



Security solution in networks and attack simulations

Alliance Kingst TONY-MAYEKO

PhD-Computer of Science
Department: Electronic and Telecommunication,
Research Unit: Laboratory Electrical Engineering
Collage: Marien NGOUABI University
School: ENSP-National Higher Polytechnic School
Country: Rep of Congo
Email: mayeko2005@yahoo.fr

Abstract The objective of this work is the implementation of a security solution for an administration, by making use of services, mechanisms, tools and procedures that are commonly called "solutions" or "measures" of security". It is a question of putting the necessary mechanisms for the protection of the resources of the information system and to prevent malicious people intending to break into the system.

Keywords Attack, intrusion, scan, port, firewall, server, proxy, antivirus, IDS, IPS, alert, vulnerability, risk, java, Open Source.

1. Introduction

Information security requirements within organizations have led to two major changes over the last few decades. Before, information security was maintained by physical means (filing cabinets locked with a padlock) or administrative means (systematic screening of applicants during their recruitment). With the advent of the computer, the need for automated tools to protect stored information has become apparent. This need is compounded for a system that can be accessed over a public telephone or data network. This collection of tools to protect data and ward off hackers is called computer security. A major change affecting security is the introduction of distributed systems and the use of communication networks and devices to transport data between a user terminal and a user. Network security measures are required to protect data in transit. This is called network security. There are no clear boundaries between these two forms of security. For example, one of the most publicized types of attacks on information systems is the (computer) virus. A virus can be introduced into a system physically via a floppy disk or via the Internet. In both cases, once the virus is present in the s, it is detected and destroyed. System requires computer security tools and filters

2. Materials and methods

2.1 Network and system security.

The corporate network implements, stores, and shares sensitive data internally and sometimes communicates with other companies or individuals. This outward openness determines the increase in productivity and competitiveness. It's impossible to forego the benefits of computerization, lock out the network to the outside world, or risk the confidentiality of corporate data. Sensitive data in the company's information system is therefore exposed to malicious actions, the nature and method of penetration of which is constantly changing. Hackers attack computers primarily through access to networks that connect the company to the outside world.

Security technical used are:



- Captive portal (authentication mechanism): This interface will play the role of a secure gateway for the purpose of authentication before Internet access.
- VPN is a secure tunnel.
- Network Intrusion Detection and Prevention System (SNORT): to protect the company's information system from attacks.
- Bandwidth sharing (TRAFFIC SHAPER) and bandwidth monitoring (NTP).
- URL filtering (SquidGuard): allows the company to apply the security policy for authorizing access to websites.
- Setting up a proxy server (proxy cache)
- Control and restriction of user rights.
- The use of IPsec, SSL/TLS or even HTTPS protocols (network protocols that allow remote access to be secured by encrypting transmitted data).
- Encryption: A method of encoding/decoding data that generally implements a logical key mechanism to make it impossible for third parties who do not have the key to read a file.
- Fault Tolerance: Security device implemented in particular at the level of hard disks that makes it possible to protect against a hard disk failure, preventing applications from stopping or stored data being corrupted.
- High availability.
- Intrusion detector is a system that can detect an attempt to break into your system. It stops most of the identified attacks. IDS monitors network traffic and analyze packets to prevent and stop suspicious actions.
- Data encryption.

2.2 Security technologies and solutions

Firewalls are mainly used for several purposes:

- Protection against malicious outside attacks: To protect against malicious outside attacks, firewalls repel various intruders: Curious people who generate traffic are more afraid of harm, but the sometimes ends up being expensive,
- Vandals saturating connections, corrupting data, etc.
- Avoid leaking uncontrolled information to the outside world.
- Monitor internal/external flows: All traffic flows between the internal and external network should be monitored. This makes it possible to view the Internet usage of the various internal users and to block access to certain pages containing illegal information.
- Ease of Network Management: Without a firewall, any network computer is potentially vulnerable to attacks from other Internet computers. Firewalls simplify security management and therefore network administration because they centralize potential attacks at the firewall level instead of the entire network.
- Many firewalls exist on all operating systems. The choice was made partly because of the limitations of the services it offers, its reliability and its widespread use in the business world.

2.3 Comparative study of firewall solutions

Our comparative study is based on the following firewalls

- **Smoothwall express:** is a project initiated in the UK in the since 2000 by Lawrence Manning (main code developer) and Richard Morrell (project manager). Their basic idea was to create a Linux distribution that could turn a PC into a firewall device. The first version of the Smoothwall firewall was published on Sourceforge.net in August 2000. The community has grown since then and the Smoothwall product has evolved as well. It should be noted that the Smoothwall distribution is open source and distributed under the GPL license. It is an operating system based on RedHat Linux (which later became the Fedora Core Project).



