International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 23 (2018) pp. 16637-16647

Ethical Hacking on Mobile Devices: Considerations and practical uses.

Miguel Hernández[1], Luis Baquero[1], Celio Gil[1] and Carlos A. Salamanca[1]

[1] *Fundación Universitaria Los Libertadores, Bogotá D.C., Colombia*

Abstract

The improvement of computer security begins with the need to know the existing risks, analyze their incidence and define the mechanisms that allow their correction later. In this initial phase of analysis is where ethical hacking is a fundamental component for the process of evolution of companies from simple functionality to the security of their systems.

This article reflects a preliminary analysis of the concepts and characteristics that make up a mobile device, the different risks to which they are exposed and the vulnerabilities that must be known in order to perform an ethical hacking.

The present work is divided into three parts, starting with the introduction where the users and the environment are discussed, the risks arising from the use of these devices are analyzed, and a SWOT matrix is elaborated which describes the management of security in mobile environments The second session deals with aspects such as specifications, mobile security, vulnerability penetration and security model; already in the third part, the topic of ethical hacking in Smartphone and the different non-intrusive techniques, as well as the scanning tools, are deepened to finally perform attack tests in the system.

Keywords: Ethical hacking, Informatic security, mobile devices, threats, vulnerabilities.

1. INTRODUCTION

An intelligent mobile device allows the development of mobility and the development of simultaneous tasks fulfilling the concept of "computing anywhere or at any time" [1].

With technological innovation, mobile phones have a great evolution which creates a great demand and leads to develop more functionalities and more similar characteristics to a computer, making work more efficient in everyday life [1].

The traditional telephone happened to connect to a telephony network and was called Smartphone, the constant demand of these devices has made them are in continuous growth, making that there is a large number of users. They are used to store confidential information, managing the daily agenda, browsing the internet, saving photographs, making videos, creating personal or professional documents and executing financial operations [2].

As a result of all these features, the Smartphone has become an indispensable tool to perform a large number of tasks as you can see the growth that is reflected in Figure 1.

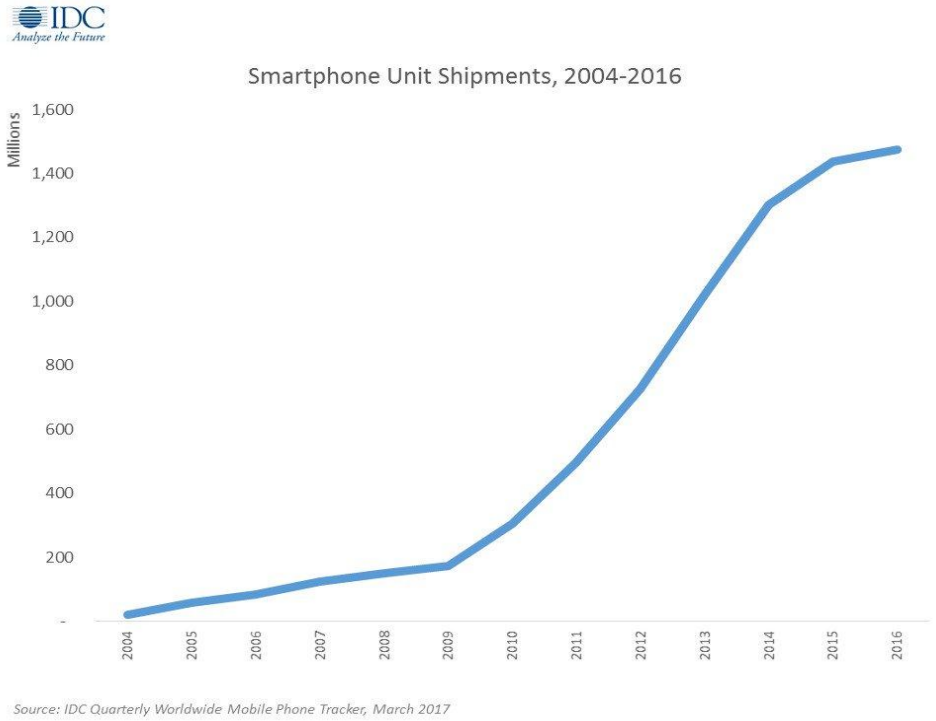

Figure 1. Distributed Units *200-2016* [1]

From the massive use of these devices both personally and in the workplace, has increased the potential for insecurity which has led to conduct studies related to this situation. The security of the information is essential due to the boom of these devices, since consumerism brings a technological era where there is a high dependence on this type of devices. Because the information opens all the doors and creates a spectrum of uncertainty, leaving the security in the hands of users, which is totally null and there is a high index of vulnerability running the risk that your information is extracted [2].

As can be seen in the comparative table described in Table 1, many of the security incidents that telephones have originate from the process of integration of hardware standards and multiple wireless technologies [3] [4].

You can also find problems such as viruses, complex programs or the loss or theft of the phone, therefore companies in their eagerness to create better phones focus on the development of features without validating the differences between the software and the hardware. On the one hand, a large gap in security features. Statistics show that only 20% of users use any application or have a policy that relates to security [5].

