Penetration and Countermeasures of Cyber-attacks against Digital Assets of an Organization: A Case Study

Santosh Kumar Sahu, ONGC Limited, GEOPIC, Dehradun
Sanjay Kumar Jena, National Institute of Technology Rourkela, Odisha
sahu_santosh@ongc.co.in

Keywords
Cyber Security, Penetration Testing, Intrusion Detection

Summary

In this paper, we have experimented different types of penetration techniques that are used to compromise computer networks. It also discussed different cases of attacking scenarios along with their behavior, severity, and countermeasures. The paper focuses on how insiders are being targeted by the attacker or involved in the malicious activity. The DoS, Probe, U2R, and R2L attacking tools are used in this experiment. As per recent studies, the insiders are the major source of a threat as compared to outsiders of a corporate network. The objective of this work is to create awareness related to information security among the employees of an organization to protect digital assets from intruders.

Introduction

Due to rapid growth in threats to the computer network and network-based applications day-by-day, it's a major challenge for organizations to design security infrastructure that countermeasure various intrusive efforts. The corporates commonly use the closed network. Typically, the closed network consists of a network that designed and implemented in a corporate environment and only accessible by known parties and users without connecting to the Internet. The intruder may be the insider or the outsider, whose intention is to access the digital resources of the organization maliciously. The insiders are the major threat as compare to the outsiders (1). To exploit the corporate network, the intruder steals credentials of the users using various reconnaissance approaches and analysis the vulnerability of the network by physically access the network.

The hackers have opened a tiny number of phishing sites to acquire sensitive information such as username, password, and other details often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication. The sites contain useful information along with malicious codes which may harm/probe your system's information. They require a platform using which communicate to your system without the knowledge of the user. Most of the cases, the insiders are intentionally or unintentionally responsible for the attack. It is frightening how careless many users are about corporate security. For example, 40% of all users who have access to a corporate infrastructure use the same login credentials on other non-corporate sites such as Facebook, Twitter, and LinkedIn. The hackers simply compromise the corporate security system by applying social-engineering attacks on their personal credentials. In the recent cyber-attack, the hackers had stolen $951 million from Central Bank of Bangladesh. As per the preliminary investigation, the hackers used stolen credentials to make requests to transfer cash that pretends as legitimate transactions.

The competitor probe information about the organization by hiring the hackers. The hackers gather information by first targeting the insiders. Therefore, the primary goal is to protect the data and ensure the data availability and integrity. Furthermore, several denials of service (DoS) attacks can be launched to stabilize the organization. The intention is to deny access to the resources of the organization for the legitimate users. To ensure the security of the digital assets of the organization, state-of-art detection approach should be adopted that is the challenging task.

In this paper, we have reviewed the threats being faced by the organization and its users and some proactive awareness to mitigate these threats. The network threats broadly classified as DoS, Probe, U2R, and R2L as per the attack patterns (2). The DoS and Probe are the two major attack categories that are frequently applied to the network. However, if the defense mechanism denies DoS and Probe attacks, then the attacker prepares for U2R and R2L attack by

Table 1: Attacking Tools used in this study

Sl. No.	Tools Name	Attack Type
1	DDOSIM	DoS
2	NEMESIS	DoS
3	JAVALOIC	DoS
4	Dequiem	DoS
5	Ufonet	DoS
6	Dark Fantasy	DoS
7	Hyenae	DoS
8	AnDDoS	DoS
9	HOIC	DoS
10	LOIC	DoS
11	NEMESIS	DoS
12	JAVALOIC	DoS
13	Nmap	Probe
14	Angry IP Scanner	Probe
15	NBTscan	Probe
16	Nikto	Probe
17	P0f	Probe
18	THC-RUT	Probe
19	Webspy	Probe
20	Zodiac	Probe
21	Dmirty	Probe
22	Nukepw	U2R
23	Loadmodule	U2R
24	Sql injection	R2L
25	Xterm	U2R
26	Password Sniffer Spy	R2L
27	Cain & Abel	R2L
28	Dict	R2L
29	ftp_write	R2L
30	Multihop	R2L

