TESTING NETWORK SECURITY USING KALI LINUX

Nesh Amlani[1], Valeriu Manuel Ionescu[2]
[1]Marwadi University, Rajkot Morbi Road, Gujarat, India.
[2]University of Pitesti, Department of Computer Science, Pitesti
[1]neshamlani@gmail.com, [2]valeriu@ieee.org

Keywords: Kali Linux, Aircrack-ng, Metasploit, network security

Abstract: *Kali Linux is a specialized Linux distribution that is focused on testing network and operating system security. The included tools range from easy to use offline tools to complex site or network audit tools. This paper investigates the ease of use for some of the tools available in the Kali Linux operating system and observations are made on how to prevent such attacks thereby improving network security.*

1. INTRODUCTION

Network security represents any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Network security manages access to the network and targets a variety of threats and stops them from entering or spreading inside the network. Network security is typically handled by a network administrator that implements the security policy.

Network security combines multiple layers of defenses inside the network and at its edge. Each network security layer implements policies and controls. Authorized users gain access to network resources, while malicious actors are blocked from carrying out exploits and threats. Below are some components of network security [10]:

• Access control: It controls who can access and how much access is permitted by administrator.

• Antivirus and antimalware software: Software to scan and protect network from viruses and malwares.

• Application security: comprises the measures taken to improve the security of an application.

• Firewalls: It is a barrier between internal network user and internet.

• Wireless security: Tools which are specifically designed to protect wireless network.

The users that threaten the network security are a specialized type of hackers, called security hackers, with a good level of expertise that try to avoid the protections implemented for a networked computer system. Depending on the legality of the actions performed, there is an unofficial classification for the types of hackers.

White Hat Hacker: are ethical hackers that is specialized in penetration testing and similar technologies and it is employed by companies to determine if their system is secure or if there are security breaches present.

Gray Hat Hacker: are hackers that test the security of informational systems even without being asked, just to show their skill or to give recommendations about how the security of the system can be improved. They usually do not destroy data and alert the system administrators about their successful security breach.

Black Hat Hacker: these persons violate the system security to have personal gain, be it material or fame. They are often involved by individuals or companies to affect the business platform of their competition.

Hackers, depending on their skill, can create their own tools or use existing ones, such as penetration testing security suites. Several examples are: Netsparker[14], Acunetix, W3af, Burpsuite [8] or Kali Linux. In this paper we will focus on the Kali Linux suite.

Kali Linux is an open source and free to use Debian based Linux operating system which is used for Penetration Testing and security auditing. It was created by Mati Aharoni and Devon Kearns and is developed, funded and maintained by Offensive Security, a company

operating in the information security and training domains [1]. It was released on 13 March 2013 and is a continuation of an older security testing suite: BackTrack. Kali Linux contains many tools which can be used for many computer research and reverse engineering.

There are many tools included in Kali Linux (interface in Fig. 1) but they are not new (0-day attack tools), in fact they are created to be easy to use by persons with limited technical skills. A long time is necessary to transform a 0-day attack into an automated one. For example, the Specter attack [12] was discovered in January of 2018, but the first automated discovery tool became available to the public in December 2018 [13]. The Kali Linux tools are well documented and many tutorials exist for them. The tools can be grouped in the following categories:

1. Information Gathering.
   - Arp-scan
   - Dnsmap
   - Nmap
   - Nikto
2. Vulnerability Analysis
   - Sqlmap
   - Nmap
   - jSQL injection
   - Oscanner
3. Password Attacks.
   - Crunch
   - John the ripper
   - Hashcat
   - THC-Hydra
4. Wireless Attacks.
   - Wifiphisher
   - Wifte
   - Aircrack-ng
   - Aireplay-ng

