Network Security
Penetration Tools for Network Security

Daniel Klasson, Kim Klasson, Anatoly Iourtchenko

Network Project
7.5 HP

10.01.2014
Preface

Through good communication and collaboration, we could all, in spite of divided work, learn, and test on both the wired and the wireless part. By working with the project in a timely manner and together guide and motivate each other to always be one step ahead of the schedule, we were able to reach our goal which among other things was to demonstrate the weaknesses and strengths in wired and wireless network protocols.

We would like to thank the Halmstad University and Cisco System, Inc. for the equipment that was used. Also big thanks to Olga Torstensson and Malin Bornhager for feedback and excellent job as supervisor and examiner. We would also thank Mati Aharoni, Devon Kearns in offensive Security for the development of Backtrack 5 R3.
Figure 3.1 – Topology................................................................................................. 10
Figure 3.2 – CDP in Wireshark.................................................................................. 10
Figure 3.3 – DTP-attack.............................................................................................. 11
Figure 3.4 – VLAN 20 Backtrack5 Interface.............................................................. 12
Figure 3.5 – Cisco Auditing Tools............................................................................. 13
Figure 3.6 – Password list.......................................................................................... 13
Figure 3.7 – Start sniffing........................................................................................... 13
Figure 3.8 – Starting Intercepter-ng.......................................................................... 14
Figure 3.9 – Gateway founded................................................................................... 15
Figure 3.10 – Listening mode (monitor mode)........................................................... 16
Figure 3.11 – #airodump-ng -w dumpfile3 mon0..................................................... 16
Figure 3.12 – Dump targeting.................................................................................... 17
Figure 3.12 – Fake authentication injection.............................................................. 17
Figure 3.14 – Fake Arp request.................................................................................. 18
Figure 3.14 – Dump file............................................................................................ 18
Figure 3.15 – anatolywif........................................................................................... 19
Figure 3.17 – De-authenticate ................................................................................... 19
Figure 3.18 – WPA PSK Handshake.......................................................................... 19
Figure 3.19 – Dictionary file..................................................................................... 20
Figure 3.20 – WPA password.................................................................................... 20
Figure 3.21 – Crack PIN, WPS Authentication......................................................... 20
Figure 3.22 – Etter.dns............................................................................................. 21
Figure 3.23 – Set Tool Kit directory.......................................................................... 21
Figure 3.24 – Set Tool Kit from directory................................................................. 21
Figure 3.25 – Set Tool Kit......................................................................................... 22
Figure 3.26 – Sub-menu ............................................................................................ 22
Figure 3.27 – Previous menu select.......................................................................... 23
Figure 3.28 – Previous menu select.......................................................................... 23
Figure 3.29 – Website cloned.................................................................................... 24
Figure 3.30 – DNS spoofing...................................................................................... 24
Figure 4.1 – Password found.................................................................................... 25
Figure 4.2 – Router GUI Results.............................................................................. 26
Figure 4.3 – Cracked 64-bit WEP key...................................................................... 27
Figure 4.4 – Cracked 128-bit WEP key.................................................................... 27
Figure 4.5 – Brute force Result................................................................................ 28
Figure 4.6 – Reaver Result....................................................................................... 29
Figure 4.7 – Ettercap spoofing command................................................................. 30
Figure 4.8 – Ettercap spoofing results...................................................................... 30
Figure A.1 – Wired part............................................................................................ 31
Figure A.2 – Wired configuration............................................................................. 31
Figure A.3 – Wired Network..................................................................................... 32
Figure B.1 – D-link DIR-615.................................................................................... 32
Figure B.2 – D-link DIR-615.................................................................................... 33
Figure B.3 – Wireless Card D-link DWL G122 revision C....................................... 33
Figure B.4 – Backtrack 5 disc................................................................................. 34
Abstract

This report, will show by demonstration with Network Penetration, how to reveal security holes by using the same methods as an outside attack and carry out attacks against wired and wireless networks when it comes to sniffing user traffic, abuse VLAN, cracking password, WEP, WPA/WPA2, hacking WPS and analysing traffic.

The tests was performed at the Halmstad University with lab equipment and at home with own equipment. Using Backtrack 5 R3 which is compatible with Linux, performance of the tests could be done by making use of various tools that comes with Backtrack.

The goal of the project was to demonstrate how to reveal security holes by using the same methods as an outside attack. By testing, demonstrate and report the security of wired and wireless network, the achievement of these goals could be done and a greater insight into network security was gained, which gives more experience and knowledge that can be taken to a future professional life.

