Logic Finder
Consulting, Development and Training

Network Security Assessment

Logic Finder takes pride in providing Network and System Audit of medium to large enterprises. We use variety of tools and use a well-defined methodology to assess infrastructure. We can also provide network security audit if required by the customer

Table of Contents

1. Executive Summary

Network security assessment incorporates the reviews of security design principles, traffic flows and network & security solutions. It helps to decide the steps needed to be followed to prepare a company for network security infrastructure.

Along with the tremendous expansion of information technology and networking, the number of malicious attacks which cause disruption to business processes has concurrently increased. Despite such attacks, the aim for network administrators is to enable these systems to continue delivering the services they are intended for. Currently, many research efforts are directed towards securing network further whereas, little attention has been given to the quantification of network security which involves assessing the vulnerability of these systems to attacks. Network Security should be a top priority for all organizations and security assessments should be conducted regularly.

.

2. Introduction

Due to rapid increase in the network traffic and growing complexity of computer networks, securing a network has become a huge challenge especially in large organizations, such as government agencies, laboratories and universities with large number of users. Despite large number of serious efforts to secure communication, a strong sense of insecurity still prevails. Attackers are working hard to be ahead of most solutions. More vulnerability is discovered and security patches are released. However, it has been the case that these patches cause more problems than they solve. Despite the evolvement in protecting IT infrastructure against attacks, there is a feeling that the level of security of enterprise is still unknown. The main challenge is how to measure the level of security following software updates, addition or deletion of software and users, introduction of new hardware into organization and much more. In small organizations, anti-viruses and firewalls are the scanning tools used to protect networks from intrusions. However, such tool slack the substance against which a security metric can be built upon since they only provide a mere snapshot of the security of any given system. In large organizations, Network Intrusion Detection Systems (NIDS) are the tools incorporated for intrusion detection and protection. To secure IT networks at enterprise level, it is necessary to evaluate the performance of these NIDS. This performance evaluation helps the network administrators to improve level of security but at the cost of degradation in the network performance.

A Network Security Assessment is an audit that is designed to find vulnerabilities that are at risk of being compromised and could cause harm to business operations, or leak sensitive information. Vulnerabilities can come in various forms and are constantly changing with new technology, viruses, and applications.

3. Project Scope

1. Discovering any external or internal security vulnerabilities
2. Identifying if a combination of lower-risk vulnerabilities could be exploited in a particular sequence to create a high-risk weakness
3. Identifying security vulnerabilities in application, file, and database servers
4. Auditing and measuring the size of potential impacts of successful attacks both inside and from outside of the company
5. Testing the viability of network defenders to detect and to respond to attacks
6. Providing evidence to support increased network security

4. Types of Network Security Assessments:

Basic Security Audit (Vulnerability assessment)

This is designed to look at the security of the network from both the inside and outside of the network and reports are produced based on the weaknesses of parts of the network, and the network as a whole. This assessment will highlight areas of risk and will advise which changes will need to be made.

Penetration Testing

This audit includes the capabilities of the Vulnerability Assessment mentioned above, plus more comprehensive external, internal, and social testing. (The social testing in itself explores, as the expression implies, examination and discussion of staff methodologies and habits). When the Pen Test finds vulnerabilities in the network, it can run software that delivers a 'payload'; this helps to reveal weak links in the system. If a hacker can deploy a payload with harmful code, they could take control of segments and potentially expose the entire network. A Pen Test is performed in order to help prevent this from happening, by finding such vulnerabilities first and then, with the client's permission, actively exploiting them. The vulnerability assessment is an acceptable way to find weaknesses and areas of risk within the network but a pen test tests the true strength of the network.

