Chapter #1: Introduction to Ethical Hacking

PENETRATION TESTING METHOD

1. An ethical hacker acts ethically against those who used the same tools and techniques to behave maliciously
2. We should make a further distinction between the role of an ethical hacker and of a security engineer. The latter focuses more on the protection of network infrastructure and specializes in perimeter security systems (firewalls, IDS, IPS, etc.). The ethical hacker has a vertical specialization in executing penetration tests within a specific context.
3. An ethical hacker never acts on his own, but instead, according to the agreement reached with the client who commissioned his work.

NECESSARY KNOWLEDGE FOR AN ETHICAL HACKER

1. First of all, you should be familiar with computer networks.
2. Secondly, you will need to study at least one programming language. I would suggest you start with Python: it is easy to learn and extremely powerful.
3. You can still opt for other programming languages, like C or Java. Their primary structures are very similar to each other.

POSSIBLE ATTACK SOURCES OF A NETWORK

1. Endpoints
2. Smartphones & Tablets
3. Outdated Softwares
4. Wrong Configuration Of Network Devices
5. Internal Threats

PHASES OF A NETWORK ATTACK

A cyber-attack almost always follows a precise process and does not originate from a single action: it is the result of a step-by-step process, the more time we spend on each one of these phases, the more efficient the final work will be.

1. Information collection; 2. Network scanning; 3. Access to the network; 4. Maintaining access to the system; 5. Canceling the log files.

PHASES OF A PENETRATION TESTING

1. INFORMATION GATHERING: We can instead rely on tools and platforms available on the Internet: Google; Whois search; DNS; Social media; Metadata; Websites with job listings; Tools like Maltego and Recon-ng; Specific browsers, like Shodan.
2. NETWORK SCANNING: Scanning a network is almost like finding yourself in a wide street in a big city, a place full of shops. All of a sudden, you start to pick the locks of each one of them hoping that at least one is open and unprotected.
3. ENUMERATION: Enumerating the network means discovering and listing all the resources available.

4. VULNERABILITY ASSESSMENT.
5. EXPLOITATION.
6. POST EXPLOITATION.
7. FINAL REPORT.

Chapter #2: The Laboratory

This consists in simultaneously executing multiple virtual machines and, therefore, more operating systems within the same physical system. A hypervisor makes the whole process much more convenient!

VIRTUALIZATION

1. Download a particular software called hypervisor.
2. Collect the .iso images of the operating systems you want to install.
3. Access the software.
4. Start the virtual machine creation process.
5. Create and boot this virtual machine.
6. Proceed with the installation of the desired operating system.
7. Use the virtual machine you have just created.

HYPERVISOR

software that allows you to run virtual machines inside your physical PC.

IMAGES OF AN OPERATING SYSTEM

CREATION OF VIRTUAL MACHINES

"File > New virtual machine" and follow the recommended procedure.

NETWORK MANAGEMENT

Use 4 different types of networks:

1. Bridged -> includes the creation of an IP address belonging to the network in which your physical PC is located.
2. NAT -> your virtual machine can connect to the Internet, but it cannot be reached from the outside.
3. Host-only -> virtual machine can only communicate with your physical host.
4. Custom -> define your personal network and let all the virtual machines communicate inside it.
5. To create it, go to "Edit -> Virtual Network Editor" and create a new network

VIRTUAL MACHINES BOOTING

the machines will all be started up and will have the IP address previously assigned.

INSTALLATION OF VMWARE TOOLS

CONNECTIVITY VERIFICATION OF VIRTUAL MACHINES

1. Verify the validity of the IP address assigned to each virtual machine.
2. Run the "PING" command on each virtual machine and verify that the response is positive.

Chapter #3: Linux Commands

BASIC COMMANDS

1. Command to execute: ls Explanation: this command allows you to list the contents of files and/or folders.
2. Command to execute: pwd Explanation: the current directory is printed.
3. Command to execute: cd Explanation: it allows you to access the selected folder.
4. Command to execute: cp Explanation: it allows you to copy files.
5. Command to execute: mkdir Explanation: it allows you to create a folder.
6. Command to execute: rmdir Explanation: it allows you to remove a folder.
7. Command to execute: touch Explanation: it allows you to create a file.
8. Command to execute: tar Explanation: it creates an archive for a certain file.
9. Command to execute: clear Explanation: it allows you to return to an initial shell.
10. Command to execute: adduser Explanation: it allows you to add a new user.
11. Command to execute: chmod Explanation: it manages file and/or folder permissions.
12. Command to execute: vi Explanation: it allows you to edit a file
13. Command to execute: cat Explanation: it allows manipulation of a file.
14. Command to execute: grep Explanation: it searches a file for particular patterns.
15. Command to execute: apt-get Explanation: package management. For example, apt-get install.

