Responding to Network Attacks and Security Incidents

www.tech-faq.com/responding-to-network-attacks-and-security-incidents.html

Network Attacks Review

A network attack occurs when an attacker or hacker uses certain methods or technologies to maliciously attempt to compromise the security of a network. Hackers attack corporate networks to use data for financial gain or for industrial espionage, to illegally use user accounts and privileges, to run code to damage and corrupt data, to steal data and software, to prevent legitimate authorized users from accessing network services, and for a number of other reasons.

External attacks are performed by individuals who are external to the target network or organization. External threats are usually performed by using a predefined plan and the skills of the attacker(s). One of the main characteristics of external threats is that they usually involve scanning and gathering information.

Structured external threats originate from criminal hackers and are usually initiated by attackers that have a premeditated thought on the actual damages and losses which they want to cause. Possible motives for structured external threats include greed, politics, terrorism, racism and criminal payoffs. Criminal hackers are highly skilled on network design, the methods on avoiding security measures, Intrusion Detection Systems (IDSs), access procedures, and hacking tools.

Unstructured external threats originate from an inexperienced attacker, typically from a script kiddie. A script kiddie is an inexperienced attacker who uses cracking or scripted tools readily available on the Internet, to perform a network attack.

Remote external attacks are usually aimed at the services which an organization offers to the public. Remote external attacks can also be aimed at the services available for internal users, aimed at locating modems to access the corporate network, and attempts to brute force password authenticated systems. *Local external attacks* originate from situations where computing facilities are shared, and access to the system can be obtained.

Internal threats originate from dissatisfied or unhappy internal employees or contractors. Internal attackers have some form of access to the system and usually try to hide their attack as a normal process.

Hackers normally launch a number of different attacks to attempt to access a network. *Footprinting* is the initial step in hacking a corporate network. The purpose of footprinting is to create a map of the network to determine what operating systems, applications and address ranges are being utilized, and to identify any accessible open ports. *Port scanning* occurs when a hacker collects information on the network services on a target network. The hacker attempts to find open ports on the target system. A hacker might use *Enumeration* to collect information on applications and hosts on the network, and on the user accounts utilized on the network. Enumeration is particularly successful in networks that contain unprotected network resources and services. A network attacker can launch an *Access attack* to exploit a security weakness in order to gain access to a system or the network. Trojan horses and password hacking programs are typically used to obtain system access. When access is obtained, the intruder is able to modify or delete data and add, modify or remove network resources. *Unauthorized privilege escalation* is another common type of attack. Privilege escalation occurs when an intruder attempts to obtain a higher level of access such as administrative privileges to gain control of the network system. A hacker can also implement a mechanism such as some form of access granting code with the intent of using it at some future stage. *Backdoors* are installed by attackers so that they can easily access the system at some later date. After a system is compromised, you can remove any installed backdoors by reinstalling the system from a backup which is secure.

A few of the more common types of network attacks initiated by hackers are listed here:

