Lab 01

Modern Network Security Threats

Name: Syed Asghar Abbas Zaidi	**Student ID:** 07201

Objectives

The objectives of this lab are:

- To research examples of social engineering and identify ways to recognize and prevent it.
- To research network attacks
- To research network security audit tools and attack tools

1. Social Engineering

Social engineering, as it relates to information security, is used to describe the techniques used by a person (or persons) who manipulate people in order to access or compromise information about an organization or its computer systems. A social engineer is usually difficult to identify and may claim to be a new employee, a repair person, or a researcher. The social engineer might even offer credentials to support that identity. By gaining trust and asking questions, he or she may be able to piece together enough information to infiltrate an organization's network.

Task 1.1: Research Social Engineering Examples

1. Use any Internet browser to research incidents of social engineering. Summarize three examples found in your research.

Taken from https://www.tessian.com/blog/examples-of-social-engineering-attacks/ , Scammers set a fake company that sent phishing emails to Facebook and Google employees invoicing them for stuff that other companies genuinely provided, and directed them to deposit money in their own accounts. They scammed $100 million dollars using this way.

Second incident, named Anthem Data Breach, which I learnt from https://phoenixnap.com/blog/social-engineering-examples. It took place in 2015, attackers targeted largest health insurers in U.S. , gained access to nearly 79 million people's private data (Like Social Security Number, date of birth, medical IDs e.t.c.) and sold them in dark web.

Third incident, which I am referring from https://www.tripwire.com/state-of-security/5-social-engineering-attacks-to-watch-out-for . In 2019, there was a deepfake attack on UK-based energy firm. People used AI-generated voice of parent company's chief executive to have the CEO transfer $243,000 to a "Hungarian Supplier" which was them.

Task 1.2: Recognize the Signs of Social Engineering

Social engineers are nothing more than thieves and spies. Instead of hacking their way into your network via the Internet, they attempt to gain access by relying on a person's desire to be accommodating. Although not specific to network security, the scenario below illustrates how an unsuspecting person can unwittingly give away confidential information.

"The cafe was relatively quiet as I, dressed in a suit, sat at an empty table. I placed my briefcase on the table and waited for a suitable victim. Soon, just such a victim arrived with a friend and sat at the table next to mine. She placed her bag on the seat beside her, pulling the seat close and keeping her hand on the bag at all times.

After a few minutes, her friend left to find a restroom. The mark [target] was alone, so I gave Alex and Jess the signal. Playing a couple, Alex and Jess asked the mark if she would take a picture of them both. She was happy to do so. She removed her hand from her bag to take the camera and snap a picture of the "happy couple" and, while distracted, I reached over, took her bag, and locked it inside my briefcase. My victim had yet to notice her purse was missing as Alex and Jess left the café. Alex then went to a nearby parking garage.

It didn't take long for her to realize her bag was gone. She began to panic, looking around frantically. This was exactly what we were hoping for so, I asked her if she needed help.

She asked me if I had seen anything. I told her I hadn't but convinced her to sit down and think about what was in the bag. A phone. Make-up. A little cash. And her credit cards. Bingo!

I asked who she banked with and then told her that I worked for that bank. What a stroke of luck! I reassured her that everything would be fine, but she would need to cancel her credit card right away. I called the "help-desk" number, which was actually Alex, and handed my phone to her.

Alex was in a van in the parking garage. On the dashboard, a CD player was playing office noises. He assured the mark that her card could easily be canceled but, to verify her identity, she needed to enter her PIN on the keypad of the phone she was using. My phone and my keypad.

When we had her PIN, I left. If we were real thieves, we would have had access to her account via ATM withdrawals and PIN purchases. Fortunately for her, it was just a TV show."

"Hacking VS Social Engineering −by Christopher Hadnagy https://www.hackersgarage.com/hacking-vs-social-engineering.html

Remember: "Those who build walls think differently than those who seek to go over, under, around, or through them." Paul Wilson - The Real Hustle

Research ways to recognize social engineering. Describe three examples found in your research.

