Fundamentals of Cyber Security

The Neotia University

B.tech, Cyber Security,2nd sem

The Neotia University

The Neotia University

SOFTWARE REQUIREMENT :

1. Turbo C++ IDE (TurboC3)
2. Borland Turbo C++ (Version 4.5)

List of Experiment:-

1. Study of Network Security fundamentals - Ethical Hacking, Social Engineering practices.
2. Study of System threat attacks - Denial of Services.
3. Study of Sniffing and Spoofing attacks.
4. Study of Techniques uses for Web Based Password Capturing.
5. Study of Different attacks causes by Virus and Trojans.
6. Study of Anti-Intrusion Technique – Honey pot.
7. Study of IP based Authentication.

The Neotia University

Experiment No. 1

AIM: Study of Network Security fundamentals - Ethical Hacking, Social Engineering practices.

Ethical Hacking- Ethical hacking and a **ethical hacker** are terms that describe hacking performed to help a company or individual identify potential threats on the computer or network. An ethical hacker attempts to hack their way past the system security, finding any weak points in the security that could be exploited by other hackers. The organization uses what the ethical hacker finds to improve the system security, in an effort to minimize, if not eliminate any potential hacker attacks.

In order for hacking to be deemed ethical, the hacker must obey the below rules.

1. You have permission to probe the network and attempt to identify potential security risks. It's recommended that if you are the person performing the tests that you get written consent.
2. You respect the individual's or company's privacy and only go looking for security issues.
3. You report all security vulnerabilities you detect to the company, not leaving anything open for you or someone else to come in at a later time.
4. You let the software developer or hardware manufacturer know of any security vulnerabilities you locate in their software or hardware if not already known by the company.

The term "ethical hacker" has received criticism at times from people who say that there is no such thing as an "ethical" hacker. Hacking is hacking, no matter how you look at it and those who do the hacking are commonly referred to as computer criminals. However, the work that ethical hackers do for organizations has helped improve system security and can be said to be quite successful. Individuals interested in becoming an ethical hacker can work towards a certification to become a Certified Ethical Hacker. This certification is provided by the International Council of E-Commerce Consultants (EC-Council).

Social Engineering practices: The practice of deceiving someone, either in person, over the phone, or using a computer, with the express intent of breaching some level of security either personal or professional. Social engineering techniques are considered con games which are performed by con artists. The targets of social engineering may never realize they have been victimized.

Also Known As: Con Games
Examples:
Using social engineering techniques, the hacker managed to get the network administrator to provide him the username and password needed to gain access to the company's server.

The Neotia University

SOCIAL ENGINEERING TACTICS AND TOOLS – USING DECEPTION TO BREAK IN

Social engineering attacks are based on one thing – information. Without information about your customers, social engineers aren't able to use the elicitation and pretesting tactics that are described below.

This information is relatively simple to obtain. A good social engineer can spend a few hours researching a target online and have enough information to make even the most seasoned contact center agent believe the social engineer is someone they are not. The increasing amount of personal information that's available using search engines, who is databases, social media (Facebook, LinkedIn, MySpace, Twitter, etc.), blogs, wikis, and photo sharing sites makes it very simple for them to find or determine:

Even social security numbers are available from some paid research services.

Once the social engineer has relevant information, they use it in these highly effective human hacking tactics:

- Elicitation
- Pretexting

The Neotia University

Experiment No. 2

Aim: Study of System threat attacks - Denial of Services.

Denial of Service: The goal of a denial of service attack is to deny legitimate users access to a particular resource. An incident is considered an attack if a malicious user intentionally disrupts service to a computer or network resource. Denial of service (DoS) attacks has become a major threat to current computer networks. To have a better understanding on DoS attacks, In particular, we network based and host based DoS attack techniques to illustrate attack principles. DoS attacks are classified according to their major attack characteristics. Current counterattack technologies are also reviewed, including major defense products in deployment and representative defense approaches in research. Finally, DoS attacks and defenses in 802.11 based wireless networks are explored at physical, MAC and network layers.