stealing insider's credential's using various social engineering attacking tools. To study different kinds of attack, and their behaviors, latest attacking tools are considered in this experiment. The tools are applied to Windows and Linux platforms and reveal the characteristics, behavior, and severity of loss due to the attacks. Also, various phishing techniques that are used by the hackers for stealing information are discussed. All the case studies discussed in this paper helps the reader to know details about different kind of threats and their countermeasures. It also provides information about various phishing methods adopted by the attackers that spread awareness about do's and don'ts. The rest of the paper organized as follows. Section 2 describes experimental details, Section 3 presents result and discussion, section 4 elaborates countermeasures against the attacks, and Section 5 contains the conclusion of this study.

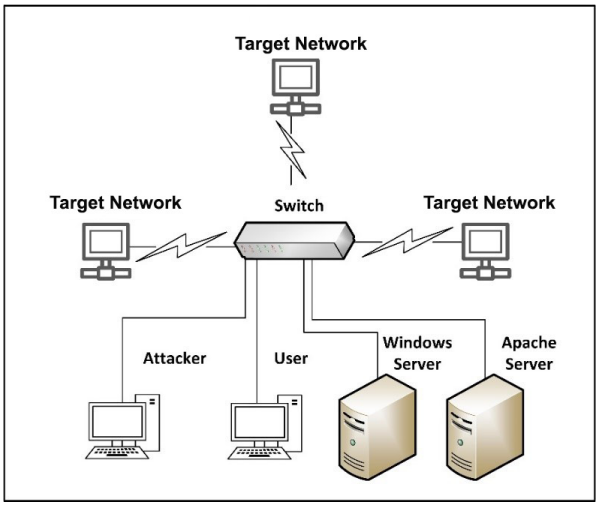

Figure 1: Testbed Network Architecture

Experimental Details

The testbed of network architecture used in this experiment is given in Figure 1. In this experiment, we have considered four workstations namely Attacker, User, Windows Server and Apache Server as given in Figure 1. All are connected to the corporate network. All the attacking tools listed in Table 1 launched on attacker PC to the servers and demonstrates its severity, behaviors, and patterns in details on User PC. The two servers are used as victim/target server that is being attacked. On the other hand, the countermeasure policies are deployed on the target server to protect such attacking efforts and provides an additional security layer to the network. The details case studies on Dos, Probe, R2L and U2R attacks are given in result discussion section.

Penetration Testing

The following penetration testing is conducted in this experiment.

DoS: The Denial of Service attack is most dangerous that violates the availability property of CIA (Confidential, Availability and Integrity) triad of the security model. The Figure 2 describes the severity of the attack. We have launched DoS attack using HOIC tool for two minutes and it consumes approximately 6 GB network bandwidth. If it continues then the whole network bandwidth may be occupied and the legitimate user not able to access their network.

Probe: The objective of this kind of attacks is to acquire as much as information about the victim. The acquired information is compiled by the attacker to know about the vulnerability exist in the victim or not. The attacker exploits using the known vulnerability exists and decides what and how to compromise the victim. Using this, the attacker knows about the victim's operating system, application control, availability of ports, network settings, security policies, application program information. In our experiment, we have applied this attack to gather information from the target host such as OS information, browser information, open ports, firewall exists or not, IDS exist or not. The basic objective of this attack is to reconnaissance and planning for launch the attack. To gather information of a host/server, Nmap is used in our experiment. The Figure 4 contains the Nmap result of a host. It contains the open and closed ports, service, states, and operating system's information.

U2R: In this attack class, the attacker has local access to the victim machine and tries to gain super user privileges. This type of attacks mostly applied by insiders who are trying to access the super user privilege. The common attacks are sechole, xterm, ntfsdos, nukepw, secret, perl, ps, yaga, fdformat, ppmacro ffbconfig, casesen, loadmodule and sql attack. Out of which, we have considered the tools which are mentioned in Table 1. In Figure 3, the sniffed network information along with the credential is given (password is darken due to security issues).