NETWORK COMMANDS

1. Command to execute: ifconfig Explanation: utility to configure network interfaces. It will be very useful to view the IP address assigned to a machine.
2. Command to execute: traceroute Explanation: this command allows you to trace the path of an IP packet to the host network. It is very useful for performing troubleshooting activities such as, for example, verifying where in the path a certain IP packet stops or is lost.
3. Command to execute: dig Explanation: this is a utility needed to query DNS.
4. Command to execute: telnet Explanation: this command allows us to make connections to remote hosts via the TELNET protocol.
5. Command to execute: telnet Explanation: this command allows us to make connections to remote hosts via the TELNET protocol.
6. Command to execute: nslookup Explanation: this is another utility to interrogate DNS and to perform inverse resolution queries.
7. Command to execute: netstat Explanation: this is a command of the utmost importance. It allows you to view the network connections opened at a certain time. Useful in troubleshooting, it allows us to verify anomalies due to network connections that were not established or lost.
8. Command to execute: ifup, ifdown Explanation: this command allows you to enable or disable network cards.

9. Command to execute: ping Explanation: the PING command is used to check whether a certain host is active or not by sending special ICMP type packets to it and waiting for a response.
10. Command to execute: route Explanation: this command is used to display the routing table of a certain host, namely the paths that the network packets must perform on the network or on particular subnets.
11. Command to execute: arp -a Explanation: the ARP -A command provides us with a table of the links between a MAC address and an IP address.

COMMANDS RELATED TO SYSTEM MANAGEMENT

1. Command to execute: uptime Explanation: this command shows you for how long a certain system has been active.
2. Command to execute: users Explanation: this command shows the user names of users connected to a system.
3. Command to execute: who / whoami Explanation: this is another command that informs us of how many users are connected to the system as well as some additional information.
4. Command to execute: crontab -l Explanation: this command allows the display of scheduled jobs related to the current user.
5. Command to execute: less / more Explanation: this command is very useful because it allows you to quickly view a file. Press the "q" key to exit this particular display.
6. Command to execute: ssh Explanation: this command allows the connection to a remote host via an SSH protocol
7. Command to execute: ftp Explanation: this command allows the connection to an FTP server via the FTP protocol.
8. Command to execute: service start / stop Explanation: this command allows you to start or stop a certain service.
9. Command to execute: service start / stop Explanation: this command allows you to start or stop a certain service.
10. Command to execute: free -h Explanation: this command shows the amount of free and used memory.
11. Command to execute: top Explanation: this command allows you to check the active processes in a system.
12. Command to execute: ps Explanation: with this command you can view the active and running processes in a system.
13. Command to execute: kill Explanation: this command is used to terminate a certain process.

Chapter #4: Mind Maps

"a diagram used to visually organize information ". This software allows you to create many different types of mind maps. (XMind)

Chapter #5: Network Theory

ISO-OSI MODEL: theoretical formulation that allows you to identify exactly in which network layer we are operating.

1. Application Layer: high-level protocols interact with each other at this layer. Some of these protocols include but are not limited to HTTP, HTTPS, FTP, and others.
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer: this level focuses on the communication between different networks. In this case, we will mainly use the Internet Protocol (IP) (router)
6. Data Link Layer: this level finds its maximum expression within the context of local networks (LAN). (switch)
7. Physical Layer: this layer includes everything related to the transfer of data within a specific means of communication (copper, fiber or radio wave network cable). (means of physical and non physical communication.)

MAC ADDRESS

1. The MAC (Media Access Control) address is a 48-bit address that is uniquely assigned by the manufacturer of each Ethernet or wireless network card.
2. Eg: 3A-34-52-C4-69-B8
3. This address is fundamental in the world of networks because it allows a machine to be uniquely identified within a local context (for example LAN).
4. Type the following command in your Windows device: “ipconfig /all”. If you are using a Linux device, enter this one: “ifconfig”.