Phishing is one of the most common forms of social engineering. Attackers send fraudulent emails that appear to come from reputable sources, such as banks or trusted colleagues. These emails often contain urgent messages, asking you to click on a link or download an attachment. For example, you might receive an email claiming there's an issue with your bank account and you need to log in immediately to resolve it.

Pretexting involves an attacker creating a fabricated scenario to obtain personal information. For instance, an attacker might call you pretending to be from your IT department, claiming they need your login details to fix an issue with your computer. They might use technical jargon to sound convincing and create a sense of urgency to pressure you into complying. Recognizing pretexting involves being cautious of unsolicited requests for sensitive information, especially if the requestor is creating a sense of urgency.

Baiting involves offering something enticing to lure victims into a trap. This could be a free music download, a movie, or even a USB drive left in a public place. When the victim takes the bait, such as plugging the USB drive into their computer, it installs malware that can steal personal information or give the attacker access to the system. To recognize baiting, be wary of offers that seem too good to be true and avoid using unknown devices or downloading files from untrusted sources.

Task 1.3: Research Ways to Prevent Social Engineering

1. Does your company or school have procedures in place to help to prevent social engineering?

Yes.

2. If so, what are some of those procedures?

It uses 2-FA authentication. Whenever I log-in my outlook from any computer, I must confirm that it is actually me logging-in from my mobile phone. Aside of that, they have made it so that you need to go through this process whenever you log-in. What this means is that some other unauthorized party can't get access to your email e.t.c. if you left computer open. As long as you didn't left the computer open with your email and HULMs "open" as well, the unauthorized party won't be able to access it.

3. Use the Internet to research procedures that other organizations use to prevent social engineers from gaining access to confidential information. List your findings.

Security Awareness Training: Regular training sessions help employees recognize and respond to social engineering tactics, such as phishing and pretexting

Phishing Simulations: Conducting simulated phishing attacks can help employees practice identifying and avoiding phishing attempts.

Email Gateways: Implementing email gateways to filter out spam and potentially harmful emails can significantly reduce the risk of social engineering attacks.

Multi-Factor Authentication (MFA): Requiring multiple forms of verification before granting access to sensitive information adds an extra layer of security.

Strong Password Policies: Enforcing the use of strong, unique passwords and regular password changes can prevent unauthorized access.

Data Encryption: Encrypting sensitive data ensures that even if it is intercepted, it cannot be easily accessed or used.

Monitoring and Incident Response: Continuous monitoring of systems and having a robust incident response plan can help detect and mitigate social engineering attacks quickly.

Policy Implementation: Establishing clear policies around social media usage, data handling, and communication can help prevent social engineers from exploiting human behavior.

2. Network Attacks and Security Audit Tools/Attack Tools

Attackers have developed many tools over the years to attack and compromise networks. These attacks take many forms, but in most cases, they seek to obtain sensitive information, destroy resources, or deny legitimate users access to resources. When network resources are inaccessible, worker productivity can suffer, and business income may be lost.

To understand how to defend a network against attacks, an administrator must identify network vulnerabilities. Specialized security audit software, developed by equipment and software manufacturers, can be used to help identify potential weaknesses. These same tools used by individuals to attack networks can also be used by network professionals to test the ability of a network to mitigate an attack. After the vulnerabilities are discovered, steps can be taken to help protect the network.

This lab provides a structured research project that is divided into two parts: Researching Network Attacks and Researching Security Audit Tools. Inform your instructor about which network attack(s)

and network security audit tool(s) you have chosen to research. This will ensure that a variety of network attacks and vulnerability tools are reported on by the members of the class.

In Task 2.1, research network attacks that have actually occurred. Select one of these attacks and describe how the attack was perpetrated and the extent of the network outage or damage. Next, investigate how the attack could have been mitigated, or what mitigation techniques might have been implemented to prevent future attacks. Finally, prepare a report based on the form included in this lab.

In Task 2.2, research network security audit tools and attack tools. Investigate one that can be used to identify host or network device vulnerabilities. Create a one-page summary of the tool based on the form included within this lab. Prepare a short (5–10 minute) presentation to give to the class and submit with your lab work.