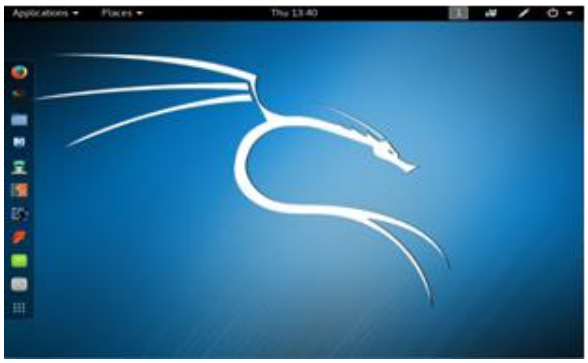

Fig. 1 Kali Linux user interface with gnome theme which is the default theme of the Kali Linux

As the list is extensive, in this paper we will focus only on several types of attacks: Brute Force Attacks; Phishing Attacks; Denial of Service (DOS) Attacks; Man in the Middle (MITM) Attacks.

The reminder of this document is organized as follows: in Chapter II are presented the attacks with their execution, in Chapter III considerations are made on how to mitigate these attacks and in the Conclusions chapter the ease of execution will be discussed and the problems encountered.

2. ATTACK IMPLEMENTATION

A. Brute Force Attack

A brute force attack has the purpose of finding the password of the Wi-Fi connection of our target by trying all the possible password combinations. In order to do this it is necessary to be able to communicate to the AP and extract the data exchanged between the client and the AP. Also, the passwords tried are not random but a list of known passwords taken from large lists (terabyte size files) existing on the internet. This means that multiple tools are necessary to complete the attack (all being part of the aircrack-ng package [4]):

• Airmon-ng: used to put our device in monitor mode.

• Airodump-ng: used to scan nearby Wi-Fi devices and to create the hash file.

• Aireplay-ng: used to de-authenticate our target Wi-Fi device.

• Aircrack-ng: used to crack the password.

The iwconfig command will be used to check the details of our Wi-Fi adapter.

The steps to de-authenticate the Wi-Fi device and to hack the password are given below (Fig. 2).

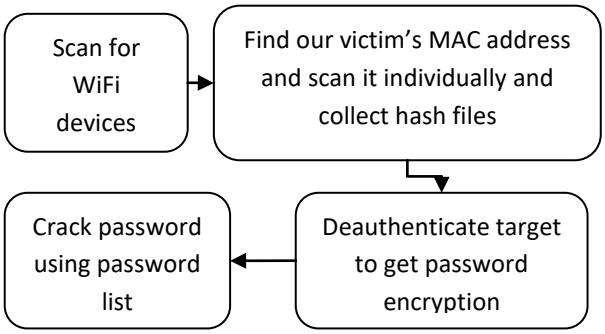

Fig. 2 The flow chart of the brute force attack

First we need to open the terminal log in as root user with the command:

- `sudo –i`

As we logged into root user now we need to start our Wi-Fi adapter, by using the command (Fig. 3):

- `airmon-ng start wlan0`

Fig. 3 Airmon-ng command

To check if our Wi-Fi adapter is working we can use (Fig. 4):

`iwconfig mon0 command;`

Fig. 4 iwconfig command output

After our Wi-Fi device is turned on, it is time to put it in monitor mode. In monitor mode our Wi-Fi adapter scans nearby Wi-Fi devices so we can find the MAC address [2] of our target device. The command is:

- `airodump-ng mon0`

As we execute the command we see that our Wi-Fi adapter starts to scan near by devices.

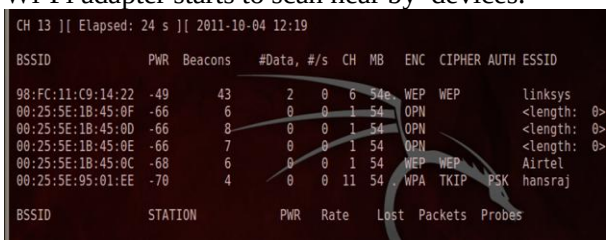

Fig. 5 Airodump-ng Command

In Fig. 5 the columns represent:

- BSSID is MAC address of that Wi-Fi device.
- ENC is the encryption method used by that device.
- CH is the channel of that device.
- ESSID is the name of that Wi-Fi device.

