misconfiguration
    - Broken authentication
    - Sensitive data exposure
    - Cross site request forgery (SRF)
    - Using components with known vulnerabilities
- Important terminologies
    - **Proxy server :** it is a server which acts as mediator for clients who want to go through the request and want to go through the request and want to alter them.
    - **Spider :** it is a type of information gathering process in which the application in this case ZAP will go through the whole web page and try to find out all the links and other important details.
    - **Passive scan :** in this type of scanning the vulnerability is detected without getting in direct contact with the target machine.
    - **Active scan :** in this the vulnerability is detected by getting in direct contact with the target machine which makes it very easy to be detected by the administrator.

4.3.2 SQL map

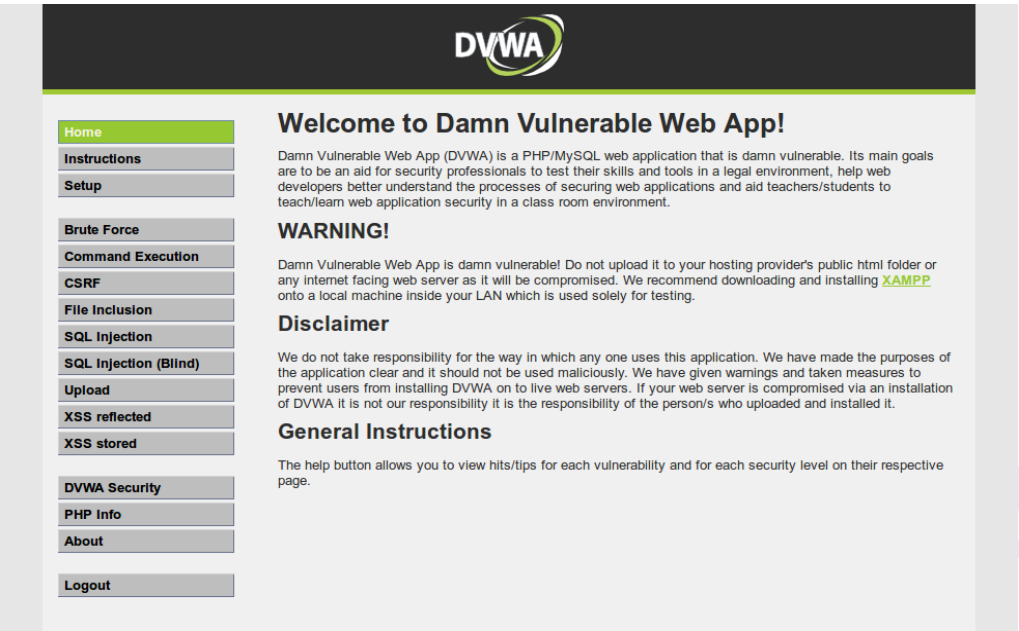
- sqlmap's goal is to detect and take advantage of SQL injection vulnerabilities in web applications.
- SQL injection vulnerabilities are caused by software applications that accept data from an untrusted source. Sqlmap can use SQL injection to retrieve information about all of the database users and their permissions and stored password hashes.
- Sqlmap is a Python-based open source penetration testing tool. It uses a command-line user interface. Sqlmap automates the detection and exploitation of SQL injection vulnerability.
- You can download the sqlmap from http://www.sqlmap.org
- Sqlmap gives full support for six SQL injection techniques : boolean-based blind, time-based blind, error-based, UNION query-based, stacked queries and out-of-band.
- Sqlmap will attempt injection attacks on all of the input fields it finds at the specified URL. If you add " --dbs " options then it causes an attempt to discover what databases are used, which can help to identify other applications running on the machine that can be targeted.
- Syntax of Sqlmap command :

  $query = "SELECT [column name(s)] FROM [table name] WHERE id=" . $_REQUEST[id];

- Sqlmap is able to detect any type of SQL injection flaw and adapt its work flow accordingly. Sqlmap tool will automatically s:
  a. Identify the vulnerable parameters.
  b. Identify which SQL injection techniques can be used to exploit the vulnerable parameter(s).
  c. Fingerprint the back-end database management system.
- A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and recover the content of a given file present on the DBMS file system and in some stem. cases issue commands to the operating system.

