Welcome to:

IT Data Security – Data Security Threat Techniques

Unit objectives

After completing this unit, you should be able to:

- Have a basic understanding of threat techniques
- Classify all the threat techniques
- Identify and understand the steps involved in various attacks

Introduction

- An event or a person who has the potential for effecting a resource which is valuable in a negative manner can be termed as a threat
- Software and Hardware systems and the data that they hold can be vulnerable to a huge variety of threats
- When selecting the security procedures and features, the specific vulnerabilities associated to the system must be considered and not just the general objectives of security
- Thus it can be said that a factor which posses the potential for impacting a resource which is valuable for an organization in a negative manner is known as threat
- The way that these factors follow to carry out the negative effect is known as threat technique

Threat Techniques (1 of 66)

- A weaknesses or fault in a system or protection mechanism that opens it to attack or damage
- Threat techniques also change according to the field of security
- The following slides describe all these threat techniques in a detailed manner according to the area of security.

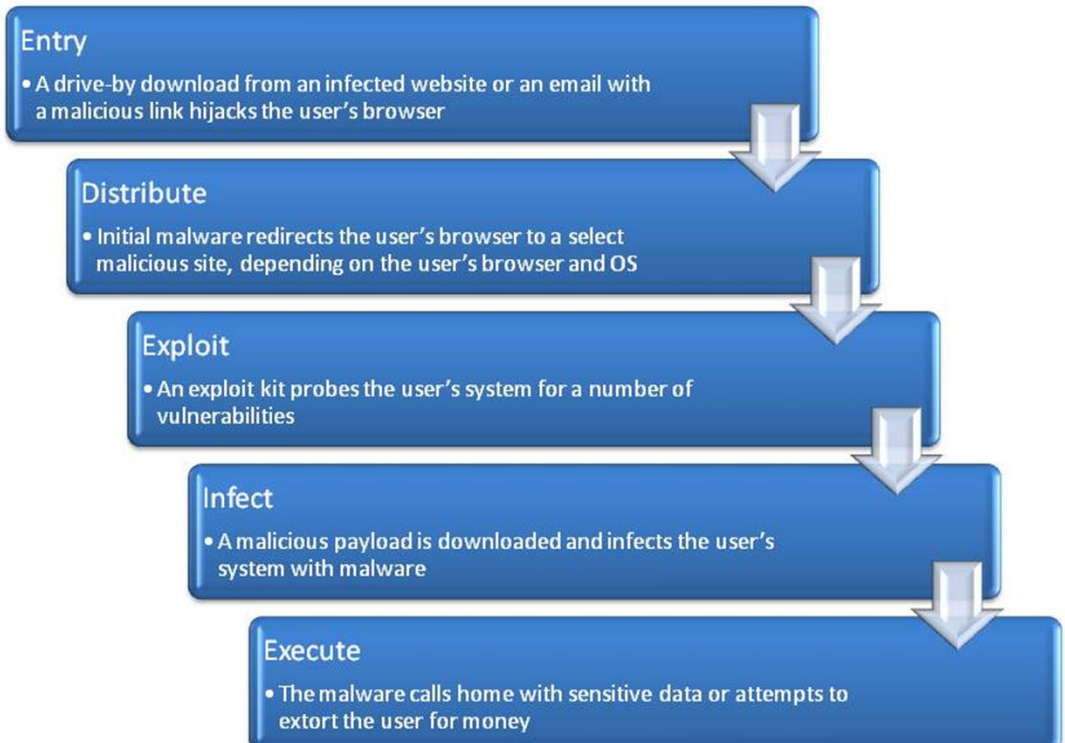
Threat Techniques (2 of 66)

- **Malware Threat Techniques**
  - Malwares exploit the holes present in security of a browser
  - Consumers are tricked to download certain software
  - This is a trick where the consumers actually download a malware to their systems.

Threat Techniques (3 of 66)

- **Malware Threat Techniques**
  - Malwares install code in hidden and un-expected places like in the window registry
  - Operating system is modified sometimes by malware
  - This makes malware difficult to uninstall

Threat Techniques (4 of 66)



Threat Techniques (5 of 66)

- Stage 1: Entry
- Stage 2: Distribution
- Stage 3: Exploit
- Stage 4: Infect
- Stage 5: Execute

Threat Techniques (6 of 66)

- Stage 1: Entry
  - This involves a drive-by download from an entry point
  - Drive-by downloads is the process of inadvertently downloading malicious web code
  - A drive-by download happens automatically and without the user knowing

Threat Techniques (7 of 66)

- Stage 2: Distribution
  - The unsuspecting user is redirected to download an exploit kit
  - Traffic distribution systems (TDS) create multiple redirections that are nearly impossible to track
  - Some TDS systems are legitimate
  - But like any software, legitimate TDS solutions are prone to being hacked and exploited

Threat Techniques (8 of 66)

- Stage 3: Exploit
  - An exploit pack is downloaded from the malware hosting site
  - A large number of exploits are executed