Because the mobile security area is very extensive, Table 2 describes a SWOT analysis in mobile environments:

Table 1. Comparison of security incidents [3][4]

INCIDENT	MOBILE	DESKTOP
1. Unauthorized access	Stealing information, making calls, sending messages, stealing passwords and stealing contacts	Theft of information, access to applications, theft of passwords
2. Equipment abuse	Theft of minutes, Internet theft (data).	Use the machine as an attacker (distributed attacks).
3. Computer viruses	Information theft, denial of cellular service, malfunction.	Information theft, denial of service, malfunction.
4. Deletion of information	Perdida de datos y contactos	Perdida de datos, contraseñas y programas instalados.
5. Theft of equipment	Theft or loss of data, misuse of telephony and internet.	Lost or stolen data.
6. Viruses, trojans, spyware	Theft of contacts, data, equipment malfunction, denial of telephone service	Data theft, passwords, sessions, computer malfunction.
7. Denial of service	You can not receive or send notifications, messages or calls	It does not respond to requests, without the availability of critical servers.
8. Sniffers	They can steal data, passwords, sessions, contacts, text messages.	They can steal data or sessions.
9. Frauds	Theft of information, credit cards, cash.	Theft of information, credit cards, cash.
10. Spam	Denial of service during synchronization with email.	Denial of service due to hard disk saturation.

Table 2. SWOT analysis in mobile environments [6]

Strengths	Weaknesses
Good security design in mobile phones.	Little culture of user safety.
Increased concern of manufacturers in mobile security.Aplicación de seguridad en el Market.	There are no restrictive policies for installing external applications.
Secure remote access.	There are several different mobile operating systems and there is no standard in mobile security.
Companies bet more on the use of mobile applications.	Use of many third-party applications.

Opportunities	Threats
Increase of mobile technologies with the handling of sensitive information.	Start of the era of malware to mobile devices.
Increase in the use of internet on the cell phone.	Use of mobile applications are increasing more and more.
Development of antivirus for mobile devices.	Volatility of data in mobile environments.
Development of policies and correct use of mobile devices.	The vulnerabilities that wireless technologies still have.
Extension of communication technologies.	Bad handling of permissions in applications.

Table 3. Comparative chart of kernel in mobile operating systems [7]

	Android	**BlackBerry Os 4.7**	**iPphone OS 3.0**	**S60 5th Edition**	**Palm WebOS**	**Windows Mobile 6.5**
Kernel	Linux with virtual machine Dalvik	Owner	OS X	Symbian	Linux	Windows CE
Connectivity	3G Wifi, GSM, GPRS	3G, GSM, CDMA, WiFi	3G, GSM, WifI	3G, GSM. CDMA, WiFi	3G, GSM. CDMA, WiFi	3G, GSM, CDMA, WiFi

As you can see in this analysis, there are a lot of strengths (security designs in the OS), but the threats are increasing every day and the lack of security policies means that one of the objectives of this article is that users become familiar with the concept of hacking on mobile devices [6].

The kernel in the operating systems is the main core and is responsible for facilitating secure access to mobile programs and is responsible for managing resources through the system call services, as described in table 3.

In a free distribution kernel such as the Linux operating system, there is a wide range of developers, which is an advantage because security and bug issues can be detected, improvements made, and these vulnerabilities adapted to the new changes. In a closed system it is much more expensive to find the errors, since the developers have greater restrictions and the detection process is much more delayed, increasing the times and costs to find the vulnerabilities.

2. SPECIFICATIONS

2.1 Mobile devices

Smart mobile devices are those that have the functionalities of mobile phones and digital assistants:

A mobile device can be defined with some processing capabilities, with permanent or intermittent connection to a network, with limited memory, which has been designed specifically for a function, but which can carry out more general ones. According to this definition there are many mobile devices, from portable audio players to GPS navigators, through mobile phones, PDAs or Tablet PCs [7].

For the wide variety of devices that are on the market there are also several features that meet the needs of users especially in hardware such as touch and LCD screens [8], the camera that goes from the 2.0 Megapixels, memories internal as removable, the performance of the battery.

2.2 Components that affect mobile security

In the hacking environment you must handle the concept of being a hacker, then know the types of hackers that there are and finally know that it is an ethical hacking.

The Royal Spanish Academy defines the term hacker as [1] [9]:

- m. y f. Inform. Hacker.
- m. y f. Inform. Person with great knowledge of computer science that is dedicated to illegally accessing foreign computer systems and manipulating them.

It can be concluded that hackers are professionals who are known to move in the computer world playing the role of a scammer who tries to compromise a system to steal digital information or can be a professional who helps defend the system from these attacks.

There are several types of hacker, the white hat is the ethical professional who focuses on protecting and ensuring information and communication systems. The black hat is the villain unethical very different from the hero who is interested only in entering and take all the information and the gray hat has all the skills of the white hat hacker but the knowledge he has uses to know how he can make fun security with the thoughts of the black hacker and do their own procedures [10].

