Cyber Reconnaissance: An Alarm before Cyber Attack

H. P. Sanghvi
Research Scholar
Institute of Forensic Science
Gujarat Forensic Sciences University

M. S. Dahiya, PhD.
Director
Institute of Forensic Science
Gujarat Forensic Sciences University

ABSTRACT
Today's cyber world is more than the internet. It is interdependent networks containing telecommunication network, embedded system and critical infrastructures. Malicious attacks on critical infrastructure become a major threat to business and government operations. An easy and fast access to network makes business successful and makes sensitive information more vulnerable to cyber thieves. Today's attacker and hacker is skillful and well equipped with various hacking tools can easily exploit a small vulnerability. Reconnaissance is a first phase of cyber-attack and we will study this phase show effective countermeasures. This paper is about the Cyber Reconnaissance and focused on Port Scanning and OS Fingerprinting attack and proposed some easy to use solutions.

General Terms
Cyber Security, Cyber-Recon.

Keywords
Cyber Attack, Information Assurance, Information Security, Cyber Reconnaissance.

1. INTRODUCTION
We are living in a world where our whole information is stored in digital format and available online for easy and faster access. Our most critical infrastructures like banking, aerospace communication, science & Technology should be available anytime. As information become online it becomes vulnerable and can be hacked by attacker. So for security of information some course of actions is mandatory. These actions are inform of various security measures as a part of achieving system hardening.

The phases of cyber-attack generally follow same pattern as a traditional crime. The first phase of attack is reconnaissance of the victim. By observing the normal operations of a target useful information can be collected such as hardware and software used, communication pattern etc.. Hackers scan and probe networks before they attack in order to get information about the target.

This paper is focused on the cyber reconnaissance specially Port Scanning and OS Fingerprinting. Some detection and remedies are also proposed.

2. CYBER ATTACK
Five pillars of information assurance are confidentiality, integrity, availability, non-repudiation and authentication. So we can consider an attack that violates any of the pillars is a cyber-attack.

So attacker is trying to violate any of the pillars or as many as possible for successful attack on a targeted system. Target could be a single host or a network, or a large information system infrastructure.

3. ATTACK PHASES
Three attack phase 1. Reconnaissance, 2. Infiltration and 3. Conclusion of a cyber-attack.

3.1 Reconnaissance Phase
In this phase weak points of the target system is identified. Enough resources should be applied for this phase to find weakness in victim's defenses or to access victim's capabilities. Any information gathered about the victim may be crucial needed to be revealed critical weakness in defense. Critical information that can be obtained during these phase is listed in below table.

Table 1 Information gathered in reconnaissance phase [6]

Network Information	• IP addresses • subnet mask • network topology • domain names
Host Information	• user names • group names • architecture type (e.g. x86 v/s SPARC) • operating system family and version • TCP and UDP services running with versions
Human Information	• home address • home telephone number • frequent hangouts • computer knowledge • dark secrets
Security Policies	• password complexity requirements • password change frequency • expired/disabled account retention • physical security (e.g. locks, ID badges, etc.) • firewalls • intrusion detection systems

3.2 Infiltration Phase
In this phase attacker's goal is to take control of the target by gaining remote access to shell or terminal as the administrator on the host. Knowing vulnerability is not enough for attacker, he should know how to exploit it.

For an attacker it is not necessary to know advanced knowledge of programming but having it improve the success

chance. Anyone can guess a weak password but developing a custom program to exploit vulnerability requires skill and programming knowledge. There are lots of tools available on internet for exploitation one of them is metasploit.

3.3 Conclusion Phase

This phase is for ensuring the goal is achieved and removing the traces which leads to the attacker. In general practice this is the most difficult phase as computers keep records of every logon, logoff, startup, shutdown, network connection, program execution and error received. So it's almost impossible for the attacker to remove all traces of intrusion from the target computer.

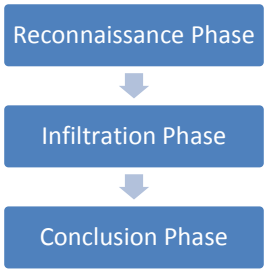

Fig 1: Phases of Cyber Attack

4. RECONNAISSANCE TYPES

Table 1 show critical information gathered during reconnaissance phase. Attacker gathers this information using two methods: Active Reconnaissance and Passive Reconnaissance.

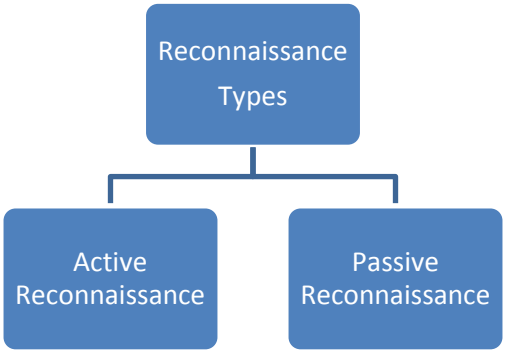

Fig 2: Types of Reconnaissance

4.1 Active Reconnaissance

Active Reconnaissance means trying to recon target using various tools like ping, traceroute, netcat etc. By using ping we can get information of pinged IP address, traceroute used for finding information of packet route and router information and netcat is used to know which ports are open to listen.

Active reconnaissance is commonly referred to as *scanning*. Scanning is more offensive than footprinting as there is more risk that the target may be alerted for possible attack.

nmap is a popular tool used for scanning. Other tools netcat, traceroute and ping are also widely used.

4.2 Passive Reconnaissance

Passive reconnaissance is also known as *footprinting* means minimizing interaction with the target which generates alert in logs. It is a gathering the information without alerting victim. If the victim host alerted then it drastically increases security against the attack.