OVERVIEW OF DOS ATTACKS IN THE INTERNET

In this section, we overview the common DDoS attack techniques and discuss why attacks succeed fundamentally.

Attack Techniques

Many attack techniques can be used for DoS purpose as long as they can disable service, or downgrade service performance by exhausting resources for providing services. Although it is Impossible to enumerate all existing attack techniques, we describe several representatives network based and host based attacks in this section to illustrate attack principles. Readers can also find complementary information on DoS attacks in Handley *et al.* 2006 and Mirkovic *et al.* 2005.

Network Based Attacks

TCP SYN Flooding. DoS attacks often exploit stateful network protocols (Jian 2000, Shannon *et al.* 2002), because these protocols consume resources to maintain states. TCP SYN flooding is one of such attacks and had a wide impact on many systems. When a client attempts to establish a TCP connection to a server, the client first sends a SYN message to the server. The server then acknowledges by sending a SYN-ACK message to the client. The client completes the establishment by responding with an ACK message. The connection between the client and the server is then opened, and the service-specific data can be exchanged between them. The abuse arises at the half-open state when the server is waiting for the client's ACK message after sending the SYN-ACK message to the client (CERT 1996). The server needs to allocate memory for storing the information of the half-open connection. The memory will not be released until either the server receives the final ACK message or the half-open connection expires. Attacking hosts can easily create half-open connections via spoofing source IPs in SYN messages or ignoring SYN-ACKs. The consequence is that the final ACK message will never be sent to the victim. Because the victim normally only allocates a limited size of space in its process table, too many half-open connections will soon fill the space. Even though the half-open connections will eventually expire due to the timeout, zombies can aggressively send spoofed TCP SYN packets requesting connections at a much higher rate than the expiration rate. Finally, the victim will be

Tilottama University

unable to accept any new incoming connection and thus cannot provide services.

ICMP Smurf Flooding. ICMP is often used to determine if a computer in the Internet is responding. To achieve this task, an ICMP echo request packet is sent to a computer. If the computer receives the request packet, it will return an ICMP echo reply packet. In a smurf attack, attacking hosts forge ICMP echo requests having the victim's address as the source address and the broadcast address of these remote networks as the destination address (CERT 1998). As depicted in Figure 1, if the firewall or router of the remote network does not filter the special 6/28
crafted packets, they will be delivered (broadcast) to all computers on that network. These computers will then send ICMP echo reply packets back to the source (i.e., the victim) carried in the request packets. The victim's network is thus congested.

UDP Flooding. By patching or redesigning the implementation of TCP and ICMP protocols, current networks and systems have incorporated new security features to prevent TCP and ICMP attacks. Nevertheless, attackers may simply send a large amount of UDP packets towards a victim. Since an intermediate network can deliver higher traffic volume than the victim network can handle, the flooding traffic can exhaust the victim's connection resources. Pure flooding can be done with any type of packets. Attackers can also choose to flood service requests so that the victim cannot handle all requests with its constrained resources (i.e., service memory or CPU cycles). Note that UDP flooding is similar to flash crowds that occur when a large number of users try to access the same server simultaneously. However, the intent and the triggering mechanisms for DDoS attacks and flash crowds are different.
Intermittent Flooding. Attackers can further tune their flooding actions to reduce the average flooding rate to a very low level while achieving equivalent attack impacts on legitimate TCP connections. In shrew attacks (Kuzmanovic *et al.* 2003), attacking hosts can flood packets in a burst to congest and disrupt existing TCP connections. Since all disrupted TCP connections will wait a specific period (called retransmission-time-out (RTO)) to retransmit lost packets, attacking hosts can flood packets at the next RTO to disrupt retransmission. Thereby, attacking hosts can synchronize their flooding at the following RTOs and disable legitimate TCP connections as depicted in Figure 2. Such collaboration among attacking hosts not only reduces overall flooding traffic, but also helps avoid detection. Similar attack techniques targeting services with congestion control mechanisms for Quality of Service (QoS) have been discovered by Guirguis *et al.* (2005). When a QoS enabled server receives a burst of service requests, it will temporarily throttle incoming requests for a period until previous requests have been processed. Thus, attackers can flood requests at a pace to keep the server throttling the incoming requests and achieve the DoS effect. Guirguis's study showed that a burst of 800 requests can bring down a web server for 200 seconds, and thereby the average flooding rate could be as low as 4 requests per second.