The results show how simple it can be to abuse a network or sniff a password if there is no attention to the safety and the security configurations that can be implemented. In other words, during this project, both learning and demonstration has been done to show how vulnerable individuals, civilians and entrepreneurs are. It is easier than someone can imagine to obtaining unauthorized information that nobody wants to share out.
# Contents

Preface .................................................................................................................. iii

Abstract .................................................................................................................. iii

1 Introduction ......................................................................................................... 1
   1.1 Background ................................................................................................. 1
   1.2 Project Goal ............................................................................................... 2
   1.3 Objective .................................................................................................... 2
   1.4 Methodology ............................................................................................... 2

2 Theoretical Background .................................................................................. 5
   2.1 Network Security ...................................................................................... 5
      2.1.1 What is Network Security ................................................................. 5
      2.1.2 What is Penetration Tool? ................................................................. 5
      2.1.3 Types of Security Threats ................................................................. 6
   2.2 Network Attacks ....................................................................................... 7
      2.2.1 What is a Network Attack? ............................................................... 7
      2.2.2 Types of Network Attack ................................................................. 7

3 Network Penetration Attacks ................................................................. 9
   3.1 Penetration Attacks Wired Network ...................................................... 9
      3.1.1 Abuse VLAN ...................................................................................... 9
      3.1.2 Password Sniffing with Cisco Auditing Tool .................................. 12
      3.1.3 Account Sniffing with Interceptor ............................................... 14
   3.2 Penetration Attacks Wireless Network .................................................. 15
      3.2.1 Penetrating WEP Key ...................................................................... 15
      3.2.2 Cracking WPA/WPA2 PSK/TKIP AUTO ....................................... 18
      3.2.3 Cracking WPS ............................................................................... 20
      3.2.4 Hi-Jacking .................................................................................... 20

4 Results and Analyse .................................................................................... 25
   4.1 Results & Analyse Wired Network ....................................................... 25
      4.1.1 Abuse VLAN Results ...................................................................... 25
      4.1.2 Password Sniffing Results .............................................................. 25
      4.1.3 Account Sniffing Results ............................................................... 25
   4.2 Results & Analyse Wireless Network .................................................... 26
      4.2.1 Cracking of WEP-128bit Results .................................................... 26
      4.2.2 Cracking WPA/WPA2 PSK/TKIP Auto Results ............................. 27
      4.2.3 Cracking WPS PIN Results ............................................................ 28
      4.2.4 Hi-Jacking Results ...................................................................... 29

5 Conclusions .................................................................................................... 30
Chapter 1

1 Introduction

1.1 Background

Wired and wireless network (Wi-Fi 802.11b, g, n, ce) is becoming more and more familiar in offices, headquarters, schools and homes. They connect and bring people to the Internet. In connection with the development it is becoming easier to detect security holes. This means that, an individual, civil or businessmen always are in a vulnerable position. The security is now more important than ever and has a great impact on the future if the development shall go in the right direction.

LSEC is a non-profit organization that has become a leader in Information Security. It has more than 500 information security professionals. This organization has a world class e-security expertise platform which allows the members to stay ahead by stimulating and supporting knowledge exchange and collaboration. The main goal of this organization is to be security aware in IT industry. [26]

Every day there are attacks against individuals, civilians and entrepreneurs. It may be a Facebook account. When for example at home or company and someone log on with their personal password through Facebook Mobile Application. Without the slightest knowledge all the personal information is suddenly in someone else's hands. Faster than someone can discover that the Facebook account has been hijacked, the person with the right knowledge and interest has already been received enough information for example full name, email address, phone number, social security number, passwords and the worst thing that can be imagine, a bank account.

Exploiting network and computer systems is rapidly expanding. Social networks are built and formed with chat clients and communication systems between hackers and exploiters. The more efficient the communication between the hackers gets, the better the attacks can be achieved.

To avoid this, the network penetration is extremely important for today's development. No one wants their information available for the wrong person, for example hackers that can steal, share or sell the information for their own profit.

By demonstrating how to reveal security holes, it can be seen if a network really is as protected as it should be. With the help of the security holes that many people usually are unaware of, a data breach can easily be done. [1] [2] [15]
1.2 Project Goal

The goal is to show how the vulnerability becomes a real risk by a demonstration on how to reveal security holes by using the same methods as an outside attack. By testing, demonstrate and report the security of wired and wireless network a greater insight into network security was gained, which gives more experience and knowledge that can be taken to a future professional life. The points below summarize the problem and goals with the project.

**Problem:** Security risks in wireless and wired networks.

**Goal:** Discovering and understanding the security holes in a network.

1.3 Objective

To achieve the goals with this study, exploration and discovery will be done with different tools to penetrate and hack into wireless and wired networks. The purpose is to find out how to crack, hack and exploit wireless (Wi-Fi 802.11a, b, g, n) and wired networks.