A network security assessment helps determine the steps that are needed to prepare an organization, and their network for the threats of today and tomorrow. Below are the initial phases of network security assessment:

1. **Assessing the vulnerabilities of networks, applications, other IT resources.** Documenting and analyzing entire IT infrastructure to find the weaknesses and potential issues.
2. **Conducting comprehensive scanning of ports, vectors, protocols.** Conducting a comprehensive scan of all ports on network to identify the IT equivalent of open windows and unlocked doors. The most common malicious network scans search for vulnerabilities in a standard range of 300 ports on a network where the most common vulnerabilities are found. However, there may be over 60,000 ports on the network that can be suspected.
3. **Understanding how network interacts with outside parties.**
4. **Probing internal network weaknesses.** Assessing interaction with internal networks. Unfortunately, it can't be assume that all threats will originate from outside the network. Internal people can pose a threat too.
5. **Reviewing wireless nets, including Wi-Fi, Bluetooth, RFID, rogue devices.** Wireless nets, rogue devices, and removable media all present vulnerabilities.
6. **Assessing and educating employees about social engineering attacks.** This includes policies around behavior such as using social media or using shared flash drives.

Basic Steps for Assessing the Security Vulnerability of Any Network

1. Identifying and realizing the approach of a company or industry like how it is structured and managed.
2. Tracing the data, systems, and applications that are exercised throughout the practice of the business.

3. Examining the unobserved data sources capable of allowing simple entry to the protected information.
4. Classifying both the virtual and physical servers that run the essential business applications.
5. Tracking all the existing security measures which are already implemented.
6. Inspecting the network for any vulnerability

5. Network Security Assessment Methodology

The best network security assessment methodology used by security consultants involves four distinct steps:

- Reconnaissance to identify networks, hosts, and users
- Vulnerability scanning to identify potentially exploitable conditions
- Investigation of vulnerabilities and further probing by hand
- Exploitation of vulnerabilities and circumvention of security mechanisms

Reconnaissance:

Different tactics can be adopted to identify hosts, networks, and users. Attackers map the target environment by using open sources (e.g., web search engines, WHOIS databases, and DNS servers) without direct network interaction through port scanning. Reconnaissance often uncovers hosts that aren't properly fortified. Determined attackers invest time in identifying peripheral networks and hosts, whereas organizations often concentrate their efforts on securing obvious public systems (such as public web and mail servers). Neglected hosts lying off the beaten track are ripe for the picking. Useful pieces of information gathered through reconnaissance include details of Internet-based network blocks and internal IP addresses. Through DNS and WHOIS querying, the networks of a target organization can be mapped, and relationships between physical locations can be understood. This information is fed into the vulnerability scanning and penetration testing phases to identify exploitable flaws. Further reconnaissance involves extracting user details (e.g., email addresses, telephone numbers, and usernames) that can be used during brute-force password grinding and social engineering phases.

Vulnerability Scanning:

Attackers carry out bulk scanning to identify accessible network services that can later be exploited to achieve particular goals; be it code execution, information leak, or denial of service. Network scanning tools (e.g., Nmap, Nessus, Rapid7 Nexpose, and QualysGuard) perform service fingerprinting, probing, and testing for known issues. Useful information gathered through vulnerability scanning includes details of exposed network services and peripheral information (such as the ICMP messages to which hosts respond, and insight into firewall ACLs). Known weaknesses and exposures are also reported by scanning tools, which can then be investigated further.

6. Top Network Vulnerability Assessment Scanning Tools:

There are several security tools with both defensive and offensive security capabilities. We use variety of these tools to perform network security assessment.

6.1. Wireshark

Wireshark is one of the popular tools for packet analysis. It is open source under GNU General Public License. Wireshark has a user-friendly GUI and supports Command Line Input (CLI). It is a great debugging tool for developers who wish to develop a network application. It runs on multiple platforms including Windows, Linux, Solaris, NetBSD, and so on.

Some benefits of using this tool include:

- A Wireshark feature live real-time traffic analysis and also supports offline analysis.
- Depending on the platform, one can read live data from Ethernet, PPP/HDLC, USB, IEEE 802.11, Token Ring, and many others.
- Decryption support for several protocols such as IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Network captured by this tool can be browsed via a GUI, or via the TTY-mode TShark utility.
- Wireshark also has the most powerful display filters in whole industry
- It also provides users with Tshark, a network protocol analyzer, used to analyze packets from the hosts without a UI.

6.2. Nmap

Network Mapper, popularly known as Nmap is an open source licensed tool for conducting network discovery and security auditing. It is also utilized for tasks such as network inventory management, monitoring host or service uptime, and much more. How Nmap works is, it uses raw IP packets in order to find out the available hosts on the network, the services they offer, the OS on which they are operating, the firewall that they are currently using and much more.