IP ADDRESS

1. The IP address appears as a numeric value of 32 bits and allows the identification of both the network and the host.
2. No machine can browse if it is not provided with an IP address. IP addresses are divided into public and private. The public ones allow browsing on the Internet, while the private ones are used inside internal sub-networks (a company's network, for example); no private IP address will ever be able to surf the Internet.
3. These are 3 examples of private IP addresses.
    - Class A private IP addresses where the initial IP address is 10.0.0.0 and the final IP address is 10.255.255.255.
    - Class B private IP addresses where the initial IP address is 172.16.0.0 and the final IP address is 172.31.255.255.
    - Class C private IP addresses where the initial IP address is 192.168.0.0 and the final IP address is 192.168.255.255.

ARP PROTOCOL

1. ARP stands for "Address Resolution Protocol". This protocol keeps track of the association between a MAC address and an IP address.
2. You can type the "arp -a" command to view the ARP table of your Windows PC.

DEFAULT GATEWAY

1. When you need to communicate within your local network, you will use the ARP protocol, which facilitates the association between a MAC address and an IP address.
2. Every time your PC does not know where to send a certain IP packet, it will send it to your default gateway for further processing and to allocate it to subsequent devices, which are part of the IP packet path.

NAT

1. NAT stands for "Network Address Translation".
2. PRIVATE IP ADDRESS -> to verify your private IP type the "ipconfig" command.
3. PUBLIC IP ADDRESS -> to check your public IP click on the following link: https://www.whatsmyip.org/.

DNS

1. DNS is another essential service of a network.
2. We can divide the DNS into two main categories: the public and the private ones. The public ones are meant to resolve the public IP addresses, while the private ones will translate the private IPs.

DHCP (Dynamic Host Configuration Protocol)

1. This protocol automatically assigns all the parameters through a central server that manages the whole network.
2. DHCP can generate two types of network packets:
   - DHCPDISCOVER. The PC that needs an IP address sends this packet to the entire network hoping that a DHCP server will be able to intercept it.
   - DHCPOFFER. When a DHCP server receives a DHCPDISCOVER packet, it tries to satisfy the request and sends a DHCPOFFER packet with all the necessary network parameters to the MAC address of the PC (the IP is obviously still unknown).
3. Client → Server
   - Discovery
   - Offer
   - Request
   - Acknowledge

PORT AND SERVICE

1. There are 65535 ports available but not all of them are used.
2. If we want to see all the active communications within our Windows device, we need to type the " netstat -ano " command.

3. For more information on the “netstat ” command

ARP-PING-TRACEROUTE

1. " ARP, PING " commands. They will allow you to solve most network problems, so it is important to learn more about them.
2. The first major distinction between them layers in the layer of the ISO OSI model in which they operate:
    - ARP -> between data link level (MAC address) and network layer (IP address).
    - PING -> network layer (IP address).

Chapter #6: Corporate Networks

No network can work without being supported by at least two devices: a SWITCH and a ROUTER .

CISCO PACKET TRACER: This kind of software allows us to create and simulate network scenarios.

LAN-WAN-DMZ

1. By internal world we mean everything happening inside our private network, where our private IP addresses are assigned. This is called LAN (Local Area Network).
2. This distinction helps us to emphasize, once again, the concept of "inside" and "outside ".
3. One of these is the so-called "DMZ", which means "demilitarized zone".

SWITCH: The main function of this apparatus is to sort packets within a network. It operates at the data link layer of the ISO/OSI model.

1. The packets sorted by the switch are called FRAME .
2. The switch automatically learns the topology of the LAN network. It can figure out to which of its ports each PC is connected. It summarizes in a table, called the CAM table
3. The switch has other more advanced features, such as MAC address filtering or other particular control operations.

ROUTER: The need to use this new network device stems from the fact that we cannot remain confined within our subnet.

FIREWALL

1. router with advanced security features. By convention, we place the firewall between the upper end of the data layer and the lower end of the network layer.
2. Main Function: carry out packet filtering. It manages the traffic entering and leaving the network, and it is based on the concept of port and/or service. It also helps us to create security rules, which we will then include in our “security policy ”.
3. This device is often referred to as a “perimeter firewall” because its natural location is on the border of the internal network. This position allows it to protect our internal network from the outside world.
4. The firewall always works according to some criteria: Source IP address. Recipient IP address. Door and/or service.

Chapter #6: Information Gathering

3 Main Types of Penetration testing

1. BLACK BOX TESTING: person who performs the security test is not aware of any details on the network infrastructure that he will have to test. only be informed of the client's company website.
2. GREY BOX TESTING: middle ground compared to the other two categories.
3. WHITE BOX TESTING: operator is aware of all the information of the network to be examined or of the area to be tested.