Threat Techniques (9 of 66)

- Stage 4: Infect
  - A malicious payload is downloaded to infect the system
  - The payload is the actual malware or virus that will ultimately steal data or extort money from the user
  - The hacker can choose from a wide range of different infectious payloads

Threat Techniques (10 of 66)

- Stage 5: Execute
  - The malicious payload makes the criminal behind it some money
  - This is done by selling credentials or by extorting the user into paying directly
  - Examples: Ransomware and FakeAV

Threat Techniques (11 of 66)

- Network Based Threat Techniques
  - Botnet
    - Botnet is a collection of compromised computers often referred to as “zombies”
    - Botnet owners or “herders” are able to control the machines in their botnet by means of a covert channel such as IRC (Internet Relay Chat)
    - Commands are issued to perform malicious activities

Threat Techniques (12 of 66)

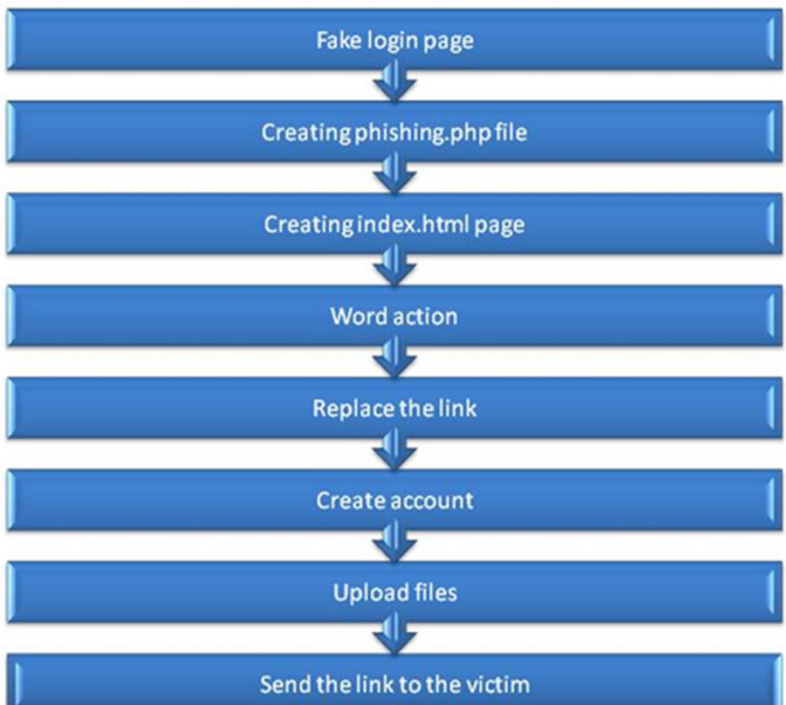
Threat Techniques (13 of 66)

- Network Based Threat Techniques
  - Botnet
    - Botnet creation is started from using vulnerabilities which are already known on a system of a victim
    - The victim's machine is infected through various method of exploitation by the attacker after a scan is done on the same
    - This phase is known as initial infection phase. The mechanism which are used in worms, viruses, etc. to infect the system is also used in botnet attacks

Threat Techniques (14 of 66)

- Network Based Threat Techniques
  - Phishing
    - This threat is a form of social engineering
    - There are 3 roles to be played by the phisher or the attacker in case of a phishing attack
      - Send out a huge count of duplicitous emails
      - Set up false websites
      - Use the confidential data gained

Threat Techniques (15 of 66)



Threat Technique (16 of 66)

- Network-based threat techniques
  - Phishing
    - Step: 1 Fake login page
    - Step 2: Creating phishing.php file
    - Step 3: Creating index.html page
    - Step 4: Word action
    - Step 5 Replace the link
    - Step 6: Create account
    - Step 7: Upload Files
    - Step 8: Send the link to the victim