Nmap is a quick essential to scan large networks and can also be used to scan single hosts. It runs on all major operating system. It also provides official binary packages for Windows, Linux, and Mac OS X. It also includes

- Zenmap – An advanced security scanner GUI and a results viewer
- Ncat – This is a tool used for data transfer, redirection, and debugging.
- Ndiff – A utility tool for comparing scan results
- Nping – A packet generation and response analysis tool

Nmap is traditionally a command-line tool run from a Unix shell or Windows Command prompt. This makes Nmap easy for scripting and allows easy sharing of useful commands within the user community. With this, experts do not have to move through different configuration panels and scattered option fields.

6.3. Core Impact

Core Impact is widely used as a comprehensive tool to assess and test security vulnerability within any organization. It includes a large database of professional exploits and is regularly updated. It assists in cleanly exploiting one machine and later creating an encrypted tunnel through it to exploit other machines.

Core Impact provides a controlled environment to mimic bad attacks. This helps to secure the network before the occurrence of an actual attack.

6.4. Qualys Guard

QualysGuard is a famous SaaS (Software-as-a-Service) vulnerability management tool. It has a comprehensive vulnerability knowledge base, using which it is able to provide continuous protection against the latest worms and security threats. It proactively monitors all the network access points, due to which security managers can invest less time to research, scan, and fix network vulnerabilities. This helps organizations in avoiding network vulnerabilities before they could be exploited. It provides a detailed technical analysis of the threats via powerful and easy-to-read reports. The detailed report includes the security threat, the consequences faced if the vulnerability is exploited, and also a solution that recommends how the vulnerability can be fixed.

6.5. Nexpose

It is a universal vulnerability management tool that provides reliable and prompt decisions to assess the security risk level of all kinds of networks. The key functions of this tool are to detect, assess and mitigate the security risk level exposed by vulnerabilities, misconfigurations, policy violations and malware in any IT environment having different operating systems, web applications and databases. It is stand-alone software which provides user interaction through web browser. It works with Metasploit to exploit vulnerabilities and calculates their weightage through common vulnerability scoring system, and then validates the security risk.

6.6. OpenVAS

Open Vulnerability Assessment System (OpenVAS) is an open source VA tool. It is easy to use containing less plug-ins. Most of the OpenVAS components are licensed with GNU. This tool is updated on daily basis because it supports high standard organizations.

7. Reason for Issue/Reissue

Many issues are related to the security of network infrastructure. Some issues are more technical and require the use of various tools to assess them properly. Others can be assessed with a good pair of eyes and some logical thinking. Some issues are easy to see from outside the network, and others are easier to detect from inside the network.

When the company's network security infrastructure is assessed, one needs to look at such areas as:

- Where devices such as a firewall or IPS are placed on the network and how they are configured.
- What hackers see when they perform port scans, and how they can exploit vulnerabilities in the network hosts?
- Network design, such as Internet connections, remote access capabilities, layered defenses and placement of hosts on the network.
- Interaction of installed security devices such as firewalls, IDSs, antivirus and so on.
- What protocols are in use?
- Commonly attacked ports that are unprotected.
- Network host configuration.
- Network monitoring and maintenance.

If a hacker exploits vulnerability in one of the items above or anywhere in your network's security, bad things can happen:

- A hacker can use a DoS attack, which can take down the Internet connection -- or even the entire network.
- A malicious employee using a network analyzer can steal confidential information in emails and files being transferred on the network.
- A hacker can set up backdoors into the network.
- A hacker can attack specific hosts by exploiting local vulnerabilities across the network.

8. Reference Design

Assessment of large networks in particular can become a very cyclic process. As network is assessed, information leak bugs can be investigated to find different types of useful information (including trusted domain names, IP address blocks, and user account details) that is then fed back into other processes.