After this we scan nearby Wi-Fi devices as we need to gather information related to our target: the MAC address (or BSSID of our target) and the channel of the device.

As we find both components (BSSID/MAC 00:23:69:98:AC:05 and channel 4), it is time to stop the scan for all the devices and to scan our target in order to create a hash file that will be used to crack the password. The command is:

- `airodump-ng --bssid 00:23:69:98:AC:05 –c 4 –w hackwpa mon0`

In the above command the *bssid* parameter is mac address, the *c* specifies the channel and *hackwpa* is the file name used to store the hash data (Fig. 6).

After we execute the command we see that our Wi-Fi adapter starts to collect information about our target device by collecting beacons we are stored in hash file generated by the command. Beacons are management frames transmitted periodically by the Access Point that contain network information (Fig. 7).

Fig. 6. Airodump-ng Specifice scan with hash file

After we collect sufficient beacons it is time to deauthenticate our target device to get the password information. Deauthenticating devices forces them to try to reconnect and this forces them to send the password information which in turn increases the attack speed. For this we use:

- `airplay-ng -0 0 –a 5C:33:8E:48:2A:94 mon0`

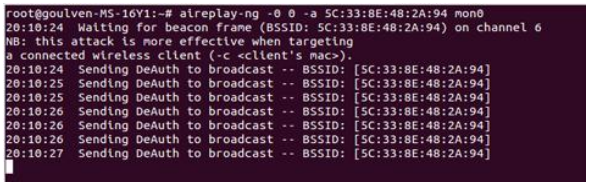

Fig. 7 De-authentication screen

In the above command the parameters: *a* specifies the MAC address of our target deivce; *0* is the number of times to de-authenticate;

After this process is complete the last step is to crack the passwork using aircrack-ng and the hash file that was generated by the scan. To crack the password we have to execute the command:

- `aircrack-ng –w wordlist.lst –b 00:23:69:98:AC:05 hackwpa*.cap`

In the above command *–w* is the wordlist that we give to try every possible combination; *-b* is mac address; *hackwpa*.cap* is the hash file.

After the process is complete (it will take more or less time depending on the complexity of the password and the number of passwords tried) we finally get the possible password (as current passphase) as seen in Fig. 8 .

Fig. 8 Final screen of aircrack-ng with the detected password

B. Phishing Attack

Phishing attacks are one of the most common and easy to perform attacks and do not need deep knowledge of computer programming. This type of attack uses social engineering tools and techniques to steal confidential information. The most common purpose of this attack is on targets credential details.

There are many types of phishing attacks but the most common type is social phishing. This type of phishing attacks has the same objectives as regular phishing attacks but the methods are different and attacker's main target is victim's social credentials.

To perform this attack, we will use setoolkit (Social Engineering tool kit) which is a pre-installed tool in Kali Linux. If it is not installed it can be downloaded from Github [5].

Below are the steps to perform Social Phishing Attacks with the purpose of creating a fake page and stealing login information (Fig. 9).

As before we need to open the root terminal.

- `sudo -i`

To start the social engineering toolkit we run:

