Analysis of Computer Network Attacks

Nenad Stojanovski[1], Marjan Gusev[2]

[1] Bul. AVNOJ 88-1/6,
1000 Skopje, Macedonia
Nenad.stojanovski@gmail.com
[2] Faculty of Natural Sciences and Mathematics, Ss. Cyril and Methodius University,
Arhimedova b.b., PO Box 162
1000 Skopje, Macedonia
marjan@ii.edu.mk

Abstract. In this paper we present an analysis of modern computer network attacks. First we will classify the attacks. We will classify the attacks by using some characteristic of the attacks and by the type of device they target. After the classification we will describe every technique that can be used to attack a network device or a computer system by following the previously given classification. After every attack description a mitigation solution will follow, if there is one available. As an addition we will describe an attack that targets wireless network as well as a mitigation solution for that attack.

1 Introduction

In the today's modern world we couldn't think living without the computer networks. Their integration is widespread into the lives of the people beginning from simple information searches to bill payment, video conferences and etc. This paper focuses on analysis of computer network attacks and ways on defending the computer systems and network devices from those attacks.

2 Classification of computer network attacks

Computer networks attacks date from the beginning of massive use of computer networks. Computer networks are made up of network devices and computer systems, which means that attacks on computer networks aren't limited only to networks devices. The attacks can be performed on all network devices, computer systems, network printers and even to phone devices and mobile devices that use the TCP/IP or any other network protocol to communicate. Computer network attacks can be classified by their impact on the target or by their target. If we classify the attacks by the first classification we can divide these two groups:

- Escalation of privileges
- Denial of Service – DoS

The second classification divides the attacks in these two groups:

- Attacks against computer systems
- Attacks against network devices

We need to mention that it is possible one of the classifications to contain the other classification. This is done because sometimes we need to describe the attacks in details. The description of the groups follows.

Escalation of privileges contains all attacks that aim to gain some kind of privileges on the target, like administrator privileges or gaining higher privileges that the current ones. As an example lets imagine that organization X has a web page which uses dynamic pages to load contents. The pages communicate with SQL server from where they manage the data. If the web pages have a vulnerability that for instance allow to inject SQL code to the queries that are sent to the SQL server, the attacker could send a query that opens an administrator's user account on the organizations portal.

The second group of attacks from this classification has a target to denial the normal functioning of the computer network or computer systems in the network. Most of the Denials of Service attacks are result of an unsuccessful privileges escalation attack.

Attacks against computer systems are attacks that focus on attacking computer systems in the network. By computer systems we mean server and workstations.
Attacks against network devices are attacks that focus on attacking network devices such as routers, switches, etc.

3 Sniffing

Sniffing of the network traffic is a technique which uses copying of the information that is contained in the packet without changing their contents or target. By using the previously defined classification this type of attack can be put in the group of attacks that aim to escalate the attacker's privileges. The main target of sniffing is to steal the administrator's user and password information. Sniffing is successful because of the design of TCP/IP and that's because TCP/IP by default isn't an encrypted protocol. Another reason why the attack is successful is because of the weak network design and it is always possible in networks that use a hub to connect all devices. As an example we will analyze a network where all the nodes are connected using a hub. User 1 sends his user and password to the e-mail server.