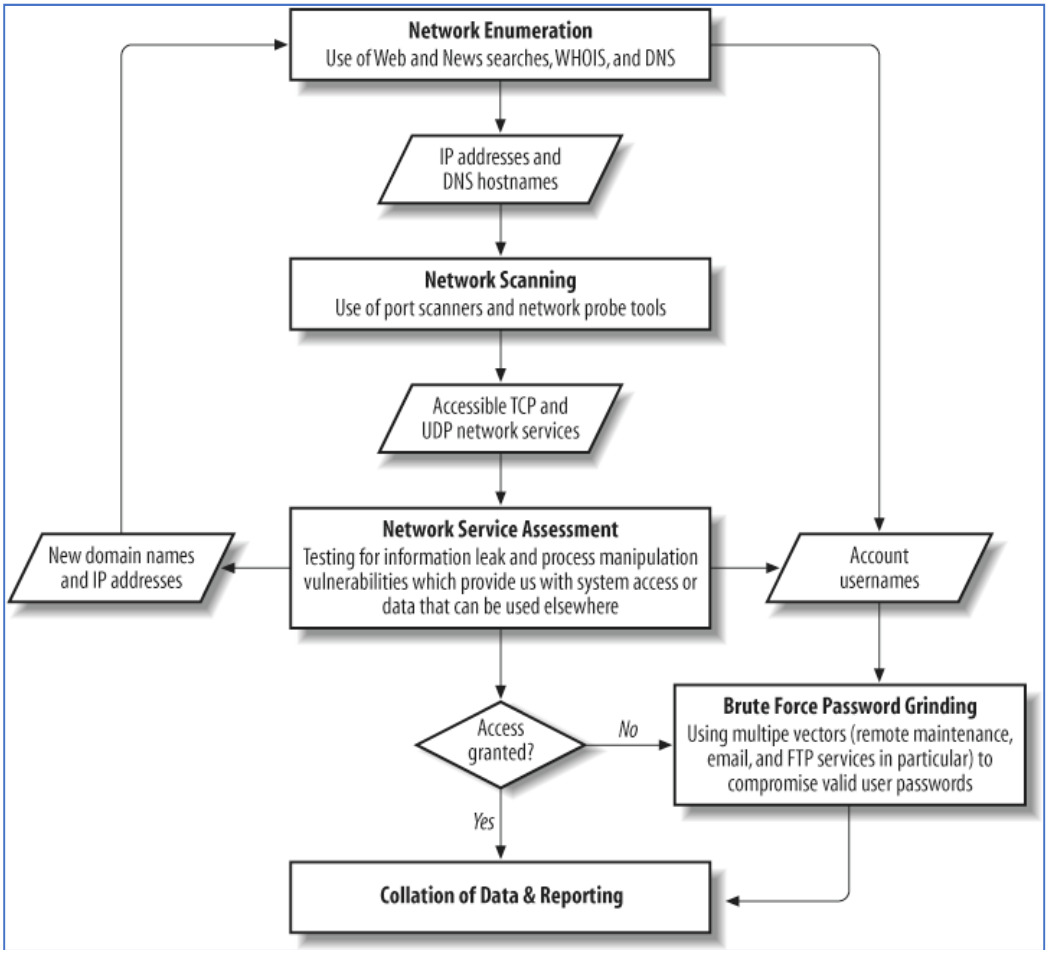

Figure: 1 Network Security Assessment Flow Chart

9. Design Overview

The overall methodology is relatively straightforward; it covers initial and full network scanning, low-level network testing (depending on the type of network and filtering mechanisms), accessible service identification, investigation of vulnerabilities, and qualification of vulnerabilities. Figure: 2 shows this flow diagram at a high-level and the data passed between each process.