R2L: In this attack class, the attacker does not have any credential to access the network, but tries to gain access either by bypassing or stealing insider's credential. The mostly popular tools are dict, netcat, sendmail, imap, ncftp, xlock, xsnoop, sshtrojan, framespoof, ppmacro, guest, netbus, snmpget, ftpwrite, httptunnel, phf, named, multihop and much more. Out of them, we have considered the attacking tools mentioned in Table 1 in this experiment. We have capture Email, Web and FTP login passwords passing through the network. The tools, automatically detect the login packets on a network for various protocols and instantly decodes the passwords. Password Sniffer Spy supports the HTTP (BASIC authentication), FTP, POP3, IMAP, SMTP protocols**.** Similarly, Cain & Abel is another powerful network sniffer commonly used by hackers. It allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force, and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords and analyzing routing protocols. The program does not exploit any software vulnerabilities or bugs that could not be fixed with little effort. It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources. However, it also ships some "non-standard" utilities for Microsoft Windows users (8).

However, in the case of HTTPS protocol, the password sniffers do not work. In this case, the hackers use Remote Administration Tools (RATs) to control, capture activities and monitors the victim system both in online and offline. A remote administration tool (RAT) is a piece of software that allows a remote "operator" to control a system as if he has physical access to that system. While desktop sharing and remote administration have many legal uses, "RAT" software is usually associated with the criminal or malicious activity. Malicious RAT software is typically installed without the victim's knowledge, often as the payload of a Trojan horse, and will try to hide its operation from the victim and security software. The most well-known RATs are listed in Table 2. The operating system password can be compromised using known vulnerability. Many tools are used to compromise Windows, Linux and Mac user and administrator passwords. The most well-known tools are Ophcrack, Kon-boot, Offline NT Password & Registry Editor, Cain & Abel, John the Ripper and Trinity Rescue Kit.

The combination of more than one attack even more dangerous. The hackers group implemented new attacking tools to deny access to the resources like ransomware. The ransomware heavily affected the digital environment in 2017. Most of the affected organization are trapped and data loss due to this. Therefore, we have also mentioned the guidelines to avoid such situation.

Table 2 List of Notable Remote Desktop Tools

RAT Name	OS	Features
Dark Comet	W	Keylogging Monitoring Remote Desktop Snapshot Access Devices Access Services Remote Control File management Hardware Destroyer Windows Registry
Black Shades	W	
JSpy	W, L, M	
Pussy RAT	W	
Bozok RAT	W	
jRAT	W, L, M	
Cyber Gate	W	
DameWare RAT	W	
Nj Rat	W, L, M	
Poison lvy Rat	W	

Note* W=Windows, L=Linux, M= Mac

Countermeasures

The following mitigation approaches are adapted to protect the digital assets of an organization.

By spreading awareness of security guidelines

To mitigate such attacks, the first and foremost approach is to educate employees about computer security by conducting security awareness training. A good security awareness program should educate employees about corporate policies and procedures for working with information technology. Employees should receive information about whom to contact if they discover a security threat and be taught that data as a valuable corporate asset. Regular training is particularly necessary for organizations with high turnover rates and those that rely heavily on contract or temporary staff. All employees belong to any discipline should participate and aware the common information security guidelines, policies and security safety measures to handle the computer systems. For example, never click a link or open an attachment without scanning with an antivirus software. Similarly for offline work, never give administrator privilege to an application, without scanning it. They would know about the dos and don'ts adopted by the organization on information security perspective. As per recent threat reviews, the insiders are the biggest threat on a compromise of corporate security policies as compare to outsiders. Hence, if all the employees aware regarding the security guidelines then it is very easy to defense network breaches. Therefore, the organization should conduct awareness programs via hands-on training and workshops to educate information security issues and its mitigation approach.

By using Enterprise Endpoint Security Solutions

Nowadays the endpoint security solutions provide comprehensive protection from virus, worms, rootkits, zero-day vulnerabilities, malicious traffic, RATs, and botnets. Some solutions based on signature and some are based on hybrid approach. The hybrid approach does not explicitly required a signature to detect unknown attacks. The detection engine working in anomaly, behavior and signature based approaches. Hence, it can detect the zero-day vulnerability attack and protect the unwanted, intrusive efforts. It provides customizable options to implement rules for web control, application control, device control and data control features. The network administrator can easily monitor, control and deploy clients using a centralized console or web console to interact the endpoint solution. The prime objective of using this solution is to monitor all the corporate systems which are connected to corporate network. None of the systems should connect the network without the endpoint client. It means the network is accessed by only the registered user that are bound to obey the network security policies. Therefore, an intruder cannot be used any corporate client machine to compromise the network.