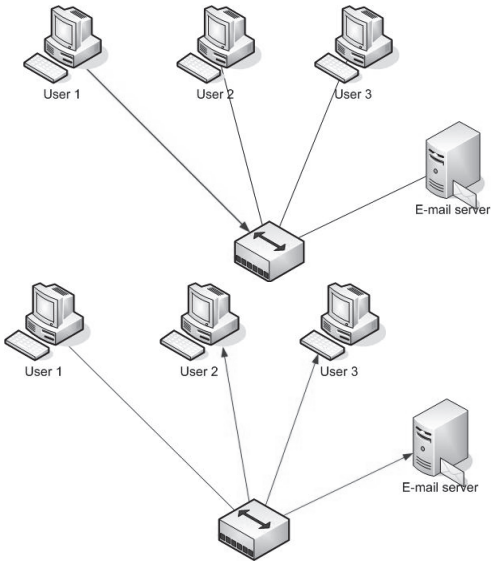

Fig 1. Sniffing environment

The hub receives the packets and sends them to every port excluding the one from where it received the packets. If someone that participates in the network uses a program capable of sniffing, he would be able to recover the user and password of User 1. The most famous sniffers are Ethereal, WireShark. Sniffing can be mitigated by changing the hub with a more sophisticated type of equipment, a switch.

4 Man In The Middle

Man In The Middle is an attack that is very similar to sniffing, even we can view Man In The Middle as an advanced form of sniffing. The difference between sniffing and MITM is that MITM is sometimes used to change the data in the TCP/IP packets, which means that with MITM it is possible to sniff an encrypted communication. For a successful MITM attack the target computer need to be tricked to thing that the attacker is one of them. With one of them it is meant that in a communication between Computer 1 and Computer 2, the attacker will appear as Computer 2 for Computer 1 and as Computer 1 for Computer 2.

Encrypted communication is sniffed by changing packets in the state where they exchange keys. If we successfully modify the keys that Computer 1 and Computer 2 are exchanging with our keys for which we know the private keys, then we could sniff the traffic that goes between Computer 1 and Computer 2. Such attacks are almost invisible and are very hard to detect. The only protection for the encrypted communication is to implement a way in the application to check the validity of the exchanged certificates.

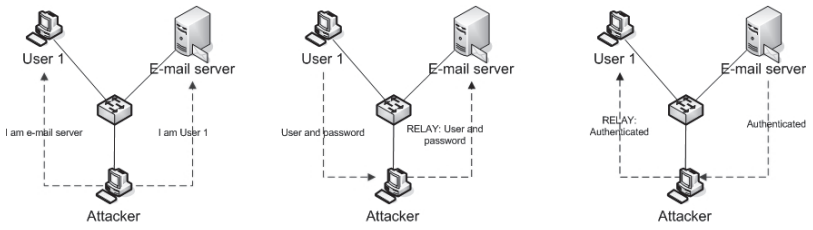

Fig 2. Man In The Middle

5 Privileges escalation by attacking services, network devices and client software

Attacks of this type are one of the most popular attacks and by their impact they are one of the most dangerous. The first attack of this type was spotted in 1985 and was named after its author "The Morris worm". These types of attacks aim to exploit certain security vulnerabilities in the code of the service. By successful exploitation of the security weakness the attackers gain access to a command shell on the target machine. Thru the command shell they are able to execute system commands which are usually run with administrator privileges. The security vulnerabilities that are exploited are vulnerabilities of the programming language in which the service was written. Later the security vulnerabilities were named by the weakness they use to exploit the service. Most popular weaknesses are stack overflows, heap overflows and format string overflows and are weaknesses of the C/C++ programming language. Since C/C++ is the programming language that is used to write system software it implies that almost all services, network devices and client software can contain the above mentioned security weaknesses. When it comes to exploitation of network devices, the only difference between the command shells is that it executes system command of the specific network device. After a successful exploitation attackers almost always install backdoors on the compromised computer systems.

Client software is immune to service attacks, since it never listens to ports that can be accessed from the outside. Because of that, an attack on client software is manifested by the client visiting a hostile server. For example, the client visits a hostile web server. A demonstration of this type of attack follows:

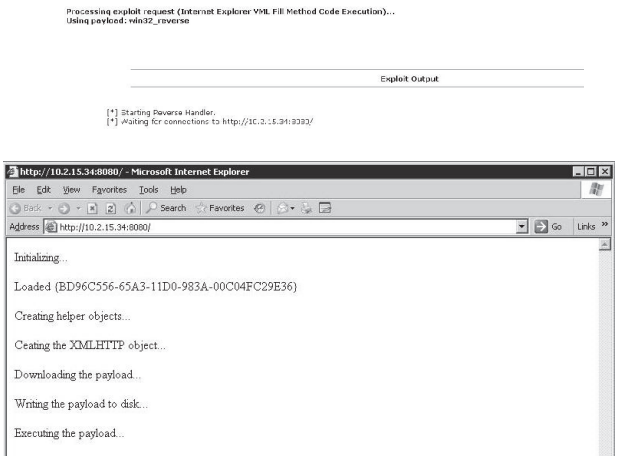

Fig 3. Illustration of a client side attack

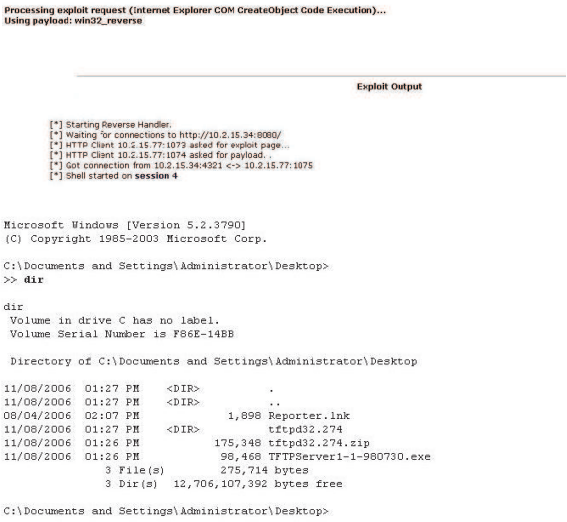

Fig 4. Illustration of a client side attack cont.

6 Attacks on web applications

In the last couple of years web application attacks have gained their popularity. Attacks of web applications are base also on programming language weaknesses. Web application attacks are limited to the database on which the web application operates. The weakness can be found in the code that executes SQL queries and exploitation is

done by inserting custom attacker SQL queries to the existing queries. Because of the SQL query injection the attack was named SQL injection and the impact is highest on web applications that use MS SQL server or Oracle as database server. In the case of these two database types the attacker can execute system code on the database server thru the use of the default stored procedures that can be found in these databases.

Since this attack is a programming error the best mitigation for it is by writing secure code. This can be done by filtering all variables from the incoming requests and changing/deleting the suspicious values.

7 Denial of Service

Denial of Service attacks have gained their popularity in 1997 and since then they are one of the most popular attacks against computer networks. This type of attacks is one of the most critical and destructive from the companies' point of view and in the last few years the loss from DoS attacks is the biggest. DoS can be divided on attacks against applications, attacks against computer systems and attacks against network devices. By using this division we can define a couple DoS attacks:

- SYN flood
- Exploitation of a security weakness
- Smurf
- Attacks against routers

SYN flood attacks use a weakness in the TCP/IP protocol suite. They exploit a weakness in the 3-way handshake. The 3-way handshake is initiated by a SYN packet which is then validated with a SYN/ACK by the other machine and in the end it is completed by an ACK packet. SYN flood exploits the 3-way handshake by initiating many connections to the server and never answers to the SYN/ACK packet with an ACK packet. On the server side for every SYN packet the server reserves a piece of memory and holds it for some time. The attacker sends a couple of thousand connections which eats the server's memory.

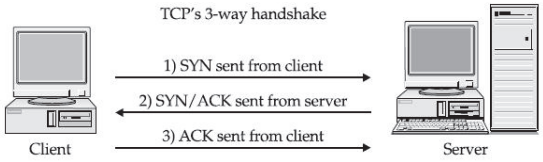

Fig 5. 3-way handshake

Exploitation of a security weakness can crash the server or crash the application. The impact depends on the location of the vulnerability. For instance if the weakness is located in the kernel code of the computer system or network device it will for certain crash the device if exploited.