- `setoolkit`

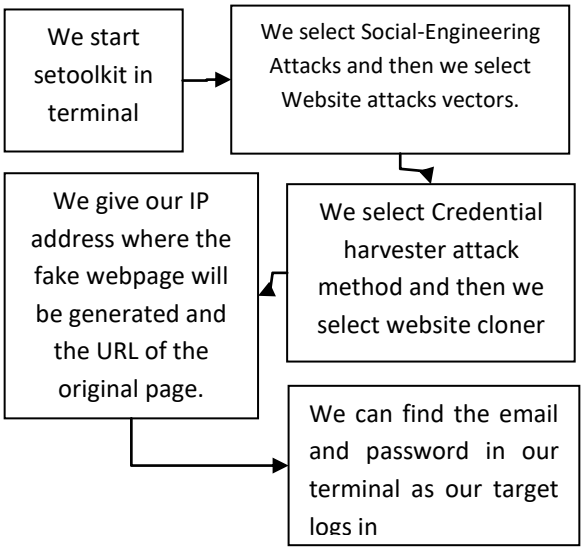

Fig. 9 The flow chart of the Social Phishing attack

We first get the welcome note and some important links and information on setoolkit. After accepting the terms and conditions an option screen is presented with the desired type of attack. To perform social phishing attacks we need to choose to option 1 (Social-Engineering Attacks), as seen in Fig. 10.

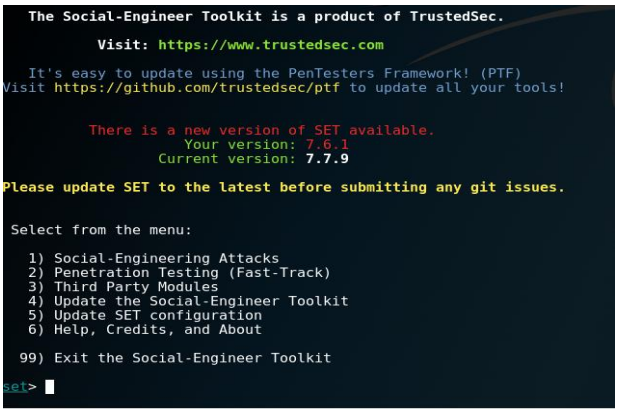

Fig. 10 Menu of setoolkit

A new screen is presented with different approaches for this attack. We first need to create a fake page therefore we choose option 2 (Website phishing attacks) as seen in Fig. 11.

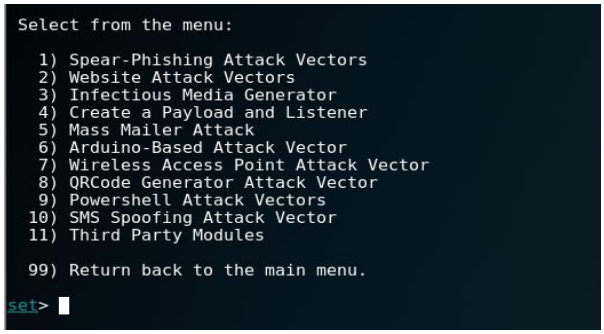

Fig. 11 Options menu for Social-Engineering Attacks

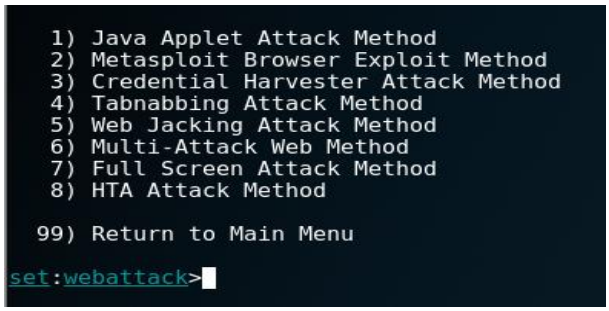

Fig. 12 Options for the Website phishing attack

In the next screen (Fig. 12) we select option 3 (Credential harvester attack method) and finally we will choose to clone a specific site (Fig. 13).

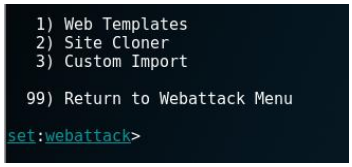

Fig. 13 In this menu you can choose to create a site or clone an existing one

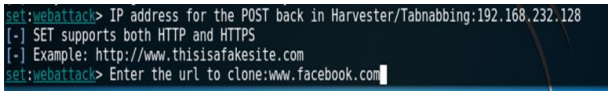

Fig. 14 Selecting the IP and the URL of the newly created site

In the next screen (Fig. 14) the site cloner option it will ask for the IP address [6] and website URL [7] that will be used to receive the credential attempts. In this case the URL www.facebook.com was used as seen in Fig. 15.