- Wi-Fi attacks on encryption protocol (WEP, WPA/WPA2/WPS, denial of service, sniffing out data from other computers on the network).
- Wired Network Attacks on Cisco devices to test, demonstrate and report the weaknesses and strengths of the wired network protocols (VLAN, VTP).
- Find and explain the options for strengthening of Wi-Fi networks and wired networks.

1.4 Methodology

Through various penetration tools, a demonstration was done to show how insecure the network really is. The tools that were used were chosen with Backtrack because it is very popular and it is a tool which is specifically designed for digital forensics and penetration testing in IT industry. This is an exploit distribution which is based on Ubuntu Linux distribution that has a far more tools than any other distributions that exists [29] [30]. It has been updated by exploit-developers and security consultants throughout the world and has been updated since it came out in February 5, 2006. It has far more built in attacks than any other distribution. [27] [28]

The tools of Backtrack are very popular all the way back since 2005-2006 which includes aircrack, aireplay, airodump and a number of other tools. Backtrack is very famous for its robust power to exploit wireless networking. The Backtrack suite is the most popular tool for Wi-Fi penetration. [17]

**Tools used:**
- Airodump-ng
- Aireplay-ng
- Aircrack-ng
Chapter 1. Introduction

- Reaver
- Set Tool Kit
- Cisco Auditing Tool
- Interceptor-ng
- Wireshark
- Yersinia

There are three different password attacks. Dictionary, brute force and Hybrid. Backtrack supports dictionary and brute force attacks and hybrid attack with hashCat. [31] [32]

Spoofing attack is when a hacker performs sniffing and listens to traffic as it is passed along the network from sender to receiver. This attack is known as man-in-the-middle attack. The hacker uses a web address of a legitimate system. This attack can be done in Backtrack with Set Tool Kit which is built into the Backtrack distribution. [33]

Reaver is a tool to hack WPS (Wi-Fi Protected Setup). This tool was accidently discovered for interesting of cracking WPA, with this tool it were also founded that it was possibly to crack WPS as well. WPS was popular since 2007 and is present since that year. It is still very common in use. After knowing these facts, it was obvious that this attack must be tested and verified if it really works.

Set Tool Kit was found after some googling for Facebook account hacking. The tool is included in Backtrack suite. One of its amazing features is that it can DNS-spoof an internet address e.g. www.facebook.com to backtrack suite pc.

Cisco auditing tool is used for three purposes - telnet password attack, to show iOS history and to brute force the SNMP community string. As todays switches and routers are using SSH which is more secure than Telnet, the tool is mostly outdated. The tool was found after some google searches for password sniffing on cisco switches and routers. [24]

Yersinia is a tool for layer 2 hacking. The tool was found after some researches how to abuse a VLAN. Yersinia can be opened by three different steps - Interactive, Daemon mode and GTK Graphical Mode. Interactive mode is the most popular one with a curses graphical interface. Daemon mode is a mode that allows someone or something to access it via a telnet session. GTK Graphical mode is a more graphical style where click and point with the mouse on the computer can be done.

Different attacks that can be done with Yersinia is CDP, VTP, HSRP, DTP, DHCP, STP, 802.1Q and X. [25]

Attacks:
- VLAN Abuse
- Password Sniffing
- Account Sniffing
- Penetrating WEP Key
- Cracking WPA/WPA2 PSK/TKIP AUTO
- Cracking WPS
- Hi-Jacking
VLAN Abuse was chosen partly to demonstrate how easy it is to obtain unauthorized information from a company or any individuals via switches.

Password Sniffing, Account Sniffing was chosen partly to demonstrate how easy it is to get unauthorized information and data from a company or individuals via switches and routers.

WEP, WPA/WPA2, PSK / TKIP AUTO, WPS & Hi-Jacking was chosen partly to demonstrate how easy it is to gain access to unauthorized information and data, and to gain access to someone else's private network / social life.

The tests were conducted in Cisco lab at Halmstad University and with own equipment. Windows server 2008 64bit, DLINK DIR-615 WLAN AP, DLINK DWL-G122 WLAN adapter and Backtrack 5 R3.
Chapter 2

2 Theoretical Background

2.1 Network Security

This part focuses on the foundations of network security. Why security today is so important and the types of security that should be avoided.

2.1.1 What is Network Security

For many people, security means many different things. Everyone defines safety in their own way. Network security is something that provides safety and protects us from attacks on our network, business, usability, integrity and confidential/personal data. [1]

The security threats today are significantly larger than it was before. Today, there is no requirement for great knowledge to succeed with an attack that another person would see as impossible.