Smurf is the primitive version of today's distributed Denial of Service attacks. It uses ping to attack the target. The attack is done by sending a ping packet to a big

number of broadcast addresses, where the ping packet contains a forged IP address from the target. Since the ping packet was sent to broadcast addresses, when the hosts from those subnets answer the ping request they probably will crash the target system because of the huge amount of ping replies.

Attacks on routers are the ones that are most sophisticated when it comes to Denial of Service. They function by sending routing protocol updates and with those updates they create black holes which bring down the whole traffic. The problem is a result to low security in the routing table updates.

Another type of Denial of Service attacks are the local Denial of Service attacks. The difference between them and the remote Denial of Service attacks is that they need to be executed locally. They are easily detected because they must be executed by a local user of the system.

8 Distributed Denial of Service

The first distributed Denial of Service attacks were spotted in the year 2000 when they successfully crashed the servers of Yahoo, CNN, eBay and many others. By design DDoS attacks implement almost all previously mentioned DoS attacks with the difference that the attacks is executed from more then one system. The DDoS environment is designed so that there is one master server who controls the entire set of zombie servers, and are all together known as a botnet. When an attack needs to be initiated, the attacker connects to the master server from where he initiates the attack and the master server sends commands and the target IP address to the zombie server.

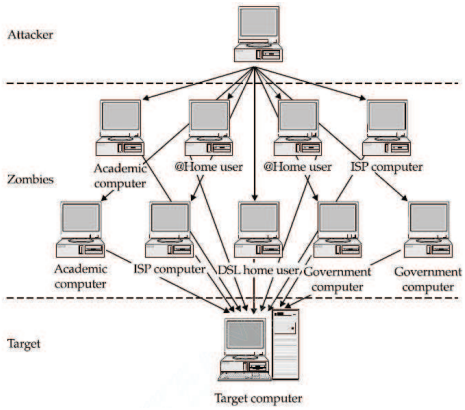

Fig 6. DDoS illustration

A botnet is built by compromising computer systems and it is done by escalation of privileges. After the computer system has been compromised the attacker installs the DDoS software on the target system and then configures it to communicate with the master server. A new trend for the attackers is to write worms that compromise com-

puter systems and later start a DDoS attack on a certain target. These worms are later release on the internet.

Defences against DDoS do exist, but they are available as a very expensive commercial product. Such a defence has been designed by Arbor Networks and Cisco and it contains an anomaly detection engine and an engine for packet blocking. The anomaly detection engine analyses the traffic and upon detecting an anomaly alerts the Cisco Guard. Cisco Guard then starts blocking packets from that source.

The most famous DDoS tools are Trinoo, Tribal Flood Network, Tribal Flood Network 2000, Stacheldraht, WinTrinoo.

9 Attacks on wireless networks

When it comes to attacking wireless networks we need to add one more attack to the all previously mentioned. The newly mentioned attack tends to attack the encryption that the wireless network uses. Wireless network use a couple of cryptographic algorithms among which WEP, WPA, LEAP, PEAP. Some of these algorithms need a second level of support in order to work. Algorithms that don't need second level support are WEP and WPA and because of this they are the ones that are the most attacked and most insecure. This attacks aims to discover the key that is needed to connect to the selected ESSID. It can be done by using two types of attacks:

- Passive attack
- Active attack

The passive attack is a silent attack and it only gathers packets that circulate in the wireless network. This means that on a computer a wireless sniffer resides that collect all of this data until it finds the key. Passive attacks need time to gather enough packets to discover the key.

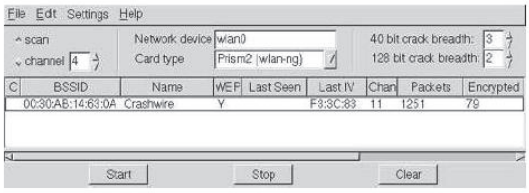

Fig 7. Passive attack

The other form of attacks actively generates traffic towards the access point. By actively generating false frames the attacker tries to generate the needed packets and the needed amount of packets. This is done by generating false authenticate and deauthenticate frames towards the access point. By doing this it is possible to trick the access point into generating authenticate and deauthenticate packets.

