Practical.No 1 : Footprinting and Reconnaissance:

Aim : Using the software tools/commands to perform the following , generate an analysis report :

A) To perform footprinting using Google Hacking .

Description :

Footprinting is an ethical hacking technique used to gather as much data as possible about a specific targeted computer system, an infrastructure and networks to identify opportunities to penetrate them. It is one of the best methods of finding vulnerabilities.

The process of cybersecurity footprinting involves profiling organizations and collecting data about the network, host, employees and third-party partners. This information includes the OS used by the organization, firewalls, network maps, IP addresses, domain name system information, security configurations of the target machine, URLs, virtual private networks, staff IDs, email addresses and phone numbers.

There are two types of footprinting in ethical hacking:

1. active footprinting

2. passive footprinting

Aim : Using the software tools/commands to perform the following , generate an analysis report :

B) To find out the information about a website

Description :

Website footprinting is the technique which is used to extract the details

related to website. When we are browsing any website or any target website, we may provide this information

- Whose website (name, contact number, emails etc)
- Which software used? Version of that software.
- Operating system details
- Domains details
- Sub-domain details.
- Scripting platform
- File name and file path

When hacker wants to get details information about any website, it may be

1) Achieved the description of website
2) Content Management system and framework
3) Web Crawling
4) Script and platform of website and web server
5) Extract metadata and contact details from website.
6) Website and web page monitoring and analyzer

Whois is the tool which is used to renowned internet record listing to identify the who owns a domain or who registered that domain and contact details.

Aim : Using the software tools/commands to perform the following , generate an analysis report :

C) To find the information about an archived website

Description :

To extract contents of a website:

Web Data Extractor pro is web scraping tool designed for mass gathering different data types. With the help of web data extractor, you can custom extraction structured data.

Start with the new project then type in URL then click on meta tag.

Aim : Using the software tools/commands to perform the following , generate an analysis report :

D) To fetch DNS information.

Description :

DNS means Domain Name System is system which allows us to convert Computer IP address into human readable domain name. Basically, DNS footprinting is used to gather information about DNS zone data. Attackers use DNS information to determine key hosts in the network

Practical.No 2 : Scanning networks, Enumeration and sniffing:

Aim : Using the software tools/commands to perform the following , generate an analysis report :

A. Port scanning .

Description :

Port scanning is a method of determining which ports on a network are open and could be receiving or sending data. It is also a process for sending packets to specific ports on a host and analyzing responses to identify vulnerabilities.

This scanning can't take place without first identifying a list of active hosts and mapping those hosts to their IP addresses. This activity, called host discovery, starts by doing a network scan.

The goal behind port and network scanning is to identify the organization of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels. Both network and port scanning can reveal the presence of security measures in place such as a firewall between the server and the user's device.

After a thorough network scan is complete and a list of active hosts is compiled, port scanning can take place to identify open ports on a network that may enable unauthorized access.

Nmap Tool: Nmap is a free, open source and multi-platform network security scanner used for network discovery and security auditing. Nmap can be extremely useful for helping you get to the root of the problem you are investigating, verify firewall rules or validate your routing tables are configured correctly.

Aim : Using the software tools/commands to perform the following , generate an analysis report :

B. Network scanning tools

Description : Network scanning consists of network port scanning as well as vulnerability scanning.

Network port scanning refers to the method of sending data packets via the network to a computing system's specified service port numbers (for example, port 23 for Telnet, port 80 for HTTP and so on). This is to identify the available network services on that particular system. This procedure is effective for troubleshooting system issues or for tightening the system's security.

Vulnerability scanning is a method used to discover known vulnerabilities of computing systems available on a network. It helps to detect specific weak spots in an application software or the operating system (OS), which could be used to crash the system or compromise it for undesired purposes.

Network port scanning as well as vulnerability scanning is an information-gathering technique, but when carried out by anonymous individuals, these are viewed as a prelude to an attack.

Network scanning processes, like port scans and ping sweeps, return details about which IP addresses map to active live hosts and the type of services they provide. Another network scanning method known as inverse mapping gathers details about IP addresses that do not map to live hosts, which helps an attacker to focus on feasible addresses.