Before reading more about what types of threats and attacks there are, it may be helpful to know the different terms of which kind of person who is behind a particular attack. List of the most common terms:

- White hat - A person looking for security holes to create a stronger and more secure network for a company.
- Hacker - A person whose mission is to find unauthorized information on a network in the form of revenge, hatred or for other purposes.
- Black Hat - The opposite of White Hat. Instead of helping the victim, their mission is to find security holes and use it for their own benefit.
- Cracker - A more specific term for someone who practice white hat and black hat.[2]

2.1.2 What is Penetration Tool?

In this world of heavy computer communication, the demand of security is rising to new levels. More and more information are stored on computers each day. New systems and software are developed and have pros and cons in terms of security. While sitting here and reading this, websites are hacked, database information is stolen, passwords are cracked and the systems are demanding new ways to secure them.

Here is where the Penetration tools come in. With this type of tool, companies and other parties can test and verify their own infrastructure security by stress testing and finding holes in their computer environment on all levels. This can be to find weaknesses on their website, if it is possible to execute codes and special characters
or to exploit other methods to gain full access to all the information in the database. Penetration tools such as (Backtrack, an OS Linux Distribution) can be used to verify and fix issues such as:

- Antivirus exploits
- Network stress testing (VOIP, WLAN, DOS)
- Operating system backdoors
- Privileges Escalations in OS (password attacks, spoofing attacks)

With this tools IT personnel in companies, firms and government can test the security, reliability and stability of their IT and computer systems and find ways to secure these holes and vulnerabilities.

### 2.1.3 Types of Security Threats

When talking about the types of security threats that exist, it is usually divided into four categories:

- **Unstructured Threats** - Form of White hat or black hat. A person who is looking for security holes for either a good cause or for personal benefit.

- **Structured Threats** - Regarding Structured threats, it is common to say that it is either a person or a group of people with some knowledge and interest in hacking. In other words, a group that fits into the form of black hat. There is a well-known organization that fit into this category.
  - This organization calls them "Anonymous" and is simply a group of anonymous people that is looking for security holes in companies or government agencies to commit either fraud or for fun creating havoc in the form of a virtual demonstration. Everything from hatred, revenge or form of political opinion.

- **External Threats** - A threat to a company by either an individual or a group who do not have access to approved computer systems and networks outside the company. Takes the form of intrusion from either the Internet or servers. A mixture of Unstructured and Structured threath.

- **Internal Threats** - A threat to a company by either an individual or a group that has access to approved computer systems and networks outside the company. Takes the form of intrusion from either the Internet or servers. A mixture of Unstructured and Structured threath.[2]
2.2 Network Attacks

This part focuses on the foundations of network attacks. What is defined as a network attack and the types of attacks that exist today? The first attack are part of the project work. There is ability to read about them further in the report. The other two are also very important and interesting.

2.2.1 What is a Network Attack?

Network Attack is an attempt to access network drives, exploiting security holes or sniffing of traffic to access unauthorized information for example passwords. For some people it is something they do for fun, other people do it for their own benefit or for a good purpose.

2.2.2 Types of Network Attack

Just as security threats, the network attacks is divided into four different categories. The first category is the main part of this project. The other three is also good to know about.

- Access - Take advantage of a security holes where encryption of account or password is missing or exists.
  - VLAN Abuse – To secure the network from VLAN abuse is important to prevent workstations environments to segment out of servers. You can easily jump into the management subnet if the configurations on the switch are misconfigured. [3]
  - WEP Key attack – Is a security algorithm for wireless networks which was introduced in September 1999 as an original 802.11 IEEE password encryption. WEP key can be recognized by 10 or 26 hexadecimal values ranging from 0 to 9 and A to F. This standard has been replaced by newer security algorithms. It was cracked with a method called related-key attack. [18] [21]
  - WPA/WPA2 Key attack - This security standard was ratified in 24 June, 2004. It established 4-way handshakes with clients and exchange appropriate cryptographic keys between clients and access-point. The password can be word with digits, upper, lower case and 26 digits long. [22]
  - WPS PIN attack - Wi-Fi Protected setup was also known as Wi-Fi simple configuration. This security standard was supposed to secure wireless networks at homes. This security standard failed in December 2011 when somebody managed to brute force the WPS PIN. The WPA passphrase was then also recovered. Pin number can look like this: 37912338 (8 characters long. [23]
Password sniffing can be described as password stealing, by monitoring traffic. Passwords is almost used everywhere so at any time a password is sent through the network, the hacker can use different tools to sniff the password. It can be for example via a virus, like spyware or keystroke logging. In backtrack there is tools like Set Tool Kit, Cisco Auditing Tools or Interceptor-ng that can be used to sniff a password. [34]

- Reconnaissance - Unauthorized access of network devices. Unstructured Threat in the form of either White Hat or Black Hat. Such an attack may consist of the following form: Internet information queries, Ping Sweeps, Port Scans and packet sniffers.

