Types of privilege escalation attack

Science, Computer Science

Basically is the act of exploiting a vulnerability like programming hole, network flaw, and design flaw or configuration oversight in a network and its services to gain access to resources normally that are protected from an application or user. There are two types of privilege escalation attack- Vertical and Horizontal attack. Where in vertical privilege escalation attack intruders need to grant himself higher privilege to lunch the attack. On the other hand in horizontal attack intruders can easily execute attack with same level privileges.

Alter data

Alteration attack in a network is like change or modify something from information passes over the network. Data alteration and data destruction are increasing rapidly again this is very hard to detect. Alteration occurs when intruders make some unauthorized alteration to data or code and attacking its integrity.

Password cracking

Password cracking is the way of converting the password has in plaintext original password that are sniffed from network. It is a term which is used to describe the penetration of a network, service, system or any other resource with or without the help of using some tools to unlock a resource that has been secured with a password. Using malicious code this process also be done easily in a network. And there is a lot of way to crack password by following some common techniques like brute force, dictionary attack etc. over a network.

Injection flaw

Injection flaw attacks refers to a wide-ranging attack vectors which allow attackers to supply malicious input to a program that can be processed by an interpreter act as part of command or query which modify execution process of that program. Injection flaws most of the time allows intruders to perform malicious actions like changing, altering, deleting or reading confidential information which they are not allowed to. Injection flaws attack are the oldest and very daring web application attacks in a network. Sometimes injection flaw attack could lead to access the whole system of a network. With injection flaw attacks, intruders could execute malicious code that interact with different vulnerable fields which could allowing them to grant access to database or shutting down the network carrying out different functions. There a numerous types of injection flaw attacks includes SQL injection, HTML injection, Host header injection, XPath injection, XML injection, CRLF injection and OS Command injection etc.

Payload Fraud

Hijacking

Hijacking is one kind of network intrusion in which an intruder takes control of a network system. Like an intruder or a hijacker takes control over the network of a power grid system. In terms of network security hijacking refers to the attacker intercepts communication message in a private or public key exchange and then redirect them, replacing their own generated public or private key for the requested one. And it will be visible as two authorized system still appear to be communication directly with each other normally. Hijacking attack could be used simply to take privileges or gain access to

confidential information or message or to enable the intruders to altering any part of information before retransmitting to them.

Phishing

Phishing is a type of fraudulent attempt to attain confidential and sensitive information for example authentication key, usernames, passwords, and credit card details (and money), sometimes could be for malicious reasons. It could be happen when an intruder masquerading as a trustworthy entity in an electronic communication, fools victims into opening malicious files, instant message or other fraud activities. Phishing is sometimes used to gain a foothold in government or corporate networks as a part of larger attack for example an advanced persistent threat (APT) attack.

Defacement

Defacement is the act of destruction of or damage in which a website is marked by intruders or attackers who actually wants to show their mark. Website defacement is alike to drawing graffiti on wall but virtually. It simply means change the appearance of websites by altering data, most of the times change the whole index page. On a popular websites with many visitors usually became the victim of defacement attack. Typically, website defacement is used to cover a larger crime being devoted behind the scenes.

Distributed

Need some text for distributed

Trojan Horse

Trojan Horse is a computer program that appears harmless, uses malicious code imitated as a trust application. Trojan Horse sometimes attached to a

genuine program or get disguised a trusted program to install a backdoor to the system. Malicious code can be inserted on benign softwares, fabricated in e-mail links, often hidden in JavaScript to make stealthy attack against vulnerable internet browsers. If a system is infected with Trojan Horse there seems unusual activity and unexpected changes even when the system should be in idle.

Malicious

Botnet

Botnet is derived from the phrase “ network of robots”. In the context of network security botnet is a network of infected computers, where the network is used by malicious activities to spread. Simply bot is basically an extensive collection of a large number of infected computer system. Traffics come from network, a group of devices or system which are connected together. Intruders are unable to execute their malicious codes manually on every computer in a network so instead attackers use botnets to manage a large number of infected systems, and do it automatically.

Malware

Malware is the short practice of “ malicious software”. Malware are harmful application designed to secretly operate on compromised system or networks without the permission of the user. Malware are created directly determined to harm or shutting down the network system or network servers, disable other electronic devices. Malware is intentionally malicious, even when masquerading as trusted program from a seemingly reputable, reliable or trusted source. Primarily malware targets confidential and sensitive information of individuals, corporate business or financial

information for monetary gain. Malware has been detected to use a diversity of various delivery techniques or attack vectors. Most of the attack vectors are operative at their objectives and only a few of them are admittedly academic for example virus, worms.