Network scanning is one of three important methods used by an attacker to gather information. During the footprint stage, the attacker makes a profile of the targeted organization. This includes data such as the organization's domain name system (DNS) and e-mail servers, in addition to its IP address range. During the scanning stage, the attacker discovers details about the specified IP addresses that could be accessed online, their system architecture, their OSs and the services running on every computer. During the enumeration stage, the attacker collects data, including routing tables, network user and group names, Simple Network Management Protocol (SNMP) data and so on.

Nmap Tool: Nmap is also used to scan networks. Nmap is now one of the core tools used by network administrators to map their networks. The program can be used to find live hosts on a network, perform port scanning, ping sweeps, OS detection, and version detection.

Ping Scan – It returns a list of hosts on your network and the total number of assigned IP addresses. If you spot any hosts or IP addresses on this list that you cannot account for, you can then run further commands to investigate them further.

Host Scan – Unlike a ping scan, a host scan actively sends ARP request packets to all the hosts connected to your network. Each host then responds to this packet with another ARP packet containing its status and MAC address. This can be a powerful way of spotting suspicious hosts connected to your network.

OS Scan – This command returns information on the OS (and version) of a host.

Aim : Using the software tools/commands to perform the following , generate an analysis report :

D. Sniffing tool

Description :

Wireshark: Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows. There is also a terminal-based (non-GUI) version called TShark. Wireshark is used to capture and analyse packets in network. It is also used as a sniffer, network protocol analyzer, and network analyser. We can also apply specific filter on network traffic to get more filtered data packets.

Practical.No 3 : Malware Threats : Worms, viruses, Trojans:

Aim : Using the software tools/commands to perform the following , generate an analysis report :

A. Password cracking.

Description :

Password cracking is the process that involves computational methods to guess or retrieve a password from stored or transmitted data, typically employing algorithms executed by a computer. It is often used by hackers or malicious actors to gain unauthorized access to a target computer system or online account by guessing or cracking the password. It can be accomplished for several reasons, such as gaining access to sensitive information, stealing data or resources, conducting espionage, or carrying out malicious activities. Security professionals also use this method to test the strength of passwords and identify vulnerabilities in a system's security. However, in most cases, password cracking is done with malicious intent and is considered illegal and unethical.

Aim : Using the software tools/commands to perform the following , generate an analysis report :

B. Dictionary attack.

Description :

Dictionary search attack: In this method, the attacker uses a list of commonly used words or phrases, also known as a dictionary, to guess the password. The attacker uses a software program that automatically tests each word in the dictionary list against the password field of the target account.

Benefits:

Faster than brute force attacks

Can crack simple passwords

Uses a pre-existing list of common passwords

Drawbacks:

Limited to common passwords

Ineffective against strong passwords

Cannot crack passwords that are not in the dictionary

Aim : Using the software tools/commands to perform the following , generate an analysis report :

C. DoS attack.

Description : Denial of Service (DoS) is a cyber-attack on an individual Computer or Website with the intent to deny services to intended users. Their purpose is to disrupt an organization's network operations by denying access to its users. Denial of service is typically accomplished by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. For example, if a bank website can handle 10 people a second by clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no legitimate users can log in. DoS attacks exploit various weaknesses in computer network technologies. They may target servers, network routers, or network communication links. They can cause computers and routers to crash and links to bog down. The most famous DoS technique is the Ping of Death. The Ping of Death attack works by generating and sending special network messages (specifically, ICMP packets of non-standard sizes) that cause problems for systems that receive them. In the early days of the Web, this attack could cause unprotected Internet servers to crash quickly. It is strongly recommended to try all described activities on virtual machines rather than in your working environment.

Aim : Using the software tools/commands to perform the following , generate an analysis report :

D. ARP poisoning in windows.

Description : ARP or Address Resolution Protocol is one of the most essential protocol layers in the OSI model. whenever a device wants to communicate with any other device in a local area network, our protocol comes into play. ARP protocol lets devices communicate with each other by translating the MAC address of the device with its IP address and vice versa. There are two identifiers to identify devices on a network.

IP addresses (logical addresses) are used to identify devices on a wide-area network (Internet).

MAC addresses (Physical addresses) are used to identify devices on a local area network.

