Network Vulnerability Assessment:

1. Malware (Malicious Software)

Malware is a malicious software that is unknowingly purchased, downloaded, or installed. The use of malware to exploit network vulnerabilities continues to rise, hitting an all time high of 812.67 million infected devices in 2018.

Vulnerability Identification:

Systems infected with malware will present with symptoms such as running slower, sending emails without user action, randomly rebooting, or starting unknown processes.
Malware is often deployed through phishing emails. In short, threat actors send emails to employees containing links to websites or embed attachments within the email itself. If an action is taken, such as clicking the link or downloading the attachment, the malicious code is executed and you can consider yourself breached.

The most common types of malware include:

- Viruses
- Keyloggers
- Worms
- Trojans

Viruses

A virus is the most common type of malware attack. In order for a virus to infect a system it requires a user to click or copy it to media or a host. Most viruses self-replicate without the knowledge of the user. These viruses can be spread from one system to another via email, instant messaging, website downloads, removable media (USB), and network connections. Some file types are more susceptible to virus infections – .doc/docx, .exe, .html, .xls/.xlsx, .zip. Viruses typically remain dormant until it has spread on to a network or a number of devices before delivering the payload.

Keyloggers

Keylogging, or keyboard capturing, logs a user's keystrokes and sends data to the threat actor. Users are typically unaware that their actions are being monitored. While there are use cases for employers using keyloggers to track employee activity, they're mostly used to steal passwords or sensitive data. Keyloggers can be a physical wire discreetly connected to a peripheral like a keyboard, or installed by a Trojan.

Worms

Similar to a virus, a worm can also self-replicate and spread full copies and segments of itself via network connections, email attachments, and instant messages. Unlike viruses, however, a worm does not require a host program in order to run, self-replicate, and propagate. Worms are commonly used against email servers, web servers, and database servers. Once infected, worms spread quickly over the internet and computer networks.

Trojan Horses

Trojan horse programs are malware that is disguised as legitimate software. A Trojan horse program will hide on your computer until it's called upon. When activated, Trojans can allow threat actors to spy on you, steal your sensitive data, and gain backdoor access to your system.

Trojans are commonly downloaded through email attachments, website downloads, and instant messages. Social engineering tactics are typically deployed to trick users into loading and executing Trojans on their systems. Unlike computer viruses and worms, Trojans are not able to self-replicate.

2. Social Engineering Attacks

Social engineering attacks have become a popular method used by threat actors to easily bypass authentication and authorization security protocols and gain access to a network. These attacks have increased significantly in the last 5 years becoming a lucrative business for hackers. Internal users pose the greatest security risk to an organization typically because they're uneducated or unaware of the threat.

Vulnerability Identification:

Accidentally downloading an attachment or clicking a link to a website with malicious code can cost thousands in damages.

The most common types of social engineering attacks include:

Phishing emails

Spear phishing

Whaling

Vishing

Phishing Email

A phishing email scam is an online threat that appears to be from a legitimate user or business. These scams attempt to trick users into providing sensitive information such as a username and password, downloading or opening an application, or transferring money. Phishing relies on creating false trust, which is why threat actors will often send emails from familiar websites.

Spear Phishing

Spear phishing is similar to phishing in that it attempts to trick a user. However, spear phishing attacks are designed to use personal information to get you to click a link. They will also sometimes use urgency or a risk of monetary value to bait their victims.

Whaling

Whaling is a type of phishing attack that targets a high-profile business executive or manager with more critical information to lose. Whaling emails are different from other phishing attacks in that the emails and web pages serving the scam appear to be official.

Vishing

Vishing, the combination of voice and phishing, is a phishing attack that takes place over the phone, typically a VoIP (Voice over IP) line. Threat actors are able to use tools specific to VoIP systems, thereby hacking their auto dialers to send robo messages from a spoofed VoIP address.

3. Outdated Or Unpatched Software :

Software developers are constantly coming out with new patches to fix bugs and errors to reduce vulnerabilities. Some applications are millions of lines of code long making vulnerabilities an inevitable part of software deployment. As a result, developers deploy patches to software to remediate these vulnerabilities, although patches may also be performance or feature upgrades.

Maintaining the security of software code is an ongoing battle, with major companies like Facebook, Apple, and Microsoft releasing patches daily to defend against new cyber threats. It's not uncommon for software and hardware vendors to announce end of life dates (EOL). These legacy products are often no longer profitable and cost resources (software developers) to support.Systems running Windows 7 after January 14th will pose a serious security risk to a company's network.

Mitigation Plan: Performing routine vulnerability scans and vulnerability assessments are one way to identify and remediate known vulnerabilities on your network.

4. Misconfigured Firewalls

One of the most significant threats to an organization is exposing your internal network or servers to the internet. When exposed, threat actors are easily able to spy on your traffic, steal data, or compromise your network.If the firewall isn't configured correctly to block this traffic then threat actors can monitor traffic or deploy an attack on your network.

Mitigation Plan:

Firewall penetration tests are performed to test the effectiveness of your security controls .

5. Default Security Features

Many systems today run on the Microsoft operating system (OS), however, Linux and Apple make up the three main operating systems used. In the case of Microsoft, their system ships with the default security settings enabled.