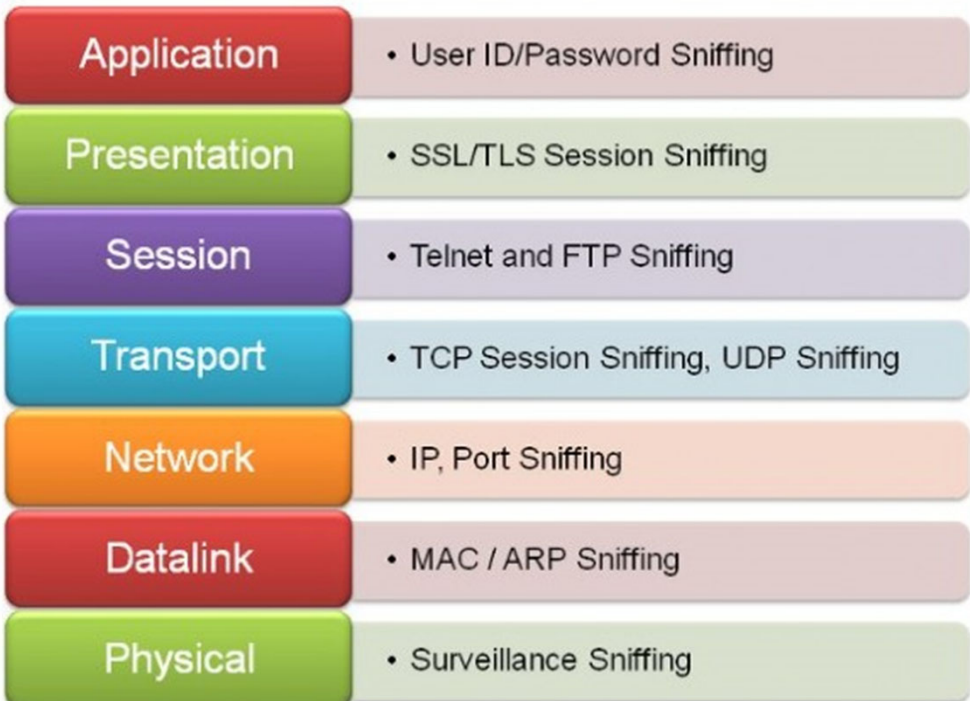
Threat Techniques (17 of 66)

- Network Based Threat Techniques
  - Sniffing
    - Sniffing includes decoding, interpreting, inspecting and capturing the data
    - It falls in the category of passive attacks
    - Various vital information is present on the TCP/IP packet that is requires by two different network interfaces to have a communication with one another
    - Fields such as destination and source IP address, port number, protocol type and sequence numbers are contained by it

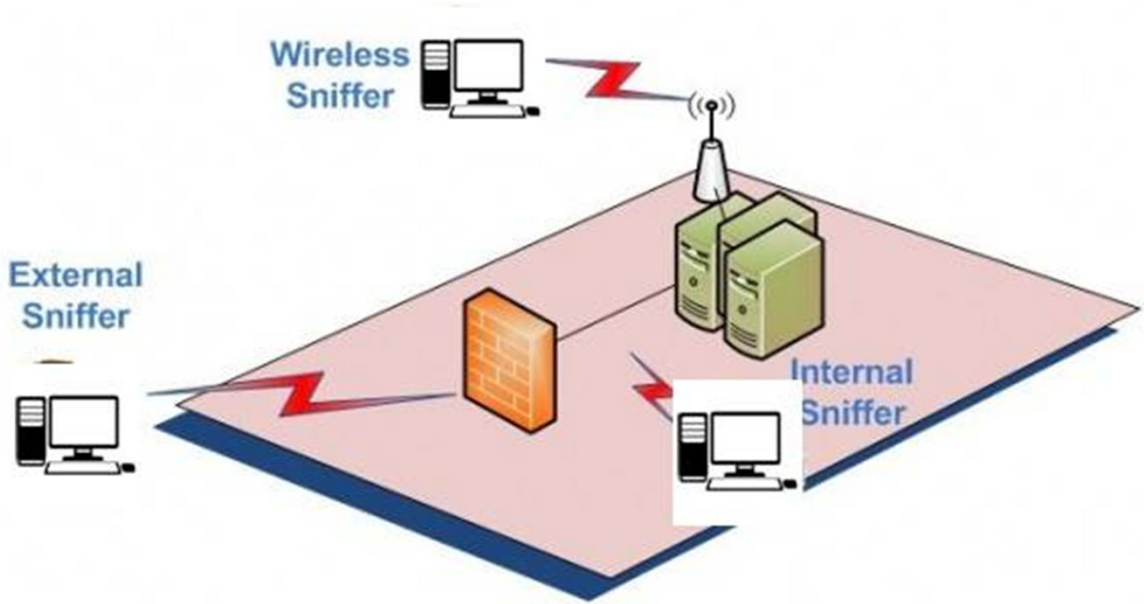
Threat Techniques (18 of 66)

- Network Based Threat Techniques
  - Sniffing
    - Sniffing attacks depend on the layer of the OSI layer targetted
    - It must be remembered that sniffing attacks can be carried out at every level whether it Level 1 or 7
    - Network traffic is captured by a person who is hooked to the LAN present internally

Threat Techniques (19 of 66)



Threat Techniques (20 of 66)



Threat Techniques (21 of 66)

- Network Based Threat Techniques
  - Sniffing
    - Types of Sniffing
      - **A LAN sniff**
      - **A protocol sniff**
      - **An ARP sniff**

Network Based Threat Techniques (22 of 66)

- Network Based Threat Techniques
  - Sniffing
    - Types of Sniffing
      - **TCP session stealing**
      - **Application-level sniffing**
      - **Web password sniffing**

Threat Techniques (23 of 66)

- Network Based threat techniques
  - Password Attack
    - Traditional way of finding out the password of a computer system
    - Unlimited opportunities have been created for the intruders
    - These limitless openings have been created due to the internet.
    - The motivation and the goal of a password hacker may differ form another but the main motive of all of them is to gain control over a particular computer network or system