Privilege based solutions

These solutions specially designed to the insiders who are intentionally or unintentionally involved in the intrusive effort. Sometimes the attacker gets access to the network as an insider and operates undetected for months by impersonating as authorized users. As a result, the security solutions are unable to detect them that becomes a major threat

to the organization. It causes a huge loss in term of reputations, financial losses and stolen intellectual property. Privileged based solution, is an intelligence security system that detects, alert, and respond to the cyber-attacks targeting privileged accounts. It is designed to identify the attacks in real-time and responds to the intrusive effort as per the action mentioned in the rule. The detection approach uses a sophisticated combination of deterministic and behavior-based approaches as per users, entities and network traffic to detect indications of compromise early in the attack lifecycle. It can also redirect the intruder into honeypots to capture the activities of the hacker for feature attack study. We can also design the rules as per the new discovered intrusive efforts that increase the detection accuracy and maintain hack proof wall against the intruder.

Content sensitive protection

To protect the sensitive data of a company, the content sensitive approach should be used to monitor particular connections that are violated the policy. Nowadays, we are using Skype, Dropbox and Google Drive to increase productivity, making file sharing extremely easy and remote communication via text, voice and video chat. On the other hand, it can also increase the chance for data leak, lost or stolen. It also exposes the organization to potential data breaches. Using this technique, we can keep track on the communication as per predefined content sensitive rules.

Monitoring the inbound traffic

The inbound traffic should be monitor using deep packet inspection (DPI) approach. The inputs connections are decoded, and corporate policy applied to them. The traffics are filtered and clusters locally or regionally. Only the known IP/region allowed to access the corporate network. If the traffics comes from outside as mentioned rules, a Honeypot should be deployed to trap the attacker's intention and study the attacking approaches to strengthen the security policy. For example, the requests that are comes from China and Pakistan should be redirected to honeypot to trap and record the intrusive efforts. A honeypot is a network security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems (9). Hence, it is easy to counteract the intrusive effort without any loss of the corporate data.

Updating the OS security patches and virus signatures

It becomes utmost essential to update/upgrade the Operating System's security patches along with the virus signatures. The patch is a piece of software that fixes security vulnerabilities and other bugs that are applied to the OS. The developers continuously develop patches of the unrecovered bugs as well as solutions for the safety related issues. The virus signatures contain the known virus definitions to identify the known attacks. Hence, to secure our digital environment, it is highly recommended to update the OS patches along with the virus signature.