You may work in teams of two, with one person reporting on the network attack and the other reporting on the tools. All team members deliver a short overview of their findings. You can use live demonstrations or PowerPoint, to summarize your findings.

Task 2.1: Research Network Attacks

In Task 2.1 of this lab, you will research real network attacks and select one on which to report. Fill in he form below based on your findings.

1. List some of the attacks you identified in your search.

NotPetya (2017), Ryuk (2018), Emotet (2014-2021), SamSam (2015-2018), Bad Rabbit (2017), Maze (2019-2020) and WannaCry Ransomware Attack (2017)

2. Fill in the following form for the network attack selected.

Name of attack:	WannaCry Ransomware Attack
Type of attack:	Ransomware
Dates of attacks:	The attack started on 12 May 2017
Computers / Organizations affected:	The WannaCry ransomware worm infected over 200,000 computers across more than 150 countries. Among the notable victims were FedEx, Honda, Nissan, and the UK's National Health Service (NHS), which had to redirect some ambulances to different hospitals due to the attack.
How it works and what it did:	

WannaCry is a type of ransomware that gains control of your system and blocks access to your files. It can infect your computer from an email attachment or through a bad website. Upon infection, a 'ransom note' pops up, offering to restore your system back to normal in exchange for $300 to $600 in Bitcoin.
It Exploited the EternalBlue vulnerability in the Windows Server Message Block (SMB) protocol.

Mitigation options:

A kill switch was discovered by security researcher Marcus Hutchins, which halted the spread. As general advice to be safe from malware like these, it is recommended to never pay the ransom as there is no guarantee that you'll get your files back. Also, paying the ransom puts a target on your back for future attacks.

It is always a good rule of thumb to always have a back-up of your own data offline. Have your system always be updated so that it has the latest security updates. MFA (Multi-factor authentication) could be used to make it so that attackers have a harder time getting to the data. EDR (Endpoint Security) could be used to detect and respond to threats in real-time.

References and info links:

https://www.etechcomputing.com/7-types-of-cyber-security-attacks-with-real-life-examples/
https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/
https://delinea.com/blog/ransomware-mitigation
https://delinea.com/blog/ransomware-mitigation

Task 2.2: Research Security Audit Tools and Attack Tools

In Task 2.2 of this lab, research network security audit tools and attack tools. Investigate one that can be used to identify host or network device vulnerabilities. Fill in the form below based on your findings.

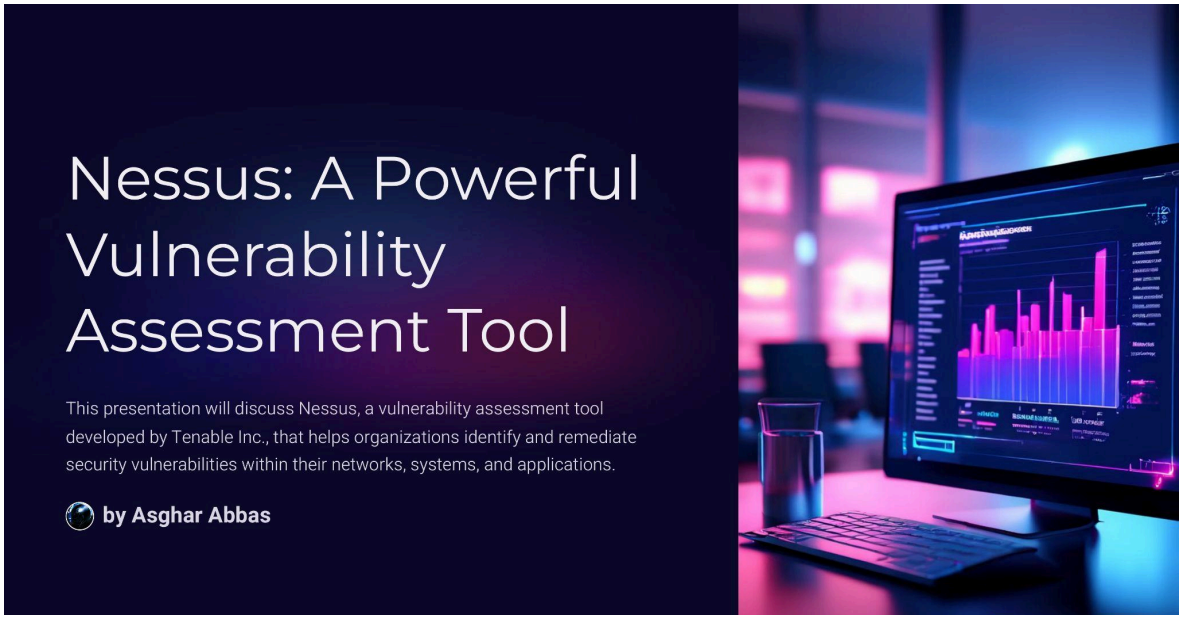
1. List some of the tools that you identified in your search.