The Nesria University

Experiment No. 3

Aim: Study of Sniffing and Spoofing attacks.

Packet sniffing and spoofing are the two important concepts in network security; they are two major threats in network communication. Being able to understand these two threats is essential for understanding security measures in networking. There are many packet sniffing and spoofing tools, such as Wireshark, Tcpdump, Netwox, etc. Some of these tools are widely used by security experts, as well as by attackers.Being able to use these tools is important for students, but what is more important for students in a network security course is to understand how these tools work, i.e., how packet sniffing and spoofing are implemented in software. The objective of this lab is for students to master the technologies underlying most of the sniffing and spoofing tools. Students will play with some simple sniffer and spoofing programs, read their source code, modify them, and eventually gain an in-depth understanding on the technical aspects of these programs.

Spoofing is an active attack by one machine on another. A dishonest person with less-than-honorable motives represents himself as being someone else or coming from somewhere else. The spoofer appears to be familiar. It's a way of gaining access that is otherwise denied to the individual. Perhaps the person intends to cause problems or perhaps the individual just wants to have a look around where he's not supposed to be.

Sniffing refers to the use of software or hardware to watch data as it travels over the Internet. There are some legitimate uses for the process. It is then called network analysis and helps network administrators diagnose problems. In the hands of the wrong person, however, a sniffing program can collect passwords and read email. Sniffing is considered a passive security attack, according to TechiWarehouse.

What problems can result?

Sniffing means a loss of privacy for those on a network. Along with the loss of privacy goes a loss of trust, which is necessary in many situations.

- Sniffing can compromise the privacy of passwords. An Ethernet sniffer can easily detect passwords.
- Sniffing can allow unauthorized persons access to financial information, including account numbers for banking and credit cards.
- Sniffing private and confidential information contained in email is very common. Having an email viewed by someone other than the intended recipient can cause problems ranging from embarrassment to a breach of national security.
- Sniffing can yield low-level protocol information. Anyone who is interested in attacking a network will then have the needed information.

The Neotia University

Prevention

New data suggests that there is no way to detect when your computer has been sniffed. They also advise that while people can take measures to make sniffing difficult, it may be almost impossible to totally prevent being sniffed.

Encryption helps. Replacing the hub with a switch may also add protection. Taking care when using public Wi-Fi may also help reduce exposure.

Consumer Fraud Reporting adds that you can help protect against spoofing by following these suggestions:

- Don't click on an email link that requests personal information, even if it looks like a legitimate site.
- Be suspicious of anyone asking for personal information.
- Don't send personal information or financial information through a Web site.

If you've been caught in a moment of carelessness and provided information you should not have, such as passwords or personal identification, notify the companies you do business with right away to put a fraud alert on your account. Also contact Consumer Fraud Reporting, a free service that helps protect consumers against fraud.

The Neotia University

Experiment No. 4

Aim: Study of Techniques uses for Web Based Password Capturing.

Many people don't understand how easy it is for attackers to take advantage of weak passwords, and therefore don't use a password manager or other means to make their passwords stronger. This post describes 9 common ways passwords get captured, roughly ordered from most to least common. Proper use of a password manager can thwart some of these attacks and limit damages from most other types of attacks.

1: You Hand it Over Voluntarily

People frequently hand over their passwords via phishing, other forms of social engineering, or when a person or entity asks for temporary use of a password.

Protection: The simplest defense is to NEVER share your password for any account with any person, organization, or web site. An additional good defense is to develop "net smarts" analogous to "street smarts" to avoid phishing scams or other forms of social engineering. If you must temporarily share your password (i.e. to import contacts into Facebook), then change your password immediately after its temporary use is complete.