ARP Cache: It is an ARP table or a collection of ARP entries that every network-connected device maintains. ARP Cache is created whenever a device's MAC address is mapped with its local IP address. Devices use the ARP cache to avoid redundant address resolution requests. but this Cache can be poisoned (Using ARP Spoofing) here the term "poisoned" basically means a fake MAC address associated with an IP address. this leads to the man-in-the-middle attack where data can be intercepted, modified, dropped, or stopped.

ARP Spoofing: ARP Spoofing, also referred to as ARP Cache Poisoning as we discussed earlier. it is a type of malicious attack in which the attacker sends a fake ARP message over a local network in order to link the attacker's MAC address with the IP address of another device on a local area network to achieve a malicious attack. If an attacker can manage the linking of the MAC address of his/her device with the IP address of any other device on a local area network, this linking leads to ARP Poisoning and allows an attacker to carry out several malicious tasks such as intercepting network traffic, modify, and even stop or dropped the data in-transit by putting an attacker in the middle of the communication of the devices (Man In The Middle Attack).

Man-in-the-Middle (MIM) Attack: ARP Spoofing also known as ARP Poisoning is the Man-in-the-Middle (MIM) Attack. In this type of attack, the attacker secretly intercepts and, in some cases, alters the communication between two parties

without their knowledge. ARP Spoofing serves as the means to achieve this interception.

- ARP Poisoning: ARP Poisoning is a wider term that contains both ARP Spoofing and ARP Cache Poisoning. It describes any form of malicious manipulation of ARP messages to compromise network security. This manipulation can involve either redirecting network traffic or spying on network communications.

- Packet Sniffing: Packet Sniffing is a passive network monitoring technique where an attacker captures data packets as they travel through the network. ARP Spoofing is often used to facilitate packet sniffing, allowing the attacker to grab sensitive information.

ARP Spoofing can have severe consequences, including:

1. Data Interception: Attackers can intercept sensitive data, such as login credentials or financial information.

2. Data Modification: It can allow attackers to modify data packets in transit, leading to potential data corruption.

3. Denial of Service (DoS): In some cases, ARP Spoofing can disrupt network connectivity for legal users.

Basic terms	ARP Spoofing	ARP Poisoning
Focus	The main focus of ARP Spoofing is to intercept or modify network traffic within a LAN(Local area network)	ARP Poisoning is a wider term that contains both ARP Spoofing and ARP Cache Poisoning.
Outcome	In ARP Spoofing, the attacker sends false ARP messages to mislead devices on the network into associating their MAC address with a legal IP address. This manipulation allows the attacker to intercept or modify data packets intended for the target IP address.	While ARP Poisoning includes ARP Spoofing, it also covers other ARP-related attacks, such as ARP Cache Poisoning. ARP Poisoning can involve either redirecting network traffic or spying on network communications.

purpose ARP Spoofing is often a component of Man-in-the-Middle (MIM) attacks, where the attacker secretly intercepts and potentially alters the communication between two parties without their knowledge. ARP Poisoning is used as a general term to describe any form of malicious ARP message manipulation aimed at compromising network security.

Aim : Using the software tools/commands to perform the following , generate an analysis report :

F. Steganography tools.

Description :

A steganography technique involves hiding sensitive information within an ordinary, non-secret file or message, so that it will not be detected. The sensitive information will then be extracted from the ordinary file or message at its destination, thus avoiding detection. Steganography is an additional step that can be used in conjunction with encryption in order to conceal or protect data.

Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. It comes from the Greek words steganos, which means “covered” or “hidden,” and graph, which means “to write.” Hence, “hidden writing.”

You can use steganography to hide text, video, images, or even audio data. It’s a helpful bit of knowledge, limited only by the type of medium and the author’s imagination.

Different Types of Steganography

1. Text Steganography − There is steganography in text files, which entails secretly storing information. In this method, the hidden data is encoded into the letter of each word.

2. Image Steganography − The second type of steganography is image steganography, which entails concealing data by using an image of a different object as a cover. Pixel intensities are the key to data concealment in image steganography.

Since the computer description of an image contains multiple bits, images are frequently used as a cover source in digital steganography.

