THE INCIDENCE OF VULNERABILITIES OF THE LAN NETWORKS IN THE INFORMATION SECURITY OF THE ADMINISTRATIVE AREA OF A GOVERNMENTAL ENTITY IN NORTHWESTERN ECUADOR

Diego Andaluz[1], Francisco Javier Aguilar [1,2], Walter Fuertes[1], Theofilos Toulkeridis[1]

[1]Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador
[2]Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Universidad Técnica de Ambato, Ambato, Ecuador

Resumen

El creciente uso de la tecnología ha provocado que la gran mayoría de la información se encuentre digitalizada, razón por lo cual hoy por hoy las organizaciones transmiten a través de las redes de datos grandes volúmenes de información. La gran mayoría de las empresas no protegen adecuadamente la información que producen, muchas de las veces invierten en seguridad física, video vigilancia, para proteger sus activos y bienes, pero se olvidan de invertir en seguridad informática para brindar protección a su principal activo que es la información, y ésta es mucha de las veces sustraída fácilmente a través de la red o en medios digitales.

La presente investigación fue llevada a cabo en el Gad Provincial de Orellana, y tuvo como finalidad evaluar las vulnerabilidades de la red de datos del Área Administrativa, haciendo uso de la metodología de ethical hacking CEH (Certified Ethical Hacker) que, a través de sus fases de reconocimiento, escaneo, obtener acceso, mantener acceso y cubrir huellas, permitió evidenciar las debilidades que tenía la red de datos y generar políticas de seguridad que permitan salvaguardar la integridad y confidencialidad de la información.

Palabras clave: Vulnerabilidad, información, red, ethical hacking.

Abstract

The growing use of technology has caused the vast majority of information to be digitized, which is why organizations today transmit large volumes of information through data networks. However, the vast majority of companies do not adequately protect the information they generate, as they invest mostly in physical security and video surveillance in order to protect their assets and properties. Such lack of investment of computer security and failure to provide protection to their main asset being information, leads often to external induced robbery through the network or within digital media.

The current research has been performed in the Decentralized Autonomous Government (DAG) of the Province of Orellana in Northeastern Ecuador, having the purpose to evaluate the vulnerabilities of the data network of the administrative area, making use of ethical hacking methodology named Certified Ethical Hacker (CEH). Such methodology allows through its recognition, scanning, accessing, maintaining access, and tracing fingerprints, to highlight the shortcomings of the data network and generate security policies that safeguard the integrity and confidentiality of information.

Key words: Vulnerability, information, network, ethical hacking.

INTRODUCTION

The increasingly dominant trend towards the interconnectivity and interoperability of networks, computing machines, applications, and even enterprises has placed the security of information systems as a central element in the entire development of the society (Calvopiña and Pilatuña, 2016). Security has gone from being used to preserve classified government data on military or diplomatic matters, to having an application of unimaginable and increasing dimensions that includes financial transactions, contractual agreements, personal information, medical files, internet commerce and business, home automation, environmental intelligence and ubiquitous computing (Calvopiña and Pilatuña, 2016). Therefore, it is imperative that the potential security needs are taken into account and determined for all types of applications (Calvopiña and Pilatuña, 2016).

Within a system or organization, vulnerabilities may exist that do not have any associated hazard that may exploit or abuse them (Areito Bertolin, 2008). Immediate attention should be given to all those in which there is a hazard, that may take advantage of them (Areito Bertolin, 2008). However, as the environment is changing dynamically, all vulnerabilities should be controlled to identify those that may allow the materialization of new hazards, in addition to those already existing (Areito Bertolin, 2008).

Therefore, the current research consists of a vulnerability analysis carried out on the data network of the Administrative Area of the DAG of the Province of Orellana in Northeast Ecuador, with the purpose of determining its incidence in the security of information.

The used methodology has been of the CEH, where in the recognition phase all possible information about the preselected objective has been collected. Afterwards, in the exploration and recognition phase, which is based on the collected information, we established a method of attacking the data network, while in the scanning phase we obtained the different services available in the target data network. With the collected information in the phases mentioned above, we proceeded to identify the vulnerable systems of the network, whereas in the phase of maintaining access to attack these systems, taking control of them, and then provide recommendations, which may allow correcting the encountered vulnerabilities, safeguarding the integrity and confidentiality of all information.