FIRST CONSIDERATIONS

GOOGLE HACKING -

GOOGLE DORKS: Google can be used for particular queries that are much more specific and in-depth than the ones we normally perform.

The "Directory Listings " is a very useful technique that consists in a list of folders and files within a certain website.

you can check the Google Hacking Database that lists hundreds of possible queries

GOOGLE CACHE:

1. The Google Cache is a useful tool that allows you to view how a Web page looked like during Google's last visit.
2. There are two ways for you to view the cache: Through Google keywords. Through dedicated websites.

WAYBACK MACHINE: Have you ever wanted to monitor how a certain website has changed over time? It is not just a fun activity.

INFORMATION FROM SOCIAL MEDIA: The social media accounts of people and companies often reveal an impressive amount of information, which has been unwittingly made public.

KEYWORDS IN JOB POSTINGS: These are three well-known job posting sites: Monster. https://www.monster.com/. Infojobs. https://www.infojobs.com. Jobrapido. http://jobrapido.com/.

METADATA EXTRACTION: A metadata is nothing more than additional information inserted within the document and it can several purposes.

USING WHOIS: While collecting information, we should be able to identify an IP address or URL string belongs to what Internet provider (the connectivity service provider) as well as the domain name holder. WHOIS is a network protocol aimed at performing this task. WHOIS can be consulted from the command line but also from Web applications that allow to enrich the search. Now let's examine both options

Command prompt: whois udemy.com

Using DNS

1. A DNS query is the simplest operation we can perform in this case. We should run the command " nslookup ", which we can use to ask the DNS to show us the association between hostname and IP address.

2. Another command we can execute on Linux systems is DIG . This command allows us to gather different information and interrogating DIG is a very simple task.

Maltego and Recon-ng: automate our information gathering

Shodan:

Chapter #7: Network Scanning

KFSENSOR: Honeypots are deliberately vulnerable machines, which are sometimes used to confuse a potential attacker.

ARPING AND LEVEL 2 NETWORK SCAN

1. The first thing we should mention is that the network can be scanned both at the data link layer and at the network layer of the ISO/OSI model.
2. We need to enter this command: "arping address IP -c 2 ".

NMAP AND LEVEL 2 NETWORK SCAN

1. Nmap does its work. 1. Name resolution. 2. NSE script pre-scan phase. 3. Host discovery. We are now at this stage. 4. Parallel reverse name resolution. 5. Port or Protocol scan. 6. Service version detection. 7. OS fingerprinting. 8. Traceroute. 9. NSE portrule and hostrule script scanning phase.
2. "-sn " is the option you should use to instruct Nmap.
3. 192.168.1.100-150 is the range of IP addresses we want to test. We could be dealing with a single address or a subnet.

PING SCAN WITH NMAP

1. The ICMP performs various control functions, including the verification of reachability of a certain host within a network.
2. Echo request. The attacking host sent the ICMP packet to the target machine. Echo reply . The target machine sent the response packet to the attacking machine.

TCP AND UDP PROTOCOL

The transport layer is mainly composed of 2 protocols: TCP and UDP . The main difference between these two protocols is that TCP is a connection-oriented protocol, while UDP has no connection.

TCP CONTROL FLAGS

1. SYN. ACK. RST. FIN. PSH. URG.
2. The presence of the RST flag shows that we need to reset the connection. This may be due to connection errors and the FIN flag indicates there are no other data that the sender should receive.
3. The three-way handshake is an exchange of packets between two entities that use TCP flags (SYN and ACK) to organize their communication.

CREATION OF CUSTOMIZED NETWORK PACKAGES

1. There are several software options that allow the creation and modification of packets that travel within a network (packet crafting).

2. " Colasof Packet Builder " gives us the possibility to choose the type of packet to create or modify.

LEVEL 4 NETWORK SCAN - CONNECT SCAN

Now we will learn together the simplest technique to perform a level 4 scan: the CONNECT SCAN . This type of scan establishes the TCP connection.

LEVEL 4 NETWORK SCAN - SYN SCAN

LEVEL 4 NETWORK SCAN - UDP SCAN: Keep in mind that the UDP protocol is connectionless and therefore behaves differently from TCP.

Chapter #8: Banner Grabbing

INSTALLING THE WEB SERVER MICROSOFT IIS

BANNER VISUALIZATION IN MICROSOFT IIS: First of all, let's connect to the Web server using "telnet "

BANNER CONFIGURATION ON KFSENSOR

Once the configuration is complete, we can use the Nmap feature called " service detection ", which will attempt to grab the banner of the listening service and inform us of what version it is.