The various terms used to describe image steganography include:

- Cover-Image - Unique picture that can conceal data.
- Message - Real data that you can mask within pictures. The message may be in the form of standard text or an image.
- Stego-Image – A stego image is an image with a hidden message.
- Stego-Key - Messages can be embedded in cover images and stego-images with the help of a key, or the messages can be derived from the photos themselves.

3. Audio Steganography – It is the science of hiding data in sound. Used digitally, it protects against unauthorized reproduction. Watermarking is a technique that encrypts one piece of data (the message) within another (the "carrier"). Its typical uses involve media playback, primarily audio clips.

4. Video Steganography – Video steganography is a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform (DCT) is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI.

5. Network or Protocol Steganography – It involves concealing data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object. Steganography can be used in the case of covert channels, which occur in the OSI layer network model.

Practical 4. Developing and implementing malwares ::

Aim : Developing and implementing malwares

A. Creating a simple keylogger in python.

Description : Key loggers also known as keystroke loggers, may be defined as the recording of the key pressed on a system and saved it to a file, and the that file is accessed by the person using this malware. Key logger can be software or can be hardware. Working: Mainly key-loggers are used to steal password or confidential details such as bank information etc. First key-logger was invented in 1970's and was a hardware key logger and first software key-logger was developed in 1983.
1. Software key-loggers : Software key-loggers are the computer programs which are developed to steal password from the victims computer. However key loggers are used in IT organizations to troubleshoot technical problems with computers and business networks. Also Microsoft windows 10 also has key-logger installed in it.

1. JavaScript based key logger – It is a malicious script which is installed into a web page, and listens for key to press such as oneKeyUp(). These scripts can be sent by various methods, like sharing through social media, sending as a mail file, or RAT file.

2. Form Based Key loggers – These are key-loggers which activates when a person fills a form online and when click the button submit all the data or the words written is sent via file on a computer. Some key-loggers works as a API in running application it looks like a simple application and whenever a key is pressed it records it.

2. Hardware Key-loggers : These are not dependent on any software as these are hardware key-loggers. keyboard hardware is a circuit which is attached in a keyboard itself that whenever the key of that keyboard pressed it gets recorded.

1. USB keylogger – There are USB connector key-loggers which has to be connected to a computer and steals the data. Also some circuits are built into a keyboard so no external wire i used or shows on the keyboard.

2. Smartphone sensors – Some cool android tricks are also used as key loggers such as android accelerometer sensor which when placed near to the keyboard can sense the vibrations and the graph then used to convert it to sentences, this technique accuracy is about 80%. Now a days crackers are using keystroke logging Trojan, it is a malware which is sent to a victims computer to steal the data and login details.

Aim : Developing and implementing malwares

B. Creating a virus.

Description :

A virus is a program that can infect other programs by modifying them. The modification includes a copy of the virus program which then goes on to infect other programs. Virus are self-replicating and can wreak havoc in a system by modifying or destroying files and causing system crashing and program malfunction.

Aim : Developing and implementing malwares

C. Creating a trojan.

Description : The name of the Trojan Horse is taken from a classical story of the Trojan War. It is a code that is malicious in nature and has the capacity to take control of the computer. It is designed to steal, damage, or do some harmful actions on the computer. It tries to deceive the user to load and execute the files on the device. After it executes, this allows cybercriminals to perform many actions on the user's computer like deleting data from files, modifying data from files, and more.

Practical 5. Hacking web servers, web applications:

Aim : Hacking web servers, web applications:

A. Hack a website by Remote File Inclusion

Description : Remote File Inclusion (RFI) is a type of vulnerability most often found on the suited PHP running web portals be on the web and the Local File

Inclusion (LFI) is similar to RFI, the only difference is that in LFI, the attacker has been uploading the malicious scripts types.

Remote File Inclusion (RFI) is a type of vulnerability found in PHP running websites or web servers. The RFI is enabling an attacker to include the remotely hosting file however through scripting on the website servers and vulnerability occurring due to usage of its user-supplied user input without final validations through it.