THEORETICAL FRAMEWORK

II.1. LAN networks

LAN networks are those that connect a network of normally confined computers in a geographic area, such as a single building or a campus. LANs, however, are not necessarily simple to plan because they are able to link many hundreds of computers and may be used by thousands of users (Joskowicz, 2007). The development of several rules of network protocols and physical media, together with the low price of computers have made the proliferation possible of LANs in all types of organizations (Joskowicz, 2007). LANs generally use broadcast transmission, at speeds of 10, 100 or 1000 Mb / s. The most commonly used topologies are bus (IEEE 802.3 Ethernet) or ring (IEEE 802.5 Token Ring) (Joskowicz, 2007).

II.2. Methodology for the Detection of Vulnerabilities in Data Networks

The methodology for the detection of vulnerabilities in data networks proposed in this study, consists of three phases supported by software tools, which seeks to obtain vulnerabilities in network equipment (both wired and wireless) and servers in the studied data networks (Franco et al., 2012). This methodology differs from others insofar as each stage is supported in software tools (Franco et al., 2012). Therefore, in each phase, the actions to be carried out and how they should be carried out through the appropriate tools have been outlined. The outline of the methodology for vulnerability detection in data networks is presented in figure 1. As illustrated, the proposed methodology consists of three phases, which are detailed below (Franco et al., 2012):

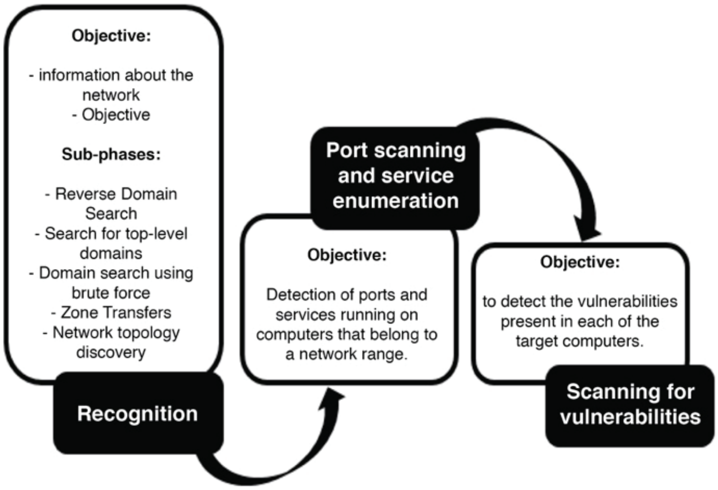

Objective:
- information about the network
- Objective
Sub-phases:
- Reverse Domain Search
- Search for top-level domains
- Domain search using brute force
- Zone Transfers
- Network topology discovery
Recognition
Port scanning and service enumeration
Objective:
Detection of ports and services running on computers that belong to a network range.
Objective:
to detect the vulnerabilities present in each of the target computers.
Scanning for vulnerabilities

Fig. 1. Vulnerability detection scheme

II.3. Social engineering

Although this technique may be used in any field, as far as computer science is concerned, it consists of obtaining sensitive and / or confidential information from a user close to a system or organization exploiting certain characteristics that are specific to the human being (Mieres, 2009). Undoubtedly, people are one of the most important security problems for any organization because unlike the technological components, they are the only element, within a secure environment, with the ability to decide to break the rules established in the policies of any information security (Mieres, 2009). Either by ignorance, negligence or coercion, they may allow an attacker to gain unauthorized access, which in this way will be able to bypass the complex security schemes and technologies that have been implemented in the organization (Mieres, 2009).

II.4. Certified Ethical Hacker (CEH)

The CEH is a certification awarded by the International Council for Electronic Commerce Consultation (EC-COUNCIL, 2013) and is aimed at systems professionals, technology consultants, systems auditors, administrators and IT security managers to encounter weaknesses and vulnerabilities in systems using the same knowledge and tools as a malicious hacker (Calvopiña and Pilatuña, 2015).

II.4. Information security

Information security is not a functional property of an information system, but rather an emergent property. Throughout the years, the perception of information security has been changing until recent times (Lara and Pacheco, 2012). It merged linked to military, diplomatic and governmental environments (Lara and Pacheco, 2012). At the business level, it started being a luxury, something that has been fine but that has not been necessary. Then it became fashionable, and even a useful and desirable recommendation, perceived as a necessary expense to be able to carry out business (Lara and Pacheco, 2012). Subsequently, it has been considered as an obligation for companies not to be legally unprotected against laws such as Law on Intellectual and Industrial Property (RMS-LOPD, LSSI-CE, LPII), Sarbanes Oaxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Basel II, Markets in Financial Instruments Directive (MiFID), among others. (Lara and Pacheco, 2012). At present, information security has become an integral element of an organization's ability to be competitive [7]. It is, therefore, a strategic asset that may not be separated from the core of any business or organization, perceiving itself as one of the best investments for the future of the company (Lara and Pacheco, 2012).