2.3 Vulnerability penetration

Pentest: (Penetration Test Assesment), this test is used a lot to perform ethical hacking, penetration tests are performed on the systems, bypassing all access controls. Threat tests are performed to have a full knowledge of the risk.

When a penetration test is carried out, the main objective is to be able to enter the system, achieving full control of the privileges as an administrator and thus control all the resources of the system and the network.

This analysis is very important to review the vulnerabilities that can be exploited by attackers and allows companies to take measures to improve these weaknesses [10].

2.4 Mobile Security

Every day mobile devices become an indispensable tool in daily life, every time more applications are developed, that's why security and privacy mechanisms are constantly being improved for the wireless world, having well-defined aspects such as authorization, authentication and reliability [11].

2.5 Security model

A mobile device by its design and functionality are low power optimizing power consumption, are also limited in their storage

and restricted to handle large amounts of data such as virus databases. A mobile device has several ways of connecting via Wifi, Bluetooth and the GSM, 3G and 4G networks, from here the principle of confidentiality and data integrity [12].

The most important threats to enter phones start with malware or Trojans, these malicious programs hide inside good programs, stealing information and running automatically to other devices [13].

2.6 Weaknesses and security

Mobile security is unique and very different from the security of wired networks, since mobile signals are transmitted by not so powerful wireless means and carries a special handling in security, therefore the mobile environment must be reinforced when they are used security solutions used in the network to provide confidentiality, integrity, authentication and that is not rejection of the device in mobile wireless parameters [14].

2.6.1 Wireless Transmission

Signaling traffic is referred to as the transmission of data over a cellular network complying with the principles of confidentiality of: traffic, signaling and user authentication, these principles must be met within the anonymity of the user's identity. The traffic must be encrypted in coding systems such as CDMA2000, UMTS, GPRS, GSM and must be used in encrypted user traffic to achieve end-to-end security [15].

2.6.2 Seguridad 802.11

More and more devices are connected to the Wi-Fi network and security issues became an important issue when discovering a large number of vulnerabilities in the WAP and WAP2 WEP standards. These risks include unauthorized access, denial of DoS service and wiretapping [16].

2.6.3 Bluetooth security

It is a wireless technology that connects devices that are at close range and is used to transmit files between devices that have this technology, one of the security problems is the confidentiality of data [17].

The use of the PIN number has security problems when the exchange of keys is presented. A PIN can be between 8 and 128 bits and can come by default on the device or the user can select one. When an attacker obtains the PIN code it is easier for him to obtain the initialization key and the link key, compromising the communication of the two devices [18].

The most known attacks through this technology are: Bluesnarfing, Bluebuggin and Bluejacking [14]. You can also perform brute force attacks and thus obtain the MAC address of the devices that are not in detectable mode within the network, two of the programs that help carry out this process are Red Fang and Blue Sniff [19].

Another way is through the so-called backdoor attack where the attacker has a trusted key that is established in the exchange of keys where the victim device has silent remote access controlling the device and managing to download data such as calendars, photos, emails and everything related to personal data [19].

A sound recommendation is to have programs developed by trusted suppliers that comply with ethical standards and that are certified with digital signatures and that the user can reject those that do not comply with the standard [20].

2.6.4 Infection modes

Through mobile devices, there are many routes of infection in which a virus can be distributed, among the most frequent we have:

Text messages and multimedia messages are a means of easy propagation of malicious software. A bot installed on a mobile phone can send infected messages to all contacts, an example of this type is commwarrior [21].

The IM IM (Facebook Messenger, Skype, WhatsApp, Hangouts), sends links to contacts to direct them to malicious sites and with only access to the IP is contaminated.

2.6.5 Threats and attacks

The first threat with a high rate is the loss or theft of mobile devices, each year hundreds of phones are within this great indicator. This factor is probably the biggest threat. Channel espionage can capture the messages that are transmitted over the network without being detected, it can mask the identity of the attacked person by impersonating the device.

In the attacks of man in the middle, the attacker intercepts the messages between two media and modifies them. Another type of very common attack is denial of service, where the attacker accesses from a point or mobile station in order to generate a lot of network traffic towards the attacked device.

In unauthorized access, the attacker can use radio equipment or programs to access unsecured networks, which in many cases are corporate wireless networks open to unauthorized users. Viruses and Spam, are small programs that spread on the network among users and that have become a big problem [17].

2.6.6 Mobile antivirus

The term antivirus no longer covers traditional malicious files but transcends malware, keyloggers and the challenging rasomwares. At present, mobile devices do not have an antivirus installed by default, since they are very limited and, in addition, they are powered by a database that must be permanently updated; reasons why antivirus companies had to update their methodologies to identify these threats using artificial intelligence because they would not only be developing an antivirus, but more robust programs based on behavior.

Among the most used techniques in the analysis of malicious files, are the following: heuristic classification, redundant exploration, integrity checkers, behavior blockers, agent based simulation and data mining [17].

3. ETHICAL HACKING IN SMARTPHONES

It is important to emphasize that the pentester or hacker must have a good knowledge about technology to be able to carry out an ethical hacking, for which they must define a methodology that allows to take an order in the execution of the test and optimize the time in the execution phase [22].