- Denial of Service - Attack of a system where the goal is to create network congestion with the results of the system crashing or working so slowly that it is basically completely useless.

- Worms, Viruses and Trojan Horses - A program or text documents that are looking to either injury, read information or deny access to systems, networks or other services. [2]
Chapter 3

3 Network Penetration Attacks

Through auditing tools, VLAN-abuse and a setup of VLANs on Cisco switches the goal is to exploit VLAN and try to find VLAN tags. With the use of password cracker in Backtrack it is possible to identify telnet passwords and log information on a router or switch.

Via Wireless signals, the client uses radio waves as a media to connect WLAN-adapters (Wireless Local Area Network) that is connected to a Wi-Fi access point (wireless router).

This report will show how to avoid getting access to the Wi-Fi network-Access Point (wireless router) through full control of all the services and protocols in the Wi-Fi network that is cracked. Exploration of WEP attacks, WPA, WPA2 and WPS attacks, de-authentication (Wi-Fi denial of service attacks), as well as access to other services and unknown areas of the Wi-Fi network.

3.1 Penetration Attacks Wired Network

3.1.1 Abuse VLAN

To be able to do this test access to cisco switches and routers with three or four computers, one or two of them with Backtrack5 will be needed. Also, set up a topology.

Figure (3.1) illustrates the topology that was used. In this topology two computers were used with Backtrack5, both in the same VLAN (VLAN 30). An ACL were used, except that VLAN 30 should be blocked to get access to VLAN 10 and VLAN 20.[3][16]

To set up an IP address on the Backtrack5 computer, open a new terminal and write the following command:
- #ifconfig eth0 (ip address) netmask (netmask)

To see information of the interface, type the following command:
- #ifconfig [3][16]
Chapter 3. Network Penetration Attacks

Figure (3.1) – Topology.

The first step before the abuse of VLAN can be done is to check so there is any connection out to the interface. To check the use of the command #ping in terminal can be used to ping the gateway and Backtrack5 host and Wireshark to capture CDP- and DTP-frames. Unfortunately as figure (3.2) illustrates only CDP-frames showed up when capturing the traffic, even if it took 10 minutes. [3][16]

Figure (3.2) – CDP in Wireshark.
To be able to abuse VLAN, tell the switch that the port that Backtrack5 computer is connected to is a trunk port. To do so a tool called Yersinia can be used by typing in terminal the following command:
- `#yersina -G` – The G stands for GTK Mode.

Next step is to launch a so called DTP attack. By clicking the Launch attack button in Yersinia and tab to DTP in the new popup window, choose to enable trunking and then press OK. Now that the switch has been deceived that it is in trunking mode, there should be three different status in Yersinia - ACCESS/AUTO, ACCESS/DESIRABLE and TRUNK/AUTO. [3][16] As figure (3.3) illustrates ACCESS/DESIRABLE was the only status that showed up.

The final step to get full access to another unprotected VLAN is to add that VLAN to the interface in Backtrack5. In this test the goal is to get access to VLAN 20. Write the following command in terminal:
- `#modprobe 8021q` – This command loads the 8021q module that is needed.
- `#vconfig add eth0 20` – This command adds VLAN 20 to the interface
- `#ifconfig eth0.20 up` – Makes the interface go up
- `#ifconfig eth0.20 (ip address) netmask (netmask)`

With a `#ifconfig` the interface can be seen as figure (3.4) illustrates. [3] [16]
3.1.2 Password Sniffing with Cisco Auditing Tool

Cisco Auditing Tool is a cisco tool that is used for three purpose.

- Telnet password attack
- Show iOS history
- Brute force the SNMP community string

In this test the goal is to sniff a password that were using in the cisco router configuration. As most of today's cisco equipment are using SSH (Secure Shell) to encrypt the information and traffics this tool is mostly outdated. Telnet sends everything in plain text, so it would be very stupid to have Telnet activated if it is a serious work with networking. This test is just for demonstration purpose.