INSTALLING A FTP SERVER

FTP BANNER GRABBING WITH NMAP

FTP BANNER GRABBING WIRH METASPLOIT

1. We start Metasploit by launching the "msf " command from terminal.
2. In "rhost ", we need to enter the IP address of the victim machine, that is where the listening FTP service is located. Once this part is completed, we can run the " exploit " command and then start the scanner
3. The scan is quickly completed, and the result obtained informs us of the presence of a Microsoft FTP server .

FTP BANNER GRABBING WITH NETCAT

NETCAT is another useful tool used for grabbing banners.

FTP BANNER GRABBING WITH TELNET

OPERATING SYSTEM DETECTION

1. We can follow two different procedures: Active mode. Passive mode.
2. In the active mode, we interact directly with the target. Nmap is a tool commonly used in active mode. On the other hand, the passive mode listens to network traffic.

OS DETECTION WITH NMAP: The option to use is "-o", so this command will be the command we need to execute

OS DETECTION WITH XPROBE: XPROBE is another tool useful for detecting the operating system

OS DETECTION WITH P0F: We need to capture some network traffic, so that P0f can complete the detection process.

Enumeration: Enumeration is an important phase of the penetration test process. I

NETBIOS enumeration. DNS enumeration. Enumeration through DEFAULT PASSWORD.

ENUMERATION WITH NETBIOS

1. Netbios is a protocol that operates at the session layer of the ISO/OSI model . This protocol allows us to explore the network resources of computers, printers or files.
2. We can use Netbios to extract several information, including the following: Hostname. Username. Domain. Printers. Available network folders.
3. The "net use " command allows us to access these resources.
4. These are the scripts we need to verify any NETBIOS vulnerabilities: smb-vuln-conficker. smb-vuln-cve2009-3103. smb-vuln-ms06-025. smb-vuln-ms07-029. smb-vuln-regsvc-dos. smb-vuln-ms08-067

ENUMERATION WITH DNS

1. with another DSN enumeration technique for which we will be using another tool, called DNSENUM.
2. With a single command we can extract different DNS records, which are the following ones: SOA. A. MX. NS. CNAME. PTR. HINFO. TXT.

ENUMERATION WITH DEFAULT PASSWORD

1. Network devices – such as routers and switches – very often have a default password. These passwords are defined directly by the device manufacturer
2. DefaultPassword is one of the many sites where default device passwords are stored

Vulnerability Assessment

1. At this link, you can find a detailed report written by SANS that lists all the steps we should take to perform a vulnerability Assessment:
2. Below is the list of tools we will use: Nessus. https://www.tenable.com/products/nessus vulnerability-scanner. Nexpose. https://www.rapid7.com/products/nexpose/. OpenVAS. http://www.openvas.org/.

INSTALLING NESSUS

SCANNING WITH NESSUS

INSTALLING NEXPOSE

SCANNING WITH NEXPOSE

WEBSITES FOR VULNERABILITY SEARCH

Packet Storm. https://packetstormsecurity.com/.

Chapter #9: Exploitation

1. Exploitation is meant to confirm if we can access our target machine from a given vulnerability
2. An exploit is a sequence of commands, or lines of code, that exploit the vulnerabilities of a certain software. It can allow us to take actions that come as unexpected to the victim machine

3. Exploits can be classified as follows: Service-side exploit: this type of exploits affects a particular service listening on the target machine. Client-side exploit: the attack starts directly from the client machine. Local privilege escalation exploit: once we have access to the target machine, we need to elevate our privileges using exploits belonging to this category.

SERVICE-SIDE EXPLOITATION: Once you have gained access to a specific machine, you can proceed recursively to gain access to other machines that may be visible only from the first compromised machine. In technical jargon, this action is called “pivoting”.

CLIENT-SIDE EXPLOITATION: In client-side exploitation, our point of view is completely different from the side-client type. In this case, the victim unknowingly unleashes the attack and establishes a connection with the attacking machine. To start the attack, it is enough for the target user to open an Excel file attached to an email or downloaded from the Internet.