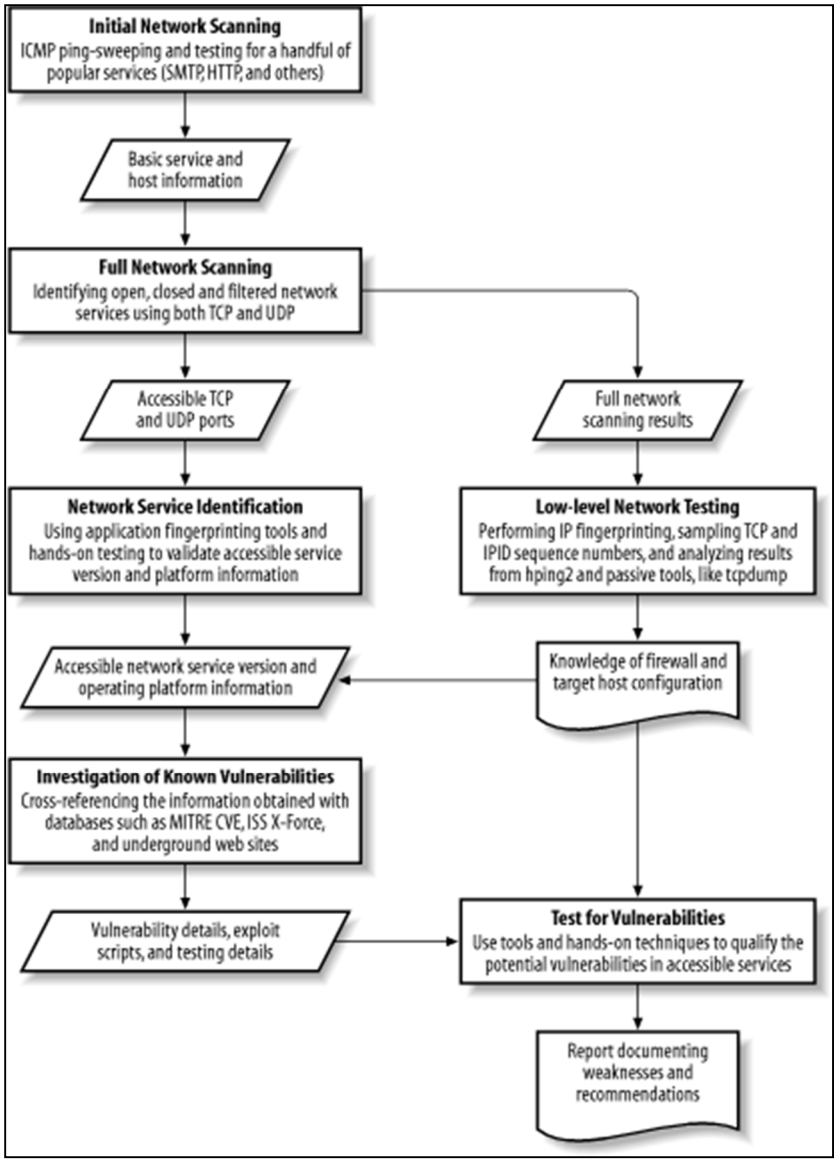

Figure: 2 A process flow diagram for network security assessment

The network security assessment is highly time-consuming to search and cross reference various web sites and information sources for accurate vulnerability information. With the help of a network security assessment, changes and improvements in an organization's architecture in order to improve overall security posture are recommended.

10. Conclusion

Regularly scheduled network vulnerability assessment can help an organization identify weaknesses in their network security before the attackers can attack. The goal of running a vulnerability scanner or conducting an external vulnerability assessments is to identify devices on the network that are open to known vulnerabilities without actually compromising the systems. While performing a vulnerability scan is an excellent start, the real value emerges from implementing a process for addressing the identified vulnerabilities. LogicFinder not only conducts the assessments using the latest in scanning technology but assures that vulnerabilities noted are addressed with easy to understand mitigation action recommendations.

The overall objective of a network security assessment is to scan, investigate, analyze and report on the level of risk associated with any security vulnerabilities discovered on the public, internet-facing devices and to provide an organization with appropriate mitigation strategies to address those discovered vulnerabilities. LogicFinder's network assessment methodology has been designed to comprehensively identify, classify and analyze known vulnerabilities in order to recommend the right mitigation actions to resolve the security vulnerabilities discovered.

11. References

1. https://www.virtual.com/blog/a-six-step-network-security-assessment-for-a-secure-2018/
2. https://www.oreilly.com/library/view/network-security-assessment/9780596510305/ch01.html
3. http://dl.hellodigi.ir/dl.hellodigi.ir/dl/book/Network%20Security%20Assessment%20Know%20Your%20Network%2C%203rd%20Edition.pdf
4. https://hub.packtpub.com/top-5-cybersecurity-assessment-tools-for-networking-professionals/
5. https://www.researchgate.net/publication/284435331_Quantitative_Enterprise_Network_Security_Risk_Assessment