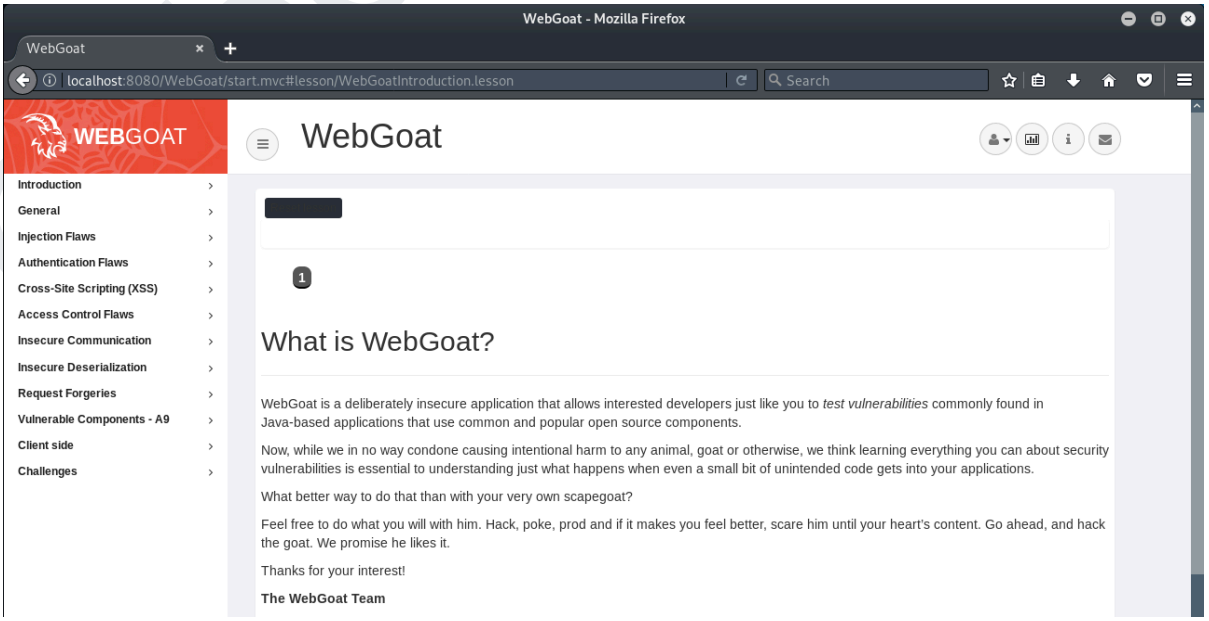
4.3.3 DVWA - Damn Vulnerable Web App

- DVWA is a PHP/MySQL web application, whose main goal is to be an aid for security professionals to test their skills and tools in a legal environment.
- As the name suggests DVWA has many web vulnerabilities. Every vulnerability has four different security levels, low, medium, high and impossible. The security levels give a challenge to the 'attacker' and also shows how each vulnerability can be counter-measured by secure coding.
- Impossible: In this level, you will face challenges like CTF and it is harder than the other level. This level gives difficulties that we face in the real world.
- High: This vulnerability level gives the user an example of how to secure the vulnerability via secure coding methods. It lets the user understand how the vulnerability can be counter-measures. This level of security should be unhackable however as we all know this is not always the case. So if you manage to bypass it, that you are doing right.
- Medium: This security level's purpose is to give the 'attacker' a challenge in exploitation and also serve as an example of bad coding/security practices.
- Low: This security level is meant to simulate a website with no security at all implemented in their coding. It gives the 'attacker' the chance to refine their exploitation skill.
- **In DVWA we can test various different kinds of Vulnerabilities.**
    a. BRUTE FORCE
    b. COMMAND INJECT
    c. Cross-Site Request Forgery (CSRF)
    d. FILE UPLOAD
    e. INSECURE CAPTCHA
    f. SQL INJECTION
    g. SQL INJECTION BLIND
    h. WEAK SESSION IDs
    i. XSS(DOM)



4.3.4 WebGoat

- WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components.
- You can start WebGoat on port 80 with the following command:
    - sh webgoat.sh start80
- If you are running an Apache server or any other process on TCP port 80, you can start WebGoat on TCP port 8080.



4.4 Password cracking and Brute-Force Tools

What is Password Cracking?

- Password cracking is the process of guessing or recovering a password from stored locations or from data transmission systems. It is used to get a password for unauthorized access or to recover a forgotten password.
- Most of the password cracking tools try to login with every possible combination of words. If login is successful, it means the password was found. If the password is strong enough with a combination of numbers, characters and special characters, this cracking method may take hours to weeks or months.

What is Brute-Force ?

- Brute-Force attack is a method of breaking a cipher by trying every possible key. Feasibility of brute force attack depends on the key length of the cipher, and on the amount of computational power available to the attacker.
- A Brute force attack is an automated process of trial and error used to guess a person's username, password, credit-card number or cryptographic key. Insufficient authentication occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate. Weak password recovery validation is when a website permits an attacker to illegally obtain, change or recover another user's password.