METASPLOIT

1. Going a little into detail, we can say that Metasploit consists of the following elements: an exploit database. a payload database. auxiliary modules for particular operations. post-exploitation modules for the penetration test phase. user interface to easily manage the whole structure.
2. The same user interface is composed of several modules, including: msfconsole. From which we can execute several exploits/payloads. MSFD. Service listening on TCP port 5554 which allows multiple users to connect to the same Metasploit instance. armitage. A graphical version of Metasploit. msfvenon. It is mainly used in the client-side exploitation phase to convert our payloads into different types of executable files.

DEMONSTRATION OF CLIENT-SIDE EXPLOITATION

1. Initial configuration of the victim machine with a Windows operating system. 2. Creation of the malicious file with Metasploit, in particular with the msfvenon interface. 3. Creation of a Web server (attacking side) on which the malicious file will be hosted. 4. Use of Metasploit and in particular of msfconsole. 5. Execution of the malicious file on the victim machine. 6. Connection established between attacker and target. 7. Interaction with the Metasploit shell

INITIAL CONFIGURATION OF THE VICTIM MACHINE

1. Victim machine (Windows 7 OS): 192.168.1.227/24. Attacking machine (SO Kali Linux): 192.168.1.133/24.
2. Then we can confirm the communication between them with the "ping " command.
3. Disable the local firewall.

CREATION OF A MALICIOUS FILE

LHOST is the local address of the attacking machine, i.e. Kali. LPORT is the door where we will listen and wait for someone to connect. FileMalevolo.exe will be the malicious file generated and located in the /tmp folder of the Kali machine.

SETTING UP A SIMPLE SERVER

PREPARATION OF THE EXPLOIT/PAYLOAD

Pay attention to the difference between PAYLOAD . An exploit allows us to take advantage of a given vulnerability. A EXPLOIT and payload is a piece of code that will be executed by using the EXPLOIT command.

HOST COMPROMISSION: With the "sessions -l" command we are able to see which are the active connections and their IDs; then with the "session -i ID " command we access the one of interest to us.

SERVICE-SIDE EXPLOITATION: We will exploit a vulnerability present on an old version of an audio software for Windows operating systems, called ICECAST

ICECAST INSTALLATION ON WINDOWS

METASPLOIT INITIAL CONFIGURATION

1. RHOST, namely the IP address of the victim machine.
2. LHOST, basically IP address of the attacking machine.

HOST COMPROMISSION

1. SYSINFO to gather more information on the operating system.
2. GETUID to view which user we are using to connect to the machine.
3. SHELL to access the local command prompt.
4. SCREENSHOT to capture a screenshot of the victim machine.
5. PS to check all the processes running on the victim machine

Post-exploitation

1. Privilege escalation.
2. Access maintenance.
3. Data collection.
4. Cyclic process of network scanning to new hosts: Network scanning. Banner grabbing. Enumeration. Vulnerability assessment. Exploitation. Post exploitation.
5. Repeated exploitation towards new hosts.

PRIVILEGE ESCALATION WITH DISABLED UAC

PRIVILEGE ESCALATION WITH ENABLED UAC

CREDENTIALS HASHDUMP: A typical action in these circumstances is to obtain the credentials hashes. A hash is a unique string generated from a certain password and based on a cryptographic algorithm. "hashdump " command

LOCAL EXPLOIT SUGGESTER: "getsystem " command a host to obtain the highest privileges.

Here you can see an EXITFUNC, LHOST and SESSION

USING THE MIMIKATZ MODULE

1. We should rely on an established meterpreter session and have the SYSTEM privileges.
2. "load mimiakatz" command., "wdigest " command

INSTALLING A BACKDOOR ON A TARGET SYSTEM

1. now install a "backdoor"

2. The backdoor that we will use will be installed on a registry key of the target machine with the possibility of starting it every time the machine is booted. This module is called " PERSISTENCE ",
3. The "-X " option starts the backdoor each time the system is booted. The "-p 8081 " option is the port on which the attacking system will listen. The "-r " option specifies the IP address of the attacking machine. The "-i 5 " option is the interval in seconds between each connection attempt.

INTERNAL NETWORK MAPPING

1. "ipconfig "
2. "arp -a " command gives us evidence of all the machines connected to that particular network segment.
3. You can see the active network connections by entering the "netstat -an " command:

Chapter #10: Final Report

EXECUTIVE SUMMARY: can be understood even by non-technical staff

METHODOLOGY: Definition of the test scope. Information gathering. Network scanning. Vulnerability assessment. Exploitation. Post exploitation. Other optional tests. Drafting of the report also through the use of automatic tools, for example with Dradis.

DETAILED ANALYSIS OF THE RESULTS