Threat Techniques (24 of 66)

- Network Based threat techniques
  - Brute-Force Attack
    - Brute-force attack can be used to crack any password
  - Rainbow Attack
    - A pre-computed list which have all the hashes for every possible character combination
  - Dictionary Attack
    - Commons words are used in this type of attack to identify the password of a system

Network Based Threat Techniques (25 of 66)

- Network Based threat techniques
  - Intercepting the Transmission
    - A successful man-in-the-middle connection is established by the attacker into the network in this type of attack.
    - Digital certificate is supposed to be sent to the browser by the server as a part of a SSL handshake process
    - The details of the process such as cipher strength, domain name, expiration date, etc. are grabbed by the attacker by stealing the certificate
    - Each request made by the browser is intercepted by the attacker from this point onwards

Threat Techniques (26 of 66)

- **Cryptographic Threat Techniques**
  - The need for encryption is two-fold
  - There are many threat techniques by which a cryptographic system can be broken.
  - These techniques are described in the next slides

Threat Techniques (27 of 66)

- **Cryptographic Threat Techniques**
  - **Cryptanalysis**
    - Combination of computing power and sophisticated mathematical formulas can defeat any algorithm
    - There are two basic goals of a cryptanalytic attack
      - To discover the plaintext
      - To discover the cipher text

Threat Techniques (28 of 66)

- Cryptographic Threat Techniques
  - Cryptanalysis Known Plaintext Attack
    - Known Plaintext Attack
    - Chosen Plaintext Attack
    - Differential Cryptanalysis

Threat Techniques (29 of 66)

- Cryptographic Threat Techniques
  - Cryptanalysis
    - Differential Fault Analysis
    - Differential Power Analysis
    - Differential Timing Analysis

Threat Techniques (30 of 66)

- **Cryptographic Threat Techniques**
  - **Birthday Attack**
    - Based on a mathematical theory known as ‘birthday problem paradox’
    - This theory states that if a set of people are selected randomly, some pair of the people will have their birthdays on the same day
    - The hash or check sum is calculated at both the ends of the data transmission and hence integrity of data is maintained
    - In birthday attack various attackers come together and capture data chunks individually

Cryptographic Threat Techniques (31 of 66)

- **Cryptographic Threat Techniques**
  - **Mathematical Attack**
    - The plain text is taken as an input by any encryption process
    - A mathematical formula is computed
    - This mathematical nature of the encryption which is public key oriented is exploited by the attackers
    - There are many attacks which are general in nature used to they cover a private key

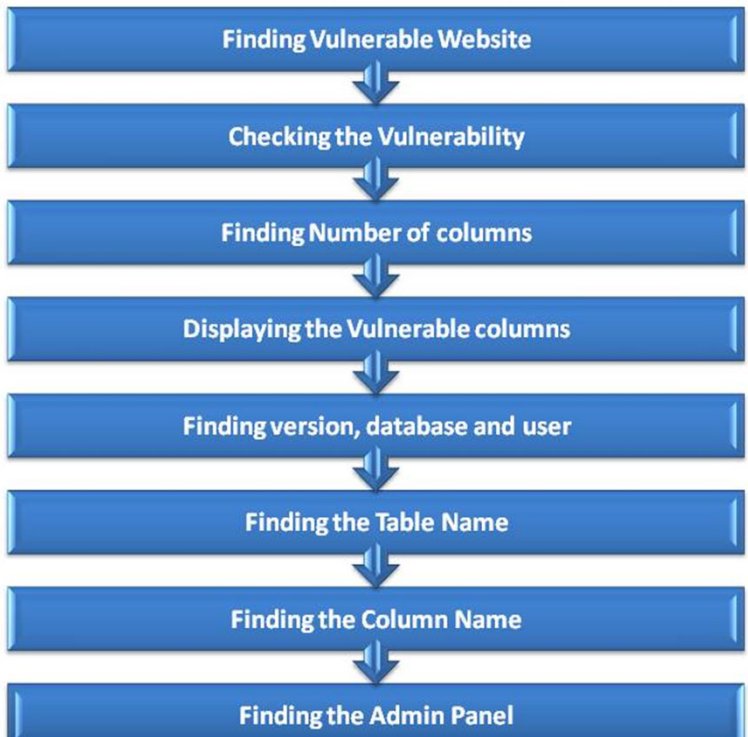
Threat Techniques (32 of 66)

- **Database Threat Techniques**
  - Databases are one of the most compromised assets
  - They have all the critical data and are thus always targeted
  - Compromising database would mean getting all the critical data that an organization has

Threat Techniques (33 of 66)

- **Database Threat Techniques**
  - **SQL Injection**
    - The most famous and common method of hacking database
    - The database of any website can be accessed by an unauthorized person
    - All the detail of the database can be acquired by the attacker

