FORENSIC INVESTIGATION METHODS ON NETWORK ATTACKS

Arockia Panimalar.S[1], Visweshwaran.G[2], Priyadharshan.R[3], Sumithra.V[4]

[1]*Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*
[2,3,4] *III BCA A, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu*

Abstract: *The paper discusses the different tools and techniques available to conduct network forensics. Network forensics deals with capturing, recording and analyzing of network events. Some of the tools discussed in this paper are eMailTrackerPro – to identify the physical location of an email sender. Web Historian – to find the duration of each visit and the files uploaded, downloaded and so on. The packet sniffers like Ethereal is used to capture and analyze the data exchanged among the different computers in the network. The second half of the paper shows a review of IP follow back procedure like packet marking with the assistance of forensic investigator to distinguish the genuine wellsprings of the attacking IP packets.*

Key Words: ***Forensic Science, eMailTrackerPro, Web Historian, Ethereal, Stack Overflow Attacks and Firewalls.***

1. INTRODUCTION

Now-a-days internet security is quick versatile in the advanced universes. Despite whether they are specifically pertinent to the work you do, network based attacks are so prominent that they are probably going to have some effect, regardless of whether you just utilize programmer stories to dispense expanded spending plans to counter. This subject is basic for working security engineers. There are a few in vogue thoughts that network can be secured by encryption and firewalls. The best place to begin exposing these notions might be to look at the most common attacks. In conventional ways, network attacks are done in media. An example is the leak of emails that appeared to come from the office of the U.K Prime Minister and were initially blamed on hackers.

2. ABOUT FORENSIC

Forensic science is the application of science to criminal and civil laws and mainly used during criminal investigation. Forensic scientists collect and analyze scientific evidences. The forensic travel from scene to crime is to collect the individual report from laboratory. The laboratory plays a major role in both civil and criminal cases. For checking the forensic related cases, the forensic uses a technically developed one. The forensic relates to a discussion or examination performed in public. The forensic science can be seen as the use of the scientific methods and processes in crime solving.

3. NETWORK ATTACKS

Earlier chapters contain stack overflow attacks and password guessing. Both of which were used as the Internet worm. A common strategy is to get an account on any machine on a target network. Still there are some patterns coming back in new guises. There is a list of top vulnerabilities, on the survey as on June 2000. A stack overflow attack on the BIND program, used by many Unix and Linux hosts for immediate account access. A stack overflow is to attack on the Remote Procedure Call (RPC) mechanism. The bug in Microsoft Internet Information Server (IIS), a web server software which allows for immediate access to the administrator. Many bugs have been found in sent mail over the year's advisory issued by CERT in 1988. The stack overflow attacks on Sun's Solaris operating system which allows intruders immediate route access. The IMAP and POP protocols allows for remote access to email.

4. DEFENSE AGAINST NETWORK ATTACKS

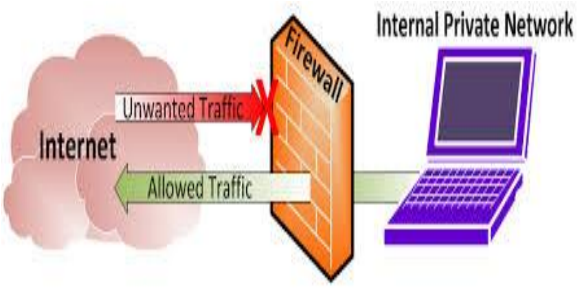
Most attacks are launched by kiddies that have been thwarted by system administrator, who monitors the security and applies to his software. This is part of the broader topic of configuration management.

4.1 Configuration Management

Configuration management is the most critical aspect of a secure network. Here the organization should check whether all the machines are running properly in the specific operating system. Configuration management is as important as having a reasonable firewall. Infact the priority has to be given to configuration and then to firewall. An opposing for buying and installing off the self product, the company takes many harder options to reveal it. Several tools are available to help the systems administrator keep things safe for their future purposes. The centralized version control was enabled for keeping it synchronized always, so that the patches can be applied every time. Satan attack will break the machine network.