To start Cisco Auditing Tool, write the following command in a Terminal session:

- #cd /pentest/cisco/cisco-auditing-tool/

Type #./cat to see a list of options to use with this command. With this command it should be able to sniff passwords from a host (the gateway to the router) so by looking at this options list, use -h (for scanning a single host) and -a (using a wordlist for password guessing) as figure (3.5) illustrates. [4]
To be able to do this test, create a password list. This can be done by terminal or by finding the way to Cisco Auditing Tool folder in root. As figure (3.6) illustrates the second option is done by creating a new file with some few common passwords often used in cisco devices that is put in the folder Cisco-Auditing-Tool. [4]

The last step to sniff a password is to write the following command in terminal as figure (3.7) illustrates:

- `./cat -h (ip address) -a (password list)`

The host it was sniffing from was the gateway to the router (192.168.200.1) with help from the password list that was created (passwords). [4]
3.1.3 Account Sniffing with Intercepter

The last test on the wired part is not far from different than sniffing a password with Cisco Auditing Tool. In this test a tool called Intercepter-ng were used. It is a powerful tool that can be used to spy on something. In this test it was used to sniff username and password when someone tries to log in to the router via a browser.

Intercepter-ng can be found via Backtrack – Privilege Escalation – Spoofing Attack – Network Spoofing – Intercepter-ng.

As figure (3.8) demonstrates a new window popped up. In this window it show how to use the tool and the active interface that is used for searching for other hosts.

![Figure (3.8) – Starting Intercepter-ng.](image)

In this test the goal is to sniff passwords. So by taking the first interface (1) with password mode (1) and w to save the session a log of traffic between the interface and the router can be done.

Start the session by typing the following command in terminal:

```
./interceptor_linux 1 1 w
```

As figure (3.9) illustrates Intercepter-ng first scans through the network for other hosts. In this test the tool found the gateway to the router and thereby started the log session.
3.2 Penetration Attacks Wireless Network

3.2.1 Penetrating WEP Key

In order to do these tests make sure there is a Wireless Network adapter which supports packet injections and monitoring mode (sniffing mode). Appendix B (figure 3) illustrates a compatible card which supports Backtrack5.

After booting the Backtrack5, ensure that the wireless card is recognized and supported. To do this, open a new terminal window and write the following command:

- `#iwconfig` – This command lists all the network adapters that are installed on the system. `#ifconfig` can also be used, which provides additional information on the interface that is used.

The following command in figure (3.10) will put the wireless adapter into listen mode (monitor mode)

- `#airmon-ng start wlan0` [8]

Figure (3.10) shows that monitoring mode is enabled on mon0.
Figure (3.10) - Listening mode (monitor mode)

Now it is time to capture the packets. There are several options here. All channels can be selected or a more specific target. First thing is to choose to dump the traffic of all the Wi-Fi channels in a dump file (.Capfile). This file will be created after the initiation of the following command:

- `#airodump-ng -w (filename) mon0` [8]

- `w` can be anything, for example: `-w dumpfile3`. This will be the cap file ending with .cap extension as figure (3.11) illustrates. [8]

In figure (3.11), choose `#airodump-ng -w dumpfile3 mon0`, to distinguish it from other previous dump files that were created.

Figure (3.11) - `#airodump-ng -w dumpfile3 mon0`

After the the Wi-Fi area is scanned, it is time for a more specific dumping of wireless packets. As figure (3.11) illustrates, use the access point that can be seen under ESSID (`anatolywifi – with WEP 64-bit encryption`).

When the traffic that is used to listen to is chosen, execute the following command as can be seen in figure (3.12):
- #airodump-ng -w (filename) -c (choose a channel) –bssid (wireless access point MAC-address). [8]

Figure (3.12) - Dump targeting

Now it is time for some more lethal attacks against this weak WEP encryption. Here is a demonstration on how to run the aireplay-ng. How it will make this access point to vomit so much data packets that it will be able to gather enough data packets to crack the WEP-password to enter and authenticate with this access point.

Fake authentication injection (figure 3.13):

Write the following command in terminal:

- #aireplay-ng -1 10000 -a (access point mac-address) -h (the mac-address) mon0 [8]

Step 1
Keep these commands running in a terminal window!

Figure (3.13) - Fake authentication injection.

Step 2
Fake ARP requests.

Enter following command (figure 3.14):

- #aireplay-ng -3 -b (access point mac-address) -h (the mac-address) mon0. [8]
The command on step 2 is very robust and makes the access point nearly exhaust itself from the fake ARP requests. It starts spitting out fast data packets after the commands that were used on step 1 and step 2.

Both step 1 and 2 doesn't need to be done. It may be enough with just step 2. After some tests the results showed that aireplay-ng -3 commands is the most important here. It will gather enough packets even without the step 1 command.