Threat Techniques (34 of 66)



Threat Technique (35 of 66)

- **Database Threat Techniques**
  - **SQL Injection**
    - Step 1: Finding Vulnerable Website
    - Step 2: Checking the Vulnerability
    - Step 3: Finding Number of Columns
    - Step 4: Displaying the vulnerable Column
    - Step 5: Finding Version, database and User
    - Step 6: Finding the Table Name
    - Step 7: Finding the Column Name
    - Step 8: Finding the Admin Panel

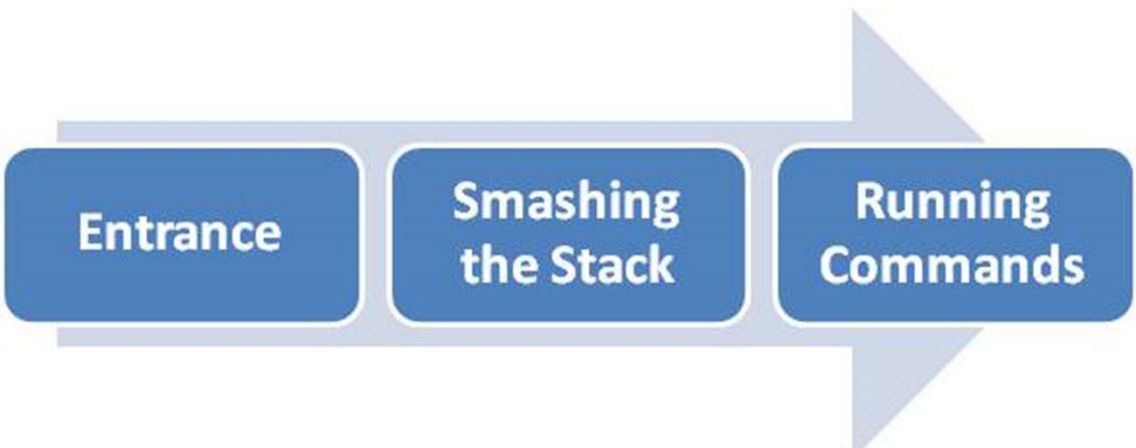
Threat Techniques (36 of 66)

- **Database Threat Techniques**
  - **Voyager Beta Worm**
    - **Step 1**: Local IP address is grabbed
    - **Step 2:** TCP Connection established
    - **Step 3**: Hit and trial
    - **Step 4**: Column creation
    - **Step 5**: Repetition of process

Threat Techniques (37 of 66)

- **Database Threat Techniques**
  - **Buffer overflow**
    - When a program attempts to put more data in a buffer
    - In this case, a buffer is a sequential section of memory allocated to contain anything
    - Writing outside the bounds of a block of allocated memory can corrupt data and ultimately crash the program

Threat Techniques (38 of 66)



Threat Technique (39 of 66)

- **Database Threat Techniques**
  - **Buffer overflow**
    - Step 1: Entrance
    - Step 2: Smashing the Stack
    - Step 3: Running Commands

Threat Techniques (40 of 66)

- **Banking Fraud Techniques**
  - There has been a significance growth in the amount of malicious applications
  - Thus, a huge challenge is represented for the organizations
  - Local attack and remote attack are the two attack vectors which are employed by the malicious applications

Threat Techniques (41 of 66)

- **Banking Fraud Techniques**
  - **Local Attack**
    - A common mistake made by end users believes that their online banking session is perfectly safe
    - Security experts continually state that everything is safe if there is a yellow padlock symbol in the browser window
    - SSL is designed as a secure tunnel from the end user computer to the bank mainframe
    - This fact is exploited by the Trojan

Threat Techniques (42 of 66)

- **Banking Fraud Techniques**
  - **Remote Attack**
    - A server which is controlled by the attacker is used in this type of attack
    - Easy to follow traces were left on the log files of the web master in the previous attacks
    - But presently attackers keep the resource locally and then carry out the attack.
    - This process is known as phishing where the user's account information is acquired by social engineering practice

Banking Fraud Techniques (43 of 66)

- **Banking Fraud Techniques**
  - **Joint Forces**
    - Serious damage can be done by an attacker if both remote and local attacks are combined
    - For example: The local host files which are present in a system can be altered by a system which has been infected due to a Trojan that has been inserted in it
    - The local host files will now redirect all the request of the user
    - This kind of behavior has been observed many a times in a number of threats which arises due to adware
    - These certificates can easily be created by free tools like Open SSL