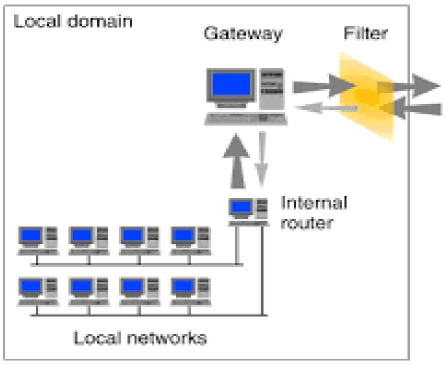
4.2 Firewalls

The most commonly used to solve the problems of Internet security is the firewall. This is a machine that stands between a local network and the Internet. The three flavors of fire walls are IP packet level, TCP session level and the application level.



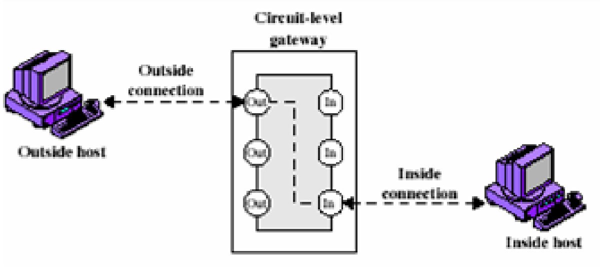
A. Packet Filtering

The firewall filters the packet addresses and port numbers. This functionality is also available in routers and in Linux. The IP spoofing is blocked and no packets are appeared to come from the host to the local network. It can also stop the service in which packets are sent to a host, or the host is to connect to itself. The basic packet filtering is made standard in Linux.



B. Circuit Gateways

The complex firewalls are called circuit gateways that reassemble and examine all the packets in each TCP circuit. Compared to simple packet filtering it is more expensive and can also provides added functionalities such as, providing a virtual private network over the Internet by doing encryption from firewall to firewall and screening out blacklisted websites or newsgroups. However, circuit level protection can't prevent attacks at the application level such as malicious code.



C. Application Relays

The third type of firewall is the application relays, which acts as a proxy for one or more services such as mail, telnet, and web. Striping up and macros incoming rules can be enforced in word documents and removing active content from web pages. These can provide very comprehensive protection against a wide range of threats. The downside is that the application relays can turn out to be a serious bottleneck. They can also get into the way of users who want to run the latest applications.

D. Ingress versus Egress Filtering

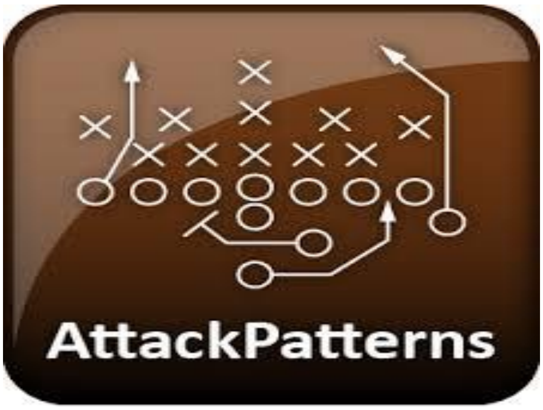
The firewalls point out and try to keep bad things out. Some commercial organizations are starting to monitor the outgoing traffics. There is a growing trend towards snitch ware, a technology that collects and forwards information about an online subscriber without their authorization of the user. The local disk and high sensitive materials are used for marketing purposes and phones for copyright enforcement. Since the prudent organizations are increasing, they want to monitor and control traffic.

D. DeMilitarized Zone (DMZ)

Multiple firewalls can be used. The De-Militarized Zone (DMZ) can be done by connecting a screened subnet outside the world, which contains a number of applications. The DMZ may then be configured into LAN connected to the internet via a broadband router, which does the network address translation. An organization can have boundary control devices that help the network operators at different clearance levels to ensure that the classified information does not escape either outward or downward. This can get in the way so much that people install unauthorized back doors, such as dial-up standalone machines to get their work done. The main controls are aimed at preventing information leaking outwards, there may be little to stop a virus getting in. Once in a place it wasn't expected, it can cause serious havoc.