II.5. Types of Attack

As expected, not all attacks are of the same nature. In fact, in this case we will only refer to a classification from the technical point of view.

II.5.1. Attacks on the Operating System

Attacks on the operating system have been a classic point of security. From this perspective, troubleshooting will be done with respect to the base system of all other software in such a way that, many times, regardless of what has been above, it will be possible to exploit and take control of the system in case that it remains vulnerable (Lara and Pacheco, 2012).

II.5.2. Attacks on applications

In this case, the variety is greater. There are many thousands of pieces of software and programs of all types and sizes available in the world (Lara and Pacheco, 2012). Of course, among so many millions of lines of code, errors will necessarily occur. For application attacks, mass usage will also be taken into account. This implies that a program managed by millions of people to read PDF files will be better targeted than one employed by a few to edit certain types of specific files in a format, which may be less known to users (Lara and Pacheco, 2012).

II.5.3. Errors in configurations

The case of configurations, whether of the operating system or of the applications, is also a sensitive point, since, however secure a software may be, a bad configuration may convert it to be as malleable as a paper. While over time companies have increasingly incorporated security measures into their factory configurations, an attacker, as a first step, will try to take advantage of standard configurations, whether applications, computer equipment, network devices, besides others (Lara and Pacheco, 2012).

II.5.3. Errors in Protocols

Another, less frequent but more serious problem, is that the errors are directly in the protocols [8]. This implies that, regardless of the implementation, the operating system, or the configuration, something that is composed of such a protocol could be affected. The classic example is the Transmission Control Protocol / Internet Protocol (TCP / IP), which is a suite of protocols being that effective and flexible, that even after more than three decades of its creation, still exists and continues in use. The problem here is that, at the time of the early 1970s, its design did not obey security aspects for certain reasons specific to its purpose of use (Lara and Pacheco, 2012).

Over time, its use has been extended to such a point that it began to be implemented in ways that the scheme itself allowed, but for purposes that had not been thought at first, becoming a double-edged sword. In spite of this, TCP / IP has never been in doubt, since all the failures have been corrected or their effects have been mitigated from the improvements made by the implementations (Lara and Pacheco, 2012).

III. CONTENT

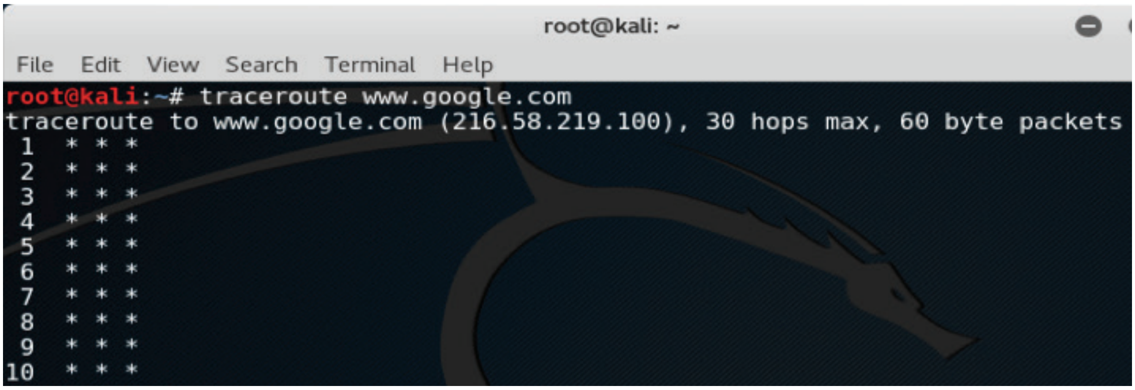
The present study has been carried out in the DAG of the Province of Orellana, where the vulnerabilities of the data network of the administrative area have been evaluated, applying the CEH methodology. Using software tools in each of the phases may determine the vulnerabilities in the network. The following table lists the used software tools in each of the phases of the CEH methodology.