Nessus, Metasploit, Wireshark, Nmap, AlgoSec

2. Fill in the following form for the network security audit tool/attack tool selected.

Name of tool:	Nessus
Developer:	Tenable, Inc.
Type of tool (character-based or GUI):	GUI
Used on (network device or computer host):	Computer host
Cost:	Free (with limited features) or Paid versions
Description of key features and capabilities of product or tool: Nessus is a powerful vulnerability assessment tool that identifies vulnerabilities in systems and applications, helping organizations maintain secure environments. It conducts configuration audits to ensure compliance with security policies and scans for malware and other security threats. Nessus also offers customizable reporting, providing detailed insights into vulnerabilities and compliance status. Its integration capabilities allow it to work seamlessly with other security tools and platforms, enabling comprehensive security management. The key features of Nessus include its extensive vulnerability scanning, flexible audit and compliance checks, and robust reporting functions, making it an essential tool for proactive cybersecurity measures.	
References and info links: https://www.comparitech.com/net-admin/network-security-auditing-tools/ https://www.ittsystems.com/best-network-security-auditing-tools/ https://www.tenable.com/products/nessus https://www3.technologyevaluation.com/solutions/54208/nessus https://www.spiceworks.com/it-security/data-security/articles/what-is-nessus-scanner/	

3. Prepare a short (5–10 minute) presentation to give to the class and submit with your lab work.



Additional Features of Nessus

1. **Malware Detection**
   Nessus can detect malware and other malicious threats within the network.
2. **Sensitive Data Discovery**
   It helps identify sensitive data within the network to prevent data breaches.
3. **High-Speed Asset Discovery**
   Nessus quickly discovers and profiles assets within the network.
4. **Customizable Reports**
   It provides detailed and customizable reports to help organizations understand their security posture.

Nessus Capabilities

Agentless Scanning
Nessus performs scans without the need for agents, making it easier to deploy and manage.

Nessus Attack Scripting Language (NASL)
This scripting language allows users to create custom vulnerability checks and simulate attacks.

Integration with Other Tools
Nessus integrates with various security tools and platforms, enhancing its capabilities in a broader security ecosystem.

Automated Scanning
Users can schedule scans to run automatically, ensuring continuous monitoring and assessment.