Figure 2 shows the cycles of ethical hacking, in this methodology the different phases and tests are observed in an environment mounted with mobile devices.

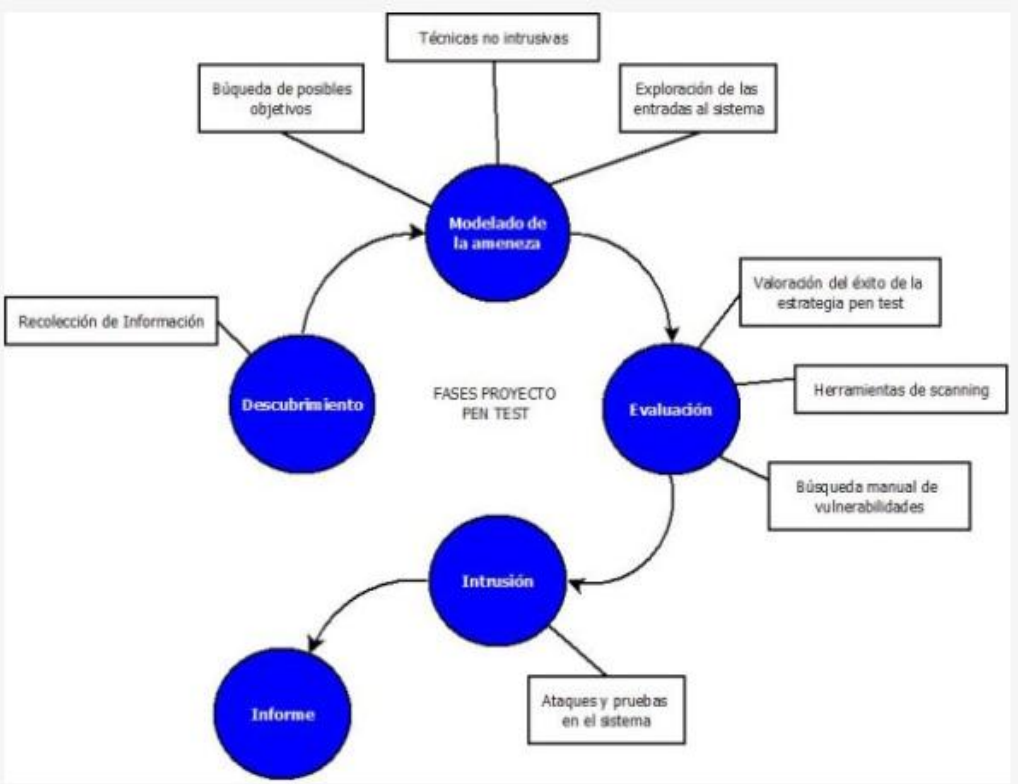

Figure 2. Phases of an Ethical Hacking [22]

3.1 Footprint Review

Footprint review is the process where the hacker develops a map that can be networks, systems or company. From here it will begin to collect all the information of the victim determining the objective as a system and the application that wants to attack.

The hacker arrives at the assembly of the map from non-intrusive methods, making use of social engineering from the website and telephone directories of the company, through this technique allows to discover initial information and build a map of the range of the network.

3.1.1 Information retrieval

This stage begins with a search through the Google search engine in order to investigate the name and if it is a company through the DNS, know the IP address of the server and collect the information.

Some examples of the filter of this search are:

- Search ads or press job offers in the systems department, because here you can find clues about the infrastructure they have or databases they use. For example, if you are looking for a webmaster who manages Apache, you would already know which web server they use.
- With the Who is command you can obtain information on the name of the company that owns the domain, address and telephones of the administrator, as well as knowing the assigned IP ranges since many companies do not pay for the information privacy service.
- In social networks such as Facebook, LinkedIn and Twitter, it handles important information for hackers and best of all that is free and can be used in a social engineering attack.
- Information retrieval (dumpuster diving), is a very useful method that allows to find keys in the pos-it that

users throw away, where the recycling paper contains information relevant to the company.

- You can find many tools to perform a deep recognition, but the most important is to make a footprinting with a command line and a browser.

In the following example, the search is performed on a Nmap Scanner page, a site managed by Fyodor where recognition and scanning tests can only be performed.