The best way to mitigate this type of attack is to change the encryption type from WEP or WPA to LEAP or PEAP.

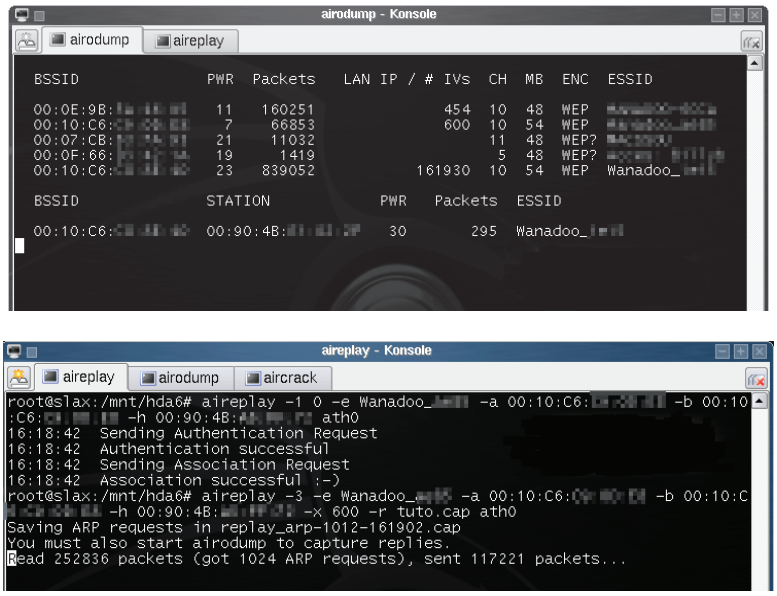

Fig 8. Active attack

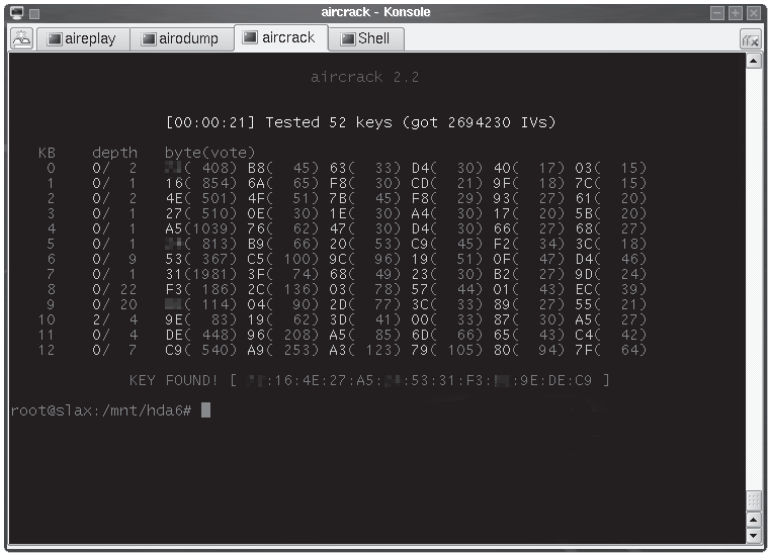

Fig 9. Key breaking

10 Conclusion

Attacks on computer network pose a great threat towards the operation of network devices or computer systems. The most dangerous attacks are the ones that we cannot defend from or the ones where the defense is very expensive. In the end we can conclude that the attacks on computer network were always present and they will stay present the only difference is the impact they will cause in the future.

References

1. Tanenbaum, Andrew S. (2003) Computer Networks
2. Stevens, Richard W. (1993) TCP/IP Illustrated Vol.1
3. Stallings, William (2004) Data and Computer Communications