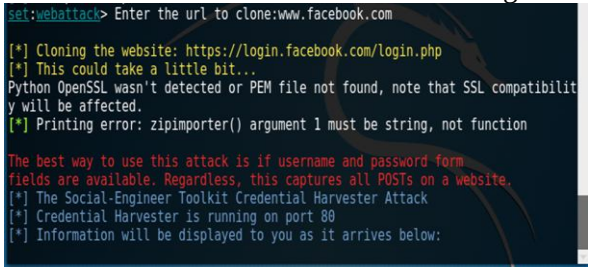

Fig. 15 Processing screen after all the steps are completed

After we enter the URL we get a screen where we can wait for the target victim to enter the login details on the fake Facebook login page. As soon as our victim enters the details, our terminal will show their capture (for this tutorial we have used test as username and test as password):
POSSIBLE USERNAME FIELD FOUND: email=test.
POSSIBLE PASSWORD FIELD FOUND: pass=test.

For the attack to be successful in real life, the attacker makes you click on a link that apparently redirects you to the desired site but has an incorrect URL (that is sometimes hard to distinguish from the real one, for example a sub domain of another site) and where some information (like the email) can be already populated. After the user enters the correct login data, a failed login attempt is triggered and the user is usually redirected to the real page. This will reduce the chances that the user will detect that the previous page was a fake one and the login data was captured.

3. Denial-of-Service (DoS) Attacks.

A Denial-of-Service attack has the purpose of making the network resource unavailable for their intended targets. The attack consists of sending a large amount of traffic or requests that cannot be processed by the target in time so that legitimate requests cannot be processed.

If the attack is performed by multiple machines that coordinate their attack it is called a Distributed Denial-of-service attack (DDoS). The reason behind this approach is that it is very hard for a single machine to exhaust the target server's resources but also because it is more difficult to block the attack's origin.

There are multiple ways on how this attack can be performed, ranging from application layer attacks (HTTP POST DoS attack) to classic IMCP flood or even intermediary hardware attacks (by destroying unsecured switches or routers that the server is connected to).

In the following section we will perform a ICMP flood DoS attack, where many ICMP packets will be sent to the target. If all the server bandwidth is filled with this data, legitimate data will no longer reach the server. For this attack we will use the *hping3* tool. The *hping3* is

available from Github [9]. The attack will be performed on a local network computer using the steps seen in Fig, 16.

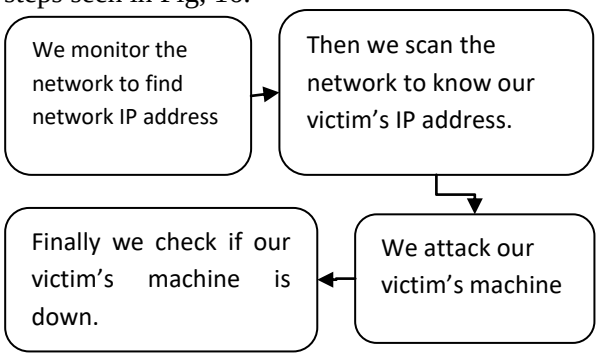

Fig. 16 Flow chart of all the steps in conducting DOS attack

As with previous implementations, we need to open the root terminal. Then it is necessary to perform a network scan so that we can know how many devices are connected and their IP address. If the computer is new to the network, a simple monitoring will tell us what is the network address of the computers is in the local network (using for example *iptraf*).