Table 1. Software tools used

HERRAMIENTA	FASE
PING, TRACE ROUTE	RECOGNITION
ANGRY IP SCANNER	SCANNING
NMAP	SCANNING
ZENMAP, NESSUS	SCANNING
SOFT PERFECT NETWORK SCANNER	SCANNING
ETTERCAP	GET ACCESS
SOFT PERFECT NETWORK SCANNER	MAINTAIN ACCESS

III.1. Recognition Phase

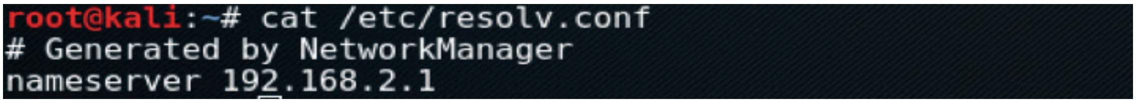
The current state of the data network has been observed, where structured cabling does not meet all ANSI / TIA / EIA-568-B standards, wiring is not properly labeled and cables are not placed in gutters. The datacenter has a virtualized server system, with a UPS that provides a 30-minute power backup to all datacenter servers and equipment, but where physical access to the equipment has not been properly secured. Then the domain gporellana.gob.ec has been pinged to know the ip address of the domain. In order to know the path that the data packets follow from a company host to the internet, we executed the traceroute command (Fig. 2).



```
root@kali:~# traceroute www.google.com
traceroute to www.google.com (216.58.219.100), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
```

Fig. 2. Execution of traceroute command

In addition, we proceeded to determine the ip address of the DNS server and the server that provides Internet access to the computers (Fig. 3).

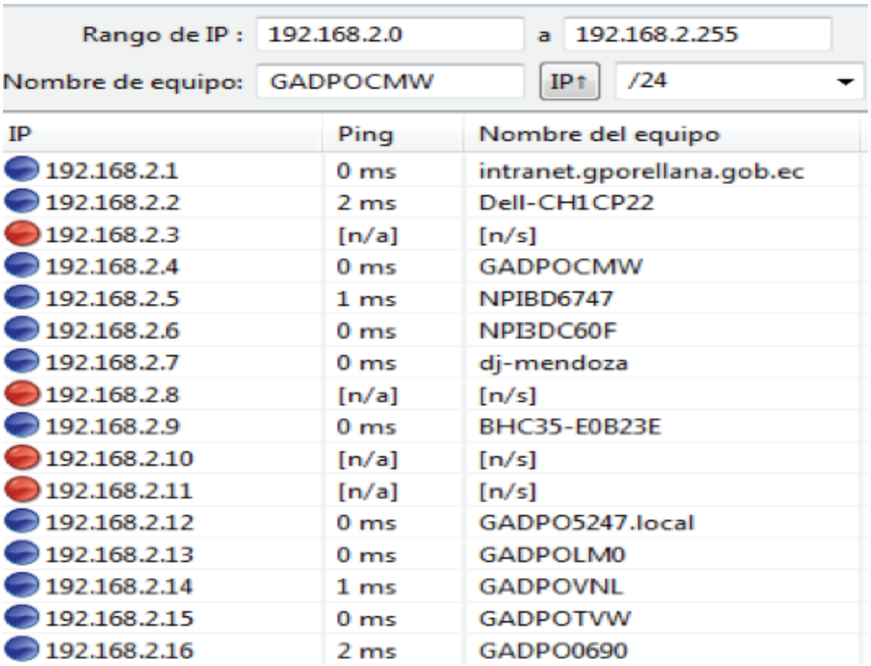


```
root@kali:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.2.1
```

Fig. 3. Determining DNS Server.

III.2. Exploration Phase

After the reconnaissance of the target network of the attack, we proceeded to perform the exploration of services, active hosts, open ports and shared resources. The Angry IP Scanner tool has been executed, with which the list of active hosts in the network has been obtained (Fig. 4).



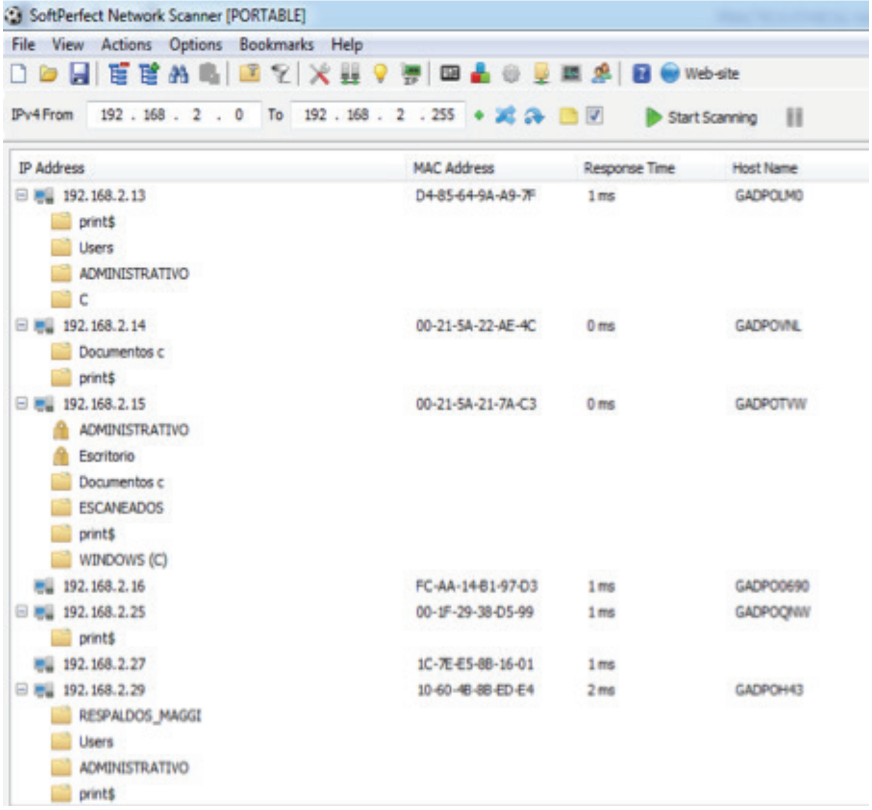
Rango de IP : 192.168.2.0 a 192.168.2.255