Figure 3. Simple Footprinting

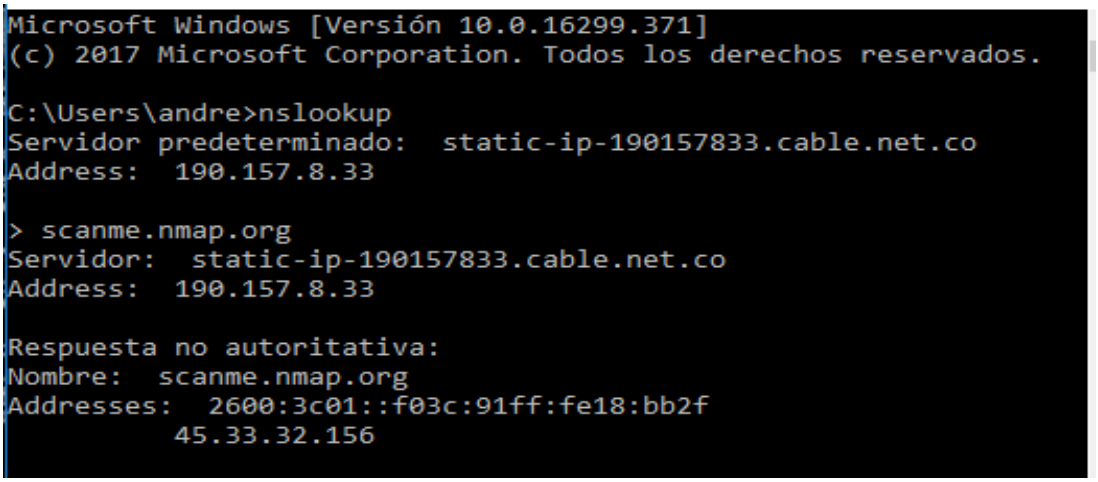

Figure 4. DNS resolution with NSLOOKUP in Windows.

As Seen in figure 3, the search yields almost eleven thousand results but the one that is needed is located first, to optimize the search you can use the google bookmarks (+, -, "", and many more). Knowing the main site of the victim, a DNS query is performed to identify the IP address. Pinging the victim's site verifies that he is active and knows his IP address.

Ping scanme.nmap.org

Haciendo ping a scanme.nmap.org [45.33.32.156] con 32 bytes de datos:

Estadísticas de ping para 45.33.32.156

Then the NSLOOKUP command is used, which allows to know if the DNS server is resolving the names in a correct way.

In the query made in Figure 4, it can be analyzed that the site has two IPV 6 and IPV 4 addresses, where the IPV 4 address is of class A since the first octet is 74 bits, so the range of the Host to analyze would be very large and would take a long time.

Set type = [NS | MX | ALL]

Permite establecer el tipo de consulta, NS servicio de

Nombres, MX servicio de correo (mail exchanger) y ALL para mostrar todo [22].

```
C:\Users\andre>nslookup
Servidor predeterminado:  static-ip-190157833.cable.net.co
Address:  190.157.8.33

> scanme.nmap.org
Servidor:  static-ip-190157833.cable.net.co
Address:  190.157.8.33

Respuesta no autoritativa:
Nombre:  scanme.nmap.org
Addresses:  2600:3c01::f03c:91ff:fe18:bb2f
          45.33.32.156

> set type=NS
> nmap.org
Servidor:  static-ip-190157833.cable.net.co
Address:  190.157.8.33

Respuesta no autoritativa:
nmap.org        nameserver = ns3.linode.com
nmap.org        nameserver = ns4.linode.com
nmap.org        nameserver = ns2.linode.com
nmap.org        nameserver = ns5.linode.com
nmap.org        nameserver = ns1.linode.com
> set type=MX
> nmap.org
Servidor:  static-ip-190157833.cable.net.co
Address:  190.157.8.33

Respuesta no autoritativa:
nmap.org        MX preference = 1, mail exchanger = ASPMX.L.GOOGLE.COM
nmap.org        MX preference = 10, mail exchanger = ASPMX3.GOOGLEMAIL.COM
nmap.org        MX preference = 5, mail exchanger = ALT2.ASPMX.L.GOOGLE.COM
nmap.org        MX preference = 10, mail exchanger = ASPMX2.GOOGLEMAIL.COM
nmap.org        MX preference = 5, mail exchanger = ALT1.ASPMX.L.GOOGLE.COM
>
```

Figure 5. Nslookup: Set type=NS and Set type=MX

```
> set type=ALL
> nmap.org
Servidor:  static-ip-190157833.cable.net.co
Address:  190.157.8.33

Respuesta no autoritativa:
nmap.org        AAAA IPv6 address = 2600:3c01::f03c:91ff:fe98:ff4e
nmap.org        text =

        "v=spf1 a mx ptr ip4:45.33.49.119 ip4:173.255.243.189 ip4:192.81.131.254 ip6:26
00:3c01::f03c:91ff:fe98:ff4e ip6:2600:3c01::f03c:91ff:fe70:d085 include:_spf.google.com
 ~all"
nmap.org        internet address = 45.33.49.119
nmap.org
        primary name server = ns1.linode.com
        responsible mail addr = hostmaster.insecure.org
        serial  = 2016070584
        refresh = 14400 (4 hours)
        retry   = 14400 (4 hours)
        expire  = 1209600 (14 days)
        default TTL = 3600 (1 hour)
nmap.org        nameserver = ns5.linode.com
nmap.org        nameserver = ns3.linode.com
nmap.org        nameserver = ns2.linode.com
nmap.org        nameserver = ns1.linode.com
nmap.org        nameserver = ns4.linode.com
nmap.org        MX preference = 10, mail exchanger = ASPMX3.GOOGLEMAIL.com
nmap.org        MX preference = 10, mail exchanger = ASPMX2.GOOGLEMAIL.com
nmap.org        MX preference = 5, mail exchanger = ALT1.ASPMX.L.GOOGLE.com
nmap.org        MX preference = 5, mail exchanger = ALT2.ASPMX.L.GOOGLE.com
nmap.org        MX preference = 1, mail exchanger = ASPMX.L.GOOGLE.com
>
```

Figure 6. Nslookup set type=All

In Figure 5, the information in the NS query can be analyzed with respect to the name servers for the domain in which the target is hosted and in the MX query information is observed about who the mail servers are for that domain.

