]HackingTeam[

Vulnerability Assessment on the WiFi Network of XXXXXX Banca

Milano

Hacking Team S.r.l.	http://www.hackingteam.it
Via Moscova, 13 *20121 MILANO (MI) - Italy*	info@hackingteam.it
Tel. +39.02. 29060603	*Fax +39.02.63118946*

DOCUMENT REFINEMENTS		
Version	Date	Revisions
1.0	28 November 2006	First issue
2.0	30 November 2006	Added identity spoofing section
2.1	05 December 2006	Added final vulnerabilities table
2.2	11 December 2006	Added countermeasures
2.3	09 January 2007	Conclusions modified and changes due to customer's feedback

INFORMATION	
Date of Issue	09 January 2007
Version	2.3
Document Type	White paper
Protocol Number	//
Overall Pages	40
Overall Attachments	0
Written by	Julian Rrushi
Approved by	Gianluca Vadruccio

INDEX

1 Executive Summary

This document describes an ethical hacking activity on the WiFi network of XXXXXX Banca carried out for the purpose of assessing its defense from both external and internal attacks. Countermeasures are detailed in the chapter 5, other conclusions and considerations are explained in the chapter 6.

There have been identified some vulnerabilities and security issues which Hacking Team deems appropriate for reporting in this document.
The vulnerabilities found along with the corresponding severity levels are the following:

- The service set identifier *voip* authenticates a wireless client through its data link layer address. By spoofing the data link layer of a legitimate wireless client an attacker may bypass this kind of authentication.
  Severity: Medium

- It has been possible to switch from the service set identifier *voip* to the service set identifier *office* and consequently access *office* resources.
  Severity: Medium

- Two routing switches had a default account enabled and were reachable via telnet.
  Severity: Medium

- It is possible to de-authenticate legitimate clients by spoofing the data link layer address of the access point to which these clients are associated.
  Severity: Low

- The authentication devices of *home* bind an authenticated user with the data link layer address of the machine he is using in that session. It is possible to bypass this authentication mechanism by spoofing the data link layer address of the machine of an authenticated user.
  Severity: Medium

2 Introduction

The IEEE 802.11, also known as WiFi (Wireless Fidelity), is a link layer protocol designed to enable Ethernet connectivity among radio devices operating in a 2.4 GHz spectrum. Networks built upon such protocol are commonly referred to as wireless networks and nowadays represent an easy to deploy networking solution. Wireless networks may be quickly integrated into existing networks, thus their employment is particularly useful in buildings where due do various reasons there are considerable difficulties with deploying wired networks.

One of the main advantages of wireless technology consists in the elimination of the burden derived from handling network cables and related support objects. As a matter of fact wireless networks do not need such cables at all. Furthermore, with such networks it is quite easy to change the work place as long as it remains within the wireless network coverage area.

Wireless technology was first invented around 20 years ago when there were deployed the very first networks which communicated through radio waves rather than cables. Nevertheless, till a few years ago there were just a few wireless local area networks (WLANs) actually deployed as wireless networks were characterized by a low transmission rate, high costs, lack of security standards, lack of interoperability with wired network devices, etc.

In their actual state wireless networks are cost effective due to the technological evolution they brought. Consequently wireless networks are widespread actually, their performance is comparable to wired networks, and companies have the possibility to integrate them into the enterprise wired network. Furthermore, WLANs will continue to grow as organizations find it more cost effective to build out networks using WiFi as opposed to cabling.

Nevertheless, if on one hand wireless networks provide undeniable advantages, on the other hand they may be exposed to serious security attacks and consequently introduce a considerable risk factor on a whole company network. Therefore the employment of WiFi technology within a company networking infrastructure should be supported by a strict security policy whose goal should be the prevention of possible attacks to wireless networks which could have a negative impact on the overall business of an entire company.

3 Attacks to XXXXXX Bank's WiFi Networks performed

Wireless networks could be exposed to security attacks as a consequence of weaknesses in both design and implementation of various standards widely deployed in such networks. Attack scenarios may vary according to the circumstances under which they take place. Nevertheless, from a high level point of view attacks to wireless networks may be categorized as follows:

- abusive introduction of wireless rogue devices
- interception
- jamming
- client to client attacks
- brute force attacks versus access points
- cryptographic attacks
- misconfiguration
- impersonation

An in depth understanding of how these attacks work and how this knowledge could be used to prevent them is of paramount importance to the design of an effective security policy.

3.1 Abusive Introduction of Wireless Rogue Devices

These attacks consist in unauthorized introduction of wireless devices into a wireless network for the purpose of defeating the architectural based security and possibly creating abusive wireless networks. There are generally two attack scenarios, namely:

1. Rogue clients: an attacker through a rogue system, usually a laptop, could try to abusively connect to an access point, particularly if the later is not configured to somehow authenticate clients before connecting them to the wireless network.
2. Rogue access points: an attacker could install a rogue highly insecure access point which gives away the access to network resources.

Both of these attack scenarios aim at gaining unauthorized access to the wireless network and in the worst case could allow penetration to the company's wired network resources.

3.2 Interception

In wireless networks an attacker could sniff the communication between legitimate wireless devices. In wireless networks such an attack is much more realistic than in wired networks as radio signals are omnidirectional. Thus, all an attacker has to do to sniff a wireless network is to be within its coverage area or to use a proper antenna to be able to act even 1000 m away from the access point. Under lack of protection mechanisms a passive analysis of intercepted traffic and/or clonation of a legitimate access point could enable an attacker to view sensitive plain text data and possibly reveal access credentials to the company's applications or operating systems.

3.3 Jamming, Flooding and Disassociation/De-authentication

Denial of Service attacks are easy to carry out against wireless networks. Such attacks may take place at the physical, data link and network layer of the OSI model.

With regard to the application of denial of service attacks at the physical level an attacker could employ a specialized device referred to as jammer which emits strong radio frequency signals that do not follow an underlying data link protocol. Jamming introduces packet collisions that cause repeated back off. As a consequence of jamming legitimate wireless devices could be prevented from communicating.

Denial of service attacks carried out at data link layer can either target a specific host or the entire wireless network. Such attacks consist in injecting a large quantity of de-associate or de-authenticate packets into the wireless network in order to flood legitimate wireless clients and disable their ability to access the local network.

At network level denial of service attacks may be carried out by sending large amounts of data for the purpose of exhausting the bandwidth of a target wireless network. As a consequence of such attack the target wireless network will be forced to drop packets. Furthermore, such attack also consumes considerable computational resources of access points.

3.4 Client to Client Attacks

A wireless network may be configured to operate in Ad-Hoc mode in which wireless clients can communicate directly with each other, i.e. without going through the access point of their service set identifier. This connectivity allows a wireless client to perform traditional attacks against another wireless client for the purpose of gaining control of its operating system or causing dysfunction in it.

3.5 Dictionary and Brute Force Attacks vs. Access Points

Various security mechanisms authenticate wireless clients through a single common password. This fact opens the way to dictionary and brute force attacks. A dictionary attack tries every word in a defined dictionary as a possible password, while a brute force attack tries every possible password till it finds the right one. These attacks are widespread actually and their negative impact on the security of wireless networks is noticeable.

3.6 Cryptographic Attacks

The attacks to cryptographic protocols employed by wireless networks generally are of high complexity. Nevertheless, discovery of such attacks is usually followed by the implementation of hacking tools which are then made publicly available.
WEP (Wired Equivalent Privacy) is a cryptographic protocol part of the IEEE 802.11 wireless networking standard to secure WiFi networks which has been subject to various attacks, namely:

- passive statistical attack built upon a statistical analysis of intercepted communication
- active attack injecting new packets built upon knowledge obtained by an analysis of intercepted plain text
- active attack based on a security break of an access point
- active attack based on a real-time interception during intervals in the order of several days allowing real-time traffic decryption attempts

Both 40-bits and128-bits WEP are susceptible to the aforementioned attacks.

WPA protocol (WiFi Protected Access) is much more resistant to cryptanalysis and statistical attacks than WEP, thus it represents a viable substitute for WEP.

3.7 Misconfiguration

Wireless access points which are improperly configured enable an attacker to compromise the security of the corresponding wireless network. Access points usually do not come configured with an authentication mechanism. Furthermore, centralized configuration control often result to be difficult, default configurations are used, and organizations happen to be oriented towards functionality considering security as a second hand issue. Distributed access points under these

conditions have a high likelihood of being improperly configured, consequently leading to exploitation.

3.8 Impersonation

During an impersonation attack in a wireless network an attacker takes on the address of a valid wireless client or access point and tries to access the services which those valid clients or access points are authorized to access. In another form of such attack an attacker impersonates an access point and lures wireless clients into connecting with it, fact that would reveal their credentials.

4 Security Evaluation of the WiFi Network and results

4.1 Hacking Tools Employed

The vulnerability assessment activity on the WiFi network of XXXXXX Banca has been supported by the following wireless hacking tools:

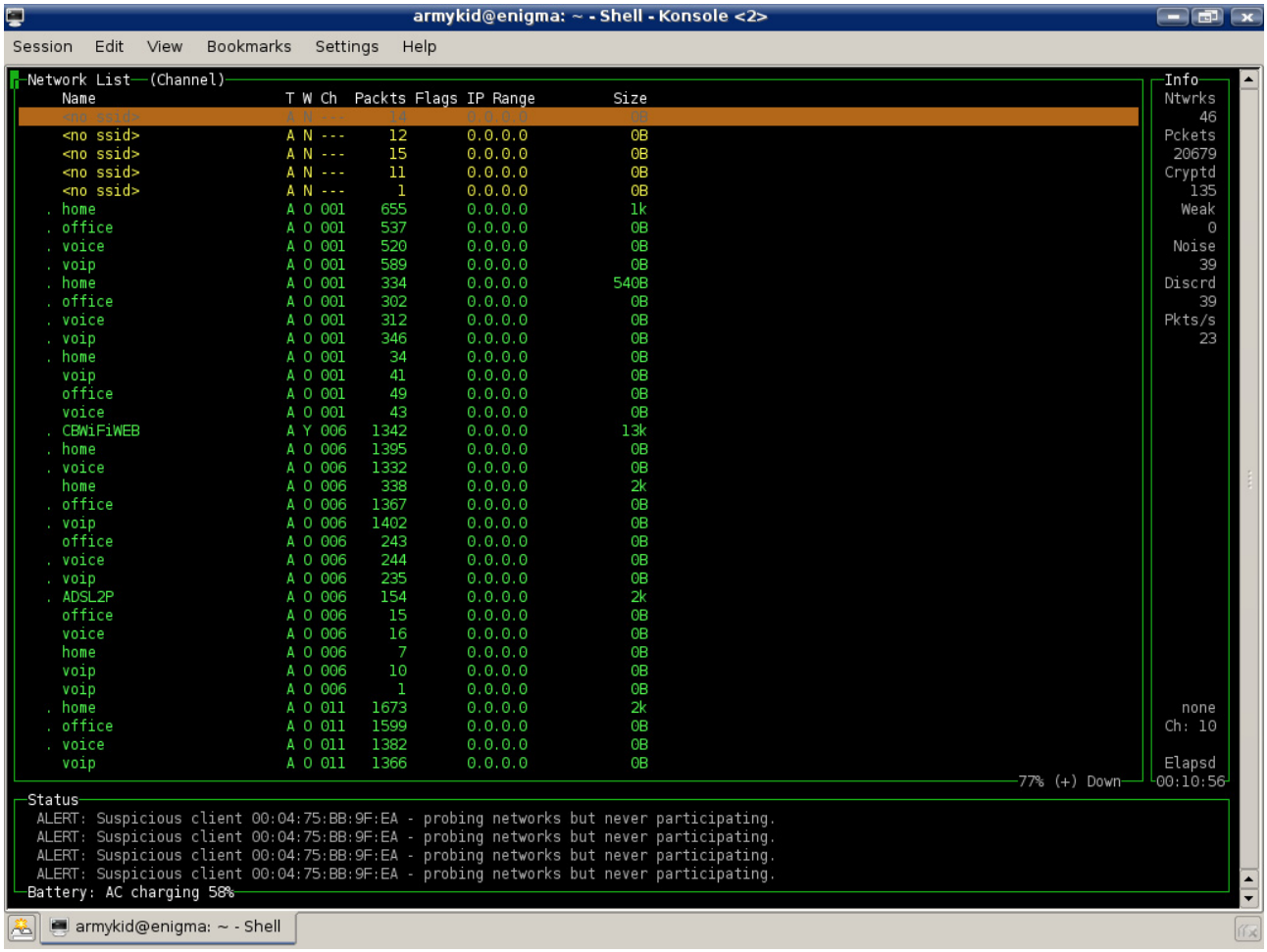
- *Kismet* used for detecting wireless networks and sniffing 812.11 traffic.
- *Airodump* used for dumping packets directly from a WLAN interface.
- *Aircrack* used for carrying out a dictionary attack against WPA for the purpose of finding the connection pass phrase.
- *Aireplay* used to inject data into the WiFi network of XXXXXX Banca. This tool forced access points to respond with encrypted packets.
- *Airdecap* used to decrypt WPA encrypted traffic.
- *Airsnarf* used for carrying out an impersonation attack.
- *Iwlist* for getting quantitative information about access points within range.
- A program developed by us to generate random words which could to be used in a brute force attack against WPA.