The remote file inclusion (RFI) is the attacker's targeted code for the malware attack in website server applications that reference outer external scripts. The perpetrator's aim is to exploit the reference function in an application to upload malware(i.e. as backdoor shells) from a remote URL located within a different domain as RFI vulnerability exists in a website or web application, an attacker can include malicious external files that run by website or website applications

In RFI attacks, third party hackers employ scripting to include likewise remotely hosting files on the web portals. In an LFI attack, a hacker used to target local files to execute the malicious harmful scripts

In Remote File Inclusion RFI attacks, hackers take the merits of the "dynamic file including" commands that are in such website/ web portal applications to send malicious external files or scripts to it. When website applications allow user input, such as URL, parameters passing value, etc. and passing to the "file including" steps without having proper validation on it, thus harmful perpetrators can be excluding the website's browsing application to include remote files with harmful scripts, LFI detects the harmful threats like actors using a local file that is stored on the target server, RFI attack, they using the file from external server resources.

This malicious malware file execution of attacks can be done with Blacklisting as well as Code fixing within it.

1. The perpetrator can be executing malicious code from an external source instead of accessing a file on the local web servers, as is the case with an LFI attack

2. The goal is to exploit the insecurity of local files uploaded on functions that fail to validate user-supplied/controlled inputs

Aim : B. Disguise as Google Bot to view Hidden Content of a Website

Description : A Bot or internet bot or web robot in technology is a software application that does certain automated tasks. They run on their scripts and don't require a human user to start them. Generally, bots perform that tasks are simple and repetitive but can be also used for complex tasks. The bot is automated that's why they have much faster execution than that of a person.

Type of Bots :

Bots can be chatbots, web crawlers, social bots, malicious bots, etc.

Chatbots –

A chatbot is a bot used in the chat conversation. These bots replace humans and show human behavior. The earliest chatbot Eliza was programmed in 1964 and answered some very simple decision tree questions. Today there are a number of Chatbots present. For e.g. – Siri, Google Assistant, Alexa, Cortana, etc. These chatbots are highly AI (Artificial Intelligence) programmed chatbots that can do much more complex tasks than simple ones. They are there for making our life a little easier. They take care of you by reminding you to take an umbrella if it's going to rain or to remind someone's birthday. From showing booked tickets to pending bills or maybe chatting with customer care also.

Web crawlers –

Web crawlers or also called web spiders. These are the bots that scan the webpages all over the internet and browse the web for indexing webpages and the content in that webpages. They are also used in data mining. Google is most known for its web crawler Googlebot. There are many web crawlers present such as- Baidu Spider, GoogleBot, Scraper, WebHarvy, Alexa Crawler, Yandex Bot, etc. Bots are mostly used in web crawling. Roughly more than half of web traffic is due to bots. All bots work on some input from the user and respond accordingly. They typically search for keywords or any data for responding with an accurate and precise output.

Social bots –

These are the bots that are present in social media sites but unlike chatbots, their tasks are simple, following someone or some page on social media or taking polls or influencing, etc. They can be used to work on a large scale without requiring much effort.

Malicious bots –

There are a number of bots present which are present in many forms and can steal user data or hack social media accounts, spread fake news, can make someone popular or damage someone's reputation, or can infect the user system by unknowingly downloading files in the user system or by any means.

Aim : C. How to use Kaspersky for Lifetime without Patch.

Description :

Quick Start Guide

Read this Quick Start Guide to get started with Kaspersky Endpoint Security Cloud. The Guide contains tips for managing the accounts of your users and installing security applications on their devices.

Quick start scenario

After you complete the scenario, the devices in your organization will be protected. The scenario proceeds in stages:

1. Create an account.

To start using Kaspersky Endpoint Security Cloud, you need an account on Kaspersky Business Hub.

To create an account:

1. Open your browser and enter the following URL: https://cloud.kaspersky.com.

2. Click the Create an account button.

3. Follow the onscreen instructions.

2. Create a workspace.

After you create the account, you can create your first workspace. We recommend that you first create one test workspace, connect your own devices to it, and then test any modifications to the settings, noting the results.