Nombre de equipo: GADPOCMW IP↑ /24

IP	Ping	Nombre del equipo
🔵 192.168.2.1	0 ms	intranet.gporellana.gob.ec
🔵 192.168.2.2	2 ms	Dell-CH1CP22
🔴 192.168.2.3	[n/a]	[n/s]
🔵 192.168.2.4	0 ms	GADPOCMW
🔵 192.168.2.5	1 ms	NPIBD6747
🔵 192.168.2.6	0 ms	NPI3DC60F
🔵 192.168.2.7	0 ms	dj-mendoza
🔴 192.168.2.8	[n/a]	[n/s]
🔵 192.168.2.9	0 ms	BHC35-E0B23E
🔴 192.168.2.10	[n/a]	[n/s]
🔴 192.168.2.11	[n/a]	[n/s]
🔵 192.168.2.12	0 ms	GADPO5247.local
🔵 192.168.2.13	0 ms	GADPOLM0
🔵 192.168.2.14	1 ms	GADPOVNL
🔵 192.168.2.15	0 ms	GADPOTVW
🔵 192.168.2.16	2 ms	GADPO0690

Fig. 4. List of active computers in the network.

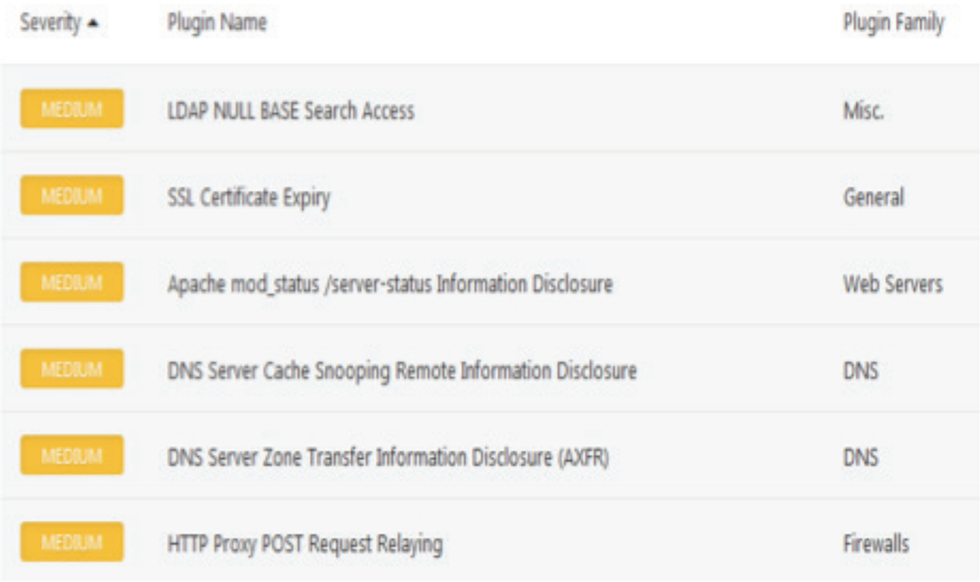
With the SoftPerfect Network Scanner tool, we proceeded to determine the shared resources in the network (Fig. 5). Then, we explored the vulnerabilities of the internet server with the use of the NESSUS tool (Fig. 6). The NetBIOS table has been obtained by entering port 139, where we obtained the ip addresses, hostnames and mac addresses of each active computer (Fig. 7).



