Malicious attacks

Malicious attacks basically seek to exploit vulnerabilities in a network. These threats can be passive or active and have very negative consequences. The difference between active and passive attacks are that active attacks makes changes or modifications to the data or attempt to gain some type of access to the network, while passive attacks do not make changes to the system at all.

According to Solomon, 2012, there are many malicious attacks and threats that can be carried out against the network, some of which are identified below: -Brute force attacks are one of the most tried and true attack methods where the attacker uses a software program to try all possible combinations of a password, security code or user ID, until one of them is successful. -Hijacking is another type of attack that involves the attacker taking control of a session between two machines and masquerades as one of them.

This can involve man-in-the-middle, browser or session hijacking. Social engineering is another common attack where the attacker tricks the user in carrying out actions for them; for example, the attacker may obtain the user’s login credentials by posing as an IT Specialist which would then help the intruder gain access to the network. -Computer viruses act like a biological virus, where it infects the host program and could cause the host program to replicate itself to other computers. Some of these viruses have become smarter with the capability to combat malware-detection programs by disabling their detection functions. Trojan horse is a malware program that masquerades as a useful program They use their outward appears to trick users into running them; they look like programs that perform useful

tasks but actually hid malicious code. -Rootkits are newer types of malware that modifies or replaces one or more existing programs to hide traces of attacks. -Spyware is a type of malware that specifically threatens the confidentiality of information. It does this by gathering information about a user through an Internet connection without the users' knowledge.

The impacts of all of the above attacks could damage or disrupt the system. It could also cause security privileges to be escalated to allow the intruder to access, modify or even delete private data. Additionally, as a result of any intrusion on the network, users would experience PC slowness, crashes and just no access at all to necessary resources. Malicious software is a major threat to the network, internal attackers, equipment theft and denial threats can pose even more of threat. Internal ttackers reside within the company and could be a cybercriminal, which is why it's important to monitor the threats constantly and carefully. Equipment theft can also pose a serious threat because if equipment ends up in the wrong hands, confidential information could be exposed like account numbers or access codes. Lastly, Denial threats make assets or resources unavailable or unusable by flooding a specific port on a server rendering authorized users no access to import resources, which could be a severe impact.

If there is a vulnerability in the network or organization, then there is a possibility of a threat. If the vulnerability can be eliminated or addressed, the risks of attacks or threats are greatly decreased. Some common vulnerabilities are listed below according to Radack, 2013: -In the user domain where the user lacks the awareness of security policies or accidental violation of acceptable use policy in the user domain. -In the workstation

domain there could be weaknesses in installed software and where unauthorized users could access the system.

In the LAN domain, transmitting private data unencrypted, unauthorized network access and where malicious software can be spread -In the LAN-to-WAN domain there could be exposure and unauthorized access of internal resources to the public and loss of productivity due to internet access. -In the remote access domain is where brute-force attacks occur on access and private data and data leakage from remote access or lost storage devices. In the system and application domain there could be unauthorized physical or logical access to resources and weaknesses in server operating system or application software. -With VoIP there could be default manufacturer passwords still in place, insecure class-of-service settings and trunk access group restriction settings. The impact of any vulnerability is of course the possibility of a threat succeeding. A vulnerability is considered a weakness and any weakness in a network or organization will quickly be exploited by an attacker.

The attacker is able to obtain information in all seven domains if one domain is not fully protected. For example, if a brute-force attack is deployed on a network and successful, it could affect users access to resources. Users could be in accordance with security policies and following correct protocol in order to protect the network as much as they can but if the brute-force attack is indeed successful, they efforts are thwarted. This is why it’s important to address each and every possible vulnerability in the seven domains of a network.

If users are equipped with the right security tools; workstations are secure with strict access control policies; LAN servers are secured with various standards and guidelines; LAN-to-WAN security should maintained while allowing users as much access as possible; WAN domain has confidential encryption of data transmission; remote access domain has security controls applied according to policies; lastly if the systems/application domain has security policies, procedures and guidelines implemented in the various applications or systems, all vulnerabilities would be addressed.