5. ATTACK PATTERNS

Attack pattern specifies a generic way of performing an attack that takes advantage in a certain environment. The pattern presents a way to counteract the development of the attack in the form of security patterns and to analyze the information collected at each stage of the attack. This section presents a template for an attack pattern, which can be used for architectural patterns and security patterns. However, certain sections of the template have been modified to fit the new attacker's viewpoint. The sections of the attack pattern template are described below.



A. Name: Specifies the generic name given to the attack in a standard attack repository (e.g., CERT or Symantec).

B. Intent: A short description of the intended purpose of the attack.

C. Context: A description of the general environment, including the conditions under which the attack occurs. This may include system defense as well as system vulnerabilities.

D. Problem: Defines the goal of the attack pattern which (from the attacker's point of view) is the "problem" of attacking the system. An additional problem occurs when a system is protected by certain defensive mechanisms and these mechanisms have to be overcome. The forces (a term used in pattern writing) are the factors that may be required to accomplish the attack, the vulnerabilities to be exploited, and the factors that may obstruct or delay the attack.

E. Solution: Describes the solution to the attacker's problem. How the attack is performed and it's expected result. UML Class diagrams may be used to describe the system before and during the attack. Sequence diagrams could be used to display the messages exchanged during the attack. State or Activity diagrams may be used to provide an additional detail.

F. Known Uses: Specific incidents that are involved in the attack. Details of previous attack are useful in deciding how to stop the attack and where to look for evidence.

G. Consequences: Describes the benefits and drawbacks of the attack from the attacker's viewpoint. In particular, whether the effort and cost of the attack commensurate with the results obtained and the possible sources of failure.

H. Countermeasures and Forensics: It portrays the measures taken to stop, moderate and follow the attack. This suggests a list of the security patterns that are successful against the attack. Here information is acquired in each stage. While following the attack, the data is recognized for a particular task. Also, it may indicate the additional information that should be collected to support a forensic investigation.

I. Evidence Locations: This section may include a diagram with selected UML classes and associations relevant to a forensic investigation. UML class diagrams are useful because of their abstraction properties. The attack pattern is not a comprehensive representation of all the classes (network components) and associations involved in an attack. Rather, the pattern should represent the classes that are relevant to the investigation. When primary sources (e.g., firewalls and IDSs) do not contain enough evidence, investigators must examine secondary sources such as terminal devices (including wireless devices), servers and network storage devices.

J. Related Patterns: This section of the template includes patterns of other attacks with different objectives, that are performed in a similar way or attacks with similar objectives that are performed in different ways.

6. CONCULSION

Preventing and detecting attacks are launched over networks and internet. The problem can be solved at any time to the attacker's toolkit. The firewall will keep the things out from the worst of attacks. The paper aims at explaining the basic underlying science. The Internet is connected to the hundreds of millions of machines that are running insecure software. The one new thing is to have emerged is the distributed denial-of-service attack, which is made possible by the target systems being connected to many hackable machines. Despite all this, the Internet is not a disaster.

7. REFERENCES

[1] Z. Anwar, W. Yuck, R. Johnson, M. Hafiz and R. Campbell, Multiple design patterns for VoIP security, Proceedings of the Twenty-fifth IEEE Conference on Performance, Computing and Communications, 2006.

[2] F. Buchman, R. Meunier, H. Rohnert, P. Sommerlad and M. Stal, Pattern-Oriented Software Architecture: A System of Patterns, Volume 1, Wiley, Chic ester, United Kingdom, 1996.

[3] E. Casey, Investigating sophisticated security breaches, Communications of the ACM, vol. 43(2), 48–54, and 2006.

[4] CERT Coordination Center, Carnegie Mellon University, Pittsburgh, Pennsylvania (www.cert.org).