- **IPCop:** is originally a fork of Smoothwall Express. This means that IPCop is based on Linux Redhat. The first version was released in December 2001. Today we are at version 2.0.6. IPCop is distributed under the GPL license.
- **Vyatta Community Edition:** Vyatta's firewall solution is available in two editions. The former is paid for, the latter is free. We find that the commercial version is maintained and updated more frequently than the free solution (about one update every six months). The marketed product is also always stable, which is not necessarily the case for the free version called Vyatta Community Edition, the latest version of which is version 6.5 released in October 2012.
- **Endian:** is an open source security distribution whose goal is to have a Linux distribution fully focused on security and the essential services of a network, in order to have maximum protection against data theft, viruses, spyware, spam and other threats from the Internet to offer. More precisely, Endian integrates a firewall that plays the role of an intermediary between a network considered insecure (Internet) and a network that one wants to secure (for example the local network), while providing services that will allow management and monitoring managed via a web interface (Unified Threat Management UTM).
- **PFsense:** based on a FreeBSD3 distribution adapted to be used as a firewall and router. The project started in 2004 with the m0n0wall project, which focused more on full-fledged computer installations than m0n0walls embedded hardware development. Pfsense includes many features provided by paid commercial firewalls and others unique to Pfsense: firewall, address and port translation, redundancy, 12 CARP: CARP on OpenBSD allows hardware failover. Two or more Fire Parents can be configured as a failover group. If there is a problem in the first, the second takes over. Pfsense also includes sync options, if changes are made on the first, they will be automatically synced on the second. Pfsync: Pfsync replicates state tables to all firewalls in the failover group. In the event of a problem, existing connections are maintained as they are switched back to a different firewall, avoiding network disruption. Inbound and outbound load balancing, VPN, IPsec, OpenVPN, RRD Graphs Reporting, Captive Portal, Relay and DHCP Server.

Given this comparison, Pfsense seems to be the best compromise between these firewalls.

What Pfsense appeals to, is the ease of installing and configuring network management tools. In fact, it is possible to configure almost all the functionalities of the services offered by a single PHP web interface.

Pfsense is a firewall solution that manages multiple services. It consumes fewer resources because it already has a proxy server, an antivirus server and an intrusion detection/prevention mechanism. Services offered Failover system using CARP protocol. Proxy, Blacklist SQUID and SQUIDGuard IDS-IPS Snort Antivirus ClamAV

3. Results & Discussion

In this part, we present an implementation of a firewall component, which has various functionalities, will be able to give the necessary security to the company's local network and detect intrusion attempts. The firewall therefore offers real control over the company's network traffic. It is used to analyze, secure and manage network traffic and thus make appropriate use of the corporate network. This must be accomplished without overloading the network with nonessential activity.

3.1 Network topology

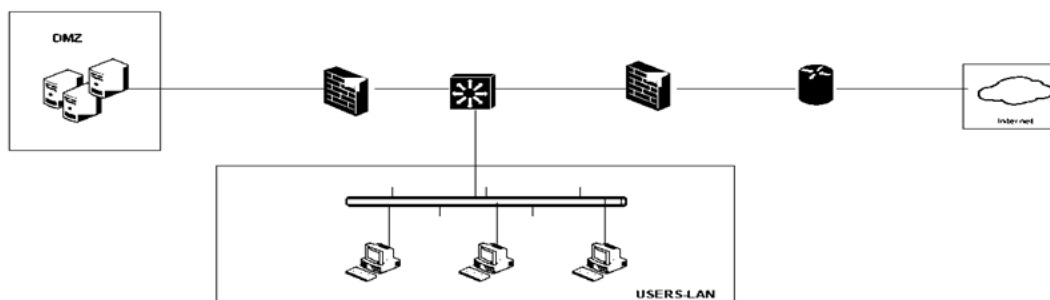


Figure 1: Network topology



- Internet represents the external network, to which the company is connected via the provider's router
- A DMZ (demilitarized zone) which contains the company's public servers: proxy server, antivirus server, email server, print server and file server.
- The users LAN, private and protected area of the company.

When certain machines on the internal network need to be accessible from the outside (a mail server, an FTP server, etc.), it is often necessary to create a new interface to a separate network, accessible both from the internal network and from the outside, without risk compromising the company's security. This is called a "demilitarized zone" to designate this isolated area hosting applications made available to the public.