IPv4 From 192 . 168 . 2 . 0 To 192 . 168 . 2 . 255

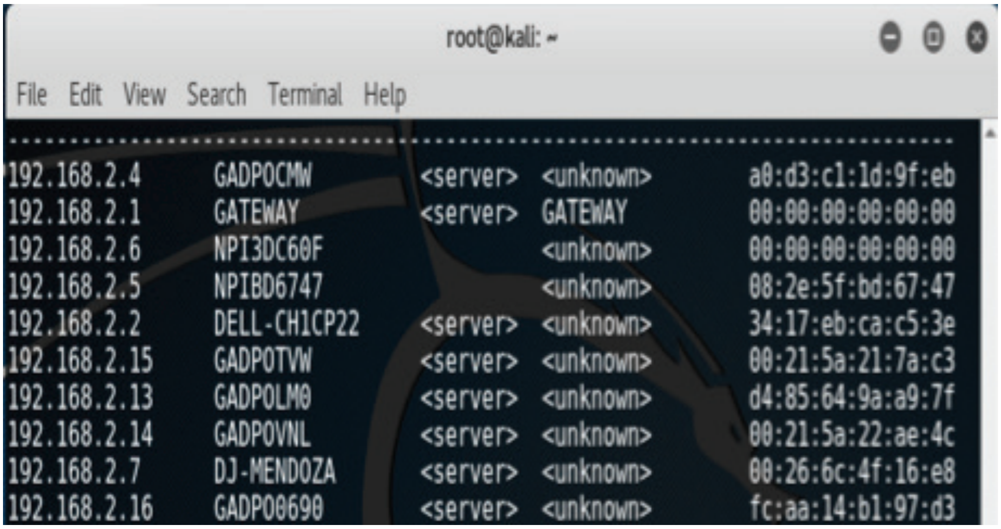
IP Address	MAC Address	Response Time	Host Name
192.168.2.13	D4-85-64-9A-A9-7F	1 ms	GADPOLM0
print$			
Users			
ADMINISTRATIVO			
C			
192.168.2.14	00-21-5A-22-AE-4C	0 ms	GADPOVNL
Documentos c			
print$			
192.168.2.15	00-21-5A-21-7A-C3	0 ms	GADPOTVW
ADMINISTRATIVO			
Escritorio			
Documentos c			
ESCANEADOS			
print$			
WINDOWS (C)			
192.168.2.16	FC-AA-14-B1-97-D3	1 ms	GADPO0690
192.168.2.25	00-1F-29-38-D5-99	1 ms	GADPOQNW
print$			
192.168.2.27	1C-7E-E5-8B-16-01	1 ms	
192.168.2.29	10-60-4B-8B-ED-E4	2 ms	GADPOH43
RESPALDOS_MAGGI			
Users			
ADMINISTRATIVO			
print$			

Fig. 5. List of shared resources on the network



Severity ▲	Plugin Name	Plugin Family
MEDIUM	LDAP NULL BASE Search Access	Misc.
MEDIUM	SSL Certificate Expiry	General
MEDIUM	Apache mod_status /server-status Information Disclosure	Web Servers
MEDIUM	DNS Server Cache Snooping Remote Information Disclosure	DNS
MEDIUM	DNS Server Zone Transfer Information Disclosure (AXFR)	DNS
MEDIUM	HTTP Proxy POST Request Relaying	Firewalls

Fig. 6. Vulnerabilities found on the server.