The option ALL obtains combined information from the two previous consultations where you can see important information such as: nmap.org is hosted in an external hosting provided by Linode and the mail service is with the server mail.titan.net which is in a network segment other than the scanme.nmap.org server. Also, the Who is tool can help corroborate and expand contact information.

Information related to 'xx.xxx.xxx.x - xx.xxx.xxx.xxx'

netname: H0STING

descr: Main Hosting Servers

remarks: Abuse contact: *****Qmain-hosting.com

country: US

person: MAIN HOSTING HOSTMASTER

address: 100 Technology Drive

address: Asheville, NC

Phone: +38068545152

With this query you can see the names of contacts, phones and emails, a positive point for the hacker giving him the possibility of social engineering, so it is worrisome that this information is disclosed in a public database.

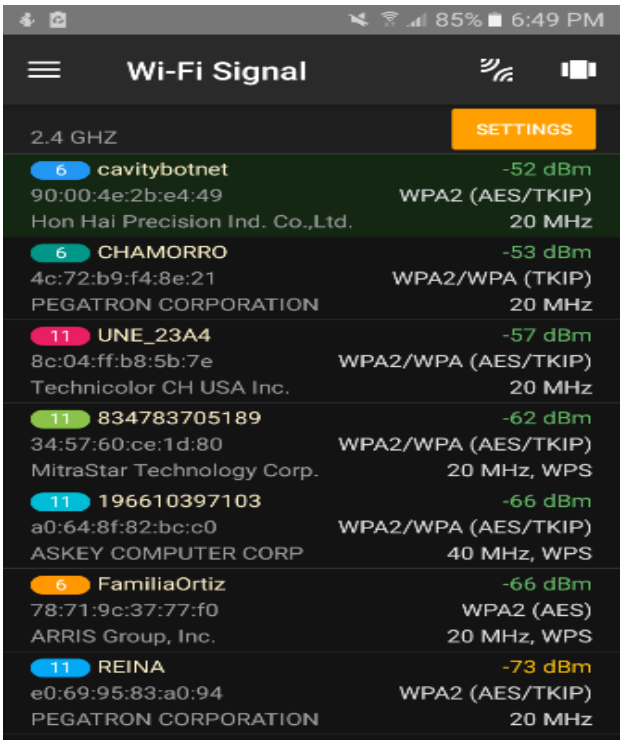

Figure 7. Scanner Inalámbrico Network Analyzer

3.2 Scanning

To start this stage it is important that the attacker enters the network, to enter the network freely, you will need the help of a tool such as a wireless network analyzer, scan the networks nearby, you can measure the power, the encryption of each network and the MAC of the router.

In Figure 7, the different networks are shown with the Network Analyzer; the main objective is to break the key and for this there are many ways, such as using programs such as HHG5XX WEP, Wifislax, where from these applications a search is made and the network to be entered is chosen, these programs begin to Run your algorithm to get the entry key, on the other hand, Wifislax is very good at finding these keys. Other programs could be Aircrack, Airmon and AirPlay, in case the network is configured in a very secure way.

The scanning procedure consists of the following stages:

- System status: After making the fingerprint review, several devices are found, now we must determine which host are alive in the network. A ping is made to all the machines that are in the network. You can perform an ICMP ping or a TCP ping. A carelessness in this phase can cause the hacker to be discovered by the technology staff and result in an ACL list blocking the IP causing delays and ruining the surprise factor [23].

  With the fping tool a scan is performed and a mobile device is found with the IP 192.168.1.101, this is active and is the only connected host for the moment.

  $ Fping -g 192.168.1.0/24
  192.168.1.101 is alive

  You can also use other simple tools such as ping-sweepers. The ping sweepers define a range of IP's

using the ICMP protocol sending echo requests and the host that responds to the request are marked as active.

If the ping lock is definitely found, a port scanner or a TCP-Ping tool can be used [24].

- Port review:

The Nmap tool is executed to scan active ports where you can see that of the 1000 ports that were tested only port 2222 is running.

nmap -T4 -A -v -Pn 192.168.1.101
Scanning 192.168.1.101 [1000 ports]
Discovered open port 2222/tcp on 192.168.1.101

- Identification of services:

In the annexed table of Zenmap, the device is searched and it is seen that port 2222 discovered is assigned to the SSH service [24].

PORT STATE SERVICE VERSIÓN

2222/tcp open ssh Dropbear sshd 0.52 (protocol 2.0)

TCP Sequence Prediction: Difficulty=198 (Good luck!)