4.2 Reconnaissance

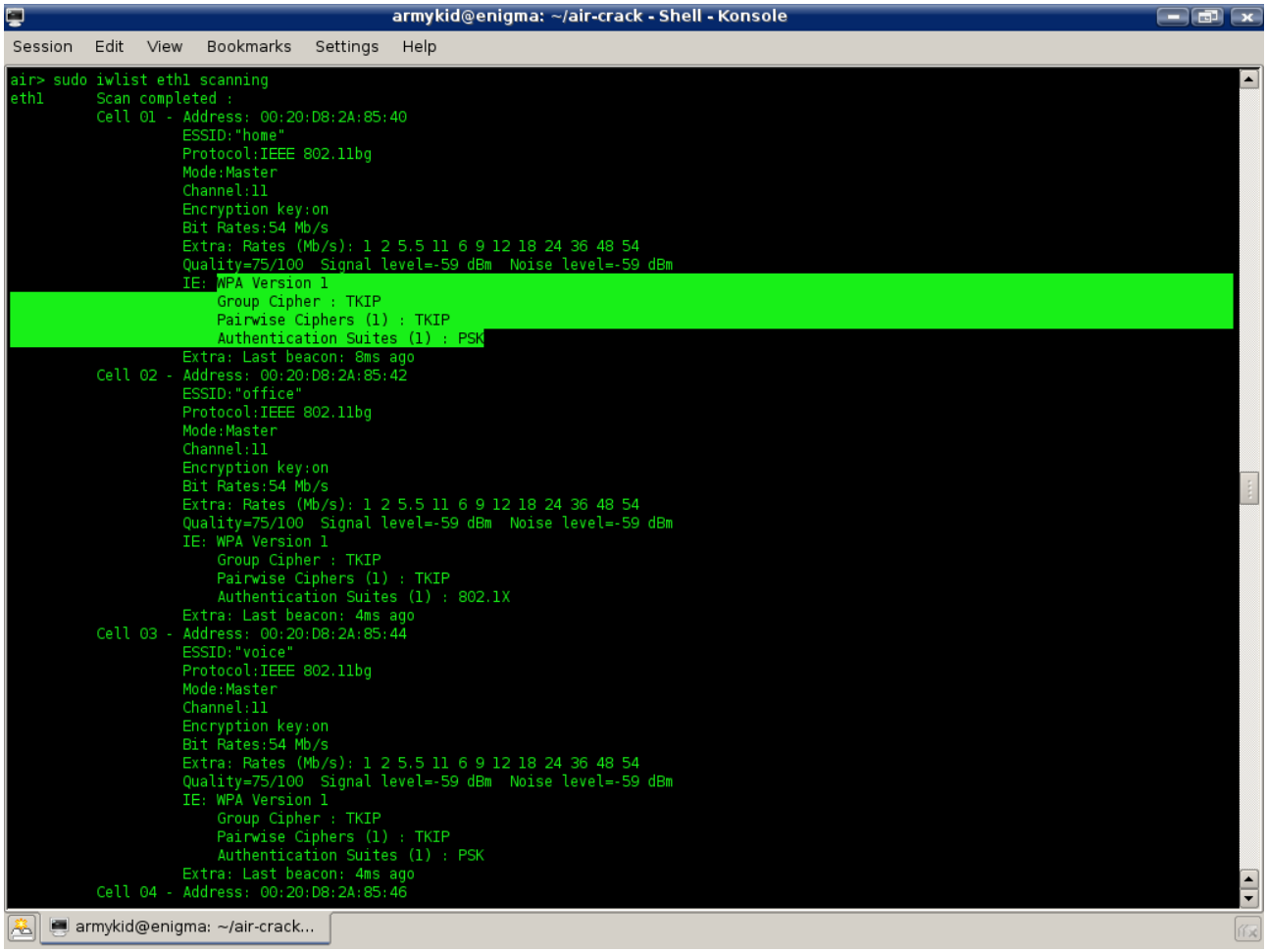
The very first step of the vulnerability assessment on the WiFi network of XXXXXX Banca consisted in acquiring as much information as possible on its organization and configuration. By employing *kismet* it has been possible to observe the existence of the service set identifiers which identify cells that were to be subject of our vulnerability assessment activity. More in detail, among other service set identifiers within range kismet located our target service set identifiers currently in use by XXXXXX Banca, namely office, home, voip, and voice. With kismet it was possible to determine the transmission channels, namely 1, 6, and 11.

With iwlist and kismet it has been possible to acquire detailed information about each service set identifier such as the security protocol employed (WPA), the 802.11 standard utilized (802.11bg), the number of clients actually connected at a certain moment, the data link layer address of legitimate clients, and the link layer address of legitimate access points.

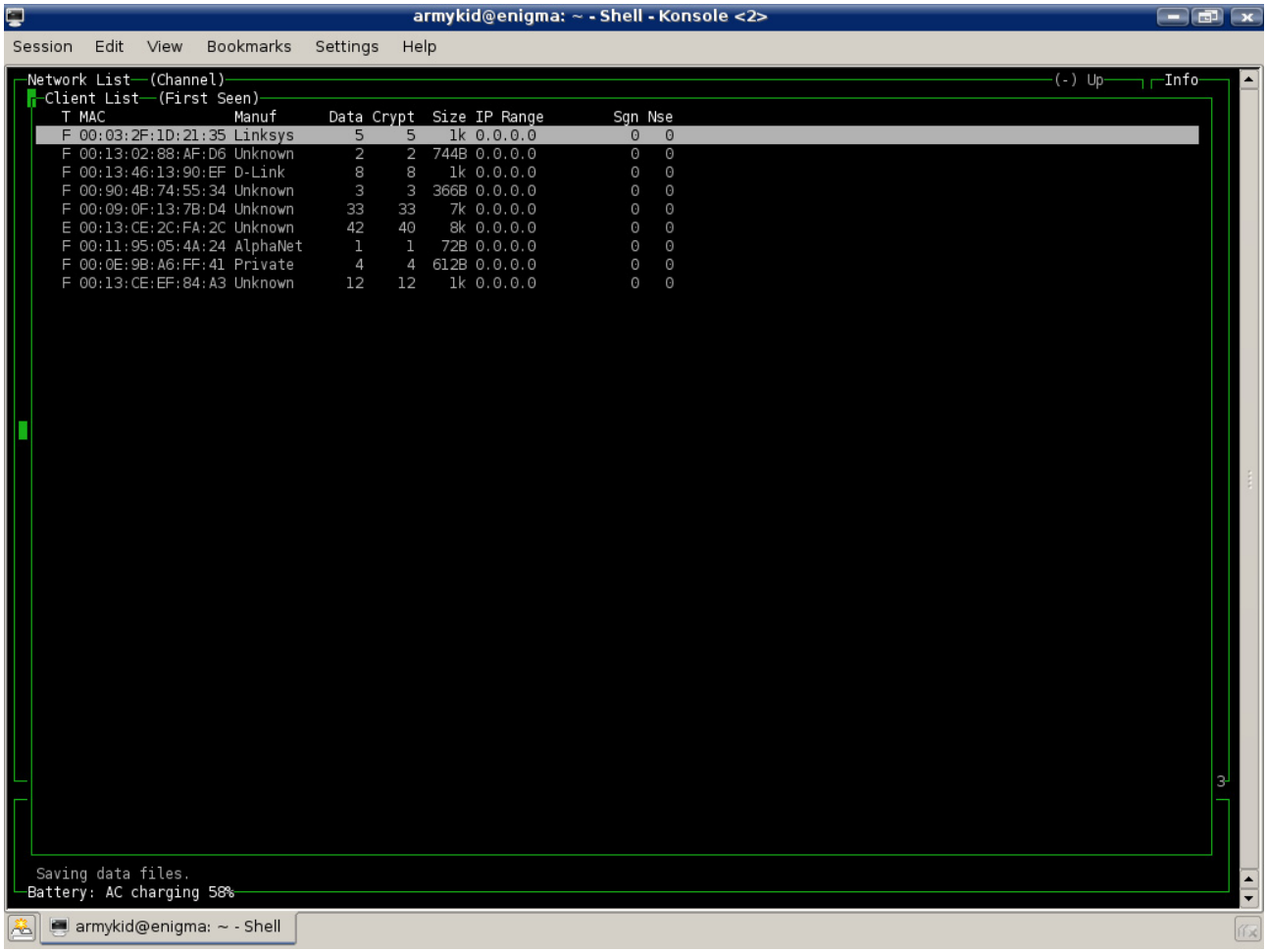
1) A list of service set identifiers within range. Among them we can identify home, office, voip, and voice. In adittion, there is also a definition of the transmission channels.



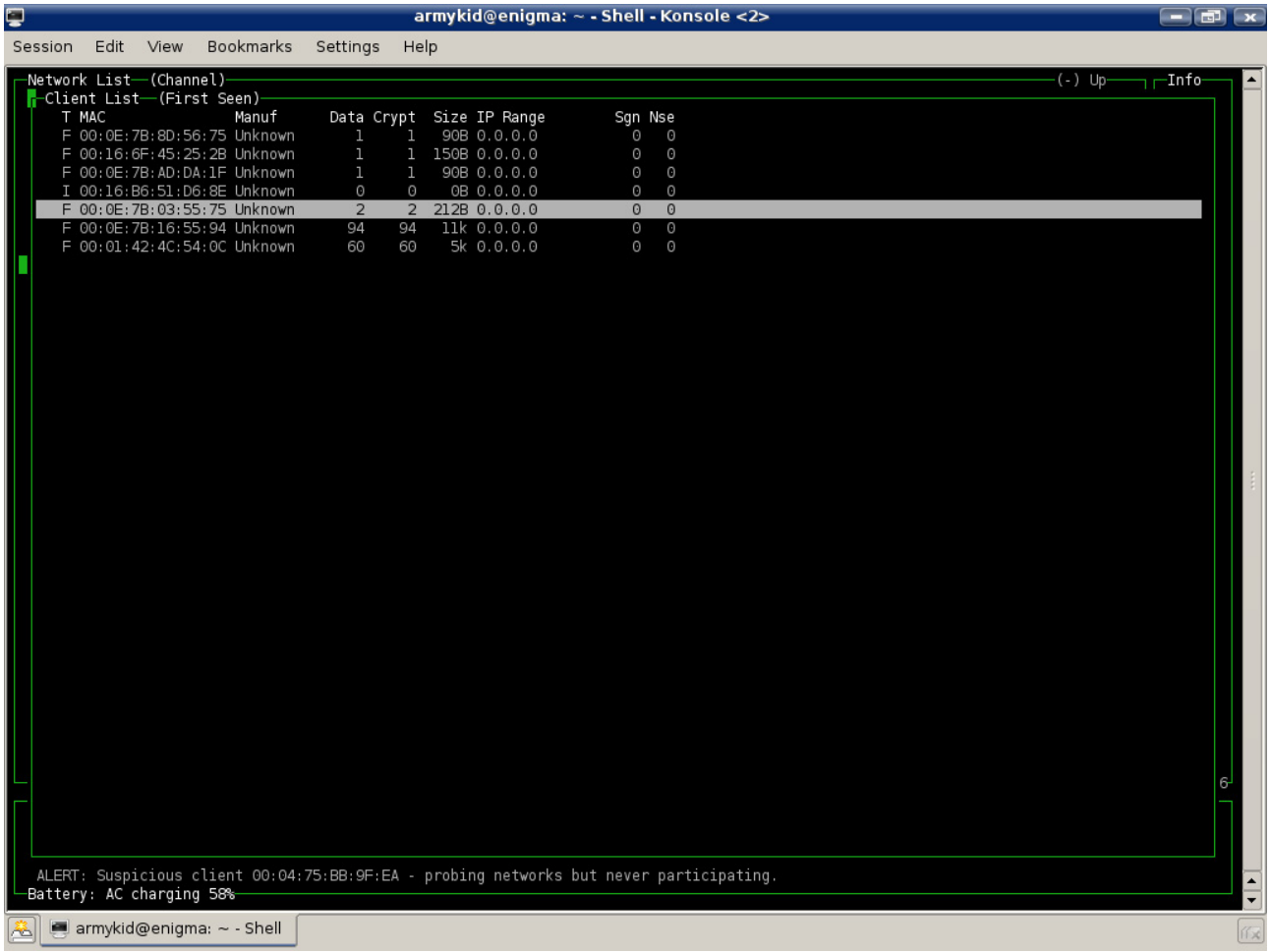
2) Detailed information about the security protocol currently in use.