4.4.1 John the Ripper

- John the Ripper is a fast password cracker, currently available for many flavors of UNIX, Windows and OpenVMS. Its primary purpose is to detect weak UNIX passwords. It can use specialized wordlists or password rules based on character type and placement.
- Website : **www.openfirewall.com**
- Download the Windows binary of john the ripper from http://www.openwall.com/john/g/john179j5w.zip
- John the Ripper is a command line tool. A dictionary attack uses a word database, and tries it repeatedly. John the Ripper has this capability.

- John will accept three different password file formats. It is encrypted in one of the formats listed by the "-test" option.
- John the Ripper supports the following cracking modes :
    1. Wordlist with or without rules;
    2. "Single crack", makes use of the login information;
    3. Incremental, tries all character combinations;
    4. External, allows you to define your own cracking mode.
- John the Ripper comes pre-installed with a small dictionary of some typical passwords located in the "/usr/share/john/password.lst" file.
- John automatically selects the correct encryption algorithm for the hashes and begins cracking. All the cracked passwords are saved in the John.pot file, which is a text file. This tool used for brute force is called "Incremental". In incremental mode john does not use a word list, but just tries all possible passwords.
- While cracking, you can press the Enter key for status, or Ctrl+C to abort the session, saving point information to a file. By the way, if you press Ctrl+C twice John will abort immediately without saving.

Cracking Modes

1. **Wordlist mode :** User must specify a wordlist and some password files.
2. **Single crack mode :** It will try using the login information as passwords. This mode is much faster than the wordlist mode, which allows using a lot of rules in a reasonable time.
3. **Incremental mode :** This is the most powerful cracking mode, it can try all possible character combinations as passwords.
4. **External mode :** You can define an external cracking mode for use with John. This is done with -/john.ini's sections called [List.External:<mode>], where <mode> is any identifier that you assign to the mode. The section should contain some functions that John will use to generate the words it tries. These functions are coded in a subset of the C language, and are compiled by John at startup.

- **John Ripper Command Line Options**

Sr.No	Command	Remark
1	word file	Set to your wordlist file name.
2	Timeout	Set to the value in minutes.
3	Beep	Set to something starting with 'Y' or 'N' to specify whether to beep when a password is found or not

4.4.2 L0PHTCRACK

- This tool used to crack Windows NT/2000 passwords. Easy to use GUI interface. It runs on MS Windows 9x, NT and 2000 systems.
- Windows stores passwords in the Security Accounts Manager (SAM). It is a binary file that is difficult to read without special tools.
- Not only will LOphtCrack guess passwords, it will extract LANMan hashes from any SAM file, the local system or a remote system and it will even sniff hashes as they cross a network. The SAM file is stored in the **\WINNT\system32\config** directory.
- LOphtCrack will extract passwords from the local or remote computers with the dump passwords from registry option.
- Attackers must get a copy of the encrypted/hashed password representations stored in the SAM database of the target machine. LOphtCrack includes a "pwdump" tool for dumping Windows NT password representation from a local or remote machine across the network. Requires administrator privileges on the target machine.

4.4.3 Pwdump

- Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is also capable of displaying password histories if they are available. It outputs the data in LOphtcrack-compatible form, and can write to an output file.
- This tool was written by Jeremy Allison in the year 1997.

- It only affects Windows XP/2000 computers, and it is used in order to dump Users and password hash tables in local or remote Windows XP/2000 computers. These hash tables allow brute force password cracking in order to try to guess the original values of the user names and passwords associated and dictionary attacks.
- Download one of the pwdump files www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7.
- Login as system admin to windows machine and then run following command at command prompt **C:\> pwdump7>c:\hash.txt** pwdump7 will dump the SAM to the screen and the > character redirects the output to a file called hash.txt
- Syntax : **pwdump [-h][-o][-u][-p] machineName**

where

-h	Prints the usage message and exits
-o	Specifies a file to which to write the output
-u	Specifies the user name used to connect to the target
-p	Specifies the password used to connect to the target
-s	Specifies the share to be used on the target, rather than searching

4.4.3 THC-Hydra

- THC Hydra is another classic password cracking tool. Strictly speaking Hydra is a network logon password cracking tool, which is actually very fast. It can perform rapid dictionary attacks against more than 30 protocols,including TELNET, FTP, HTTP, HTTPS, SMB etc.
- Hydra tries all possible password combinations against a server on the Internet until one valid one is found to log in to the server. It is a powerful tool for hackers and network administrators alike.
- You can download from http:// www.thc.org/thc-hydra/
- Hydra also has a special command line option: Use "-e ns" empty passwords and where the password is the username.