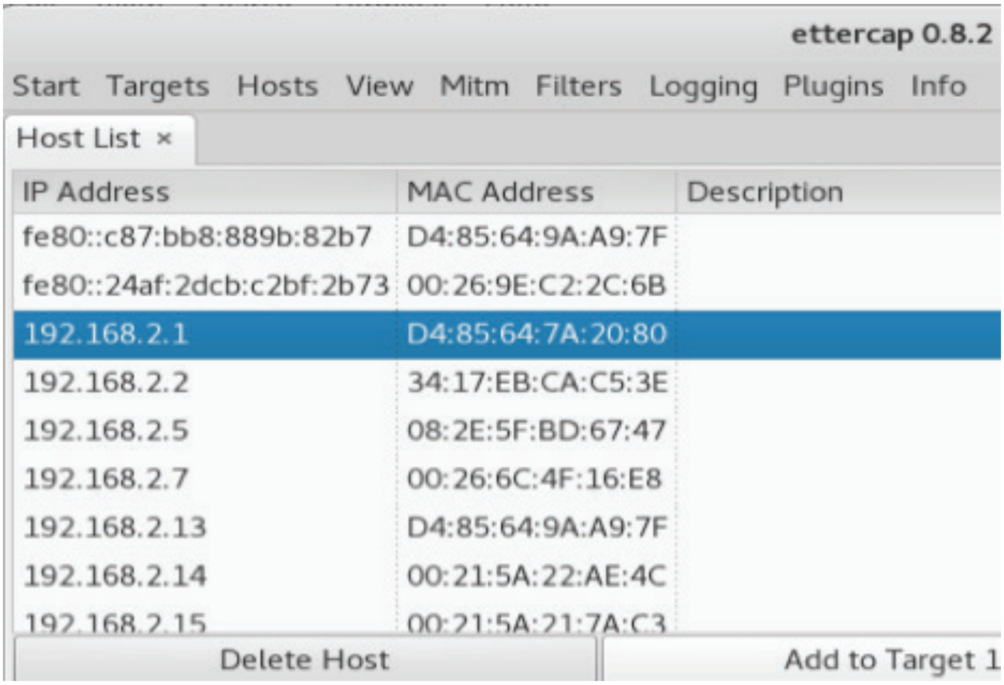
```
---------------------------------------------------------------------------
192.168.2.4     GADPOCMW      <server>  <unknown>      a0:d3:c1:1d:9f:eb
192.168.2.1     GATEWAY       <server>  GATEWAY        00:00:00:00:00:00
192.168.2.6     NPI3DC60F               <unknown>      00:00:00:00:00:00
192.168.2.5     NPIBD6747               <unknown>      08:2e:5f:bd:67:47
192.168.2.2     DELL-CH1CP22  <server>  <unknown>      34:17:eb:ca:c5:3e
192.168.2.15    GADPOTVW      <server>  <unknown>      00:21:5a:21:7a:c3
192.168.2.13    GADPOLM0      <server>  <unknown>      d4:85:64:9a:a9:7f
192.168.2.14    GADPOVNL      <server>  <unknown>      00:21:5a:22:ae:4c
192.168.2.7     DJ-MENDOZA    <server>  <unknown>      00:26:6c:4f:16:e8
192.168.2.16    GADP00690     <server>  <unknown>      fc:aa:14:b1:97:d3
```

Fig. 7. Table of NetBIOS

III.3. Access phase

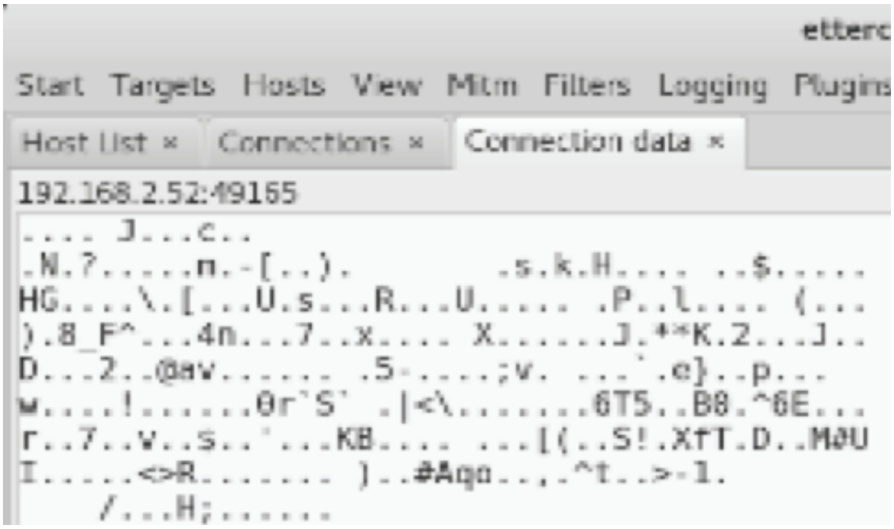
By using the Ettercap tool, one performed the attack of the man in the middle, in order to be able to capture mail passwords and user accounts. The attack has been completed by intercepting the communications between a target host and the gateway or Internet server of the network. We obtained the list of active computers in the network, in order to choose the two computers that will be object of the interception of transmission of messages.

In the interception, it has been possible to capture encrypted information from the Open Fire instant messaging service.