- An *eavesdropping* attack occurs when an attacker monitors or listens to network traffic in transit, and then interprets all unprotected data. Hackers only need a sniffer technology to eavesdrop on a internet Protocol (IP) based network to capture traffic in transit.
- *IP address spoofing* occurs when an attacker assumes the source IP address of IP packets to make it appear as though the packet originated from a valid IP address. The aim of an IP address spoofing attack is to identify computers on a network.
- Sniffing occurs when attackers capture and analyze network traffic. The tools used for sniffing are called sniffers or protocol analyzers. *A Sniffer attack* occurs when hackers use Sniffers to monitor, capture and obtain specific network information, such as passwords and valuable customer information.
- *Password attacks* are aimed at guessing the password for a system until the correct password is determined. Network attackers can obtain user ID and password information and can then pose as authorized users and attack the corporate network. Attackers can utilize attacks such as dictionary attacks or brute force attacks to obtain access to resources with the same rights as the authorized user.
- A *Brute force* attack attempts to decode a cipher by attempting each possible key to find the correct one. This type of network attack systematically utilizes all possible alpha, numeric, and special character key combinations to discover a password that is valid for a user account. Brute force attacks are also typically used to compromise networks that utilize Simple Mail Transfer Protocol (SNMP).
- A *Denial of Service (DoS)* attack is aimed at preventing authorized, legitimate users from accessing services on the network. A DoS attack can be initiated by sending invalid data to applications or network services until the server hangs or simply crashes. The most common form of a DoS attack is TCP attacks.
- A network attacker can increase the enormity of a DoS attack by initiating the attack against a single network from multiple computers or systems. This type of attack is known as a *distributed denial of service (DDoS)* attack. Network administrators can experience great difficulty in fending off DDoS attacks, simply because blocking all the attacking computers, can also result in blocking authorized users.
- A *man-in-the-middle (MITM)* attack occurs when a hacker eavesdrops on a secure communication session and monitors, captures and controls the data being sent between the two parties communicating. The attacker attempts to obtain information so that he/she can impersonate the receiver and sender.

The best method of protecting a network against external and internal attacks is to *implement an Intrusion Detection System (IDS)*, and to configure it to scan for both external and internal attacks. All forms of attacks should be logged and the logs should be reviewed and followed up.

To protect your network against network attacks and security breaches, you need to be able to *predict the types of network threats to which the network is vulnerable*. This should include an analysis of the risks that each identified network threat imposes on the network infrastructure.

You should *create an Incident Response plan* to assist you with dealing with all security breaches and incidents in an orderly manner. Reacting to network attacks by following a planned approach defined by a security policy is the better approach. These security policies should clearly define the response to follow for each different type of incident, the individual(s) who are responsible for dealing with these incidents, and the escalation proedures which should be followed. Ensure that the Incident Response plan details response procedures that should take place when the network is being attacked or security is being compromised.

Your Incident Response plan should indicate who the members of the Incident Response team are. The members of the *Incident Response team* would be responsible for dealing with network attacks and security breaches when they occur. The Incident Response team should consist of individuals who are skilled and trained to deal with security incidents in a systematic manner so that the organization can quickly recover from security incidents and resume its normal operations.

Analyzing a Security Incident

A security incident can fall in either of the following broad categories of threats:

- *Cracking in progress attacks*: Cracking is the terminology utilized to refer to the illegal process of changing software, deciphering encrypted data, or evading authentication solutions to break into a system or network to access data. Cracking in progress attacks refer to threats occurring where the attacker's presence still exists on the network. If the network attacker is no longer present on the network, there is a big possibility that the attacker might still return. After an analysis of the evidence of the incident indicates this type of threat, the Incident Response team should be prepared for almost anything. Most hackers though try not to get caught. They usually access the system, install a backdoor, hide their activities, and then leave the system, only to return at some later date. Cracking in progress attacks are not typically encountered on networks while they are actually happening.
  Should you however discover a hacker actively busy on the network you can do either of the following
    - Immediately prevent the hacker from performing any further activities by blocking access to the system from the connection used by the hacker.
    - Monitor the activities of the hacker to try and establish the source.
- *Denial of Service (DoS) attacks*: DoS attacks are aimed at preventing authorized, legitimate users from accessing services on the network. There are numerous different forms of a DoS attack.
  The different methods hackers can use to initiate DoS attacks are listed here:
    - The hacker can flood the network with invalid data until traffic from authorized network users cannot be processed.
    - The hacker can flood the network with invalid network service requests until the host providing that particular service cannot process requests from authorized network users. The network would eventually become overloaded.
    - The attacker can disrupt communication between hosts and clients by modifying system configurations, or through the physical destruction of the network.