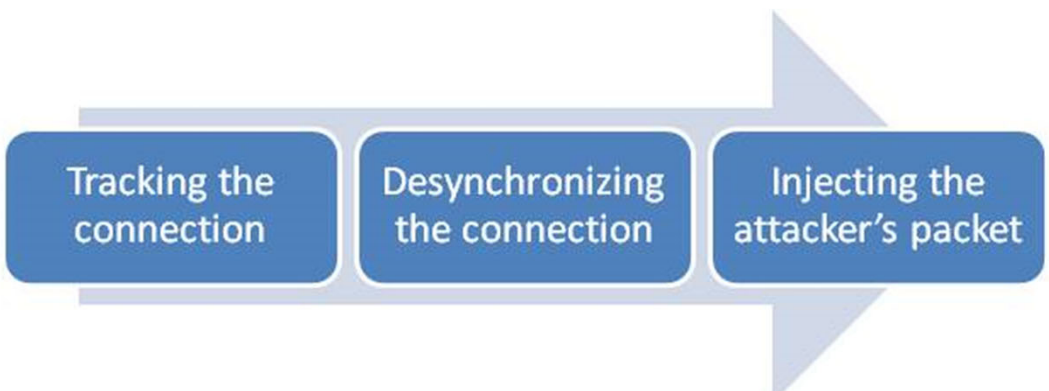
Threat Techniques (44 of 66)

- **Web-application Threat Techniques**
  - Web security at the application level is often ignored
  - Most security breaches online occur through the application rather than the server
  - Some of these threat techniques are elaborated in the slides which follow

Threat Techniques (45 of 66)

- **Web-application Threat Techniques**
  - **Session Hijacking**
    - To sneak in to a system as a genuine user and hijack a system
    - An attacker can hijack a genuine user's session by finding an established session
    - Once the session has been hijacked, the attacker can stay connected for hours without arousing suspicion
    - All routed traffic destined for the user's IP address comes to the attacker's system

Threat Techniques (46 of 66)



Threat Technique (47 of 66)

- **Web-application Threat Techniques**
  - **Session Hijacking**
    - Step 1: Tracking the Connection
    - Step 2: De-synchronizing the Connection
    - Step 3: Injecting the attacker's packet

Threat Techniques (48 of 66)

- **Web-application Threat Techniques**
  - **Log Tampering**
    - Web applications maintain logs to track the usage patterns of an application
    - User logins, administrator logins, resources accessed, error conditions, and other application-specific information are often maintained in logs
    - These logs are used for proof of transactions, fulfillment of legal record retention requirements, marketing analysis, and forensic incident analysis
    - An attacker, in an attempt to cover tracks, will usually delete logs, modify logs, change user information, and otherwise destroy all evidence of the attack

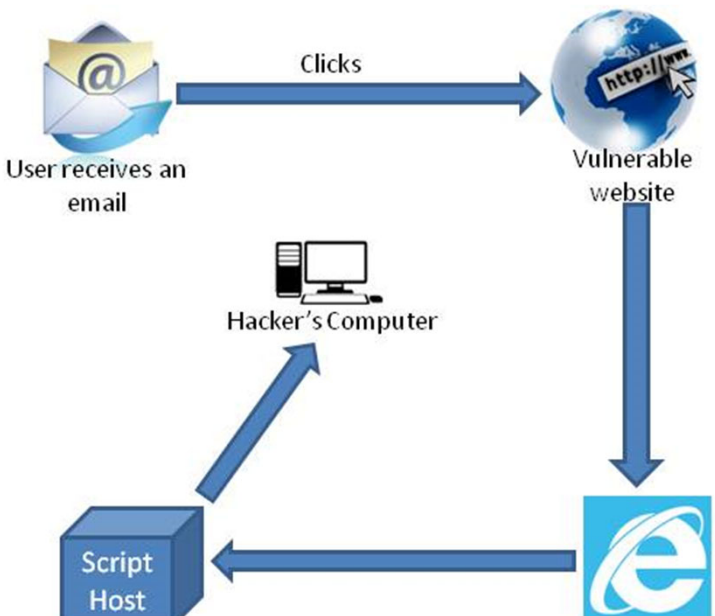
Threat Techniques (49 of 66)

- **Web-application Threat Techniques**
  - **Pharming**
    - The traffic is redirected to a fake host is this type of attack
    - DNS that is Domain Name System is a very important part of the infrastructure of the internet
    - A database which is hierarchical in nature is published by DNS which has all the server name in hierarchy
    - Domain Name System Security Extension (DNSSEC) is an extension of DNS that provides three distinct services:
      - Key distribution
      - Data origin authentication
      - Transaction and request authentication

Threat Techniques (50 of 66)

- **Web-application Threat Techniques**
  - **Cross-site Scripting Forgery**
    - Cross-site scripting is also called XSS
    - An attack can be carried out by an attacker when a input from a user is used by a web application
    - This web application once exploited by the attacker will do things which otherwise are not allowed
    - This input can be propagated to other users as well

Web-application Threat Techniques (51 of 66)



Threat Techniques (52 of 66)

- **Web-application Threat Techniques**
  - **Cross-site Scripting Forgery**
    - **Step 1**: The link which has been sent from the hacker to the user is clicked by the user
    - **Step 2**: A cross site scripting bug is present which generates a request to the website
    - **Step 3**: Script which is malicious in nature is sent back to the web browser to the user
    - **Step 4**: The malicious code is executed by the script host
    - **Step 5**: The sensitive data is sent to the computer of the hacker

Threat Techniques (53 of 66)

- **Physical Security**
  - CCTV cameras, locks, guards and alarms etc. are the common controls involved in physical security
  - While these countermeasures are important in securing an information system physically but they are not the only protections that must be considered
  - Physical security is the protection of hardware, personnel, programs, data and networks from physical events including natural disasters, fire, burglary, terrorism and theft etc.