We recommend that you create a separate workspace for each company that you manage, even if a company has only a few users. By doing this, you will be able to do the following:

1. Change settings for each company individually.

2. Keep track of the license count, and the increase or decrease of the number of users in the company.

3. Assign administrator rights to a user within the company, who can access only that company's workspace.

To create a company workspace:

4. Open your browser and enter the following URL: https://cloud.kaspersky.com.

5. Click the Sign in button.

6. Follow the onscreen instructions.

3. Perform initial setup of Kaspersky Endpoint Security Cloud.

After you create a company workspace, you must perform initial setup of Kaspersky Endpoint Security Cloud. The initial setup begins automatically when you start Kaspersky Endpoint Security Cloud Management Console for the first

time. The Welcome to Kaspersky Endpoint Security Cloud window is displayed. Follow the onscreen instructions.

When initial setup is complete, Kaspersky Endpoint Security Cloud Management Console is ready to use.

4. Deploy security applications on your users' devices.

When your first workspace is prepared, follow the main setup steps provided in the Information panel → Getting started section. These steps include adding user accounts, connecting devices to Kaspersky Endpoint Security Cloud, and creating a certificate for iOS devices.

These steps are divided into three groups:

1. Preconfigured

You already took these steps when you created the workspace.

2. Required

You must take this step to start protection of the devices.

Add users by providing their email addresses. An invitation is sent to the email address and it contains the download link to the security application. When the user clicks the link, Kaspersky Endpoint Security Cloud recognizes the device operating system, thus ensuring that the proper software is downloaded.

As an alternative, you can simultaneously protect multiple devices that are running Windows. To do this, you can deploy security applications by using a Group Policy script.

3. Recommended

We recommend that you take these steps to enhance the protection of devices.

1. Once the software has been downloaded and installed on the device of the user, assign the user as the device owner.

2. Create an Apple Push Notification service (APNs) certificate. The APNs certificate is created in one run. You must follow the steps for its creation without interruption, because the signing process has a time stamp that will expire if the creation process takes too long.

5. Manage protection.

After the security application is installed on a device, the device is assigned the Default security profile. This is the security profile with the default settings that are recommended by Kaspersky experts.

In the Security management → Security profiles section, you can create different security profiles. Every new security profile holds the default settings until you modify them. You can also copy existing security profiles.

Each security profile holds four tabs for the respective platforms: Windows, macOS, Android, and iOS.

When you assign a security profile to a user, the security profile is applied to all devices owned by the user. Only the Default security profile can be applied to devices without owners.

When creating a security profile, take into consideration the organizational structure of the company that you manage. For example, the security profile for a developer may differ from the one used for a sales representative or a human resources assistant. Name each security profile accordingly.

We recommend that you prevent users from modifying or deleting the security applications installed on their devices. Therefore, define the following settings:

1. For Windows devices, do the following:

1. On the Windows → Advanced → Interaction with end users tab, make sure that Password protection is enabled.

2. Select the operations that a user will be allowed to perform only with the password.

2. For Mac devices, do the following:

1. On the Mac → Advanced → Interaction with end users tab, choose whether you want the Kaspersky Endpoint Security for Mac application icon visible on the menu bar or not.

2. On each device in system preferences, use the macOS account type settings (admin or standard user) and the "lock" icon ( ) to prevent the user from removing the software.

3. For Android devices, do the following:

1. On the Android → Security settings tab, make sure that Screen lock is enabled to protect the device from unauthorized access.

2. On the Advanced tab, make sure that Kaspersky Endpoint Security for Android cannot be removed.

4. For iOS devices: on the iOS → Security settings tab, make sure that Screen lock is enabled to protect the device from unauthorized access.

After defining the required settings of security profiles, you can assign security profiles to the intended users.

6. Specify licenses.

After you have created a workspace, you are granted a 30-day trial license that is embedded in your workspace. To continue using Kaspersky Endpoint Security Cloud after the trial license expires, you must purchase a commercial license or a subscription. Click Information panel → License, and then enter the activation code.

The activation code will be distributed automatically to the security applications, which may take 15 minutes, as the applications attempt to sync with the workspace every 15 minutes.

7. Define other settings (optional).

You can define other optional settings.

1. By default,

background scan

is enabled for devices running Windows. Autorun objects, system memory, and the system partition are scanned when the device is idling for five or more minutes. If you want, you can click the Settings tab and set the schedule for the malware scan. From the Devices tab, you can start the malware scan task.