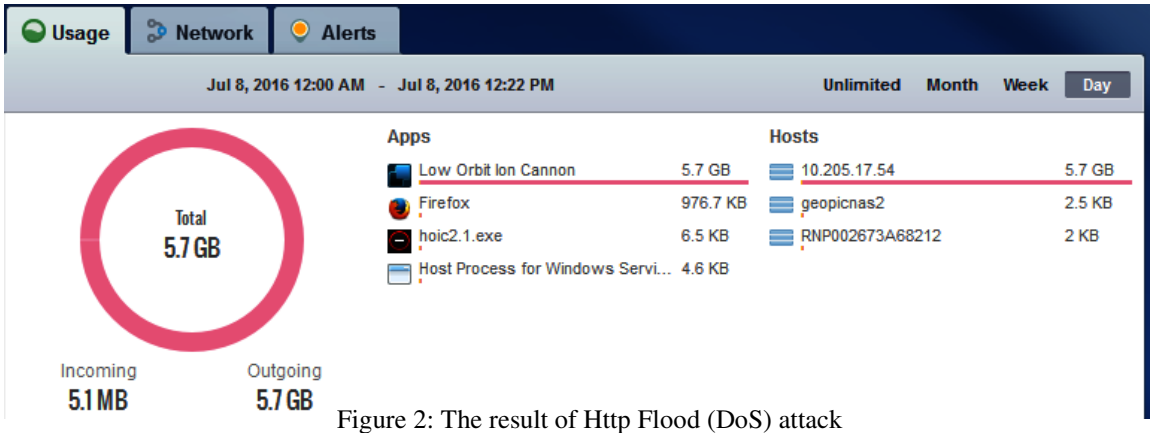

Figure 2: The result of Http Flood (DoS) attack

Figure 3: Sniffing Password over Network using Wireshark

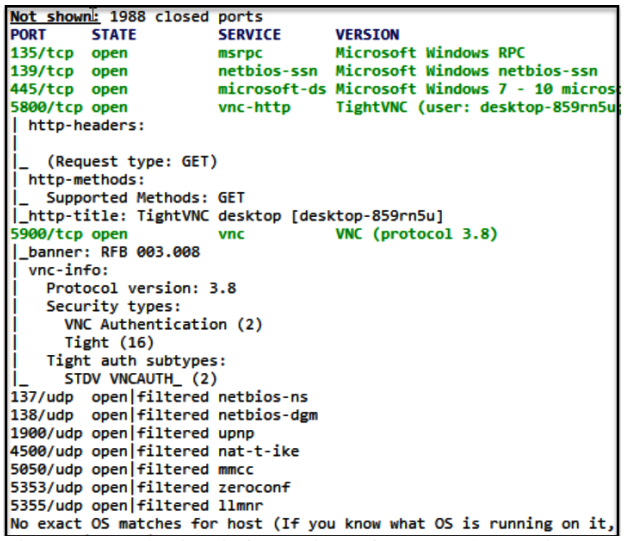

Figure 4: Gathering information of a target host using NMap.

Conclusions

Based on the present studies, every organization should focus to strengthen the security policies by adopting the state of art mechanism. The aware content protection, application and device control, real-time monitoring and intrusion-detection/prevention mechanisms become utmost essential for withstanding such intrusive efforts. Furthermore, all the user should know the basics of information security principles. It is the prime duty of the organization to create awareness, by conducting workshops and training programs to educate the employees regarding the do's and don'ts while interacting with the system. The network administrator should have adequate knowledge of the security principles, countermeasures, and monitoring the network in real-time. It is recommended to use a sandbox or virtual honeypot to protect zero-day attacks and other novel attacks.

Acknowledgments

The authors wish to thank Mr. C. Kumar, GM (Programming), Mr. M. K. Mathur, DGM (Programming) of ONGC and Shri A. Bharadwaj, HOI, GEOPIC for providing an opportunity to carry out this work and permitting to publish this paper. Authors thankful to Mr. L. Balu, and Mr. A. Bisht for their encouragement and suggestions during the writing of this manuscript. Views expressed in the paper are of the authors and not necessarily of the organization they represent.

References

Intimus Security Consulting: Steps to improve your Data Security and ensure your Customers' Trust, White paper.

Sahu Santosh Kumar, Jena Sanjay, "A Detail analysis of intrusion detection datasets", IACC14, IEEE, 2014.

Mirkovic, Jelena, and Peter Reiher. "A taxonomy of DDoS attack and DDoS defense mechanisms." ACM SIGCOMM Computer Communication Review 34.2 (2004): 39-53.

Shmatikov, Vitaly, and Ming-Hsiu Wang. "Security against probe-response attacks in collaborative intrusion detection." Proceedings of the 2007 workshop on Large scale attack defense. ACM, 2007.

Paliwal, Swati, and Ravindra Gupta. "Denial-of-service, probing & remote to user (R2L) attack detection using genetic algorithm." Int. J. Comput. Appl 60.19 (2012): 57-62.

Beghdad, Rachid. "Efficient deterministic method for detecting new U2R attacks." Computer Communications 32.6 (2009): 1104-1110.

Arai, Kohei, Supriya Kapoor, and Rahul Bhatia. Intelligent Systems in Science and Information 2014.

Cain and Abel: Url: http://www.oxid.it/cain.html
Wiki: Url: https://en.wikipedia.org/