Threat Techniques (54 of 66)

- Physical security
  - Dumpster diving
    - To look for information in the thrash of someone else
    - An attacker can dive in the dumpster of an organization to retrieve information life calendar, phone list or the chart of an organization etc.
    - All the media that is stored in the system of the organization must be erased and education of all the employees is a must

Web-application Threat Techniques (55 of 66)

- **Physical Security**
  - **Social Engineering**
    - This method relies heavily on the interaction made by the employees of the company
    - This method involves to trick people such that they break the procedure of security which are effective
    - The natural helpfulness and weakness of an employee is another criteria that the social engineers rely on
    - For example: An authorized employee can be called by the social engineer that a certain problem needs to be solved urgently which require access to the network on an immediate basis

Web-application Threat Techniques (56 of 66)

- Physical Security
  - Social Engineering
    - Baiting
    - Phishing
    - Pre-texting
    - Spear phishing
    - Tailgating

Threat Techniques (57 of 66)

- **Wireless Network Threat Techniques**
  - Wireless networking provides many advantages, but it also coupled with new security threats
  - Although implementation of technological solutions is the usual respond to wireless security threats and vulnerabilities
  - Some of the wireless network threat techniques has been mentioned in the slides to follow

Threat Techniques (58 of 66)

- **Wireless Network Threat Techniques**
  - **Wi-Fi Hacking**
    - A wireless access point can be hacked only if one is close enough to the network
    - 300 feet that is 100 meter is the limit of the access points

Wireless Network Threat Techniques (59 of 66)

Threat Technique (60 of 66)

- **Wireless Network Threat Techniques**
  - **Wi-Fi Hacking**
    - Step 1: Open a Terminal
    - Step 2: Put the Wireless Adapter in Monitor Mode
    - Step 3: Monitor the available Aps with Airodump-Ng
    - Step 4: Connect to the Access Point
    - Step 5: Broadcast De-authenticate Users on the AP

Threat Techniques (61 of 66)

- **Wireless Network Threat Techniques**
  - **DoS Attack**
    - A message is sent by the user in a typical connection in order to ask the server for authentication.
    - When the user receives this approval then only he is allowed to access the server.
    - Now when the server tries to send the approval of the requested authentication it is not able to send it as all the report have false return addresses
    - For some time now, DDoS/DoS attack have been pausing a lot of problem.
    - These attacks are successful in many cases as the organization do not update their plans of incident response nor do they turn their technologies for mitigating threads

Wireless Network Threat Techniques (62 of 66)

- **Wireless Network Threat Techniques**
  - **DoS Attack**
    - **Step 1**: Users are directed
    - **Step 2**: Compromising the systems
    - **Step 3**: DoS or DDoS attack are launched
    - **Step 4**: Crashing of systems

Threat Techniques (63 of 66)

- **Bluetooth Device Threat Techniques**
  - The use of wireless communication systems and their interconnections via networks have grown
  - RF communication are easier to use than wired or infrared communication, but it also makes eavesdropping easier
  - Because wireless RF communication can suffer threats, additional countermeasures are needed to protect against them

Threat Techniques (64 of 66)

- **Bluetooth Device Threat Techniques**
  - **Blue Jacking**
    - Phone book manipulation attack is cause through bluejacking.
    - The attacker can also transfer the data into his own device and can edit or misuse it according to his needs
    - This transferring of data into the hacker's device is an example of Bluesnarfing attack
    - Bluejacking can be done without engaging into any tedious process

Threat Techniques (65 of 66)

- **Bluetooth Device Threat Techniques**
  - **Blue Jacking**
    - **Step 1**: First, access is gained to the contacts in the device (phonebook or Outlook)
    - **Step 2**: A new contact is created by selecting “Create a Contact” option
    - **Step 3**: A message is entered in the field where the contact name is supposed to be entered. This message is from the attacker to alarm and scare the victim. The message is entered in the device from which blue-jacking is to be done
    - **Step 4**: This contact/message is now saved in the phonebook of the device
    - **Step 5**: Now, this message is to be transmitted. This is done by sending the contact through Bluetooth
    - **Step 6**: After choosing the “Bluetooth” option to send contact/message, identify nearby devices and then select the target device
    - **Step 7**: The target device will now be blue-jacked after receiving the message

Threat Techniques (66 of 66)