Now that everything is done, it is time to start by opening the dump file, dumpfile4-01.cap (figure 3.15). [8]

3.2.2 Cracking WPA/WPA2 PSK/TKIP AUTO

The process of WPA/WPA2 needs a different approach than WEP. Start by listening on the access point and the channel it is on.

To listen to the access point with ESSID anatolywifi, use the following command (figure 3.16):

- #airodump-ng w (filename)-c (channel)-BSSID (AP MAC address) (interface) [10]
De-authenticate an authenticated user from the access point anatolywifi. To de-authenticate the desktop computer, which is associated and authenticated with anatolywifi, enter the following command (figure 3.17):

- `#aireplay-ng -0 1-a (AP MAC address)-c (client mac address) mon0` [10]

To de-authenticate all clients on the access-point, issue the following command instead of a specific client. These commands will DoS everyone on access point:

- `#aireplay-ng -0 1-a (access-point mac-address) mon0`. [10]

Verify that it captured the three-way handshake between the client that were de-authenticated and the access point anatolywifi into the dump file. If it is a success, start brute forcing the handshake with dictionary file that contains thousands or millions of words.

Now that WPA handshake is captured between access point anatolywifi and the client (the other pc that were de-authenticated) the brute forcing can be started with the handshake. To begin, use downloaded dictionary files with .txt extensions. These dictionary files will be transferred to same directory as the dump file for convenience purposes.
To test that it works, the WPA-password will be stored in this .txt dictionary file.

Now it is time to brute-force the dump file that captured the handshake (figure 3.20):

- `#aircrack-ng (dump file) -w (dictionary file) [10]`

3.2.3 Cracking WPS

The WPS (Wi-Fi Protected Setup) authentication protocol is used in many homes and small businesses access points. Figure (3.21) illustrates how to crack the PIN code, WPS authentication. The program used is called Reaver. There is a specially designed program to crack WPS enabled access points. This program must be downloaded manually using the terminal, extracted and installed on Backtrack5. [11] [15]

3.2.4 Hi-Jacking

By spoofing the DNS in Backtrack5, redirect all traffic going through the access-point to the Backtrack5 pc. It does not matter what someone does or write on Facebook. The victim will always be connected to the cloned Facebook page that was copied using the Set Tool Kit. [15]

To start this attack, first edit this file as figure (3.22) illustrates.
After the etter.dns file is edited, go to the next step which is to launch Set Tool Kit. The tool Set Tool Kit is integrated in Backtrack5 distribution, so no installation is needed.

To launch this tool kit, enter the command as figure (3.23) illustrates.

- `cd /pentest/exploits/set/` [16]

After the above directory has been changed, write the following command (figure 3.24).

- `./set` [16]

After Set Tool Kit is launched, enter option 1 as figure (3.25) illustrates. [16]
Chapter 3. Network Penetration Attacks

Choose option 2 (figure 3.26). [16]

Choose option 3, in figure (3.27). [16]
Chapter 3. Network Penetration Attacks

Figure (3.27) - Previous menu select. [16]

Choose option 2, in figure (3.28), and it will ask what IP-address that it want to use. [16] Enter the IP-address of the Backtrack5 laptop that is associated with access point anatolywifi.

Figure (3.28) - Previous menu select.

Next the Set tool kit will ask for website that it want to clone [16], so enter www.facebook.com, in figure (3.29).
Open up a new terminal window and enter following command, in figure (3.30). This command starts spoofing the DNS server of the access-point and redirects all traffic that starts with *.facebook.com to 192.168.0.107 (the Backtrack5 laptop). [16] Next it will check the whole subnet mask of the IP range 192.168.0.0 and list all hosts connected to the Access-point.

The command in figure (3.30) uses etter.dns file that was edited in previous snapshots to spoof all traffic to Backtrack PC IP 192.168.0.106.
Chapter 4

4 Results and Analyse

4.1 Results & Analyse Wired Network

This part focuses on the results of Wired Network.

4.1.1 Abuse VLAN Results

If all steps to abuse a VLAN is correct, it should be able to ping to that VLAN that was set up. [3] The first topology that was used did not work. The configuration in the switches and routers was so confusing that a new topology was made with a better configuration and structure. This configuration was probably to secure, because it was impossible to abuse. This is positive, since an extremely safe configuration was included as a bonus.

4.1.2 Password Sniffing Results

In this test it was a success with the sniff telnet password in the cisco router. As figure (4.1) illustrates the tools search through every password that has been typed in the text file. As the figure (4.1) illustrates, the password was cisco. With this information the telnet session with the router and all the fun with the configuration can be started.

![Figure (4.1)](image)

*Figure (4.1) – Password found.*

4.1.3 Account Sniffing Results

When this test was done, the information given was more than expected. The goals were to get the password. But, while logging in to the router via the browser using a
username and password, there were also some more information about the username to the router as figure (4.2) illustrates.