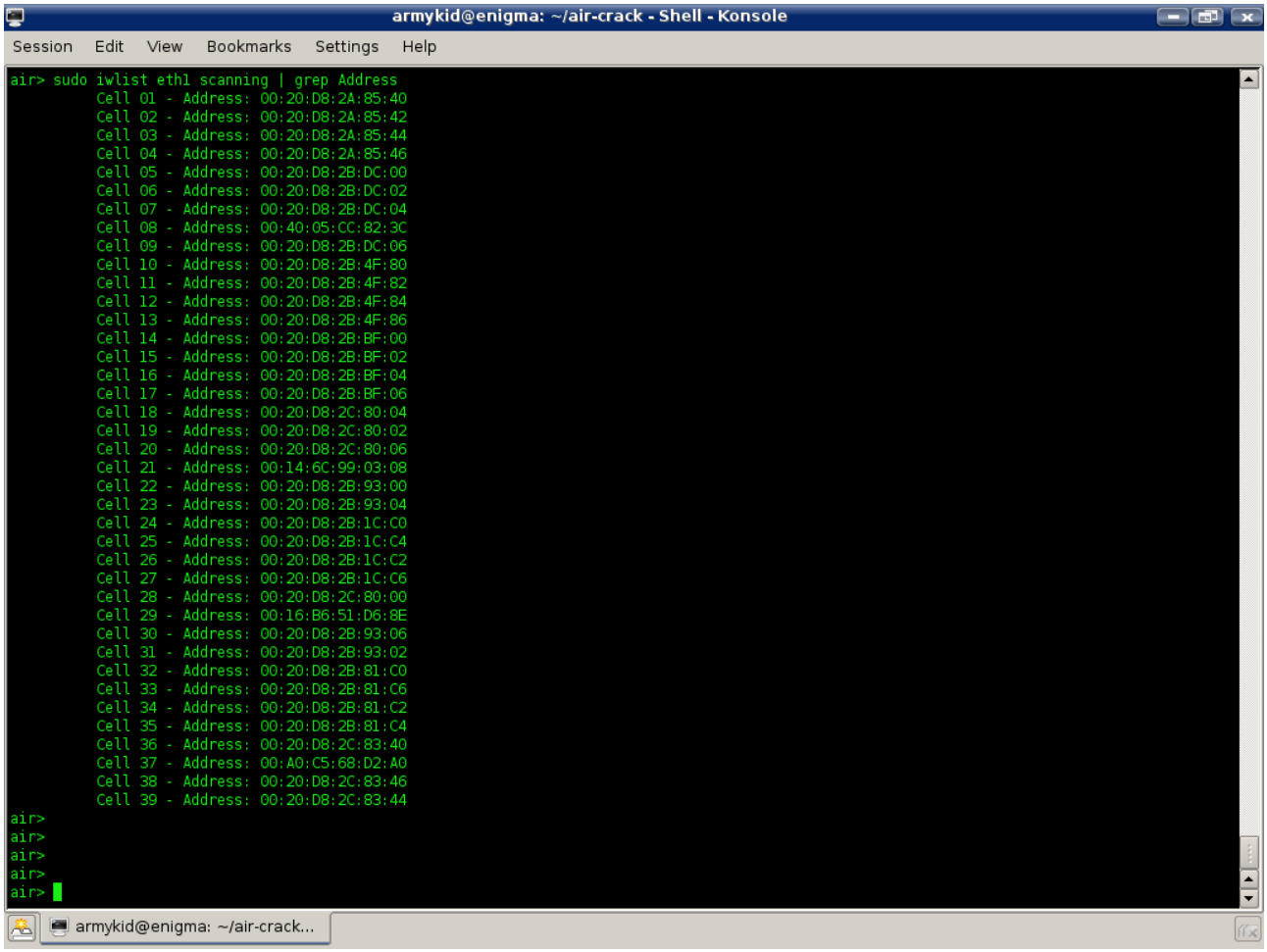
3) A list of data link layer addresses which belong to legitimate wireless clients.



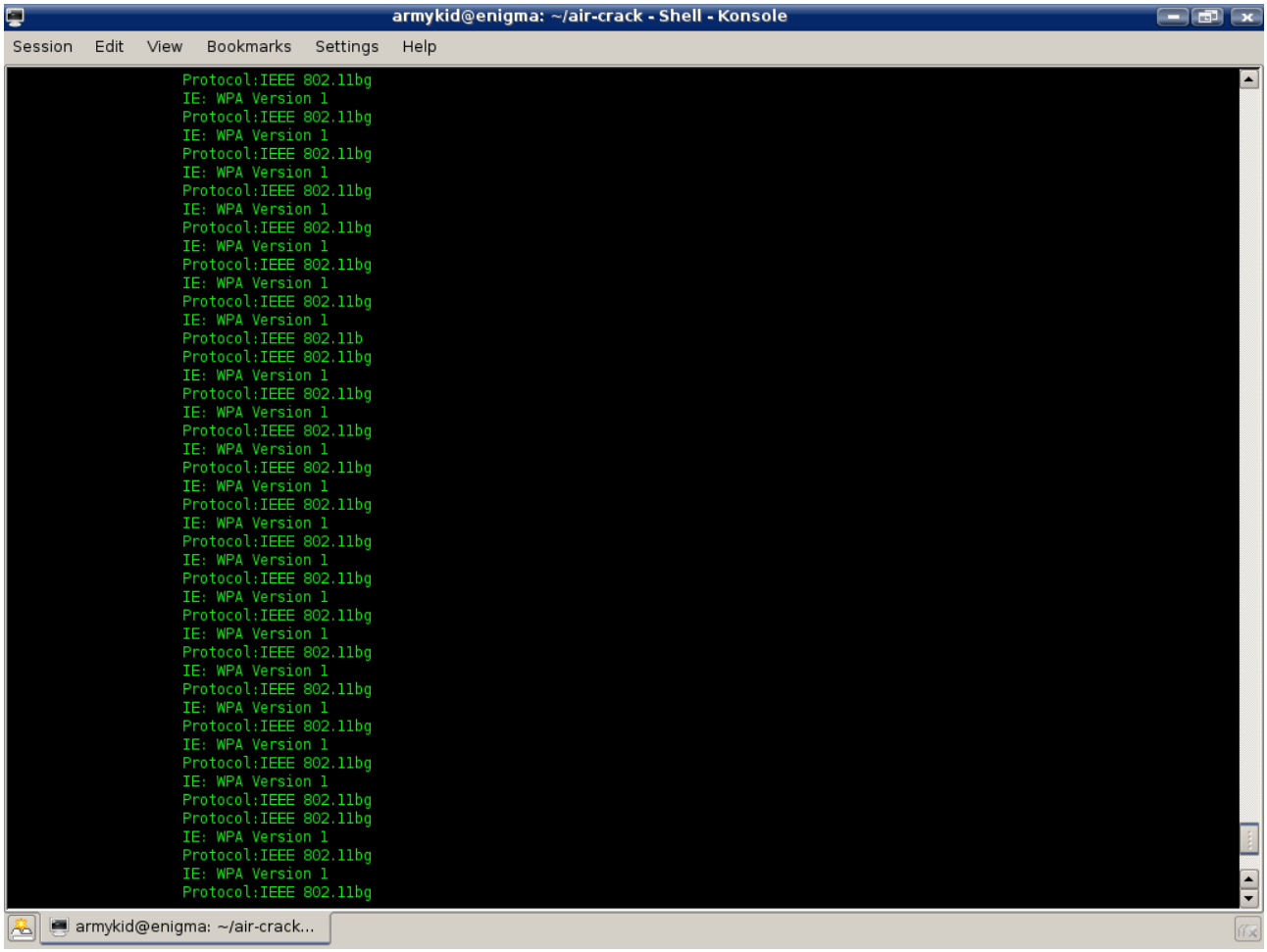
4) Another list of data link layer addresses which belong to legitimate wireless clients.



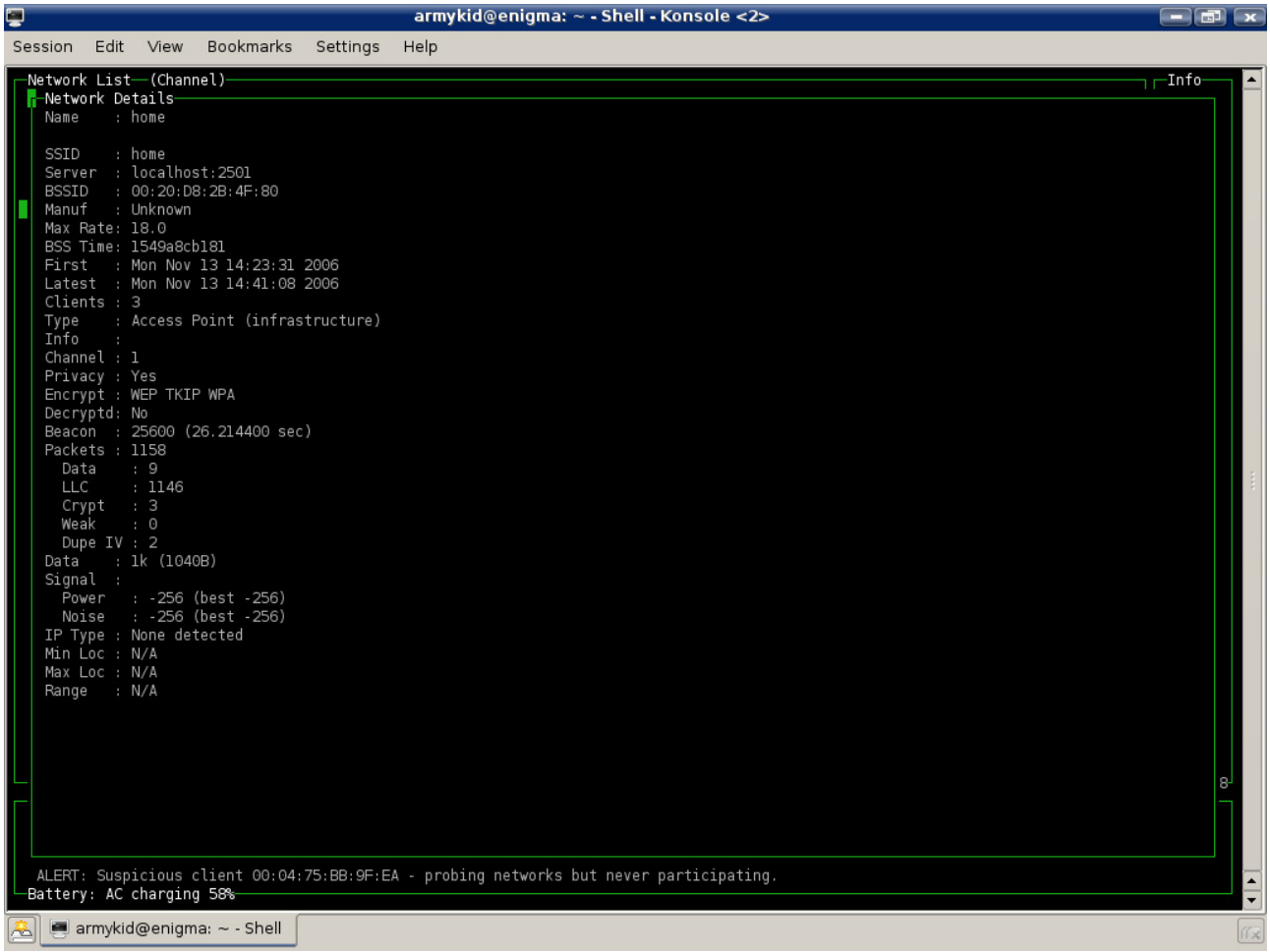
5) A list of data link layer addresses which belong to access points within range.