  With respect to DHCP, a denial of service (DoS) attack can be launched through an unauthorized user performing a large number of DNS dynamic updates via the DHCP server. With DNS, DoS attacks occur when DNS servers are flooded with recursive queries in an attempt to prevent the DNS server from servicing legitimate client requests for name resolution. A successful DoS attack can result in the unavailability of DNS services, and in the eventual shut down of the network. With wireless networks, the network attacker usually initiates a DoS attack in an attempt to prevent authorized wireless users from accessing network resources by using a transmitter to block wireless frequencies.

The different forms of DoS attacks are:

- Smurf attack: Smurf attacks exploit Internet Control Message Protocol (ICMP). The methods which you can use to handle Smurf attacks are listed here:
-
    -
        - Disable hosts from responding to ICMP packets transmitted to a broadcast address.
        - Disable IP broadcast traffic on perimeter routers.
        - To stop spoofed traffic from moving over the network, enable ingress filtering on perimeter

routers.

- *SYN flooding attacks*: This form of DoS attack uses SYN packets in the attack to deplete system resources. The methods which you can use to handle SYN flooding attacks are listed here:
  - Enable ingress filtering on service provider routers.
  - Configure firewalls to block SYN attacks when they actually happen.
  - To allow a greater number of simultaneous connection attempts, you should increase the size of your TCP connection buffers.
  - Consider decreasing the time out setting for TCP connection attempts.

- *Network scanning*: Scanning occurs when intruders collect information on the services and resources on a target network. Here, the intruder attempts to find open ports on the target system. A few scanning methods used by network attackers to gather information on your network are:
  - With the Vanilla scan/SYNC scan, TCP SYN packets are sent to the ports of each address in an attempt to connect to all ports. Port numbers 0 – 65,535 are utilized.
  - With a Strobe scan, the attacker attempts to connect to a specific range of ports which are typically open on Windows based hosts or UNIX/Linux based hosts.
  - A Sweep scan scans a large set of IP addresses in an attempt to detect a system that has one open port.
  - A Passive scan occurs when network traffic entering or leaving the network is captured and the traffic is then analyzed to determine what the open ports are on the hosts within the network.
  - With a User Datagram Protocol (UDP) scan, empty UDP packets are sent to the different ports of a set of addresses to determine how the operating responds. Closed UDP ports respond with the Port Unreachable message when any empty UDP packets are received. Other operating systems respond with the Internet Control Message Protocol (ICMP) error packet.
  - With a FTP bounce, the scan is initiated from an intermediary File Transfer Protocol (FTP) server in an attempt to hide the location of the attacker.
  - In a FIN scan, TCP FIN packets that specify that the sender wants to close a TCP session are sent to each port for a range of IP addresses.

  Because the attacker uses network scanning to basically collect information on your network, you should immediately block access to the network.

- *Evidence of previous compromise*: There may be occasions when you discover puzzling files on a server. This could be indicative that the system was attacked without you being aware of it. This type of attack should be dealt with immediately because the hacker could be returning at any time to fully compromise your systems.

What is a compromised system?

A compromised system is a system that had its security defences penetrated by a hacker through some form of vulnerability being exploited. In this case, the hacker usually assumed some form of control over the target system.

Systems end up being compromised when hackers find vulnerabilities in the system. A few vulnerabilities that hackers typically exploit to access and compromise systems are:

- Errors in the configuration of a network service.

- A known weakness in an underlying protocol utilized by a service hosted on the system.
- An operating system bug.
- An application bug.

A *few recommendations for dealing with compromised systems* are listed here:

- The system should be disconnected from the network.
- You should immediately report the attack to management and your law enforcement body, and you should also report the event to an incident response center.
- If possible, you should perform imaging of the system for analysis of the attack.
- Look for any modifications made to the following components:
    - System files.
    - Data files.
    - Configuration files.
    - Configuration settings
    - Deleted data.
- You should use a clean install to recover a compromised system.
- The system should then be hardened from attacks of the same nature.

Collecting Evidence of Network Attacks

Before you attempt to determine the existing state of a machine that is being attacked, it is recommended that you first record information such as the name and IP address of the machine, the installed operating system, operating system version, installed service packs, and record all running processes and services.