The DMZ thus acts as a "buffer zone" between the network to be protected and the hostile network.

Servers located in the DMZ are referred to as "strongholds" due to their outpost position in the corporate network.

The security policy implemented on the DMZ is generally as follows:

- Traffic from the external network to the DMZ allowed.
- Traffic from the external network to the internal network prohibited.
- Traffic from the internal network to the DMZ allowed.
- Traffic from the internal network to the external network allowed.
- Traffic from the DMZ to the internal network prohibited.
- Traffic from DMZ to external network denied.

3.2 Implementation

In this part we realize the implementation of some tools that enable the port scan and the vulnerability scan. The first casualties of a successful attack are an organization's data, uptime, and reputation. From there, we point out the importance of vulnerability scanning.

We used **Black track** as tool of security testing.

BackTrack is a security-oriented Linux distribution whose purpose is to bring together the necessary and useful tools for testing the security of a network system. Based on Slackware up to version 3 and Ubuntu later and with a limited wealth of tools, BackTrack offers a very extensible and customizable environment; Install your own tools if needed, add other tools, configure and customize tools, etc.

After installed, the menu below should be displayed



Figure 2: Black track menu

3.3 The scenarios of tests

3.3.1 Scenario 1: Port scan attack

The scan of ports (or port scanning) consists in trying to open a connection on each port TCP (or UDP) of a machine in order to determine the services it offers and find thus possible vulnerabilities such as a service with a known flaw. The scan port belongs to the reconnaissance phase.



Thus, it is considered by firewalls and security systems in general as an attack strictly speaking even if it is only a discovery of services.

However, this discovery usually gives the basic information needed to machine attack.

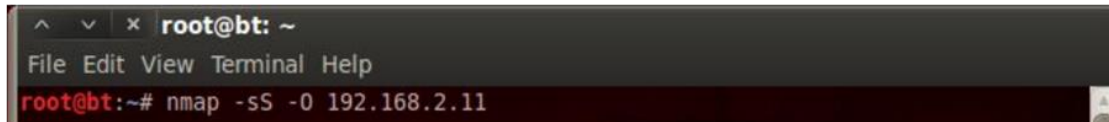
3.3.1.1 Testing tool

To perform the port scan attack, we are going to use Nmap. The latter a scan of TCP and UDP port, in command line is also in graphical mode. It allows to detect if a machine is on a network, to identify the services running on it and even to deduce in certain cases the type of operating system.

3.3.1.2 Procedure of the attack

At the level of the attacker's machine, we perform the port scan in order to recover the list of open TCP ports and type of operating system used.

We must use the following command

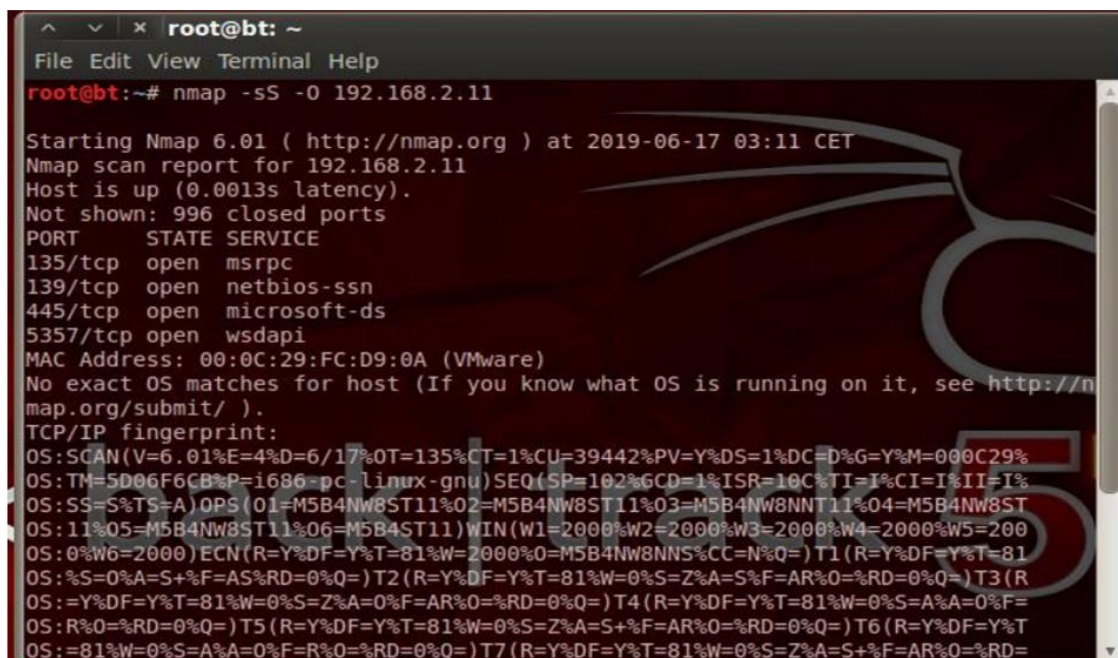


```

root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap -sS -o 192.168.2.11