![Figure (4.2) - Router GUI Results.](image]

The only problem with the username was that the last letter or number disappeared. But for the truth it is not hard to guess the last letter or number. In this test the username was KIMDAN and the password was cisco.

4.2 Results & Analyse Wireless Network

This part focuses on the results of Wireless Network.

4.2.1 Cracking of WEP-128bit Results

In this test were 64-bit and 128-bit WEP key cracked. The results went well.

Figure (4.3) shows a 64-bit (10 hexadecimals) WEP key that was configured on the D-Link DIR-615. The 128-bit WEP key (as can be seen in figure (4.4)) is longer and consists of 26 hexadecimals. The procedure is the same for cracking WEP 64 and WEP 128-bit encryption. It may need more data packets from the access point to be able to crack it. But as long as it is managing to gather packets, fake authentication works and the robust fake ARP request on the step 2 command that was used, it should be possible to crack the 128-bit WEP.
Chapter 4. Results and Analyze

4.2.2 Cracking WPA/WPA2 PSK/TKIP Auto Results

In this test it was a success with the cracking. The procedure is the same for all WPA options except EAP that requires a different method that is also harder to crack. The WPA/WPA2 PSK/TKIP make no difference when attacking these dump files, if the handshake is captured from a successful authenticated user with the password cracked in the dictionary file.

In this test the password was found by running a brute force with the downloaded password list. As figure (4.5) illustrates the password was YAMAHA 2013.
4.2.3 Cracking WPS PIN Results

In this test it was a success to crack the WPS pin and also the WPA password. This is a serious vulnerability of WPS-enabled access-point. No matter how strong the WPA password is, the result will be devastating. It will not matter what letters or how long the WPA password is. So it is strongly recommended to turning off WPS on access points.

Figure (4.6) illustrates the result from letting Reaver do its attack on the access-point. After WPS is cracked the Reaver steals the WPA password no matter how the WPA password length and complexity is.
4.2.4 Hi-Jacking Results

In this test it was a success to spoof and see traffic from different hosts trying to access the fake clone of Facebook. As figure (4.7) illustrates both a stationary pc trying to access the fake clone and also Anatolys girlfriend trying to access the page through her iPhone can be seen.

By continuing with this test, the passwords were obtained for those accounts.

Figure (4.7) - Ettercap spoofing command.

Figure (4.8) – Ettercap spoofing Results
Chapter 5

5 Conclusions

Backtrack distribution is a very powerful tool that was used to penetrate network authentication and network protocols. With all the tools that Backtrack have it is possible to steal all sorts of information from end-users without noticing anything.

Throughout this project it was learned and understood how to abuse WEP, WPA, WPS, Facebook, Router & Switch passwords and sniff traffic. When it comes to Abuse VLAN the configuration was probably to secure, because it was impossible to abuse. This is positive, since an extremely safe configuration was included as a bonus.

The weakness and threats of Wi-Fi networks is the most concerning in this project. Wi-Fi-Networks are broadcasting the signals through Wi-Fi channels, mac-address (Media access control) from access-points and by that clients are revealed. The Wi-Fi networks will never be a safe place for businesses and companies.

It is good that companies and organizations know about these threats and use proper security and do not get exploited like the demonstration in this report. It is recommended that companies and business rely on wired networks, such as Fiber Optic Networks.

This project was done on own equipment and lab equipment from Halmstad University. No harm were wished for showing all these attacks that was done and this project has been for learning purposes and all physical equipment used, can be found in Appendix.

The project has been concentrated in two parts, wired and wireless networks. During the time worked on this project, there have been a lot of problems. For each problem solving, there will always be new ones. The biggest problem has been to get the VLAN Abuse to function properly, yet a lot have been learned and a continuation will probably take place for trying to figure out what the problem is even though the project is finished.
Appendix

Appendix A

Figure A.1 - Wired part.

Figure A.2 – Wired Configuration.
Appendix B

Figure A.3 – Wired Network.

Figure B.1 - D-Link DIR-615.
Figure B.2 - D-Link DIR-615.

Figure B.3 - Wireless Card D-Link DWL G122 revision C.
Figure B.4 - Backtrack5 disc.
Acknowledgments

We would like to thank the Halmstad University and Cisco System, Inc. for the equipment that we used. Also big thanks to Olga Torstensson and Malin Bornhager for feedback and excellent job as supervisor and examiner. We would also thank Mati Aharoni, Devon Kearns in Offensive Security for the development of Backtrack 5 R3.
Bibliography