Collecting evidence of network attacks, involves the following activities:

- Obtaining the following valuable information:
    - Application event log information.
    - System event log information.
    - Security event log information.
    - All other machine specific event logs, such as DNS logs, DHCP logs, or File Replication logs.
- Recording all information which indicates malicious activities. This should include:
    - All files that have been modified, corrupted, or deleted.
    - All unauthorized processes running.

The main locations that you can gather evidence of network attacks are listed here:

- *System logs*: Maintaining system logs can be invaluable when faced with a network attack. When the system is under attack, you should immediately transfer a copy of your logs to a system which is not being attacked.
- *Network logs*: This includes IDS, router, and firewall logs; which are ultimately important when you need to gather information on an intrusion. Network logs are a good source of information when it comes to analyzing

the extent to an attack.

- *System state*: Hackers are also able to change system state. It is therefore recommended that you copy your system state information to a safe location and then analyze this information at a later stage.
- *Network state*: Sniffers can provide important information on the different traffic which accessed a server. You can also use a Sniffer to recreate sessions. This would enable you to analyze the sequence of events that occurred.

Neutralizing Network Attackers

There are a number of methods which you can use to neutralize the activities of network attackers. The actual method(s) which you utilize should be dictated by your security policies and your Incident Response plan.

A few common methods of neutralizing the activities of hackers include:

- Creating and applying access control lists on firewalls and routers.
- Disconnecting the system being attacked.
- Disconnecting the host being attacked from the network
- Disconnecting the site from the Internet

It i important to review an attack after it has been neutralized. Doing this could provide you with some valuable information on how to prevent the same attack from occurring. While you might not be able to completely prevent the attack from reoccurring, you should at least be able to alleviate the risk.

A hacker also almost always creates some sort of strange network traffic. You can use a Sniffer on the network to detect the presence of strange network behaviour.

How to Detect Network Intrusions

The best method which you can employ to detect network intrusions is to actually monitor for intrusions on a daily basis. While most hackers attempt to disguise their initial network attack activities, you look for any strange activities or strange files on your network.

The network also provides a variety of sources of logging information:

- *Firewall logs*: You should configure your firewalls to log all traffic that it blocks. Monitoring firewall logs is a quick way to detect an intruder’s activities. If you have configured your firewalls correctly, you should be able to discover when an attacker probes the network. Probing activities usually create extensive audit logs.
- *Intrusion detection system (IDS) logs*: Intrusion Detection Systems (IDSs) continuously monitor the network activities passing through it, and can detect any scanning and probing activities or traffic patterns that are suspicious. An IDS sends alarms when any intrusive activities are detected, and can also be configured to implement preventative measures to stop any additional unauthorized access. An intrusion detection system can be located at a number of places on the network. Sensors should be located on both the private internal network and on the external demilitarized zone. These sensors would collect all information which could be indicative of an intruder’s activities.IDS systems can be located on a host, on a network, or you can implement a combination of both methods:
    - *Network based intrusion detection*; probes or sensors are used throughout the network to monitor traffic.
    - *Host based intrusion detection*; IDS software which will monitor traffic received by hosts needs to be installed on the hosts on the network. Host based IDSs monitors the activities of the intruder and can

analyze whether the specific attack was a success.