Business's default domain password policy:

- **Enforce password history** stores the number of previous passwords used. The longer a password is used the more susceptible it is to being compromised.
- **Maximum password age** determines how long the password remains in use before it expires. Experience tells us that users will not change their password unless they are forced to do so.
- **Minimum password age** determines the period of time (in days) that a password can be used before the system requires the user to change it.
- **Minimum password length** is self explanatory. The longer the password the more difficult it is to crack.
- **Password complexity requirements** include use of special characters (!$&), numbers (123), and a mixture of uppercase and lowercase letters.

- **Store passwords using reversible encryption** means encrypting and storing passwords as well as being able to decrypt them.

Mitigation Plan:

Microsoft recommends changing the password history from 10 to 24 passwords and reducing the maximum password age from 90 days to 42 days. It's ultimately the responsibility of the network administrator to ensure that the domain, workstations, and devices are set up to adhere to cyber security policies within the organization.

Vulnerability scanning tools:

1. **Tenable Nessus**
   Tenable shares scanners, schedules, scan policies, and results between different teams with customization of workflows for efficient network vulnerability management.
2. **Rapid7 Nexpose**
   Rapid7 works from discovery to mitigation of vulnerabilities. It works in physical, virtual, cloud, and mobile environments.
3. **Tripwire IP360**
   Tripwire has a continuous network management program that discovers, analyzes, and responds to vulnerabilities. Viewing capabilities help security teams develop both risk management strategies and policies to help remediation.
4. **OpenVAS**
   OpenVAS is an open-source scanner that helps security teams patch holes using a database of test plugins. With this, a framework for the management of a complete vulnerability management solution is included.

CrowdStrike Falcon:

CrowdStrike Falcon is a unifier of antivirus (NGAV), endpoint detection and response (EDR), cyber threat intelligence, and security hygiene. It uses the identification of known malware, machine learning for unknown malware, exploit blocking, and advanced Indicator of Attack (IOA) behavioral techniques to defend enterprises from breaches.

A network vulnerability scanner should identify devices, ports, operating systems, and software connected to a network, then connect this information with the latest found vulnerabilities. They can also detect misconfigurations and lack of security controls/policies within a network.Vulcan Cyber is a cyber risk management platform that simplifies your vulnerability management and

helps you own your risk. Our platform has the ability to integrate with any of these scanners so you have a comprehensive system that works for your enterprise.

Mitigation Plan:

STRATEGY # 1 – ASSET DISCOVERY & VULNERABILITY IDENTIFICATION

You need to know what you are protecting. The first step to take towards vulnerability mitigation is to deploy a discovery scan. This will catalog every device connected to your network and list every operating system, mapping those systems to their IP addresses, and enumerate the open ports and services on those systems. You can then run vulnerability scanning on each of these devices to check for openings. Determine your network's weaknesses and use this information to reduce the attack surface available for exploitation. Scans are not the only way to identify vulnerabilities. A thorough cybersecurity risk assessment is an essential and comprehensive way to identify vulnerabilities in your organization that a scan alone cannot catch.

STRATEGY # 2 – PATCH MANAGEMENT

As we mentioned before, bugs and vulnerabilities in software are inevitable. "Patches" are mitigations released by the creators of the various software and hardware to fix various bugs discovered. Applying those patches in a timely manner is critical to securing your system. Besides for threat actors taking active advantage of unsecured systems, leaving vulnerabilities unpatched opens your organization up to compliance and regulatory fines.

An effective patch management life cycle is a combination of the strategies mentioned here. Make yourself aware of the typical patch release schedules that the relevant companies tend to go by. Microsoft, for example, has a monthly "patch Tuesday" to look out for. CISA releases regular updates and keeps a catalog of Known Exploited Vulnerabilities.

STRATEGY # 3 – CONTINUOUS MONITORING AND CHANGE MANAGEMENT PLANS :

A proactive approach to vulnerability management is the most effective way to stay ahead. Unfortunately, this is not the kind of process that is ever complete. Continuous monitoring of security controls and patch releases, regular scanning and analysis of results is needed to ensure you maintain your vulnerability management goals. Change management is a critical factor in securing your systems and networks. Have policies and procedures in place to ensure that any changes, additions or subtraction (to devices, software and even the human workforce) are accounted for and considered as to how they affect the status quo.

STRATEGY # 4 – INCIDENT RESPONSE

Even with all the preemptive steps and precautions in the world, things can and will still happen. You will have an easier time reacting to a breach or attack if you have an incident response plan in place. Being able to respond to a threat event quickly and thoughtfully will reduce your exposure, minimize impact and hopefully assist operations to get back to normal as soon as possible. An incident response plan will also ensure all employees and teams know their roles, are ready to act and can efficiently mitigate any issues. Test your plan regularly and ensure you consider it as part of change management. These vulnerability management best practices are a healthy and effective way to approach risk mitigation yet the overall process can be overwhelming without the correct tools. Modern risk and compliance management platforms will offer automated tools to streamline the process throughout the cycle.

Conclusion :

Network vulnerabilities are always at threat of being compromised as malicious actors search to exploit and gain access into your business's system. Malware and social engineering attacks are the single greatest threat to an organization and its users. Outdated software often contains vulnerabilities that are not present in the current version and pose a security risk. Finally,

misconfigured firewalls and default policy settings on operating systems are at serious risk of exposure to a threat actor.