After this we will use the *nmap* tool to scan the local network:

- `nmap 192.168.232.0/24`

Then we will select our target (in this case a web server, having the http or https ports open). To test if a port is open we can use:

- `nmap -p 80 192.168.43.253`

Now that we established our target we will execute our command to send a lot of traffic so to fill the entire bandwidth. This attack will work regardless if the server is configured to drop the ICMP packets. The command used is:

- `hping3 -S --flood --interface wlan0 --rand-source ipaddress.`

```
root@kali:~# hping3 -S --flood --interface wlan0 --rand-source 192.168.43.253
HPING 192.168.43.253 (wlan0 192.168.43.253): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.43.253 hping statistic ---
8334173 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Fig. 17 The hping3 command

To check that the target will no longer accept connections we can try to open a web page or try to ping that computer from a different host (the latter only works if the server firewall does not drop the ICMP packets).

- `ping 192.168.43.253`

```
root@kali:~# ping 192.168.43.253
PING 192.168.43.253 (192.168.43.253) 56(84) bytes of data.
From 192.168.43.112 icmp_seq=1 Destination Host Unreachable
From 192.168.43.112 icmp_seq=2 Destination Host Unreachable
From 192.168.43.112 icmp_seq=3 Destination Host Unreachable
From 192.168.43.112 icmp_seq=4 Destination Host Unreachable
From 192.168.43.112 icmp_seq=5 Destination Host Unreachable
From 192.168.43.112 icmp_seq=6 Destination Host Unreachable
From 192.168.43.112 icmp_seq=7 Destination Host Unreachable
From 192.168.43.112 icmp_seq=8 Destination Host Unreachable
From 192.168.43.112 icmp_seq=9 Destination Host Unreachable
^C
--- 192.168.43.253 ping statistics ---
12 packets transmitted, 0 received, +9 errors, 100% packet loss, time 266ms
pipe 4
```

Fig. 18 Ping check the attacked server from a different machine

4. Man In The Middle (MITM) Attack

MITM attacks are one of the most dangerous attacks that can be performed in a local network, because they are hard to detect and hard to trace. Most MITM attacks are conducted in the local network because they are based on local network techniques such as ARP.

To conduct a MITM attack we need to intercept the entire network data traffic between our victim and the gateway and then intermediate the traffic exchanged between the two, as seen in Fig. 19.

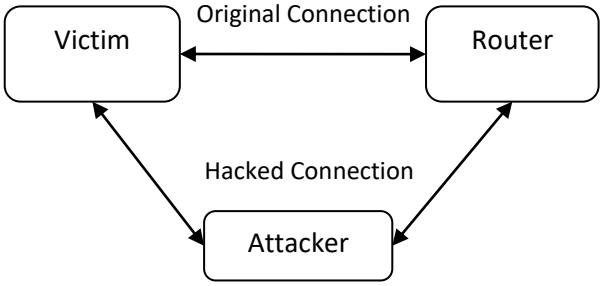

Fig. 19 MITM attack model diagram

There are many ways to perform this step: by posing as an Access Point and one of the partied connects to it; by performing an ARP spoofing where an attacker sends false ARP messages with the intention of associating a legitimate IP with the attackers MAC thereby redirecting the traffic; by performing a DNS spoofing through poisoning incorrectly configured DNS servers with additional (malicious) DNS resolvers.

After a successful MITM attack, the attacker has access to all the traffic exchanged and for example we can spoof our victim's URL, or we can see which website our target has opened or we can force our victim to open the website that we wish.

There are many tools for performing a MITM attack: bettercap; arpspoof; xerosploit; websploit. In the following section we will use

websploit. As with the other tools you can download websploit from Github [11].