- *Event logs (Windows hosts)*: Event Viewer is used to monitor events that took place on a computer. Event Viewer stores events that are logged in a system log, application log, and security log. The system log contains events that are associated with the operating system. The application log stores events that pertain to applications running on the computer. Events that are associated with auditing activities are logged in the security log. This makes Event Viewer a good mechanism to monitor for, and troubleshoot problems. To open Event Viewer, select Start, Select Administrative Tools, and then select Event Viewer. Simply click the Event log you would like to examine. An audit trail can be defined as a list of audit entries which portray the life span of an object, or file and folder. When an event or action takes place that's configured for auditing, the action or event is written to the security log. Security auditing events are thus written to the security log of the system, and can be accessed from Event Viewer.The main types of events which you should audit are listed below:
    - Computer reboots and computer shutdowns.
    - Computer logons and computer logoffs
    - Access to objects, and files and folders
    - System events, such as when the following occurs:
        - Computer reboots and computer shutdowns.
        - System time is modified
        - Audit logs are cleared.
    - Performance of user and computer account management activities, such as:
        - Creating new accounts
        - Changing permissions
        - Modifying account statuses
- *Syslog data (UNIX hosts)*: For Unix logging, Syslog is utilized. With Syslog, you have to be logging at the appropriate level if you want to detect security incidents on devices.

Understanding Penetration Testing

Penetration testing refers to testing the security of the defense mechanisms of a network or system, to determine whether it works, and whether there are existing vulnerabilities.

Penetration testing can test numerous different network components:

- Local area network (LAN)
- Dial-in Wide area network (WAN) links
- leased-line WAN links
- Firewalls
- Operating systems
- Servers
- Applications
- workstations

Penetration testing can also assist administrators in revealing a number of vulnerabilities in the defenses of a network:

- Incorrect configuration settings.
- Weaknesses in security processes and policies.

The *different penetration testing methods* which can be performed are listed here:

- *Remote penetration testing*: This method of penetration testing is performed from outside of the network being tested. Remote penetration testing can be carried out with no knowledge on the network, or with information and documentation on the network.
- *Internal penetration testing*: This method of penetration testing is performed from within the network being tested. Internal penetration testing is typically performed by carrying out a number of different tests, and by examining system configuration settings.

The *benefits of penetration testing* are:

- There are readily available intrusion tools in the hacking community which can be used to perform penetration testing on the network. No additional equipment needs to be purchased to perform the test.
- Penetration testing can be used to verify the effectiveness and validity of existing security policies and procedures.
- Penetration testing usually results in administrators increasing their knowledge on the systems and the network.
- By assuming the role of a hacker and then scrutinizing the network, administrators are able to identify both security strengths, and possible security weaknesses which can be exploited by criminal hackers.
- Through penetration testing, you can verify that all unusual traffic patterns are being detected by your IDS.
- You can also verify that the filters configured on firewalls are operational, and are filtering traffic as expected.
- You can use the information obtained in a penetration testing exercise to request financial support for intrusion detection systems, and firewall solutions.

A typical penetration test performed on a network should consist of the following steps:

- *Create the attack plan*: The attack plan should list all the steps that must be performed in the penetration test. An attack plan usually contains the following components:
    - The target of the attack.
    - The goal of the attack
    - A precise description of what you expect to discover.
    - The method ou plan to use to reach the goal.
    - A list of all limitations.
    - A list of possible complications
- *Scan the network*: This is usually the first penetration test performed. Hackers usually initially scan and probe the network to learn information about the network and to discover vulnerabilities:
    - *Nessus*is a freely available security scanning tool that you can use to remotely scan a network for security vulnerabilities. Nessus can run in either of following modes:

        - In Nondestructive mode, Nessus simply checks for security weaknesses which criminal hackers can exploit.
        - You can also configure Nessus to exploit any detected vulnerabilities.
    - *Network mapper (Nmap)*is another freely available tool that you can use to scan networks for vulnerabilities. Network mapper can be used to determine the following information:
        - The hosts residing on the network.
        - The operating system version running on each host.
        - The services hosted on each host.
- *Use the data collected from scanning to formulate an attack on the network*. Hackers first collect as much information from scanning, and then use this information to plan an attack against a target network.
- *Perform the actual attack*: Using all information gathered and the attack plan, the next step would be to actually attempt to penetrate the security of the network to determine what the impact of these actions is.
- *Resolve all issues*: Any issues discovered during the previous step should be resolved. It is recommended that you regularly perform penetration testing on the network.