```

Figure 3: Command for scanning ports in black track tool



```

root@bt: ~
File Edit View Terminal Help
root@bt:~# nmap -sS -o 192.168.2.11

Starting Nmap 6.01 ( http://nmap.org ) at 2019-06-17 03:11 CET
Nmap scan report for 192.168.2.11
Host is up (0.0013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5357/tcp  open  wsddapi
MAC Address: 00:0C:29:FC:D9:0A (VMware)
No exact OS matches for host (If you know what OS is running on it, see http://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN (V=6.01%E=4%D=6/17%OT=135%CT=1%CU=39442%PV=Y%DS=1%DC=D%G=Y%M=000C29%
OS: TM=5D06F6CB%P=1686-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=I%CI=I%II=I%
OS: SS=S%TS=A)OPS(O1=M5B4NW8ST11%02=M5B4NW8ST11%03=M5B4NW8NNT11%04=M5B4NW8ST
OS: 11%05=M5B4NW8ST11%06=M5B4ST11)WIN(w1=2000%w2=2000%w3=2000%w4=2000%w5=200
OS: 0%w6=2000)ECN(R=Y%DF=Y%T=81%W=2000%O=M5B4NW8NNS%CC=N%Q=)T1(R=Y%DF=Y%T=81
OS: %S=0%A=S+F=AS%RD=0%Q=)T2(R=Y%DF=Y%T=81%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T3(R
OS: =Y%DF=Y%T=81%W=0%S=Z%A=0%F=AR%O=%RD=0%Q=)T4(R=Y%DF=Y%T=81%W=0%S=A%0%F=
OS: R%0=%RD=0%Q=)T5(R=Y%DF=Y%T=81%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T
OS: =81%W=0%S=A%0%F=R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=81%W=0%S=Z%A=S+F=AR%O=%RD=

```

Figure 4: Result for scanning ports in black track tool

3.3.1.3 Results

This test shows us:

- The list of open ports with the service name,
- The physical address of the victim computer and the operating system used.
- All this information forms a means to perform the pentest and make the system exploitable to intruders

3.3.2 Scenario 2: Denial of Service attack

A denial of service (Denial of Service, or DoS) is an attack designed to make an organization's services or resources unavailable for a period of time. Generally, this type of attack takes place against a company's machines and servers, making them inaccessible to their customers. The purpose of such an attack is not to change or delete data or even to steal information. This harms the operation of a service or the reputation of a company offering a service on the internet by preventing it from operating properly.

Principle:

To send a very large amount of packets, the size of which is relatively important, at the same time, or even for a long period of time.



The principle of the Distributed Denial of Service (DDoS) consists in using a large amount of "Zombies" posts with the intention of crippling victim machine response.

3.3.2.1 Testing tool

LOIC (Low Orbit Ion Cannon) is a dedicated tool for DDOS type attacks, already used by "Anonymous" during their attacks on government sites during the Tunisian revolution in December 2010 and many other attacks used a almost everywhere in the world.

3.3.2.2 Procedure of the attack

The basic functioning of LOIC is as follows: the user specifies an IP or a URL sets a port, type of attack.



Figure 5: DoS attack with LOIC

3.3.2.3 Results

Distributed Denial of Service (DDOS) attack the targeted site by flooding the server with TCP packets, UDP packets, or HTTP requests with the intent to disrupt the service of a particular host.

4. Key Contributions

- Identify any security vulnerabilities present on your site or application
- Reduce the risk of business interruption following a computer attack
- Protect the data of customers and prospects
- Demonstrate to any customers the security of your service

5. Conclusion

In perspective, improvements are possible to increase the performance of the solution of security according to the emergence of new technologies and over IP security.

Acknowledgements

We thank to the journal team, for their valuable comments and suggestions which have led to an improvement of the manuscript.

References

- [1]. [K.E], Karnel Erickson "Hacker Basic Security" 2021, page 20-56"
- [2]. [E.O], Dr. Erdal Ozkaya, Cybersecurity – Attack and Defense Strategies: 3rd ed. 2022, page 11-39"