Below (Fig. 20) are all the steps to conduct MITM attack.

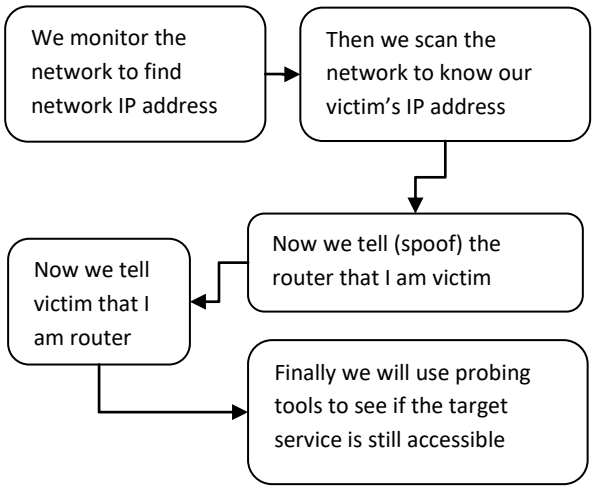

Fig. 20 Flow chart of all the steps for a MITM attack

As with previous attack implementation, we need to open the root terminal. Then it is necessary to perform a network scan so that we can know how many devices are connected and their IP address. If the computer is new to the network, a simple monitoring will tell us what is the network address of the computers is in the local network (using for example *iptraf*).

After this we will use the nmap tool to scan the local network:

- `nmap 192.168.232.0/24`

Now we will start websploit tool by running:

- `./websploit`

The list of modules can be shown by using the *show modules* command. We will use:

- `use network/mitm`

We will need to set the options for this attack as the default ones are not correctly set (as seen in Fig. 21):

- `set interface wlan0`
- `set router ip`
- `set target ip`

The tool allows different modules that will extract a different type of data after the attack is successful: urlsnarf – for link detection, dsniff – for password sniffing, msgsnarf – for messanger sniffing and driftnet for image sniffing. We will use:

- `set sniffer urlsnarf`
- `run`

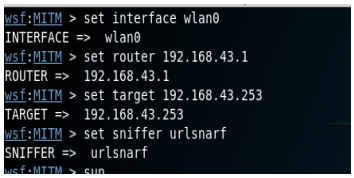

Fig. 21 The websploit configuration

After running the commands the attack will execute and we will have access to the links the target has accessed as seen in Fig. 22.

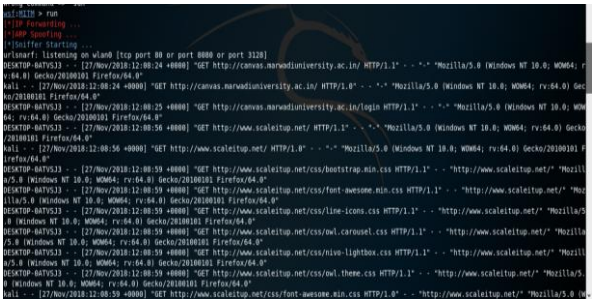

Fig. 22 The output after the urlsnarf captures data

5. IMPLEMENTATION DISCUSSION

In brute force attack an attacker needs to have a big password list (to increase the chances that your wordlist will contain the correct password), a fast processor (maybe a cluster of computers) and a large amount of time. In order to prevent this type of attack one should use strong password minimum 8 characters with many different combinations of special character.

In Phishing attacks it is necessary to make sure that the page is very similar to the original/replaced page or the victim will detect that the page is fake and will not input the login information. As a defense technique, a good indication that there is a problem is if the URL of the page, especially for the login pages, is not secure (it uses http instead of https) and the name is not the expected one (example of bad URLs include sub domains: www.facebook.mysite.com or variations of that name: www.facelook.com and www.mysite.com/facebook/).

Sometimes the browser will alert the user that there is a problem with a specific site or that it is known for its malicious behaviour, but this is not always the case.

In DoS attacks a potential attacker needs first to gain acces to the computer or computers that will perform the attack and hide the access to the compromised computers. If the data flow or the technique is not successful, the attacker

can either use multiple machines to force all more traffic at same target or change the method.

In order to protect from this type of attack, a network administrator should monitor the internal network and place restrictions on specific data flows (limiting specific connection attempts per second for example or the amount of data for ICMP traffic). For external attacks, it is necessary to contact the service provider and ask to stop unwanted traffic from the attackers IP address.