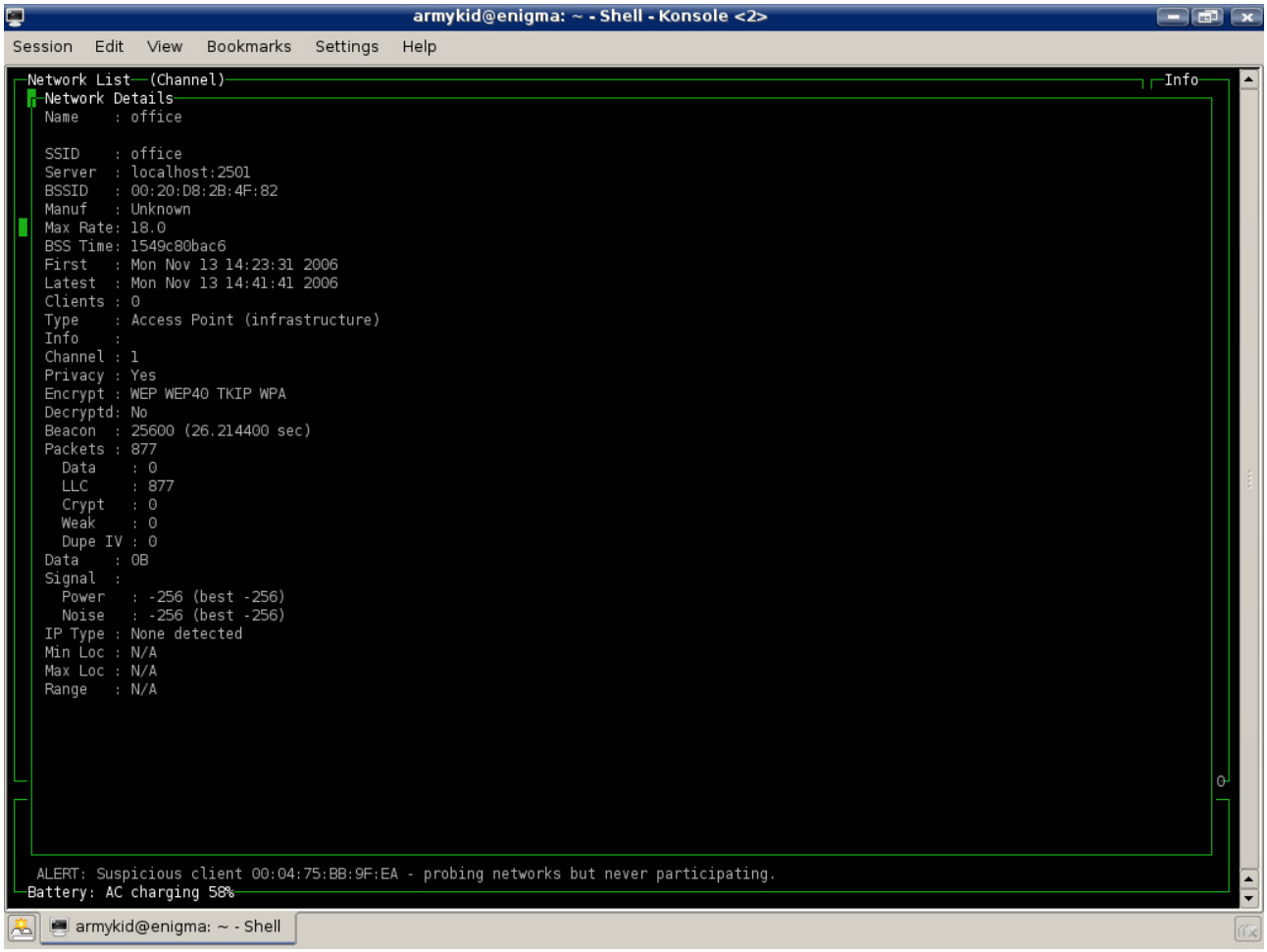
6) The 801.11 standard in use.



7) Example of detailed information about a target service set identifier.



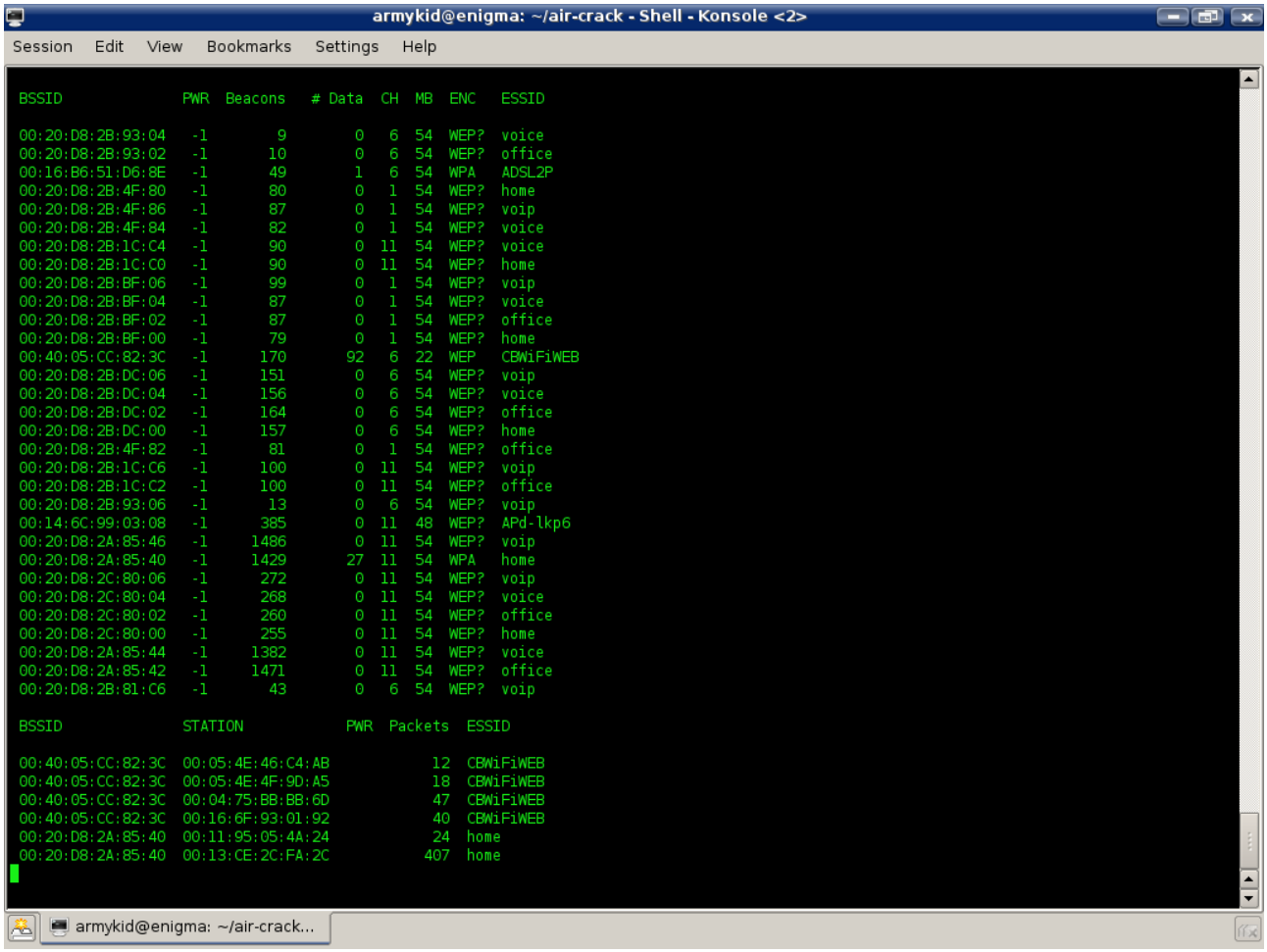
8) Another example of detailed information about a target service set identifier.



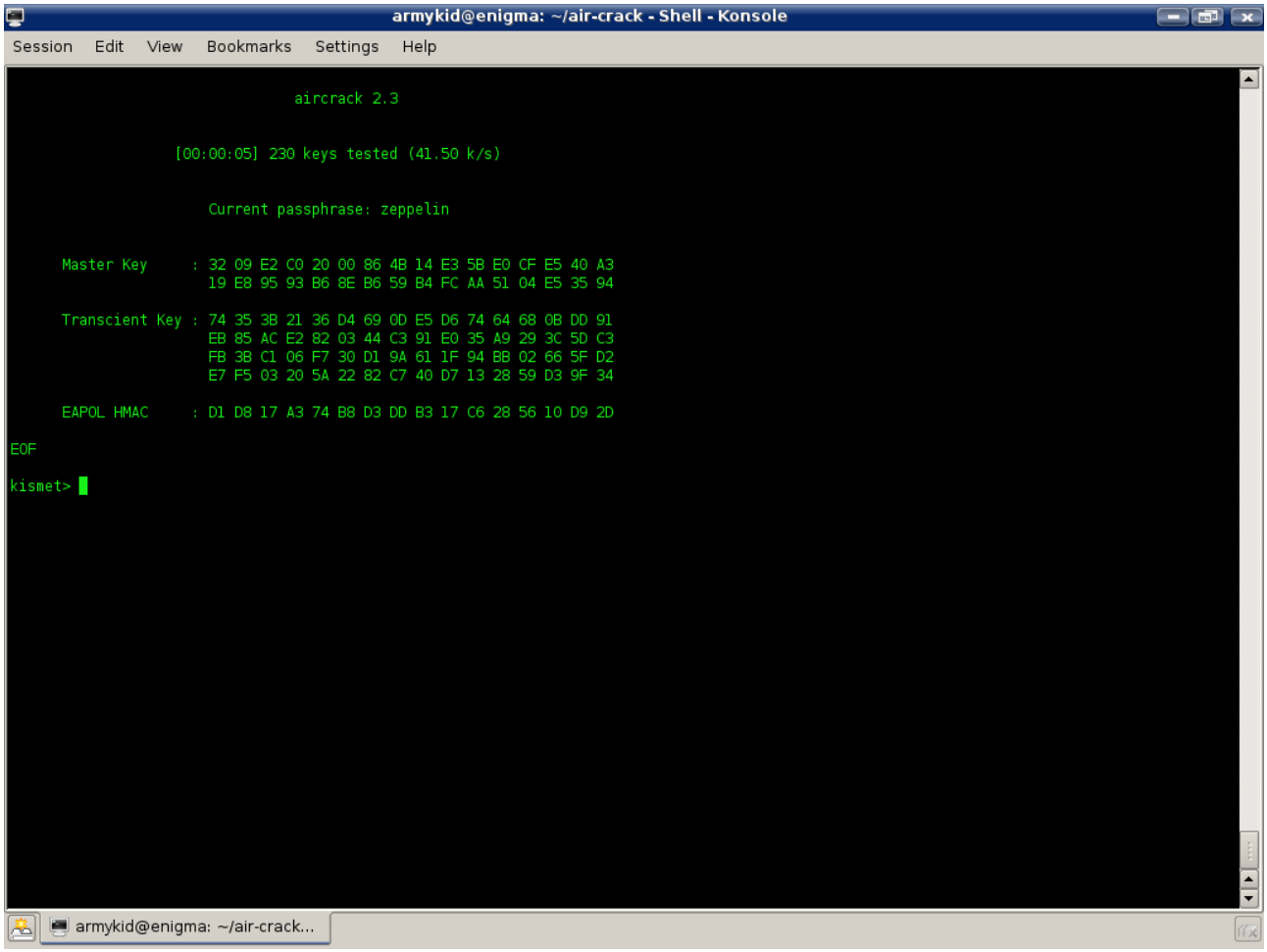
4.3 External Attacks

The connectivity to the WiFi network of XXXXXX Banca is protected by WPA, thus an attacker has to find the pass phrase in order to be able to connect to this network. WPA currently resists to cryptanalysis and statistical attacks. The only attack actually feasible to find the pass phrase is a dictionary attack. We gathered packets with airodump and fed them to aircrack for the purpose of carrying out a dictionary attack. We used a dictionary of Italian words and another one containing common passwords. Non of these dictionaries contained the right pass phrase. In order to accordingly distribute both assessment efforts and time we did non insist on the dictionary attack. Nevertheless, a dedicated attacker would spend much more time and computational resources on this objective, and would use huge dictionaries possibly composed of combination of a base word with other characters, combination of two or more standard language words, etc. There exist efficient tools which generate potentially dangerous dictionaries for use in dictionary attacks. We ourselves coded a program which generates random passwords of a defined length.