Nessus: Risk Prioritization

Vulnerability Scoring Systems

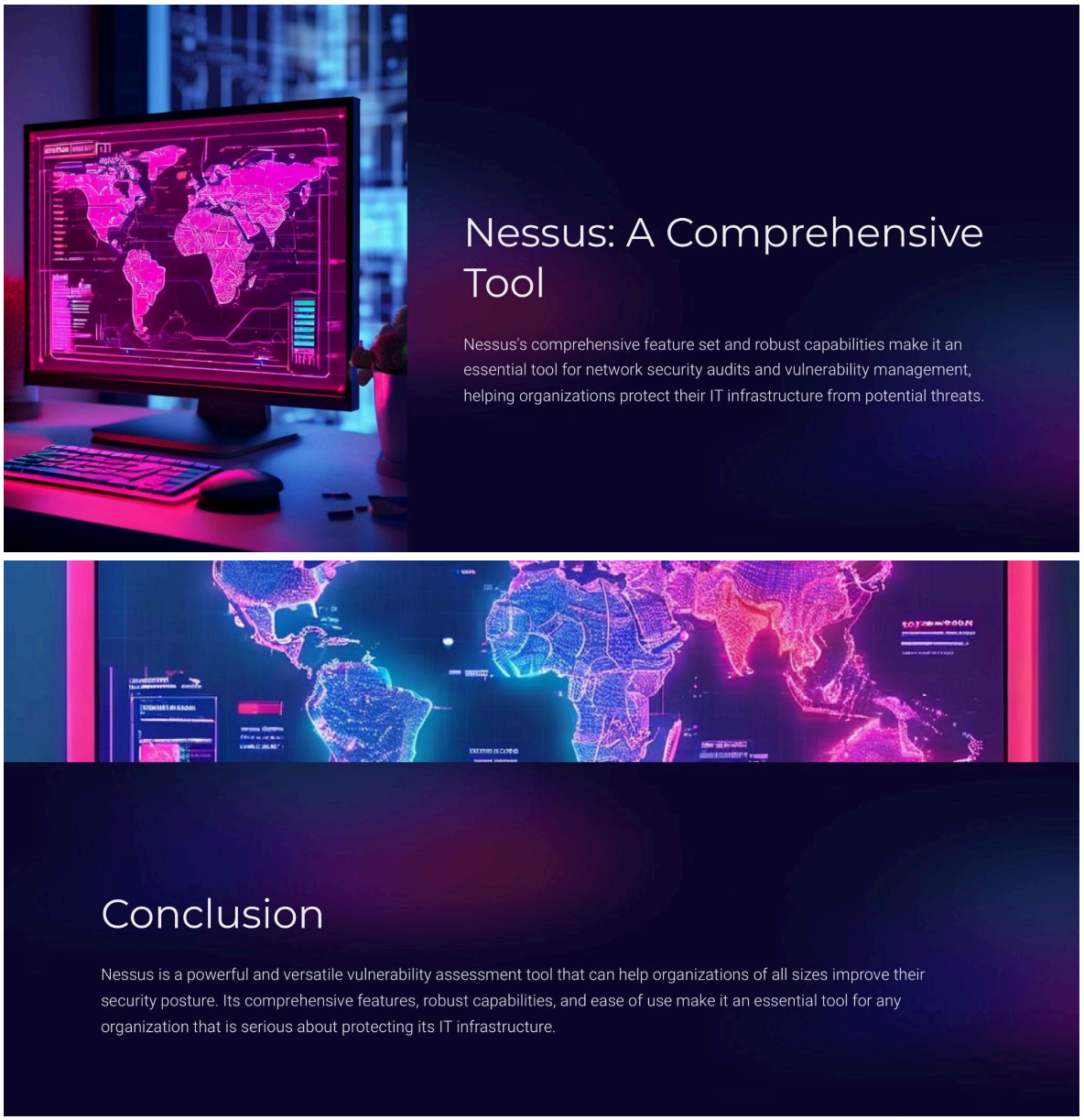
Nessus uses vulnerability scoring systems like CVSS v4, EPSS, and Tenable's VPR to prioritize remediation efforts.

Prioritization

This helps organizations focus on the most critical vulnerabilities first, ensuring efficient and effective remediation.

Nessus in Network Security Audit and Attack Tools

1. **Penetration Testing**
   Nessus is a vital tool for penetration testers to identify and exploit vulnerabilities during security assessments.
2. **Vulnerability Management**
   Organizations use Nessus to manage and remediate vulnerabilities, ensuring their networks remain secure.
3. **Compliance Audits**
   Nessus helps organizations meet regulatory compliance requirements by auditing configurations and identifying non-compliant systems.
4. **Security Audits**
   It is used in security audits to assess the overall security posture of an organization.



