ACONCEPT PAPER OF AN INNOVATIVE NETWORK SCANNING FRAMEWORK.

BY: GROUP 111

13/04/2017

Contents

1 INTRODUCTION

Competitive advantage is the ability of a network to derive abnormal protection in the competitive attackers. it is built the way the firm organizes and performs discrete activities of the value-chain. Innovation is important in sustaining a competitive advantage since it can represent rare, valuable and potentially inimitable sources of strong defensive mechanisms. Network scanning provides defensive techniques against intrusion of attacker on a network targeting alive hosts on a network by finding the scanning patterns in our log (manually or automatically by IDs) will give us an indication of a probable upcoming attempts to gain unprivileged access to our syste

2 BACKGROUND OF THE PROBLEM

An intelligent hacker will conduct a lot of research before attempting to gain privileged access to your systems. If the intelligence gathered shows a poorly defended computer system, an attack will be launched, and unauthorized access will be gained. However, if the target is highly protected, the hacker will think twice before attempting to break in. It will be dependent upon the tools and systems that protect the target. Again, the key here is the amount of information he has gathered beforehand. In the computer hacking world, intelligence gathering can be roughly divided into three major steps:

2.1 FOOT PRINTING

The information collected by the hacker makes a unique footprint or a profile of an organization security posture. With foot printing, using rather simple tools, we gather information such as:

- Administrative, technical, and billing contacts, which include employee names, email addresses, and phone and fax numbers.
- IP address range.
- DNS servers.
- Mail servers.

2.2 SCANNING

The art of detecting which systems are alive and reachable via the Internet, and what services they offer, using techniques such as ping sweeps, port scans, and operating system identification, is called scanning. The kind of information collected here has to do with the following:

- TCP/UDP services running on each system identified.
- System architecture (Sparc, Alpha, x86).
- Specific IP addresses of systems reachable via the Internet.
- Operating system type.

3 PROBLEM STATEMENT

Today the number of automated scanners is constantly increasing, and as a result, more and more attacks are successfully initiated. In order to be better prepared, we need to fully understand the scanning tools and the methods that these tools are using against us.

We need to identify the intruders behavior and understand the scanning techniques. If we have an intrusion detection system, or planning on implementing one in the future, finding scanning patterns in our log (manually, or automatically by the IDs) will give us an indication of a probable upcoming attempt to gain unprivileged access to our systems.

4 OBJECTIVES

4.1 Main Objective

To improve Integrity, reliable service delivery and confidentiality of Information over a network to intended users.

A penetration testing over the security of a network by simulating an attack from malicious source.

4.2 Other Objective

Enhancing security of User and group names, System banners, Routing tables and SNMP information .

5 METHODOLOGY

ICMP sweeps (ICMP ECHO requests) use ICMP packets to determine whether a target IP address is alive or not, by simply sending an ICMP ECHO request (ICMP type 8) packets to the targeted system and waiting to see if an ICMP ECHO reply (ICMP type 0) is received. If an ICMP ECHO reply is received, it means that the target is alive; No response means the target is down. Blocking ICMP sweeps is rather easy, simply by not allowing ICMP ECHO requests into your network from the void.

Broadcast ICMP Sending ICMP ECHO request to the network or/and broadcast addresses will produce all the information you need for mapping a targeted network in even a simpler way. The request will be broadcast to all alive hosts on the target network, and they will send ICMP ECHO reply to the attacker source IP after only one or two packets have been sent by him.

TCP Sweeps The TCP connection establishment process is called the three way handshake, and is combined of three segments. When will a RESET be sent? Whenever an arriving segment does not appear correct to the referenced connection. Referenced connection means the connection specified by the destination IP address and port number, and the source IP address and the port number . Bear in mind that firewalls can spoof a RESET packet for an IP address, so TCP Sweeps may not be reliable.

UDP Sweeps (Also known as UDP Scans) This method relies on the ICMP PORT UNREACHABLE message, initiated by a closed UDP port. If no ICMP PORT UNREACHABLE message is received after sending a UDP data gram to a UDP port that we wish to examine on a targeted system, we may assume the port is opened.

6 OUTCOME

A network scanning framework to scan for port, exploits, vulnerabilities, misconfigurations, launch DOS attack and crack passwords A network intrusion detection/prevention system, that can detect a variety of attackers and probes, such as buffer overflows, stealth port scans, web application attacks, SMB probes, and OS fingerprinting attempts. To have a framework for developing and executing exploit code against a remote target machine that to say able to check whether the intended target system is susceptible to the chosen exploit ,choosing and configuring a payload(code that will be Executed on the target system upon successful entry, for instance a remote shell or VNC server) and able to find the encoding technique to encode the payload so that the intrusion prevention system will not catch the encoded payload.

References

[1] C.R.KOTHARI ,Former Principal, college of Commerce University of Rojasthan, Jaipur(India)

[2] http://en.wikipedia.org/wiki/snort(software).

[3] http://en.wikipedia.org/wiki/metasploit.