2. The security applications mostly use the Kaspersky Security Network cloud service in their operation and to a lesser extent the application's anti-malware databases. If you want, you can click the Settings tab and set the schedule for the

anti-malware database update. On the Devices tab, you can start the anti-malware database update task.

3. On the Settings tab, you can configure which event notifications you want to view in your events overview.

The information about events is not aggregated. Each event is sent in a separate email message. If you want to configure the delivery of event notifications, be ready to receive a large number of email messages.

4. On the Distribution packages tab, you can download the software directly and prepare new software when it is available. The newly prepared software will then be distributed to newly invited users.

Practical 6. SQL injection and Session hijacking :

Aim : SQL injection and Session hijacking :

A. SQL injection for website hacking,

Description : SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will unknowingly run on your database.

Look at the following example which creates a SELECT statement by adding a variable (txtUserId) to a select string. The variable is fetched from user input (getRequestString):

SQL Injection Based on 1=1 is Always True

https://www.hackthissite.org/index.php?id=2 order by 3

Aim : B. Session hijacking.

Description : TCP session hijacking is a security attack on a user session over a protected network. The most common method of session hijacking is called IP spoofing, when an attacker uses source-routed IP packets to insert commands into an active communication between two nodes on a network and disguise itself as one of the authenticated users. This type of attack is possible because authentication typically is only done at the start of a TCP session.

Another type of session hijacking is known as a man-in-the-middle attack, where the attacker, using a sniffer, can observe the communication between devices and collect the data that is transmitted.

Different ways of session hijacking :

There are many ways to do Session Hijacking. Some of them are given below –

Cross Site Scripting(XSS Attack)

Attacker can also capture victim's Session ID using XSS attack by using javascript. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker.

- IP Spoofing

Spoofing is pretending to be someone else. This is a technique used to gain unauthorized access to the computer with an IP address of a trusted host. In implementing this technique, attacker has to obtain the IP address of the client and inject his own packets spoofed with the IP address of client into the TCP session, so as to fool the server that it is communicating with the victim i.e. the original host.

- Blind Attack

If attacker is not able to sniff packets and guess the correct sequence number expected by server, brute force combinations of sequence number can be tried.

Practical 7. Wireless network hacking, cloud computing security, cryptography :

Aim : Wireless network hacking, cloud computing security, cryptography :

1 .Using Cryptool to encrypt and decrypt password,

Description : Cryptool is an open-source and freeware program that can be used in various aspects of cryptographic and cryptanalytic concepts. There are no other programs like it available over the internet where you can analyze the encryption and decryption of various algorithms. This tools provides graphical interface, better documentation to achieve the encryption and decryption, bundles of analytic tools, and several algorithms.

What is Cryptool?

- A freeware program with graphical user interface (GUI).
- A tool for applying and analyzing cryptographic algorithms.
- With extensive online help, it's understandable without deep crypto knowledge.
- Contains nearly all state-of-the-art crypto algorithms.
- “Playful” introduction to modern and classical cryptography.
- Not a “hacker" tool.

Aim : 2. Implement encryption and decryption using Ceaser Cipher.

- Description : The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the "shift" or "key".

- The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It's simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

- Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

- For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.

- Here is an example of how to use the Caesar cipher to encrypt the message "HELLO" with a shift of 3:

1. Write down the plaintext message: HELLO

2. Choose a shift value. In this case, we will use a shift of 3.

3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

H becomes K (shift 3 from H)

E becomes H (shift 3 from E)

L becomes O (shift 3 from L)

L becomes O (shift 3 from L)

O becomes R (shift 3 from O)

4. The encrypted message is now “KHOOR”.

- To decrypt the message, you simply need to shift each letter back by the same number of positions. In this case, you would shift each letter in “KHOOR” back by 3 positions to get the original message, “HELLO”.

(Encryption Phase with shift n)

(Decryption Phase with shift n)

Examples :

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Shift: 23

Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE

Shift: 4

Cipher: EXXEGOEXSRGI

Practical 8. Pen testing

Aim : Penetration Testing using Metasploit and metasploitable

Description : Metasploit Framework is a powerful open-source penetration testing framework. You get to know all the information about penetration testing, IDS signature, and software vulnerabilities. It allows the execution and development of the exploit code against a remote target tool. Metasploit is not illegal itself, but it depends on what you use it for.