Damage Control: Your damages are limited to one account if you have a unique password for each account. Immediately change the password of the affected account.

2: You Hand it Over Unknowingly

This overlaps with the previous attack. You think you are on the web site you intended but you actually mistyped it by one character, you clicked a bad link to get there, or you were tricked by tab napping. So you end up on a fake or spoof web site that looks legitimate. When you log in, it collects your credentials then passes you on to the real site. A variation on this theme is an attack which layers extra fields over a legitimate web site. You are tricked into typing private personal information such as birthday, mother's maiden name, social security number, etc. and then this information is used to "recover" your account .

Protection: A good defense against this ploy is to only login to a web site by selecting it from your password manager's drop down menu (even if the tab was one you thought you opened yourself). This will automatically log you in to the correct site, which the password manager stores. Another type of defense is for your browser to use a security service that warns you when you might be about to open a hazardous web site – but this may slow down browsing.

Damage Control: Your damages are limited to one account if you have a unique password for each account. Immediately change the password of the affected account.

The Neotia University

3: Mass Theft of Password Files

Most people don't realize that user names and passwords routinely get stolen while your computer is off and disconnected from the internet. How? Web sites with many users and weak security are prime targets for attackers who want to steal a password file which lists all user names and passwords. Recent examples include Monster.com and RockYou.com. While most sites do not store passwords as clear text, many sites store passwords in a form that can be read using widely available rainbow table software. For people who use the same password on many sites, the theft of this password on one site can be the starting point for an attack on all of your accounts.

Protection: A simple and effective defense for users is to only use long, randomly generated passwords. How long? 15 characters. Rainbow tables easily crack passwords 8 or fewer characters long and in some cases up to 14 characters.

Damage Control: In the unlikely case that a rainbow table attack manages to crack one of your 15 character passwords, at least your damages will be limited to one account if you have a unique password for each account. Change the password of any account that becomes compromised due to mass theft.

4: Brute Force

Brute Force refers to discovering passwords through trial and error, similar to trying every possible combination on a lock. The most well known form of brute force attack is for password cracking software to methodically try millions of passwords on one specific user name on a specific account. A typically weak password can be cracked in less than a day using this method.

Security conscious online vendors like banks or e-mail services provide some protection against such brute force attempts by denying access if there are too many attempts per hour. However, different forms of brute force can be used to get around these safeguards. A common example is software which automatically logs in to millions of different accounts per day by combining popular user names, passwords, and web sites (i.e. try password1 at Jsmith@gmail.com, 123456 at dj@facebook.com, qwerty at Mrodriguez@yahoo.com, etc.). As such methods become more widely adopted, it would not be surprising if nearly all accounts with short user names and short passwords get compromised.

Brute force is also used as a supplementary attack after a first password is captured. For example, if the password badpassword1 was captured by phishing, brute force can be used to try similar passwords on other accounts.

Protection: Brute force attacks are highly unlikely to crack very strong passwords. So just use strong passwords. I suggest randomized 15 character jumbles.

Damage Control: Your damages are limited to one account if you have a unique password for each account. Immediately change the password of the affected account.

The Nettia University

5: Eavesdropping: Keystroke Logger on Your Browser

Many people believe that nothing bad can happen to people who only visit safe, well respected sites. They are wrong. Malicious JavaScript can be injected into any browser on any system, visiting any web site. Keystroke logging is something that is done by some of these JavaScript injections. In most browsers, malicious JavaScript can log keystrokes in all open tabs, until the browser is closed. Usernames and passwords entered during the session can be captured this way.

Protection: Keystroke logging via browser is growing more common but is unfortunately one of the more difficult threats to defend against. Defenses include:

- Use Firefox in conjunction with the No Script extension. While this is a strong defense, the overall complication of using No Script (popup, white lists, and blacklists) is more of a hassle than the average Joe wants to deal with.
- Some security suites attempt to defend against this threat with browser plug-ins, but these can dramatically slow down browsing.
- A simpler option is to only access the internet using the Google Chrome browser, which is designed so that malicious JavaScript can be theoretically contained to a single tab. At least other tabs will be safe.
- Some password managers such as RoboForm enter passwords and usernames in a way which most JavaScript keystroke loggers cannot intercept.

