National Research Journal of Information Technology & Information Science
Volume: 13 (July) Year: 2026 (Special Issue)
PP: 52-55
ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

SCANNING METHODS AND TOOLS USED FOR CYBER SECURITY

Kiranjit Kaur

Assistant professor
Dept. in Computer Science, Guru Nanak College, Moga

INTRODUCTION

Scanning is an important activity in cybersecurity that helps us to identify weakness in computer systems and networks so that we can protect our system and network before the attackers exploit it. As the technology is growing, the number of networks and systems becoming complex and the risk of security threats also increasing day by day. Vulnerability scanning is the process of automatically checking systems, networks and devices to find the weakness in security. This weakness may be due to outdated software's, Weak configurations Open ports or missing security patches.

Vulnerable scan finds security weakness in systems and networks and reduces the chances of cyber-attacks. It also helps planning security measures by showing which weaknesses are more serious and need immediate attention.

TYPES OF VULNERABILITY SCANNING

There are different types vulnerability scanning.

1. Network based scanning

Its focus on identifying weaknesses in network devices such as routers, switches, Firewalls, open port networks. This Scanning check open ports, insure services and weak network configurations.

2. Host based scanning

This scanning Scans for individual systems such as computers, servers and workstations. It looks for vulnerability in OS, installed software and user accounts.

3. Database scanning

This scanning is used to detect Security flaws in database systems such as SQL, Orace, NoSQL. This scanning checks improper user privileges, unpatched database software, exposed database and weak passwords. It's required to protect customers data, financial data and important business information.

4. Wireless network scanning

Wireless network scanning focus on identifying weakness in wireless net such as Wi-fi. It checked for poor authentication methods, weak encryption methods and presence of unauthorized access points. Wireless network scanning is important because they are the easy target for attackers.

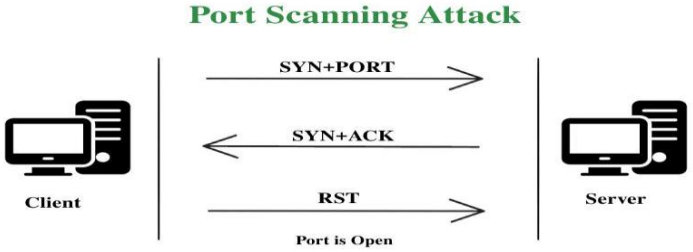
CYBER ATTACK METHODS AND PREVENTION

Following are some methods which are used by attackers to attack the system and communication network. These methods are also used by white hat hackers to prevent security breaches before its occurrence.

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

1. OPEN PORTS

Port is a virtual door that allow data to enter or leave the system. Port is used to check from which service data is coming such as web browser, e-mail application, file download program. Port number varies from 0 to 65535. Open port means a computer is ready to communicate and after communication port automatically closes. Attackers identify open ports by using a technique called port scanning. In this scanning Attacker detect which ports are open, it sends packets to these ports and analyze the response received from the target ports. Based on the response attacker plan the attack. this method also used by white hat hackers to detect weak port and generate alarm before crime occur.



PREVENTION

- **Secured Firewalls**

  A firewall can be used to track the traffic of open ports, including both incoming and outgoing traffic from the network.

  Identification of an open port is that the target post involved here is bound to respond with packets, which shows that the target host listens on the port.

- **Strong Security Mechanisms**

  Computer systems with strong security can protect open ports from being exploited.

  Security administrators should be well aware that any harmful attack should not be allowed access to computer open ports.

2. TRAFFIC PROBE

In this technique attacker analyze network traffic between different devices such as computers, servers, workstations, routers. Whenever user do some communication traffic probing closely analyze the movement of data. It collects information about source, destination, type of communication, volume and frequency of traffic and protocol used. Attackers use this information for as a base for attack. traffic probing is also useful for white hat hackers to detect unusual patterns in network and prevent suspicious activity before it occurs. Benefits of traffic probes are real time network visibility, prevention of data breaches, early detection of cyber-attacks, improved incident investigation and better network performance management.