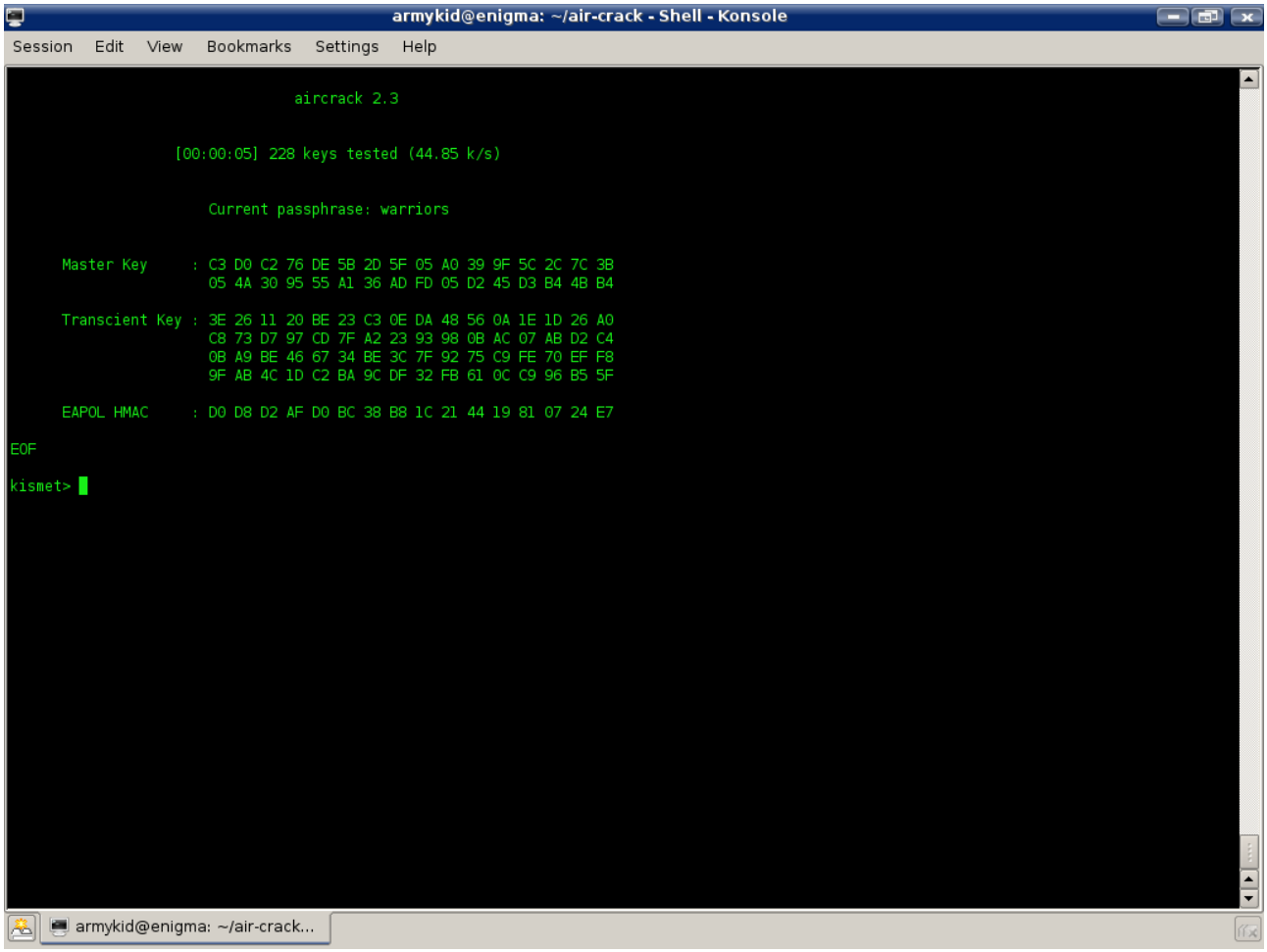
1) Airodump dumping packets which will be used by the dictionary attack.



2) Aircrack carrying out a dictionary attack using an Italian words dictionary.



3) Aircrack carrying out a dictionary attack using a dictionary of common passphrases.



4.4 White-Box Vulnerability Evaluation

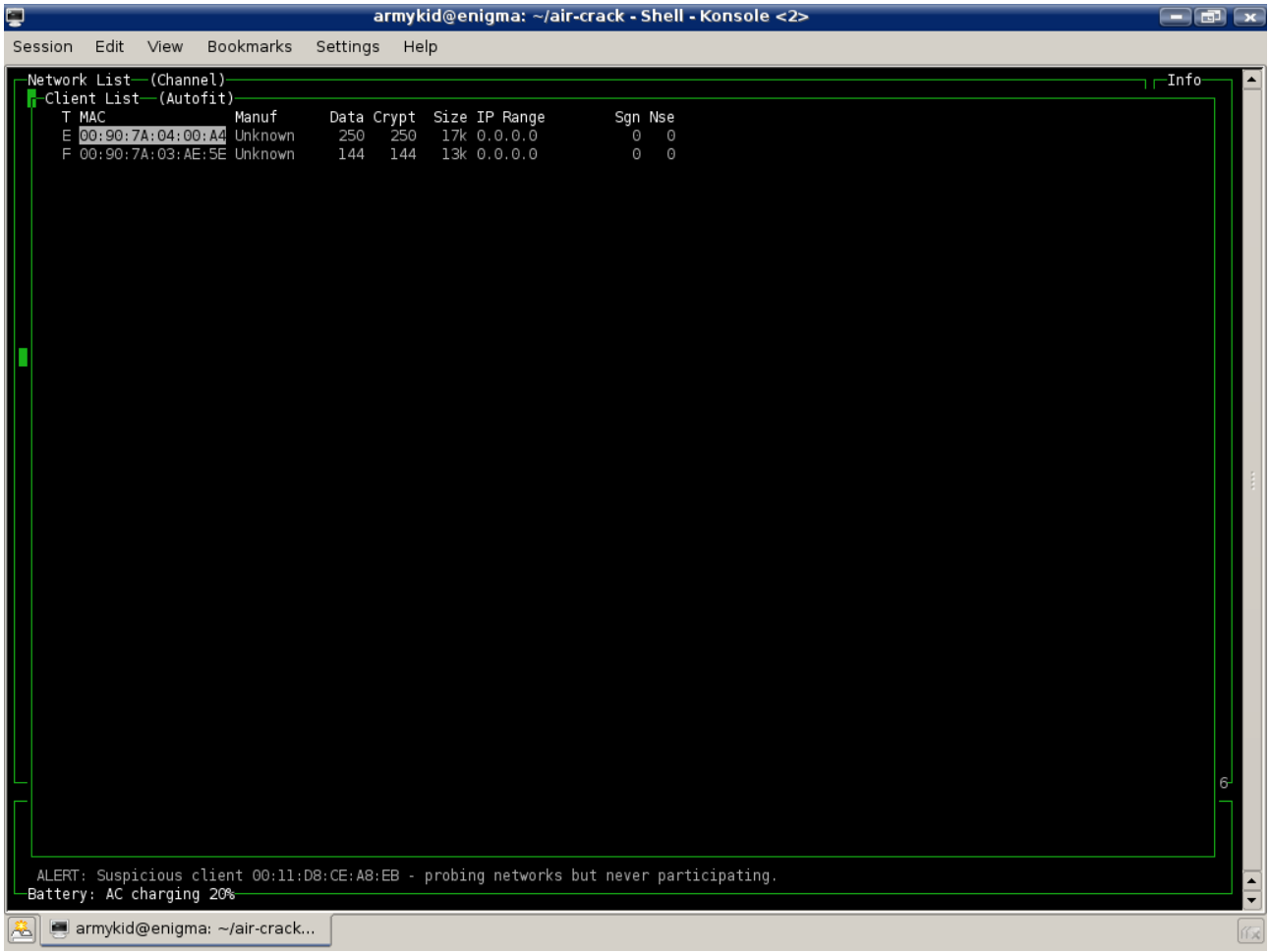
At this stage we were given the WPA pass phrase, namely *"XXXXXXone"*. Such pass phrase is 9 bytes long and is composed of lower case letters only. The WPA pass phrase should be a random sequence of either characters (upper and lower case letters, numbers, and punctuation) or hexadecimal digits (numbers 0-9 and letters A-F). In either case the pass phrase should be sufficiently long to resist to brute force attacks. In fact it may be up to 63 bytes long. Longer and the more random the WPA password, the safer it is to use. We coded a randomly word generation program and reached the "*XXXXXX*" pass phrase in just **45-60 minutes**, while the whole pass phrase *"XXXXXXone"* requires much more time but it is still possible to reach it using computer clusters.

4.4.1 Bypassing authentication in SSID voip

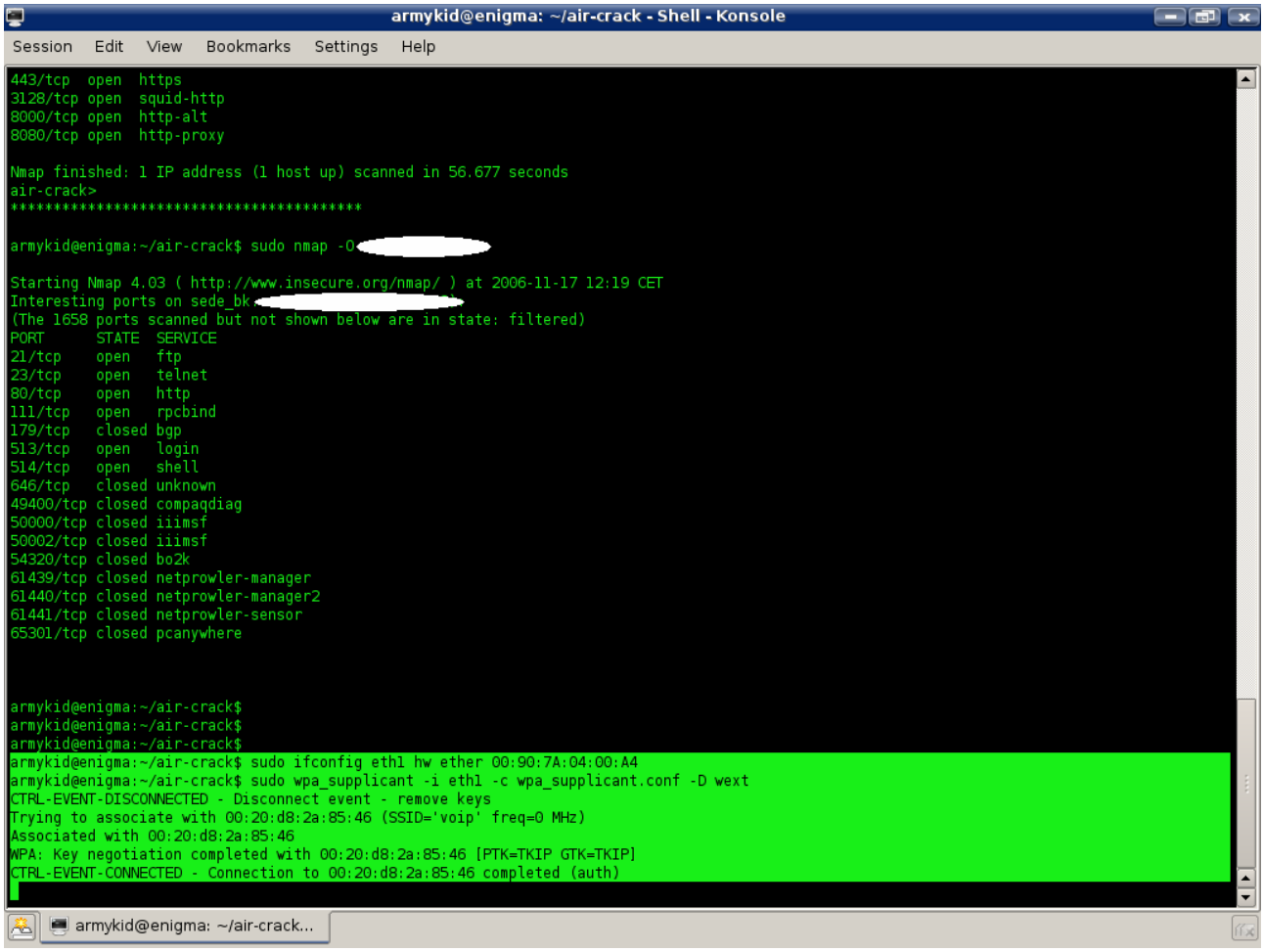
The service set identifier voip authenticates wireless clients upon their data link layer address. After the authentication a DHCP (dynamic host configuration protocol) server assigns to each one of the authenticated clients a dynamic IP address and sends them routing and domain name information.