IP Address	MAC Address	Description
fe80::c87:bb8:889b:82b7	D4:85:64:9A:A9:7F	
fe80::24af:2dcb:c2bf:2b73	00:26:9E:C2:2C:6B	
192.168.2.1	D4:85:64:7A:20:80	
192.168.2.2	34:17:EB:CA:C5:3E	
192.168.2.5	08:2E:5F:BD:67:47	
192.168.2.7	00:26:6C:4F:16:E8	
192.168.2.13	D4:85:64:9A:A9:7F	
192.168.2.14	00:21:5A:22:AE:4C	
192.168.2.15	00:21:5A:21:7A:C3	

Fig. 8. List of available equipments to be attacked.



```
192.168.2.52:49165
.... J...c..
.N.?......n.-[..).          .s.k.H.... ..$.....
HG....\.[...U.s...R...U..... .P..l.... (...
).8_F^...4n...7..x.... X.......J.*ᵏK.2...J..
D...2..@av....... .5·....;v.  ...`.e}..p...
w....!.......0r`S`  .|<\.........6T5..B8.^6E...
r..7..v..s..`...KB.... ...[(..S!.X†T.D..M@U
I......<>R........ )..#Aqo...,.^t..>-1.
    /...H;......
```

Fig. 9. Encrypted message

III.4. Phase of maintaining access

With the collected information in the scanning phase, it has been possible to access shared information that users had without any security, and even some computers with Windows operating system had shared the C drive, so they are vulnerable to serious damage in the system.

III.5. Phase of covering tracks

When accessing resources of a network, in order not to leave traces behind, records should be erased of the made accesses. In the case of the current study it has not been possible to violate the internet server, so we did not need to carry out this phase.

RESULTS EVALUATION

Having applied the different phases of the CEH methodology, within reconnaissance phase the network did not comply with all structured cabling standards, while the access to the data center has not been adequately assured, so that anyone may enter and cause damage to equipment and lose vital information of the entire organization.

The application of the ping command to the domain gporellana.gob.ec, did not respond so it did not allow to access more information like name servers. However, when querying the file resolv.conf, it has been possible to obtain the name server used in the local network. En la fase exploración se pudo conocer los equipos activos en la red, así como también a quien pertenecen los equipos.

In the exploration phase, it has been possible to know the active teams in the network, as well as to whom the teams belong. We determined that a proper nomenclature had not been established to give a name to the equipment and names are placed that provide information of the owner of the equipment, facilitating to anyone the attack or subtraction of information. We encountered shared resources, with sensitive information, the same ones that have no access restrictions, being vulnerable to being subtracted, and even completely erased.

When attempting to intercept instant messaging conversations, it has been evidenced that these travels encrypted through the network, so they have not been an easy target, to be violated or altered. In addition, at the time of port scanning the network administrator has been able to detect and block the attack.

CONCLUSIONS

Physical access to the data center were not properly insured, so anyone has been able to enter, manipulate the equipment, and cause great loss of information, as well as financially damaging to the organization.

The organization does not have established security policies, which provide protection to the stored information, for which it is highly susceptible of being erased, altered or stolen.

The data server provides protection to the communications of email, messaging, telephony, because, when traveling encrypted, it is difficult to interpret them.

The application of the CEH methodology enabled to identify the vulnerabilities in the data network of the Provincial Government of Orellana and to make IT staff aware of the risk they represent for the most important asset of the organization, such as their entire information and data sets.

REFERENCES

Areitio Bertolin, J. (2008). Identificación de vulnerabilidades. En *Seguridad de la Información*. Madrid: Paraninfo.

Franco, D. A., Perea, J. L., & Puello, P. (2012). *Metodología para la Detección de Vulnerabilidades en Redes de Datos.* http://www.scielo.cl: http://dx.doi.org/10.4067/S0718-07642012000300014

Joskowicz, J. (2007). Redes LAN. http://s3.amazonaws.com/academia.edu.documents/38627860/Redes_de_Datos_2007.pdf

Lara, H., & Pacheco, F. (2012). Tipos de Ataque. En *Ethical Hacking 2.0* (págs. 47-53). Buenos Aires: Fox Andina.

Mieres, J. (2009). Ingeniería Social. En *Ataques Informáticos debilidades de seguridad comunmente explotadas* https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf

Onofa Calvopiña, F. O., & Pilatuña Chica, I. , (2016). *Análisis y evaluación de riesgos y vulnerabilidades del nuevo portal web de la Escuela Politécnica Nacional, utilizando metodologías de hackeo ético.* http://bibdigital.epn.edu.ec/handle/15000/16740

Onofa Calvopiña, F., & Pilatuña Chica, I. (2015). Certified Ethical Hacker (CEH). En *Análisis y Evaluación de Riesgos y Vulneravilidades del Nuevo Portal Web de la Escuela Politécnica Nacional, Utilizando Metodologías de Hackeo Ético* (pág. 20). Quito. http://repositorio.uisrael.edu.ec/handle/47000/647