The identification of Bluetooth services is done through the Blue Diving program that works on the Linux platform and at the moment of executing it it shows the active bluetooth services in the device [25].

From the menu of the tool, option 3 Scan and Info is selected, where it displays the list with the devices it finds, this option is selected and it begins to do the recognition.

Start scanning for Bluetooth devices...

Found host LG-P500h

addr 74:A7:22:B4:EC:A3 class 0x5a020c unkown

Service Ñame: Headset Gateway Ch: 1

Service Ñame: Handsfree Gateway Ch: 2

Service Ñame: Object Push Ch: 3

Service Ñame: BRCM Advanced Audio

Service Ñame: OBEX File Transíer Ch: 4

Information ...

BD Address: 74:A7:22:B4:EC:A3

Device Ñame: LG-P500h

LMP Versión: 2.1 (0x4) LMP Subversión: 0x8107

Manufacturer: Broadcom Corporation (15)

Features pagé0:0xbf Oxfe 0x8f Oxfe 0x9b Oxff 0x79 0x83

- Traces of the operating system:

The Nmap tool is run again to find out which operating system the device has and throws the following information.

nmap -0 192.168.1.101
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.31
OS detection performed.

- Vulnerability scan:

Vulnerability scanning can be performed with the Nessus tool pointing to the IP address of the Smartphone, the report shows a list with a high vulnerability and eight casualties.

Table 4. Report vulnerabilities found in the mobile.

No.	Importance	Vulnerability
1	High	Nessus Scan Information
2	Low	Multiple Ethernet Driver Frame appending Information Discloksure (Etherleask)
3	Low	ICMP Timestamp Request Remote Date Disclosure.
4	Low	TCP/IP Timestamps Supported
5	Low	OS Identification
6	Low	Common Platform Enumeration (CPE)
7	Low	Traceroute Information
8	Low	Port SSH (222/TCP) – Service Detection
9	Low	SSH Server Type and Version Information

.

3.3 Enumeration

3.3.1 Null Sessions

The enumeration is a scanning subphase and is based on collecting the greatest amount of information from the victim, taking advantage of a weakness in one or more of the protocols or services that are active [26].

Sessions are reviewed running Net Use, but it generates an error where the domain controller does not respond with the following message.

C:\>net use \\192.168.1.10l\IPC$ ">""> /u:">"">

System error 67 has occurred.

The network name cannot be found.

3.3.2 List resources

In this test you can also find errors such as:

C:\>neí view \\192.168.1.101

System error 53 has occurred. The network path was not found.

Como el mensaje no se difundio por que Windows no proceso correctamente la instrucción que se envía y no la difunde en los equipos de trabajo.

Se realiza un Nbstat y no responde por que el sistema operativo Android no enumera la tabla del NetBIOS:

C:\>nbtstat -A 192.168.1.101

Wireless Network Connection: Node IPaddress: [192.168.1.102] Scope Id:

[] Host not found.

3.3.3 Enumeration SNMP

To perform the enumeration SNMP is executed from SNMPCheck, which makes a tour and shows the resources of the system, the connection does it correctly and generates an error because it does not find a response from the remote host [26].

root@bt:# ./snmpcheck-1.8.pl -t 192.168.1.101

O) Try to connect to 192.168.1.101

(*) Connected to 192.168.1.101

(*) Starting enumeration at 2011-11-27 01:58:00

(*) Error: No response from remote host '192.168.1.101'.

3.4 Access

3.4.1 Rupture of passwords

A scan is made on the network with the Wireshark sniffer from where the login password to the social network Facebook is obtained when analyzing the contents of the package.

Using the medusa tool on the victim device pointing to the SSH and a key dictionary it was possible to obtain a valid user to perform the session with the phone.

root@bt: medusa -h 192.168.1.101 -u root -P passwords.txt -M ssh -n 2222

ACCOUNT CHECK: [ssh] Host: 192.168.1.101 (1 of 1, 0 complete)

User: administrator (1 of 1, 0 complete) Password: admin (1 of 5 complete

ACCOUNT F0UND: [ssh] Host: 192.168.1.101

User: root Password: admin [SUCCESS]

3.4.2 Session hijacking

Once the connection information to the device is known, the putty tool is executed, which allows remote connection through the port that is open.

Putty is opened and the IP address of the telephone 192.168.1.101 is placed, it is configured to open SSH session on port 2222, user XXXXX and password XXXX previously obtained in jellyfish are placed and with this information the hacker is already inside The phone shell ready to steal information.

3.4.3 Clear evidence

The evidence can be deleted from the phone's log in a very easy way with the command of Linux RM and thus not leave any trace.

4 CONCLUSIONS

Ethical hacking is a tool for data protection and prevention. Due to the proliferation of mobile devices, tablets and smartphones and the large number of applications, the phenomenon of computer insecurity has increased considerably and therefore these are highly vulnerable, because of the above, what is intended with this article is to be constantly ahead of those who try to attack us by doing their own tests and attacks with the help of computer experts.