As we had already acquired a list of data link layer addresses of legitimate wireless clients, all we had to do to bypass such authentication was to change the data link layer address of the wireless network card used by our attacking machine and set it to one of the authorized data link layer addresses. After that we send DHCP requests to the DHCP server which went ahead and assigned a dynamic address to our attacking machine along with sending routing and DNS information.

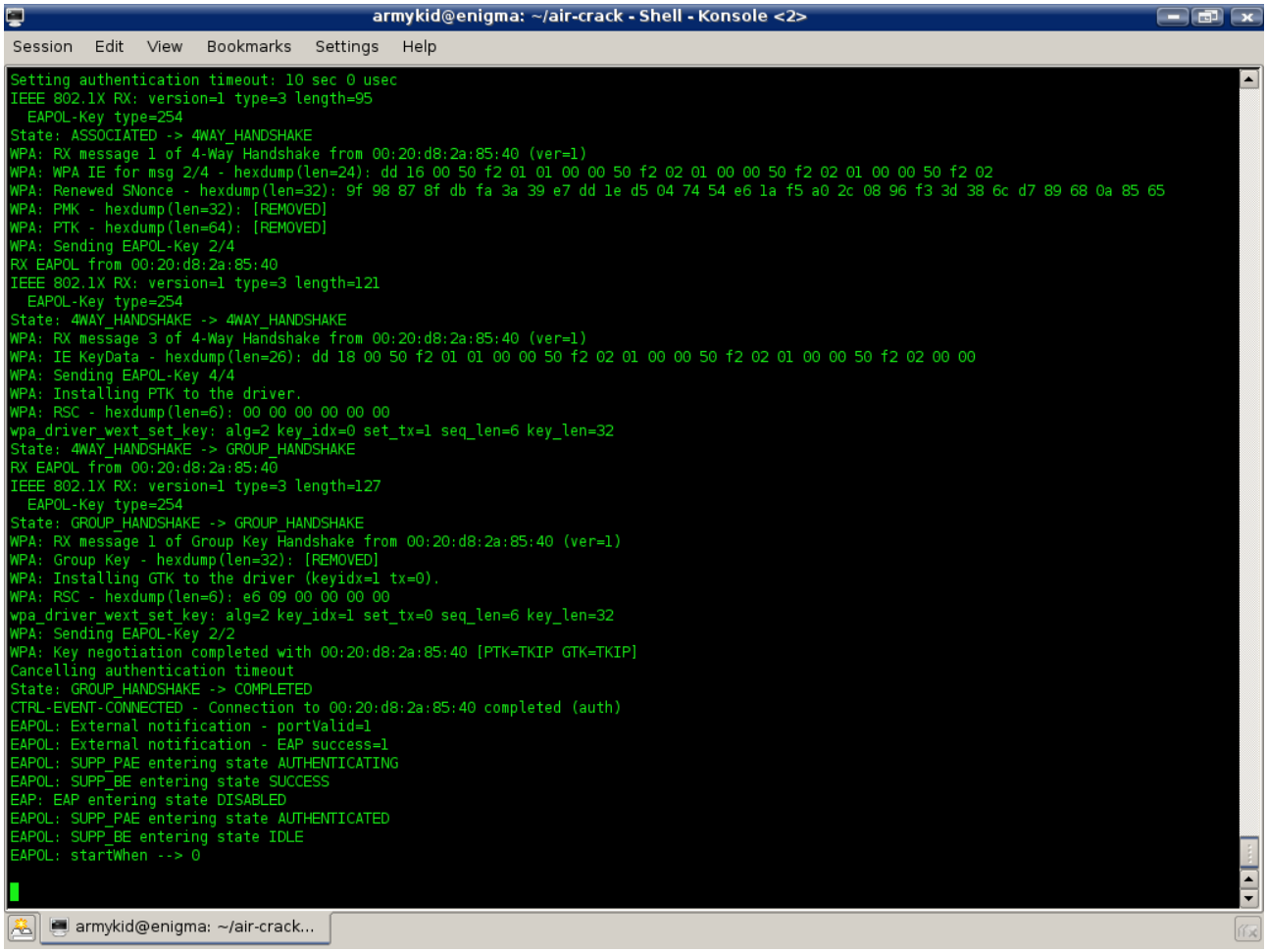
1) One of the data link layer addresses we could spoof for the purpose of bypassing authentication.



2) The operation of assigning a spoofed data link layer address to our attacking machine.



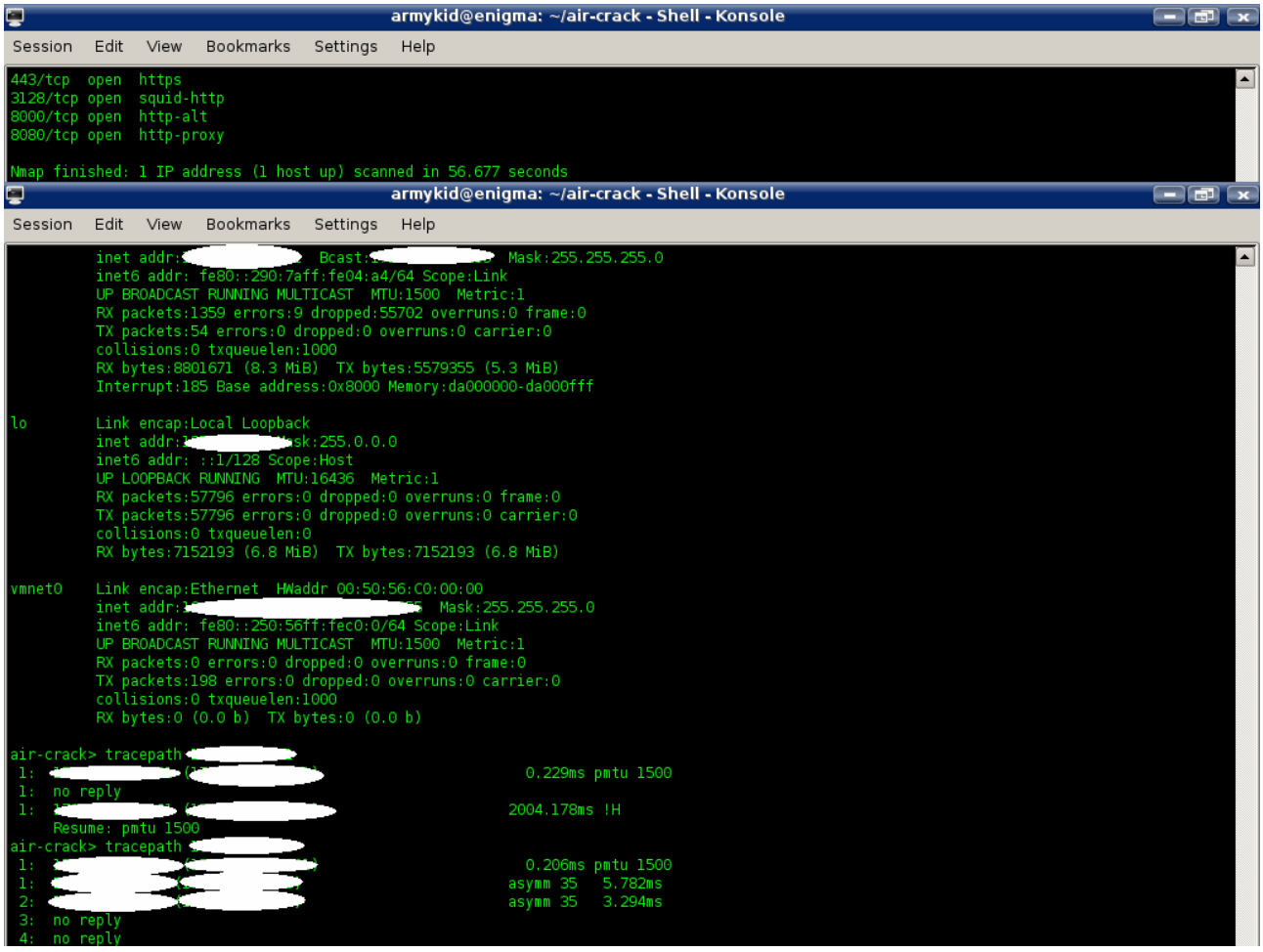
3) A successful connection with a spoofed data link layer address.



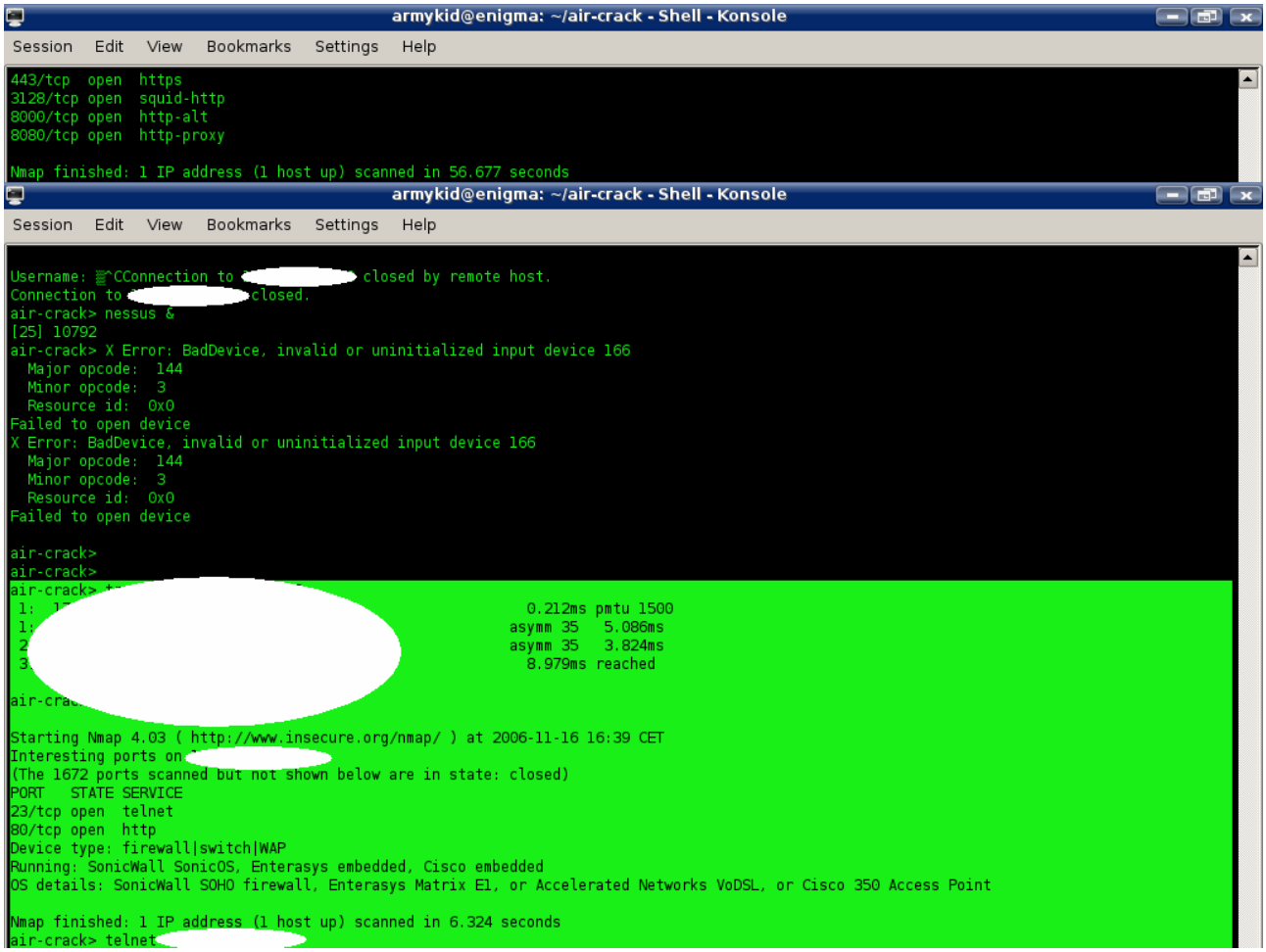
4.4.2 Network Security Misconfiguration

During the vulnerability assessment on the WiFi network of XXXXXX Banca it was found that critical resources which are intended to be accessed by authenticated wireless clients connected to other service set identifiers such as office may be accessed by clients connected to voip. Although the service set identifier office is protected by public key cryptography, whatever client who successfully authenticated to voip could reach office resources. After we spoofed the data link layer address and received dynamic network information in the service set identifier voip, we were able to reach office resources whose access would require an authentication to the service set identifier office.

