Scribe: Cryptography and Network Security (Class.6.D)

Ankit Saurabh

7-Oct-2020

1 Introduction

In earlier lecture, we learnt about VPN and perimeter level defenses against it. In this lecture we learnt about Firewall starting from packet filtering to detection and prevention of these attacks.

2 Packet Filtering(continuation from last lecture)

Basically, Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt. For this first we learnt basics of Networking.

2.1 Networking

In a TCP connection, Port number less than 1024 are assigned permanently, These are allocated to servers while rest are assigned to general client requests.Here servers are like name servers and we are the client. Some of the examples are -
FTP - 20, 21
Telnet - 23
HTTP - 80
SMTP - 25
HTTPS - 443
Port numbers for Client are variable. As we know, there are 2^16 ports for TCP. So, port numbers from 1024 to 16383 are used for Clients.

2.2 Types of Packet Filtering

There are 2 types of packet filtering - stateless and stateful. All these packet filtering happen only headers, ports or IP Addresses. Stateful packet filtering is better than stateless packet filtering because in stateless, as it allow all incoming traffic once permitted. Suppose, there was a SMTP packet from port 25 sent at

port 2048. Next, it will allow all incoming traffic on 2048 without checking.
A **stateful filtering** only allow traffic on high port to a machine that initiated an outgoing request on low port. If client send a request to the server then it expects some kind of response, if it does not get any response then it resend the request. FTP (File Transfer Protocol), Telnet are the example of Stateful Protocol.
In **telnet** Client tell server its port number. The ACK bit is not set while establishing the connection but will be set on the remaining packets. Then the server acknowledges.

A **stateless filtering** does work well for inbound traffic as it can block external request to internal server based on port number. The typical use of a stateless firewall filter is to protect the Routing Engine processes and resources from malicious or untrusted packets.

3 IP Fragmentation

In TCP communication, the packet starts with IP header, then TCP header and then data packets. But, in subsequent packets firewall does not care TCP header packet as it already know its TCP. It simply appends data. But sometimes, there is small offset in data packets. Due to this, new data packet rewrite some of the old packet's data. When offset is very low it overwrites IP header. This can be used to attack for spoofing IP address. It can be solved by using Application level proxies/ Application level gateways. In fact our institute, at present use Application level gateway.

4 Intrusion Detection

Now these intrusions can be prevented as well as detected. In this lecture we majorly learnt about Intrusion detection. We looked 2 major ways- 1) To discover system modification
2) Look for attacks in progress- these are network traffic analysis, system calls analysis

4.1 Tripwire

In tripwire attack, attacker gains gains the user access to the system. After that they gain root access. Then they attack on a trusted application so that user can't detect. There they change system binaries and create back doors for them for future activities.

To detect tripwire, system creates hashes such that even when one of the hash gets changed complete hash is affected and system gets the suspicion by comparing it to the previous hash.

Now, attackers can even escape it since they have root access and they might replace system binary in memory itself. Also, system cannot detect intrusion that dont change sytem files.

4.2 Difficulties

In general there are basic models of detection-
1) Maintain data on known attacks
2) Look for activity with corresponding signatures. This can be done by detecting Anomalies.

4.2.1 Unbalanced training data

There are little data containing realistic attacks, anomalies.

4.2.2 Poisoning the training data

Since statistical methods detect changes in behavior, attacker can gradually manipulate it.

4.2.3 Feature extraction to classify anomalous activities is hard

By many measures, attack may be within bounds of "normal" range of activities.

4.2.4 False identifications (False positives) are very costly

System Admin spend many hours examining evidence.

5 Conclusion

In this lecture, we learnt about Protocol level mitigation and perimeter level defense. Then we learnt about Detection and Prevention, in which we learnt about Intrusion detection system. It does anomaly detection based on either network behaviour or host behaviour as there is a baseline behaviour and for new pattern we check for intrusion.