Today lots of information is available on internet. For example www.whois.com is a web site providing information of DNS and other services freely which is widely used by the attacker for gathering target web server and host related information.

One more example for gathering such information passively, if any company puts an advertisement for opening for a system administrator and asking proficiency in Linux environment then it can be inferred easily that this company use Linux environment widely.

5. TOOLS & TECHNIQUES USED

In order to gather information from the target host attacker normally use port scanning and OS fingerprinting techniques. Namp is used for port scanning, TCPDump is used for collecting data, Snort is used for detection of port scan and OS fingerprinting.

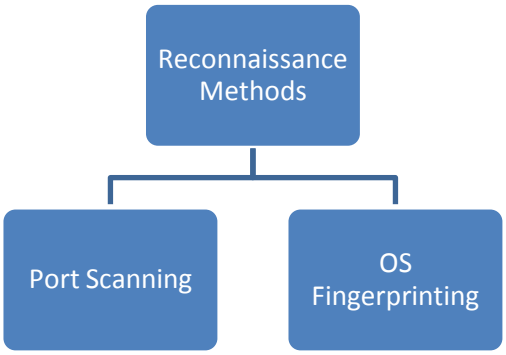

Fig 3: Reconnaissance Methods

5.1 Port Scanning

Port Scanning is a systematically scanning computer ports as whole information is going in and out is through port and port scanning identifies open ports to a computer. Through port scanning attacker infer which services are visible and where attack is possible. Basic principal of port scanning is that to retrieve data from the opened port and analyze it.

There are several methods to perform port scanning. Each method has its pros and cons. Some methods are TCP Null, TCP SYN, TCP Xmas, TCP FIN and UDP port scan.

There are several methods for detection and blocking of port scan attack. Any service or peripheral that recognize scan packet and drop it, is a effective method for blocking scan. But normally we find that different scans have their unique signature. A NULL, XMAS, or FIN scan would be detected and blocked by a stateful device. By default snort is installed with stateful IDS active that's why snort can detect FIN, NULL, and XMAS scans.

TCP SYN and UDP scans appear to be legitimate connection attempts to the target but their only distinguishing characteristic is that they hit multiple ports. This should certainly not occur five times in less than a second from the same source. By correlating connection attempts it can be concluded that the source IP was performing a scan on target machine, as the source made five connection attempts to different ports in less than a second.

5.2 OS Fingerprinting

OS Fingerprinting is a method for determining which operating system does the remote computer runs. OS Fingerprinting is mostly used for cyber reconnaissance as most exploitable vulnerabilities are operating system specific.

Like trying to find vulnerability of IIS server on Linux machine is leads to a failure. If an attacker succeed to get remote operating system name then it will be easy for him to exploit the vulnerability of a target system and has to concentrate only on the known vulnerability which leads to great chance of success in comparatively less time and less risk of getting detected..

OS fingerprinting also has several method like port scanning method to successfully fingerprint the operating system. Basic method behind OS fingerprinting is to distinguish each OS characteristic which can be acquired from the remote system. These method can be examining default TCP window size in a packet, measuring data in ICMP packets, guessing TCP initial sequence number etc..

TCP Banner is one of the method for OS fingerprinting. Namp and Ring are the tool widely used for OS fingerprinting.

OS fingerprinting relies on data gathered from normal IP address traffic so it is very difficult to block OS fingerprinting. One way to do is that block direct access to sensitive computer systems. This can be done by Network Address Translation (NAT) which leaves only one machine susceptible to most external OS fingerprinting.

6. COUNTERMEASURES

There is a remarkable research work done to detect cyber attack at reconnaissance phase. Reconnaissance is a primary and starting phase of any cyber attack so if any solution for detecting cyber reconnaissance can be a good achievement in the course development of effective early warning system.

Cyber attack is sequence of reconnaissance, infiltration and conclusion phase. A layered protection is always best but defense strategies for different network will be different. Stateful firewall, Intrusion Detection System, Intrusion Prevention System and NAT are preferable solutions. Firewall should be configured to allow only necessary traffic and also configured to log multiple connections from the same IP address. This implementation assures block scans such as FIN, NULL, XMAS and detect SYN scan as firewall is stateful.

Snort like tool should be used which work as IDS that monitors traffic and detect anomalous activity. Snort should be configured to detect multiple connection from the same IP address.

Using NAT is a good practice as it will put only single IP visible and block OS fingerprinting attempts. Apply all latest patches to block vulnerable points.

7. CONCLUSION

This paper is targeting on the Reconnaissance phase of the cyber attack and we have studied Port Scanning and OS fingerprinting. This paper shows some types of Port Scanning and OS fingerprinting and also listed some countermeasures against the attack.

This paper does not cover all possible reconnaissance events but covered events helps security professionals. In future new techniques of countermeasure against the Port Scan attack and OS Fingerprinting attack can be included and also more attacks can be included and their countermeasures can be proposed.

8. REFERENCES

[1] Collin Engelbert Peter van Loon, 2012, Offensive Cyber, Royal Netherlands Army.

[2] Leyla Bilge & Tudor Dumitras, 2012, Before We Knew It An Empirical Study of Zero-Day Attacks In The Real World, ACM Conference on Computer and Communications Security.

[3] Dell SonicWALL, 2012, Anatomy of Cyber Attack

[4] Homeland Security, 2009, A Roadmap for Cyber security Research.

[5] Don Davidson, 21-01-2013, Thwarting Stealthy Attacks with Anti-Reconnaissance, http://www.port80software.com/support/articles/antireconnaissance_security.asp

[6] U.S. Naval Academy, 21-01-2013, SI110: Phases of a Cyber-attack/Cyber-recon, http://www.usna.edu/cs/si110arch/si110AY12F/lec/l32/lec.html

[7] SANS Institute 2003, Network Reconnaissance – Detection and Prevention