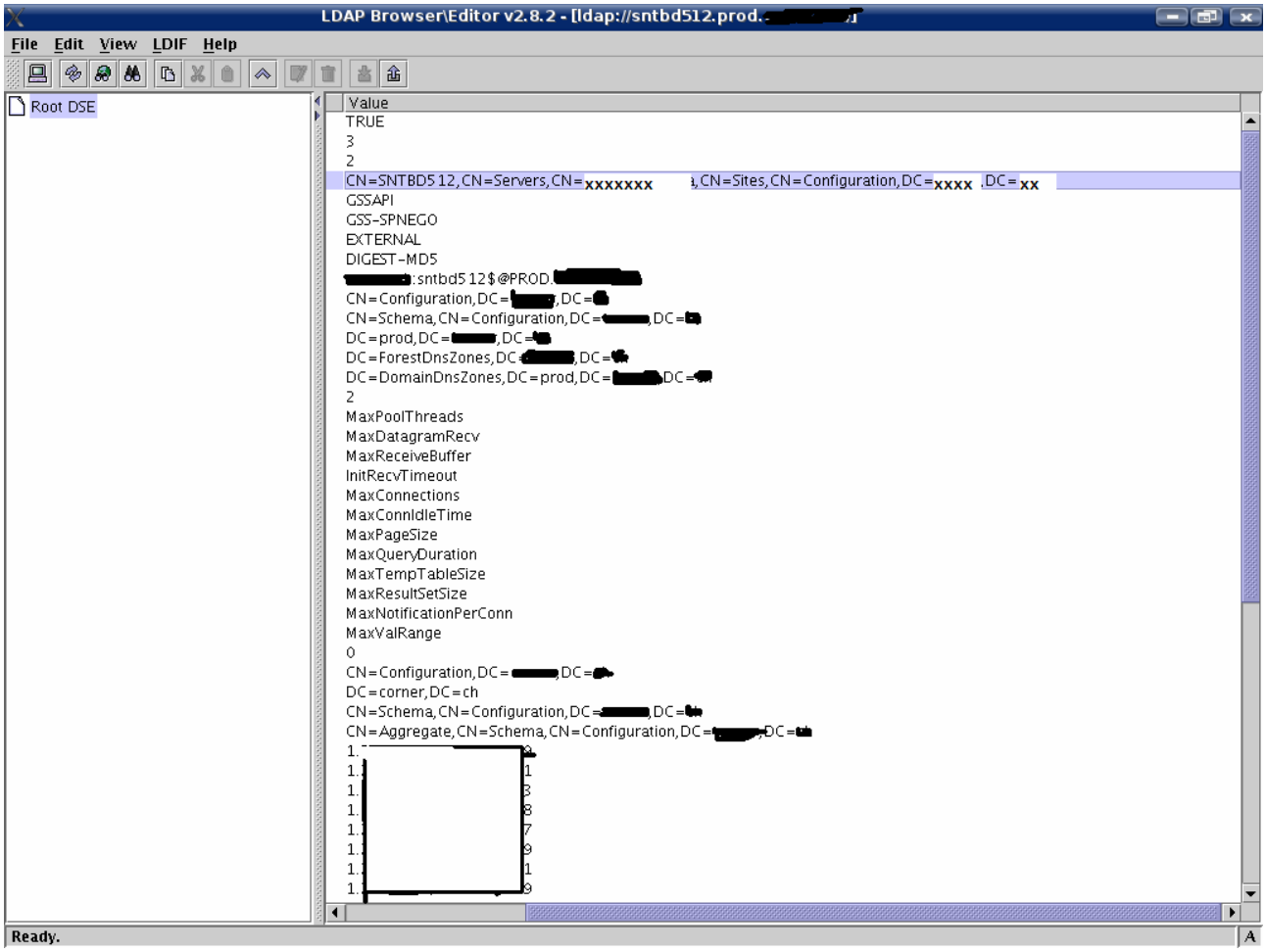
1) Verifying connectivity to critical systems (part 1).



2) Verifying connectivity to critical systems (part 2).

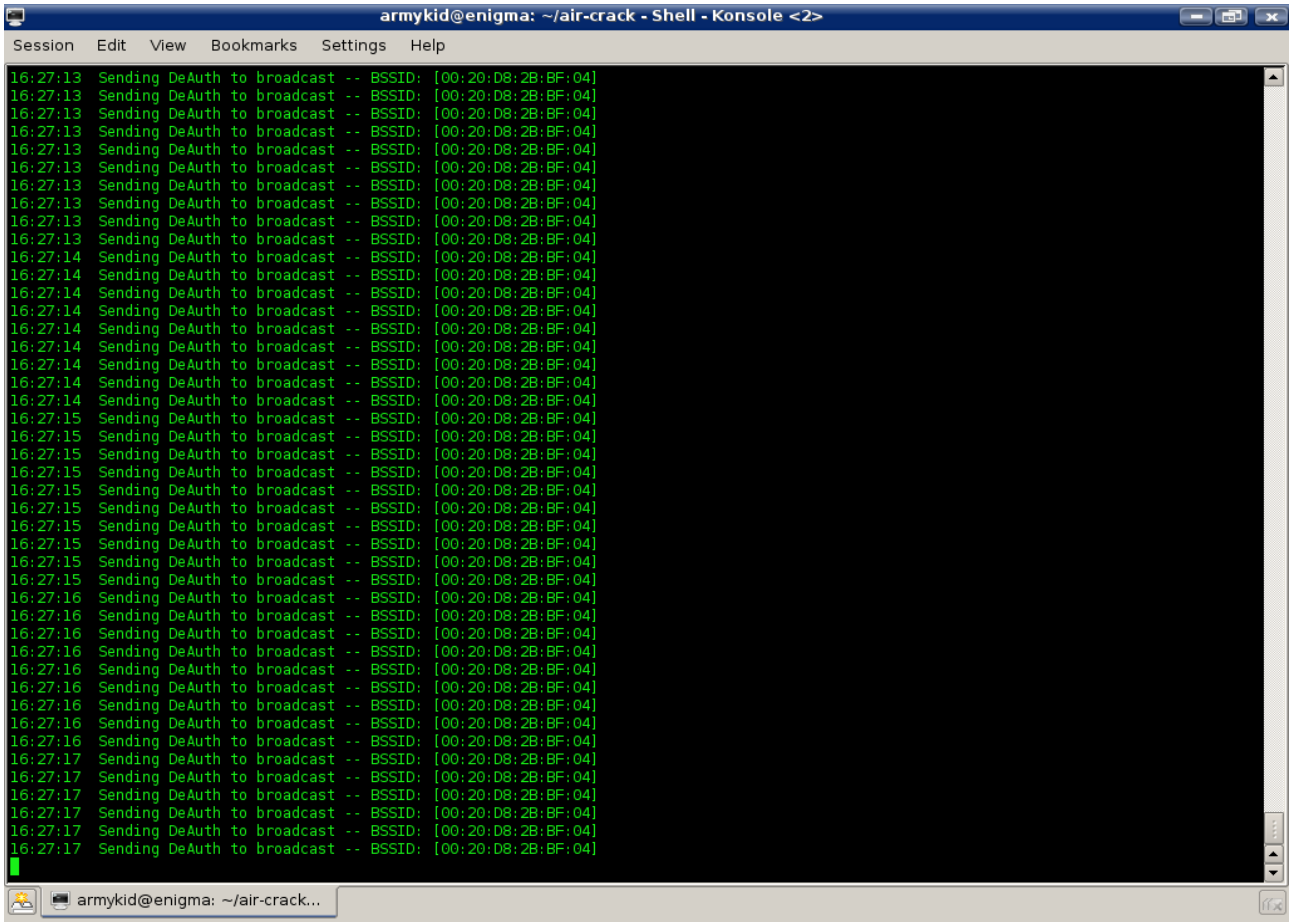


3) Accessing an LDAP server once inside.



4.4.3 Denial of Service Attacks

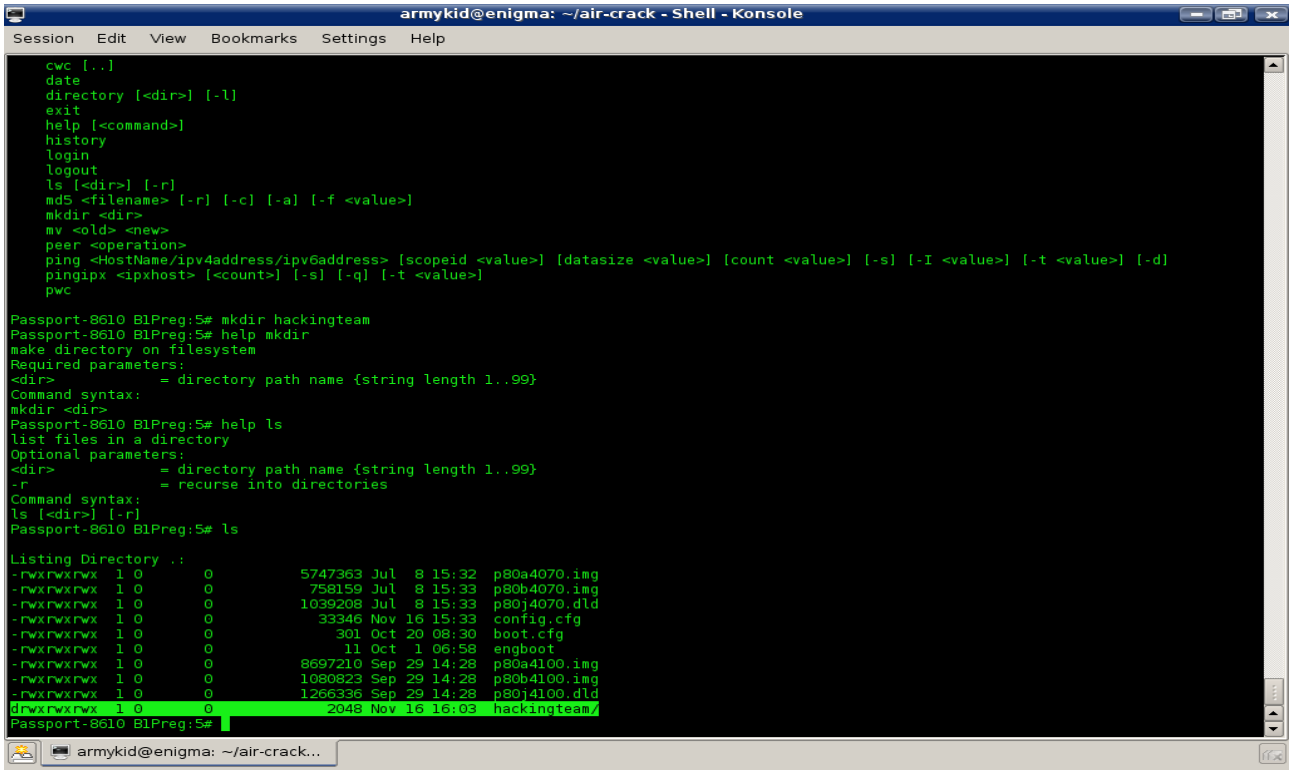
During our tests it has come out that is possible to de-authenticate legitimate clients by spoofing the data link layer address of the access point to which these clients are associated. This vulnerability alone is not harmful as after being de-authenticated a victim client connects to another access point or simply reconnects to the access point. Furthermore, such a failure is transparent to the user.