Major keywords in the Metasploit framework

The module is a software application in the Metasploit framework that carries out tasks like exploiting and scanning and the targets.

They are the key components of the framework and are broken down into 7 types below:

1. Exploits
2. Payloads
3. Auxiliaries
4. Encoders
5. Evasions
6. Nops
7. Post

Payloads are the simple scripts that are often used in module exploits by taking advantage of the system's vulnerabilities. Auxiliary modules are the only modules that are not exploited. Several interesting features allow them to do more than just exploiting.

Aim : Cyberlaw :

Cyberlaw section under IT act 2000 - 43,65,66A, 66B,66C,66D,66E,66F,67A, 67B ,71,72,73 and 74 , Penalty and preventive measures to be taken for the crime associated with each case if

any and real life cybercrime cases under each section.

Description :

Section 43: Penalty and Compensation for damage to computer, computer system, etc

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network –

(a) accesses or secures access to such computer, computer system or computer network or computer resource;

(b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;

(c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;

(e) disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;

(i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injurously by any means;

(j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

he shall be liable to pay damages by way of compensation to the person so affected.

Section 65, whoever tampers with computer source documents knowingly or intentionally conceals, destroys or alters or causes another to conceal, destroy or alter any computer source code shall be punishable with imprisonment up to three years or with fine which may extend up to rupees two lakhs or with both.

Section 66A. Punishment for sending offensive messages through communication service, etc.—

Any person who sends, by means of a computer resource or a communication device,

_____

(a) any information that is grossly offensive or has menacing character; or

_____

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device;

_____

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages,

_____

shall be punishable with imprisonment for a term which may extend to three years and with fine.

_____

Explanation.--For the purposes of this section, terms "electronic mail" and "electronic mail message" means a message or information created or transmitted or received on a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record, which may be transmitted with the message.]

Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device.

Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C. Punishment for identity theft.

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D. Punishment for cheating by personation by using computer resource.

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E. Punishment for violation of privacy.

Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.

Explanation. --For the purposes of this section--

(a) transmit means to electronically send a visual image with the intent that it be viewed by a person or persons;

(b) capture, with respect to an image, means to videotape, photograph, film or record by any means;

(c) private area means the naked or undergarment clad genitals, *[pubic area], buttocks or female breast:

(d) publishes means reproduction in the printed or electronic form and making it available for public;

(e) under circumstances violating privacy means circumstances in which a person can have a reasonable expectation that--

(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

(ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

Section 66F. Punishment for cyber terrorism.

(1) Whoever,--

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by--

(i) denying or cause the denial of access to any person authorised to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorisation or exceeding authorised access; or

(iii) introducing or causing to introduce any computer contaminant,

and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70; or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorisation or exceeding authorised access, and by means of such conduct obtains access to information, data or computer data base that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer data base, with reasons to believe that such information, data or computer data base so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or

incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise,

commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life

Section 67. Punishment for publishing or transmitting obscene material in electronic form.

Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B. Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

Whoever,--

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees:

Provided that provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form--

(i) the publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper, writing, drawing, painting representation or figure is the interest of science, literature, art or learning or other objects of general concern; or

(ii) which is kept or used for bona fide heritage or religious purposes.

Explanation--For the purposes of this section, "children" means a person who has not completed the age of 18 years.

Section 71. Penalty for misrepresentation.

Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or 1 [electronic signature Certificate], as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72. Penalty for Breach of confidentiality and privacy.

Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 73. Penalty for publishing electronic signature Certificate false in certain particulars.

73.

Penalty for publishing 1[electronic signature] Certificate false in certain particulars.--(1) No person shall publish a 1[electronic signature] Certificate or otherwise make it available to any other person with the knowledge that--

(a) the Certifying Authority listed in the certificate has not issued it; or

(b) the subscriber listed in the certificate has not accepted it; or

(c) the certificate has been revoked or suspended,

unless such publication is for the purpose of verifying a 1[electronic signature] created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 74. Publication for fraudulent purpose.

Whoever knowingly creates, publishes or otherwise makes available a 1 [electronic signature] Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.