- **Bluetooth Device Threat Techniques**
  - **Blue-bugging**
    - An attacker gains control of the phone book
    - This attack is called blue-bugging.
    - This attack causes a phone call initiation.
    - Attacker can also use a different mechanism by which he can access the keypad of the target phone
    - This way, even if a call is initiated, it traces back to the victim's number

Checkpoint (1 of 4)

1. Malware threat technique can be carried out in how many steps?
   - 4
   - 5
   - 3
   - 7

2. Which of the following option shows the steps of malware threat technique in correct order?
   - Entry, Distribution, Exploit, Infect, Execute
   - Distribution, Entry, Exploit, Infect, Execute
   - Exploit, Entry, Exploit, Infect, Execute
   - Infect, Entry, Exploit, Infect, Execute

3. Which of the following is a step of phising?
   - Fake login page
   - Creating phishing.php file
   - Creating index.html page
   - All of the above

Checkpoint solutions (1 of 4)

1. Malware threat technique can be carried out in how many steps?
   - 4
   - ***The answer is 5***
   - 3
   - 7

2. Which of the following option shows the steps of malware threat technique in correct order?
   - ***The answer is Entry, Distribution, Exploit, Infect, Execute***
   - Distribution, Entry, Exploit, Infect, Execute
   - Exploit, Entry, Exploit, Infect, Execute
   - Infect, Entry, Exploit, Infect, Execute

3. Which of the following is a step of phising?
   - Fake login page
   - Creating phishing.php file
   - Creating index.html page
   - ***The answer is All of the above***

Checkpoint (2 of 4)

4. Which of the following option shows the steps of session hijacking in correct order?
   - Tracking the Connection, Desynchronizing the Connection, Injecting the Attacker's Packet
   - Desynchronizing the Connection, Tracking the Connection, Injecting the Attacker's Packet
   - Injecting the Attacker's Packet, Tracking the Connection, Injecting the Attacker's Packet
   - Tracking the Connection, Desynchronizing the Connection, Injecting the Attacker's Packet

5. How many steps are involved in blue-jacking?
   - 5
   - 4
   - 7
   - 10

6. Which of the following option shows the steps of buffer overflow in correct order?
   - Entrance, Running Commands, Smashing the Stack
   - Smashing the Stack, Entrance, Running Commands
   - Entrance, Smashing the Stack, Running Commands
   - Running Commands, Smashing the Stack, Entrance

Checkpoint solutions (2 of 4)

4. Which of the following option shows the steps of session hijacking in correct order?
   - ***The answers is Tracking the Connection, Desynchronizing the Connection, Injecting the Attacker's Packet***
   - Desynchronizing the Connection, Tracking the Connection, Injecting the Attacker's Packet
   - Injecting the Attacker's Packet, Tracking the Connection, Injecting the Attacker's Packet
   - Tracking the Connection, Desynchronizing the Connection, Injecting the Attacker's Packet

5. How many steps are involved in blue-jacking?
   - 5
   - 4
   - ***The answer is 7***
   - 10

6. Which of the following option shows the steps of buffer overflow in correct order?
   - Entrance, Running Commands, Smashing the Stack
   - Smashing the Stack, Entrance, Running Commands
   - ***The answers is Entrance, Smashing the Stack, Running Commands***
   - Running Commands, Smashing the Stack, Entrance

Checkpoint (3 of 4)

7. How many steps are involved in DOS attack?
   - 3
   - 6
   - 5
   - 4

8. How many steps are involved in Wi-Fi hacking?
   - 4
   - 5
   - 6
   - 3

Checkpoint solutions (3 of 4)

7. How many steps are involved in DOS attack?
   - 3
   - 6
   - 5
   - ***The answer is 4***

8. How many steps are involved in Wi-Fi hacking?
   - 4
   - ***The answer is 5***
   - 6
   - 3

Checkpoint (4 of 4)

9. Which of the following is not a step of cross-site script forgery?
   - This sends malicious script back to the user's Web browser
   - The script host executes the malicious code
   - This sends the sensitive data to the hacker's computer
   - None of the above

10. What is tailgating?
   - When a malicious party sends a fraudulent email disguised as a legitimate email
   - When one party lies to another to gain access to privileged data
   - When an unauthorized party follows an authorized party into an otherwise secure location, usually to steal valuable property or confidential information
   - All of the above

Checkpoint solutions (4 of 4)

9. Which of the following is not a step of cross-site script forgery?
   - This sends malicious script back to the user's Web browser
   - The script host executes the malicious code
   - This sends the sensitive data to the hacker's computer
   - ***The answer is None of the above***

10. What is tailgating?
   - When a malicious party sends a fraudulent email disguised as a legitimate email
   - When one party lies to another to gain access to privileged data
   - ***The answer is When an unauthorized party follows an authorized party into an otherwise secure location, usually to steal valuable property or confidential information***
   - All of the above

Unit summary

Having completed this unit, you should be able to:

- Have a basic understanding of threat techniques
- Classify all the threat techniques
- Identify and understand the steps involved in various attacks