Task 2.3: Reflection

1. What is the impact of network attacks on the operation of an organization? What are some key steps organizations can take to help protect their networks and resource?

Network attacks can severely impact organizations by corrupting critical data, leading to significant financial losses, data theft, operational disruptions, and long-term reputation damage. To mitigate these risks, organizations should implement comprehensive security measures, including firewalls, regular security audits, antivirus and anti-malware software, data backups, access control, network monitoring, intrusion detection systems, and user education. By adopting these strategies, organizations can strengthen their defenses against network attacks and minimize potential damage.

2. Have you actually worked for an organization or know of one where the network was compromised? If so, what was the impact on the organization and what did it do about it?

The 2014 Christmas DDoS attack on PlayStation Network and Xbox Live, orchestrated by the hacking group "Lizard Squad," targeted nearly 160 million gamers by overwhelming the servers with fake traffic. This caused significant disruptions, rendering the networks inaccessible for several days during the holiday season. The attack underscored the vulnerabilities in gaming networks and the potential for major disruption through DDoS attacks.

In response to the 2014 Christmas DDoS attack, both PlayStation Network (Sony) and Xbox Live (Microsoft) worked to quickly restore services and enhance their network security to prevent future disruptions. Sony strengthened its infrastructure, offered compensation to affected users, and extended PlayStation Plus subscriptions, while Microsoft improved its DDoS protection and kept users informed throughout the recovery process. Both companies learned from the incident and took significant steps to bolster their defenses against similar attacks.

3. What steps can you take to protect your own PC or laptop computer?

To protect your PC or laptop from network attacks, install reputable antivirus software to detect and remove malicious threats, and enable the built-in firewall to monitor network traffic. Regularly update your operating system and software to patch vulnerabilities. Use strong, complex passwords and consider a password manager for added security. Additionally, install anti-malware tools, back up important data regularly, and use pop-up blockers to prevent malicious code execution. Enable tamper protection settings to safeguard your security configurations, and stay informed about the latest threats to avoid phishing and social engineering attacks.

Assessment Rubric
Lab 01
Modern Network Security Threats

Name: Syed Asghar Abbas Zaidi	**Student ID:** 07201

Points Distribution

Task No.	LR 2 Research	LR5 Presentation	LR9 Report
Task 1.1	5	-	
Task 1.2	5	-	
Task 1.3	5	-	
Task 2.1	15	/10	
Task 2.2	15	/10	
Task 2.3	15	-	
Total	/60	/20	/10
CLO Mapped	CLO1		

Affective Domain Rubric		Points	CLO Mapped
AR 7	Report Submission	/10	CLO 1

CLO	Total Points	Points Obtained
1	100	
Total	**100**	

For description of different levels of the mapped rubrics, please refer the provided Lab Evaluation Assessment Rubrics and Affective Domain Assessment Rubrics.

Lab Evaluation Assessment Rubric

#	Assessment Elements	Level 1: Unsatisfactory Points 0-1	Level 2: Developing Points 2	Level 3:Good Points 3	Level 4:Exemplary Points 4
LR9	**Report**	All the in-lab tasks are not included in report and / or the report is submitted too late.	Most of the tasks are included in report but are not well explained. All the necessary figures / plots are not included. Report is submitted after due date.	Good summary of most the in-lab tasks is included in report. The work is supported by figures and plots with explanations. The report is submitted timely.	Detailed summary of the in-lab tasks is provided. All tasks are included and explained well. Data is presented clearly including all the necessary figures, plots and tables.
	Research	No research or extremely inadequate research.	Insufficient research evident. Few sources used, some unreliable. Major issues with citations and references.	Basic research evident. Limited range of sources used. Some issues with citations and references.	Solid research demonstrated. Several reputable sources used. Citations and references accurate.
	Presentation	No presentation or a completely ineffective one.	Adequate presentation with some organization. Delivery needs improvement. Limited audience engagement.	Well-prepared presentation. Clear structure and satisfactory delivery. Adequate audience engagement.	Engaging and well-structured presentation. Clear delivery, and confident engagement with the audience