DDoS/ DoS

Buffer overflow

Buffer overflow is the most common type of DoS attack. The concept is to send huge amount of traffic to a network address than the developers have built the system to handle. Using buffer overflow attack attackers intension is to remain busy the victim server and makes it inaccessible to the legitimate user. Thus the victim might be in trouble to handle their regular operations and works.

ICMP Flood

Leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific machine. The network is then triggered to amplify the traffic. This attack is also known as the smurf attack or ping of death.

UDP Flood

SYN Flood

Sends a request to connect to a server, but never completes the handshake. Continues until all open ports are saturated with requests and none are available for legitimate users to connect to.

Operating Method

Obfuscation

Simply speaking, obfuscation is the process of taking a readable string of characters, and turning it into something that is unreadable (obfuscated). Though the result may be difficult to interpret or identify, the obfuscated result still performs the same actions as the original string. Often, this technique is used by attackers to hide malicious activity in executable code. This paper will use the built-in obfuscation capabilities in the attack tool, when simple string-matching filters are the final obstacle to overcome. Obfuscation is the process of manipulating data is such a way that the IDS signature will not match the packet that is passed but the receiving device with still interpret it properly. [8] For instance, sending a packet encoded differently or adding extraneous null characters. An example is the string:

However, a Web server would interpret both strings the same under the interpretation rules of the HyperText Transfer Protocol (HTTP). [8] This particular example was very popular for a time and so both NIDS and Web Server vendors are no longer fooled by this simple example, but the principle is still solid for any interpreter that allows alternate command forms. This particular method can also get by both HIDS and NIDS if done correctly. We will revisit this issue later.

Encryption and Tunneling

Encryption and tunneling of encrypted data is another strategy that can be used to avoid IPS inspection. Encrypting the attack by sending it through an SSH connection or in a VPN tunnel makes it virtually impossible for the IPS to inspect the data. To do this, the IPS has to be placed at a point in the

network which lies after the tunnel termination (Burns & Adesina, 2011). In this scenario the attacker uses any attack against the HTTPS Web site, such as SQL injection, buffer overflows, and directory traversals, that would work on the HTTP site. Because HTTPS uses SSL to provide a secure network connection, the traffic is encrypted and therefore flows past the NIDS without triggering an alert. Encryption can also prevent an attacker from being detected as they do other unsavory things after they have compromised the host.

Fragmentation

By splitting up malicious network packets into smaller fragments, an attacker might be able to circumvent the network security mechanisms in place. This approach is known as fragmentation. The issue with fragmentation is that the IPS has to reassemble the packets in order to identify the attack. Each fragment contains a value in the header that informs the receiver of the data's position in the original data stream. If the fragments are modified in such a way that the fragments are overlapping, reassembly becomes complex, as it is not clear which of the fragments' data should be used. To add to the confusion, different operating systems treat overlapping fragments differently. So if the IPS reassembles the packets differently from the end host, it may reassemble the fragments to a non-malicious payload and allow it.

At the same time, the end host reassembles the same fragments into a malicious payload, thus allowing the attacker to compromise the system (Baggett, 2012). Judy Novak's paper on fragmentation reassembly discusses these issues and demonstrates how Snort uses a preprocessor to handle

fragments differently based on the systems it’s configured to protect (Novak, 2005). In the demonstration section of this paper, both simple fragmentation and overlapping fragments will be used in some scenarios.

Fragmentation is simply breaking an attack into multiple packets.. Fragmentation of packets occurs normally and hosts are equipped to handle receiving data in multiple pieces and potentially in the wrong order. A Quick example is depicted in Figure 1. In this example the attack packet “ DATA” is broken into four different packets. The host at the receiving end will reassemble the fragmented packets and receive the data payload in the fragmented order and then put the packets into the correct sequence using the unique packet sequence number assigned to each packet. But a NIDS is only going to see the parts. Each part is not an attack packet so the NIDS will not alert anyone. Some NIDS’s will reassemble packets to avoid fragmentation attacks. But not all NIDS have the processing overhead available to reassemble fragmented packets. But even if the NIDS that can reassemble packets it will have a physical limit to how many it can or will reassemble. So, an attacker can send a fragmented attack and simultaneously send a large amount of fragmented ‘ junk’ packets (an example of a combination attack using the overflow method discussed later).

While the IDS is attempting to reassemble all the ‘ junk’ packets, the fragment attack may go though unnoticed by the IDS. Or if the attacker does not have the resources to flood the NIDS, the attacker can also attempt to wait out the capture buffer on the NIDS. The NIDS will, as in the example at the right, get the first three packets but not the entire attack signature, since

the last part of the fragment is not received in the appropriate time interval, the first three are dropped by the time the fourth gets to the IDS and host. All four will be reassembled on the host in a successful attack but the NIDS will not alert.