None of these suggestions are sure to stop browser-based keystroke loggers, but if you implement one or more of these suggestions you'll at least reduce your chances of getting your usernames and passwords logged by malicious JavaScript. The only perfect defense is to not connect to the internet at all.

Damage Control: Your damages are limited to logins captured while browsing, so long as you have a unique password for each account. Immediately change the password of the affected accounts. If using a browser-based or web-based password manager, you should also change your master password.

6: Eavesdropping: Public Wi-Fi Monitoring

Passwords are frequently stolen on public computers and over public Wi-Fi connections, using free Wi-Fi traffic monitoring software that is simple to operate.

Protection: Never log in to online accounts using a public computer. When using open Wi-Fi hot spots, you should only log in with your own notebook with services that enforce secure log-ins and sessions (HTTPS), perhaps using the Firefox Add-on HTTPS Everywhere to help. It is far safer to access email and other accounts using your phone data service, if you have one.

Damage Control: If you discover that this type of attack has occurred, then you will need to change the password for all of your accounts as well as your master password. If you know exactly when the attack occurred, you can change passwords only for the accounts you used during that session.

The Nebula University

Experiment No. 5

Aim: Study of Different attacks causes by Virus and Trojans.

Virus: The most potent and vulnerable threat of computer users is virus attacks. Virus attacks hampers important work involved with data and documents. It is imperative for every computer user to be aware about the software and programs that can help to protect the personal computers from attacks. One must take every possible measure in order to keep the computer systems free from virus attacks. The top sources of virus attacks are highlighted below:

- Downloadable Programs
- Cracked Software
- Email Attachments
- Internet
- Booting From CD

Trojans: Trojan horse attacks pose one of the most serious threats to computer security. If you were referred here, you may have not only been attacked but may also be attacking others unknowingly. This page will teach you how to avoid falling prey to them, and how to repair the damage if you already did. According to legend, the Greeks won the Trojan war by hiding in a huge, hollow wooden horse to sneak into the fortified city of Troy. In today's computer world, a Trojan horse is defined as a "malicious, security-breaking program that is disguised as something benign". For example, you download what appears to be a movie or music file, but when you click on it, you unleash a dangerous program that erases your disk, sends your credit card numbers and passwords to a stranger, or lets that stranger hijack your computer to commit illegal denial of service attacks.

The following general information applies to all operating systems, but by far most of the damage is done to/with Windows users due to its vast popularity and many weaknesses. Linux, MacOS X, and other operating systems are not as frequently infected, but they are far from immune.

Repairing the Damage

1. **Anti-Virus Software**: *Some* of these can handle *most* of the well known trojans, but *none* are perfect, no matter what their advertising claims. You absolutely MUST make sure you have the very latest update files for your programs, or else they will miss the latest trojans. Compared to traditional viruses, today's trojans evolve much quicker and come in many seemingly innocuous forms, so anti-virus software is always going to be playing catch up. Also, if they fail to find every trojan, anti-virus software can give you a false sense of security, such that you go about your business not realizing that you are still dangerously compromised. There are many products to choose from, but the following are generally effective: AVP, PC-cillin, and McAfee Virus Scan. All are available for immediate downloading typically with a 30 day free trial. For a more complete review of all major anti-virus programs, including specific configuration suggestions for each, see

The Neotia University

the Hack Fix Project's anti-virus software page. When you are done, make sure you've updated Windows with all security patches .

2. **Anti-Trojan Programs**: These programs are the most effective against trojan horse attacks, because they specialize in trojans instead of general viruses. A popular choice is The Cleaner, $30 commercial software with a 30 day free trial. To use it effectively when you are done, make sure you've updated Windows with all security patches, then change all your passwords because they may have been seen by every "hacker" in the world.