In MITM attack most tedious part is gaining access to the target's traffic without the victim noticing.

To prevent a MITM attack, strong encryption needs to be used on the Access Points, Virtual Private Networks should be used, HTTPS should be forced for server access and other encryption methods should be used.

6. CONCLUSIONS

Kali Linux is a security testing Linux distribution that is easy to use as it includes numerous online tutorials. Even if the security audit and attack tools are not zero day tools [3], there are many cases when businesses do not patch their systems and discovering older network security breaches can still be benefic. It is therefore good to know how to use the tools included in this distribution.

The easiest way to use Kali Linux is by starting it from an USB drive. However on the test system used, a boot mode error was encountered, as seen in Fig. 28.

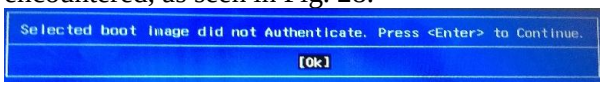

Fig. 23 Boot mode error

The only way to pass and be able to boot from the USB drive, was to select legacy mode and boot in this mode.

In this paper four attacks were executed from those available in the Kali Linux application list. The implementation problems and recommendations for defending against these attacks were presented.

7. REFERENCES

[1] Offensive Security, "Official Kali Linux Releases", web, https://www.kali.org/kali-linux-releases/, accessed: 01-10-2018.

[2] IETF, "IANA Considerations and IETF Protocol Usage for IEEE 802 Parameters", web, https://tools.ietf.org/html/rfc5342, accessed: 01-10-2018.

[3] Jay Beale, "Breaking the Zero-Day Attack on Linux (the Strutshock Vulnerability and Equifax)", January 29th, 2018, web, https://www.beyondtrust.com/blog/breaking-zero-day-attack-linux-struckshock-vulnerability-equifax/, accessed: 01-10-2018.

[4] Github, aircrack-ng, web, https://Github.com/aircrack-ng/aircrack-ng, accessed: 01-10-2018.

[5] Github, setoolkit, web, https://Github.com/trustedsec/social-engineer-toolkit, accessed: 01-10-2018.

[6] IETF, "RFC: 791 INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION", web, https://tools.ietf.org/html/rfc791, accessed: 01-10-2018.

[7] IETF, "RFC 1738 Uniform Resource Locators", web, https://tools.ietf.org/html/rfc1738, accessed: 01-10-2018.

[8] Portswigger Web Security, "BurpSuite Professional", web, https://portswigger.net/burp/Burp%20Suite%20Pro%20Data%20sheet.pdf, accessed: 01-10-2018.

[9] Github, hping3, web, https://Github.com/antirez/hping, accessed: 01-10-2018.

[10] Cisco, "What Is Network Security?", web, https://www.cisco.com/c/en/us/products/security/what-is-network-security.html, accessed: 01-10-2018.

[11] Github, websploit. Web, https://github.com/websploit/websploit, accessed: 01-10-2018.

[12] Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre attacks: Exploiting speculative execution," ArXiv e-prints, Jan. 2018

[13] Andrea Mambretti, Matthias Neugschwandtner, Alessandro Sorniotti, Engin Kirda, William Robertson, Anil Kurmus, "Let's Not Speculate: Discovering and Analyzing Speculative Execution Attacks",web, https://domino.research.ibm.com/library/cyberdig.nsf/papers/D66E56756964D8998525835200494B74/$File/RZ3933.pdf, accessed: 01-10-2018.

[14] Netsparker Ltd., "Netsparker Web Application Security Solution", web, https://www.netsparker.com/statics/netsparker-desktop-datasheet.pdf, accessed: 01-10-2018.