3. VULNERABILITY PROBE

This method is used in Cyber security to identify weakness or gaps in computer systems networks. These weaknesses if left unnoticed it can be exploited by hackers or attackers to access data, disrupt services. We can use vulnerability probe to examine digital systems to find security flaws before attackers use them. It scanned systems using automated tools and predefined security rules. These tools scan network, servers, databases and applications for

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

various security flaws such as outdated software's, open ports, misconfigured settings and unpatched operating systems. Benefits of vulnerability probes are prevention of cyber-attacks, improved overall security posture, Early detection of security weakness, Continuous security improvements and help in compliance with security standards

4. NETWORK SNIFFERS

Network sniffers are tools that capture and monitor data packets through a computer network. They sniff network traffic and detect security threats. This tool is used by security professionals to detect network problem, verifying security policies, digital forensic and incident investigation.

How it works:

1. Network interface is set to Promiscuous mode.
2. Capturing and storing network packets
3. Packet decoding and analysis
4. displaying traffic information
5. identifying security issues

TOOLS FOR SYSTEM/NETWORK SCANNING

1. OPENVAS

It is a popular open-source vulnerability scanning tools used to identify weakness in system, network and communication devices and report them so that they can be fix in time. It's used to detect attacks before attacker exploit the system. It is like a security checker that check the system and point out where it is weak or unsafe. It is widely used by network administrator, ethical hackers and security teams.

How It Works:

1. Classifies system resources.
2. Assigns enumerable values to resources.
3. Detects vulnerabilities in each resource.
4. Prioritizes and recommends remediation steps.

2. METASPOLIT

It is powerful and widely used security tool that help security professionals to identify, test and validate security flaws in system and networks. It provides a well-structured environment that includes large collection of vulnerabilities and way to test them.it allow testers to safely simulate real world attacks in a legal and controlled manner.

How it works:

1. identify the target system
2. Gathering information
3. selecting, configuring and launching the exploit
4. Gaining access and testing impact
5. Analyzing results and fixing issues

ISSN: 2350-1278
Peer Reviewed & Refereed Journal (IF: 7.9)
Journal Website www.nrjitis.in

3. NETCAT AND SOCAT

Network concatenate is powerful networking tool used in cyber security and network administration. Due to its flexibility and ease of use it is commonly used for network testing, troubleshooting and vulnerability scanning. It helps security professionals to identify security weakness.

SOCAT is a socket concatenating tool used in cyber security and network administration. It's used for vulnerability testing, traffic redirection and secure communication testing. It help security professionals to analyze complex network behaviors and identify weakness in network configuration, help in firewall and security testing.

CONCLUSION

In this paper various vulnerability detection and scanning tools are discussed in detail. There is need to update these tools, as technology is growing day by day. Attackers are using updated tools to attack or steal data so to prevent these attacks security professional require up to date knowledge and scanning tools only then they can detect and protect system, networks before attack.

REFERENCES

1. M. K. Hasan, A. A. Habib, Z. Shukur, F. Ibrahim, S. Islam, and M. A. Razzaque, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and Computer Applications*, vol. 209, p. 103540, 2023.
2. N. Pattnaik, S. Li, and J. R. Nurse, "Perspectives of non-expert users on cyber security and privacy: An analysis of online discussions on twitter," *Computers Security*, vol. 125, p. 103008, 2023.
3. P. Goodman and A. Dinaburg, "The Past, Present, and Future of Cyberdyne," *IEEE Security Privacy*, vol. 16, no. 2, pp. 61–69, 2018.
4. W. J. Bill Caelli, "Cyber Warfare - Techniques, Tactics and Tools for Security Practitioners," *Computers Security*, vol. 31, no. 4, p. 637, 2012.
5. R. R. Schell, "Cyber Defense Triad for Where Security Matters," *Commun. ACM*, vol. 59, no. 11, 2016.
6. J. Park and A. Tyagi, "Using Power Clues to Hack IoT Devices: The power side channel provides for instruction-level disassembly," *IEEE Consumer Electronics Magazine*, vol. 6, no. 3, pp. 92–102, 2017.
7. A. Luse, A. Al Marzooq, and J. Burkman, "Windows ME: Using Antiquated Software to Learn About Security," *IEEE Potentials*, vol. 37, no. 2, pp. 10–12, 2018.
8. M. Kamal and M. Tariq, "Light-Weight Security and Data Provenance for Multi-Hop Internet of Things," *IEEE Access*, vol. 6, pp. 34439–34448, 2018.
9. H. Xia, Z. Li, Y. Zheng, A. Liu, Y.-J. Choi, and H. Sekiya, "A Novel Light-Weight Subjective Trust Inference Framework in MANETs," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 2, pp. 236–248, 2020.