The Neotia University

Experiment No. 6

Aim: Study of Anti-Intrusion Technique – Honey pot.

Anti-Intrusion Technique: The basic underlying principles of intrusion control and distill the universe of anti-intrusion techniques into six high-level, mutually supportive approaches. System and network intrusions may be prevented, preempted, deflected, deterred, detected, and/or autonomously countered. This Anti-Intrusion Taxonomy (AINT) of anti-intrusion techniques considers less explored approaches on the periphery of "intrusion detection" which are independent of the availability of a rich audit trail, as well as better known intrusion detection techniques. Much like the Open Systems Reference Model supports understanding of communications protocols by identifying their layer and purpose, the authors believe this anti-intrusion taxonomy and associated methods and techniques help clarify the relationship between anti-intrusion techniques described in the literature and those implemented by commercially available products. The taxonomy may be used to assess computing environments which perhaps already support Intrusion Detection System (IDS) implementations to help identify useful complementary intrusion defense approaches.

Honey pot: In computer terminology, a **honey pot** is a trap set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honey pot consists of a computer, data, or a network site that appears to be part of a network, but is actually isolated and monitored, and which seems to contain information or a resource of value to attackers. This is similar to the police baiting a criminal and then conducting undercover surveillance.

Honeypots can be classified based on their deployment and based on their level of involvement. Based on deployment, honeypots may be classified as:

1. production honeypots
2. research honeypots

Production honeypots are easy to use, capture only limited information, and are used primarily by companies or corporations; Production honeypots are placed inside the production network with other production servers by an organization to improve their overall state of security. Normally, production honeypots are low-interaction honeypots, which are easier to deploy. They give less information about the attacks or attackers than research honeypots do.

Research honeypots are run to gather information about the motives and tactics of the Blackhat community targeting different networks. These honeypots do not add direct value to a specific organization; instead, they are used to research the threats organizations face and to learn how to better protect against those threats.Research honeypots are complex to deploy and maintain, capture extensive information, and are used primarily by research, military, or government organizations.

The Neotia University

Experiment No. 7

Aim: Study of IP based Authentication.

IP security refers to security mechanisms implemented at the IP (Internet Protocol) Layer to ensure integrity, authentication and confidentiality of data during transmission in the open Internet environment. The primary objective of recent work in this area, mainly by members in the IETF IP Security (IPsec) working group is to improve the robustness of the *cryptographic* key-based security mechanisms at IP layer for users who request security.

How can IP Security be achieved?

Currently, there are two specific headers that can be attached to IP packet to achieve security. They are the IP Authentication Header (AH) and the IP Encapsulating Security Payload (ESP) header.

If confidentiality is not required, the Authentication Header (AH) alone can provide security (in this case, connectionless data integrity and data origin authentication) to IP datagram. The implementation can be host-host, host-gateway or gateway-gateway. But only host-host implementation is encouraged. The reason is that, in the case that security gateway provides security service for the trusted hosts behind the gateway, The security attack can still arise when the trusted hosts become untrusted. In other words the security can be violated for two communicating end user if the security (without confidentiality) does not cover completely the communicating path, but instead stop at the gateway, even though SA is established. Certainly in any kind of implementation, the untrusted systems (i.e., the systems that don't have the SA established) can't have the ability to attack data authentication (always referring to both data integrity and data origin authentication).

The IP Encapsulating Security Payload (ESP) header provides integrity, authentication, and confidentiality to IP datagram. It can provide a mix of optional security. ESP header can be applied alone, in combination with the IP Authentication Header (AH), or in a nested way, e. g. by using Tunnel-mode. The ESP header implementation can be host-host, host-gateway, or gateway-gateway. The ESP header is inserted after the IP header and before a higher-level protocol header (Transport-mode) or the encapsulated IP header (Tunnel-mode). Gateway-to-gateway ESP implementation, using encryption/decryption , is critical for building Private Virtual Networks (PVN) across an untrusted backbone in an open environment such as the Internet.

The Nectia University

The Neotia University