A new device is not that it is so remotely vulnerable, if the user makes an adequate handling of the phone without connecting to insecure networks, much less entering passwords on sites that do not handle encryption security that make the device an attack target for the attacker can steal information, however the beginning of the attacks is due to the bad manipulation of the user, nor does it serve to have port blocking by default or the deletion of permissions to install unknown applications if the user gives permissions without reading or having knowledge of what is which is installing making the phone's security vulnerable.

For this reason an ethical hacker makes 'pentests' or penetration tests, these tests are composed of a set of methodologies and techniques. These methodologies and techniques reproduce access attempts from different points of entry of a computer

environment, the primary objective is to find vulnerabilities in order to circumvent the security of the system by escalating privileges, finding errors and bad configurations, for which it uses both his knowledge in computer science as a wide range of tools, and in this way, pass a report so that measures are taken and thus reduce the risk in an organization.

REFERENCES

[1] Alvarez del Vayo Fernando, "Cómo ha cambiado la venta de smartphones en los últimos años," 2017.

[2] W. Steven and T. Jaramillo, "Identificación De Los Ataques Más Realizados En Un Sitio Concurrido Por Personas Que Utilizan Sus Dispositivos Móviles Y Determinación De Las Vulnerabilidades Más Comunes En El Sistema Operativo Android.," 2016.

[3] F. Edition, *Security in Computing*, FIFTH EDIT. .

[4] D. Y. Londoño Arenas and J. F. Hurtado Rivera, "Esquema de seguridad para protección de dispositivos móviles con el sistema operativo android," 2014.

[5] "Security of Smart Phones," no. June, 2006.

[6] "Seguridad de Dispositivos Móviles Ataque, Defensa y Prevención."

[7] A. B. Alonso, I. F. Artime, M. Á. Rodríguez, R. G. Baniello, and E. P. S. I. G. I. De Telecomunicación, "Dispositivos móviles."

[8] Riza Luiza, "Smartphones: Hardware," *Smartphones: Hardware*, 2011. [Online]. Available: http://ezinearticles.com/?Smartphones:-Hardware&id=5843735. [Accessed: 27-Apr-2018].

[9] Real Academia Española, "DLE: hacker - Diccionario de la lengua española - Edición del Tricentenario," *23 edición*, 2014. [Online]. Available: http://dle.rae.es/?id=JxlUKkm. [Accessed: 29-Apr-2018].

[10] J. D. Demott, A. Sotirov, and J. Long, *Gray Hat Hacking , Third Edition Reviews*. 2011.

[11] S. E. Pacheco Veliz and C. D. Piazza Orlando, "Estudio y análisis de seguridad en dispositivos móviles. BYOD y su impacto en las organizaciones," p. 139, 2016.

[12] "High-Speed Mobile Networks.pdf." .

[13] Craig Heath, *Symbian OS Platform Security: Software Development Using the Symbian OS Security Architecture*. 2006.

[14] L. Rondeau and D. Hopkins, "Mobile Device Vulnerabilities & Securities," *Mob. Device Vulnerabilities Secur.*, pp. 30–35, 2014.

[15] GSMA, "GSM - About Us." [Online]. Available: https://www.gsma.com/aboutus/gsm-technology/gsm. [Accessed: 27-Apr-2018].

[16] 802.11p, *IEEE Standard for information technology -- Amendment 6: wireless access in vehicular environments*. 2010.

[17] D. Shih, B. Lin, H. Chiang, and M. Shih, "Security aspects of mobile phone virus: a critical survey," *Industrial Management & Data Systems*, vol. 108, no. 4. pp. 478–494, 2008.

[18] H. Rifa, J. Ruiz, and J. Rivas, *Análisis forense de sistemas informáticos*. 2013.

[19] "White paper on Mobile OS and efforts towards open standards By Dotcom Infoway White paper on Mobile OS and efforts towards open standards," *Main*.

[20] S. Standing and C. Standing, "Mobile technology and healthcare: the adoption issues and systemic problems.," *Int. J. Electron. Healthc.*, vol. 4, no. 3–4, pp. 221–235, 2008.

[21] J. A. Morales, P. J. Clarke, Y. Deng, and B. M. Golam Kibria, "Testing and evaluating virus detectors for handheld devices," *J. Comput. Virol.*, vol. 2, no. 2, pp. 135–147, 2006.

[22] K. Astudillo B., "Hacking Ético 101," *CCNA Secur.*, vol. 1, pp. 1–292, 2008.

[23] C. Tori, "Hacking Etico," vol. 1, p. 334, 2008.

[24] V. R. G. Ávila, "Diseño e implementación de un sistema de monitoreo basado en SNMP para la Red Nacional Académica de Tecnología Avanzada.," p. 86, 2014.

[25] P. Arnedo, Blanco, "Herramientas de análisis forense y su aplicabilidad en la investigación de delitos informáticos," *Univ. Int. la Rioja*, pp. 1–91, 2014.

[26] "Ataques MITM," 2012.

[27] Comisión de Regulación de Comunicaciones CRC, "Identificación de las posibles acciones regulatorias a implementar en materia de Ciberseguridad Documento de análisis y consulta," pp. 1–65, 2015.