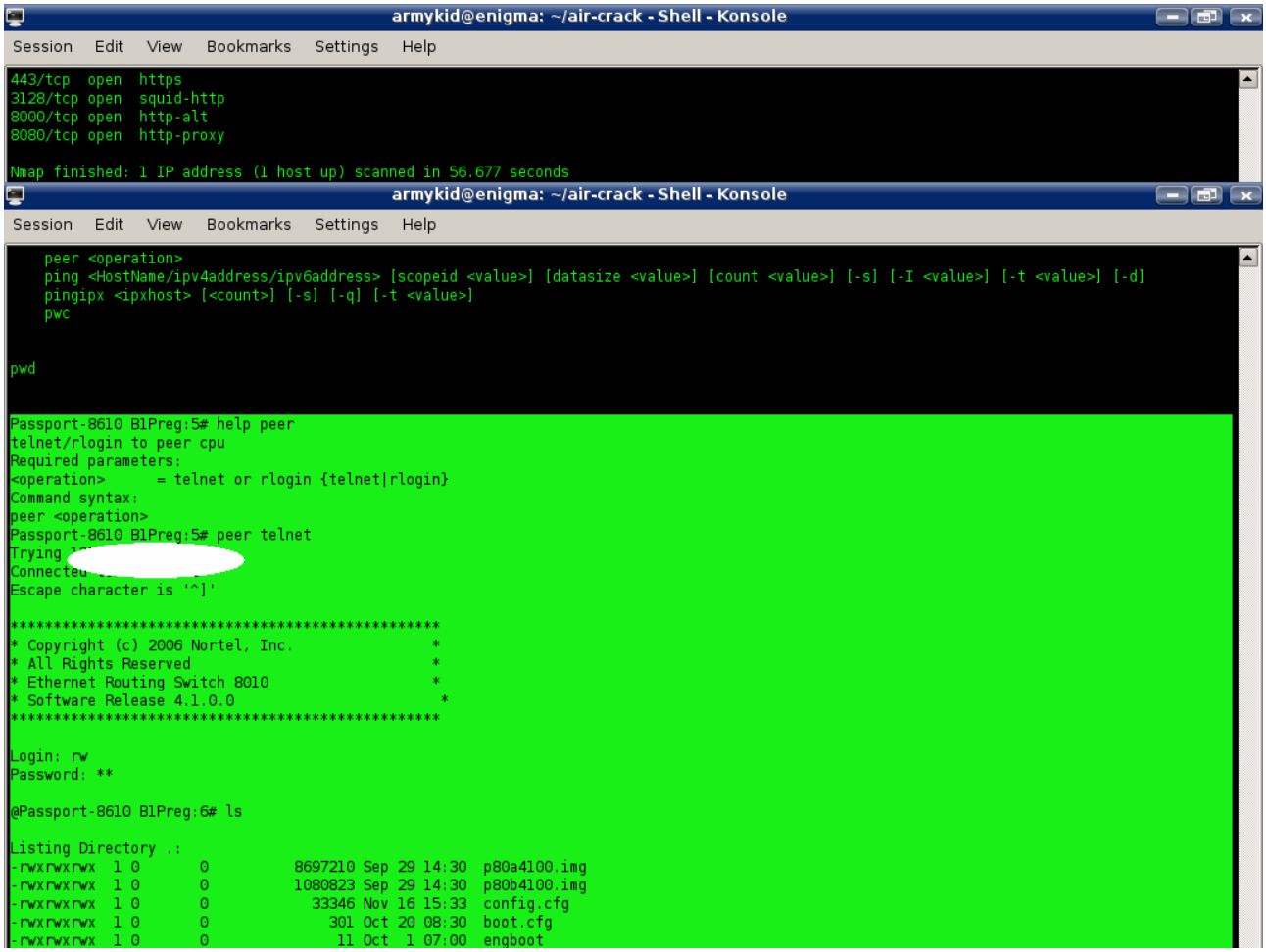
4.4.4 Unauthorized Remote Access to Routing Switches

Two highly critical routing switches, namely xxx.yy.zzz.65 and xxx.yy.z.33, accepted and allowed telnet connections. Their complete identification data follows: Ethernet Routing Switches 8010 of Northern Telecom, release 4.1.0.0. After a thorough check on the manufacturer's list of default user name and passwords it came out that the account rw/rw was still active and intact in these switches. Through telnet we gained interactive access on xxx.yy.zzz.65 and xxx.yy.z.33 and created a directory called hackingteam and hackingteam-2, respectively.

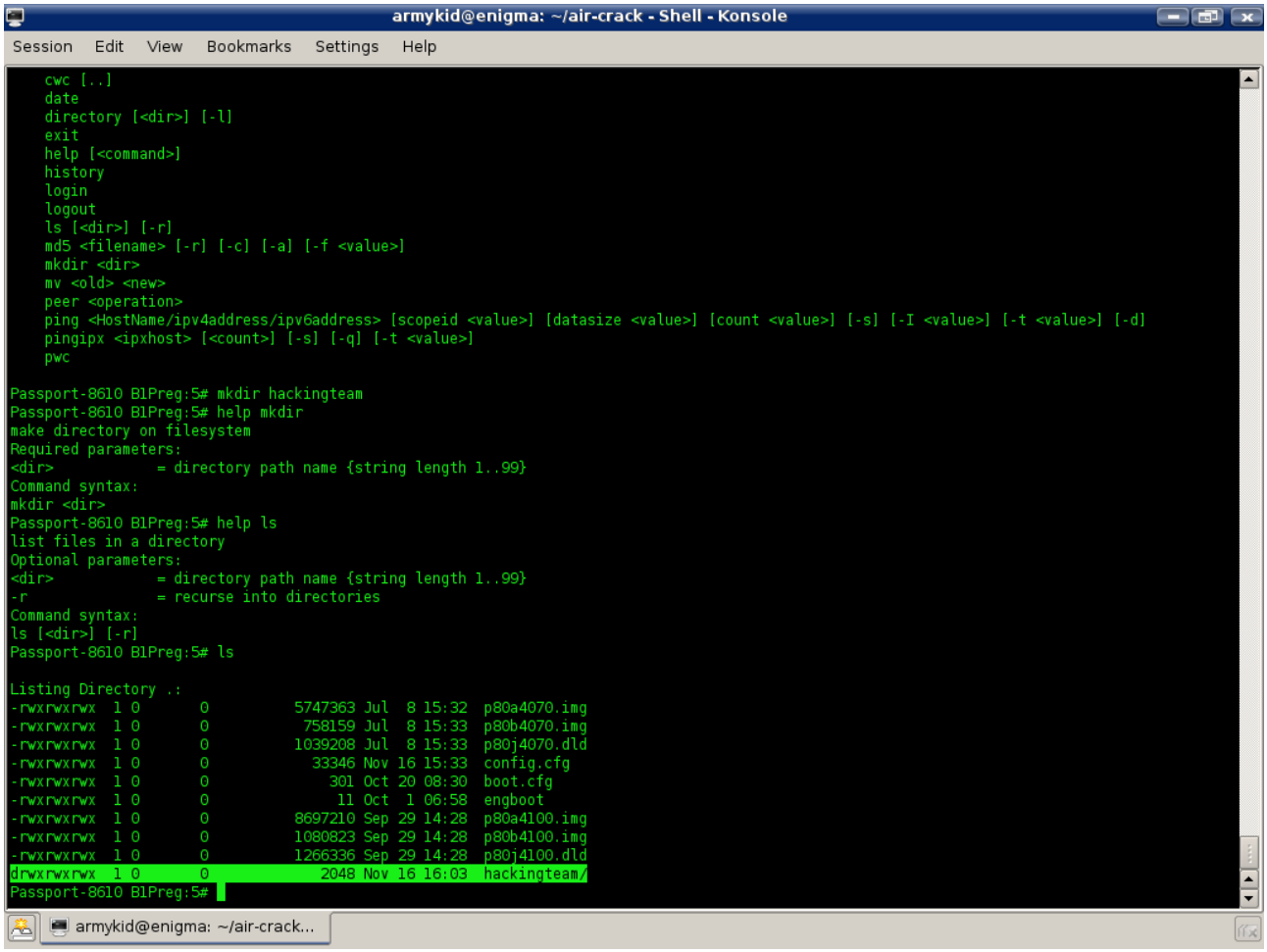
1) Inside xxx.yy.zzz.65



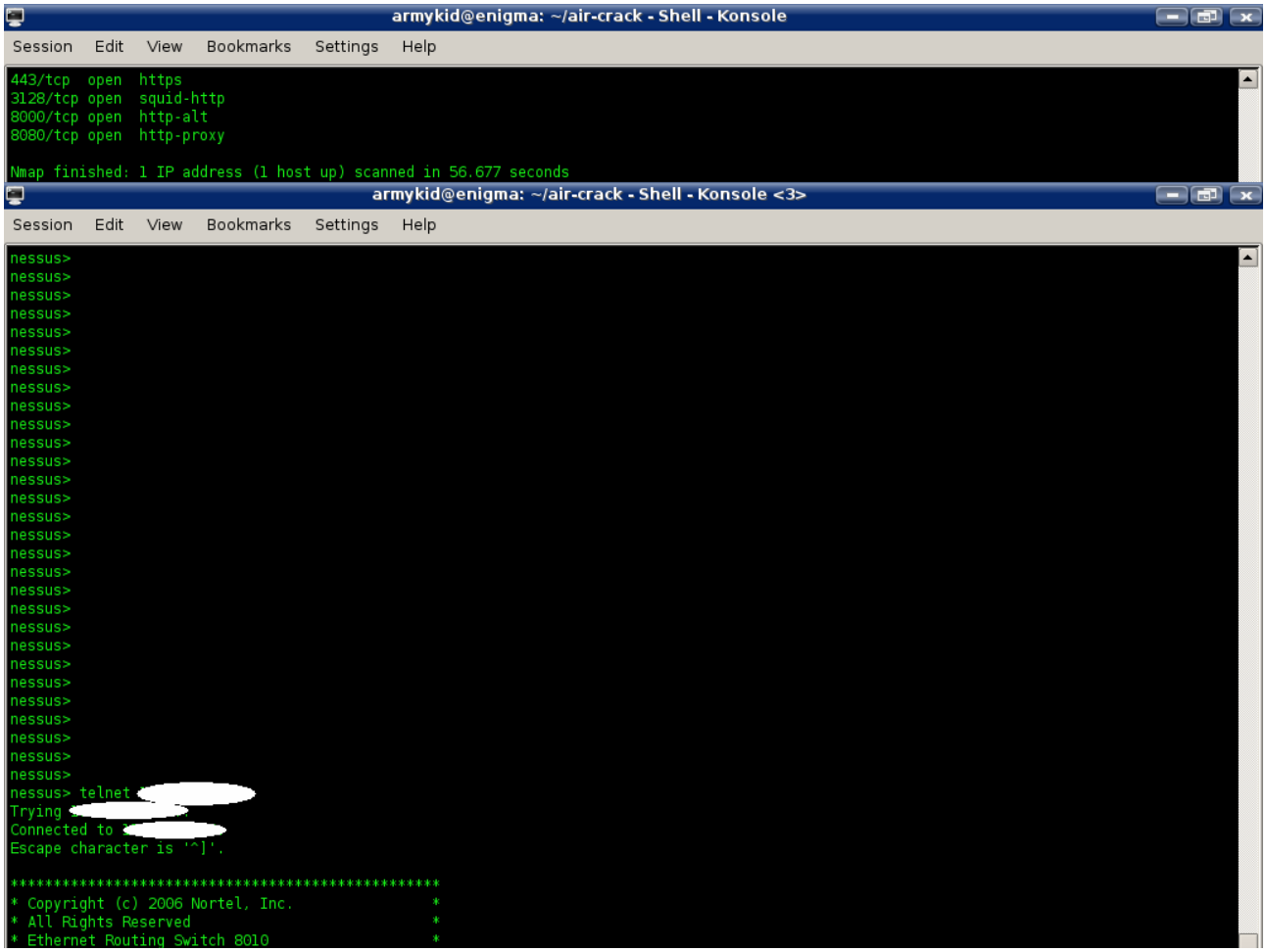
2) Passing from one processor to another (from 5 to 6) in xxx.yy.zzz.65



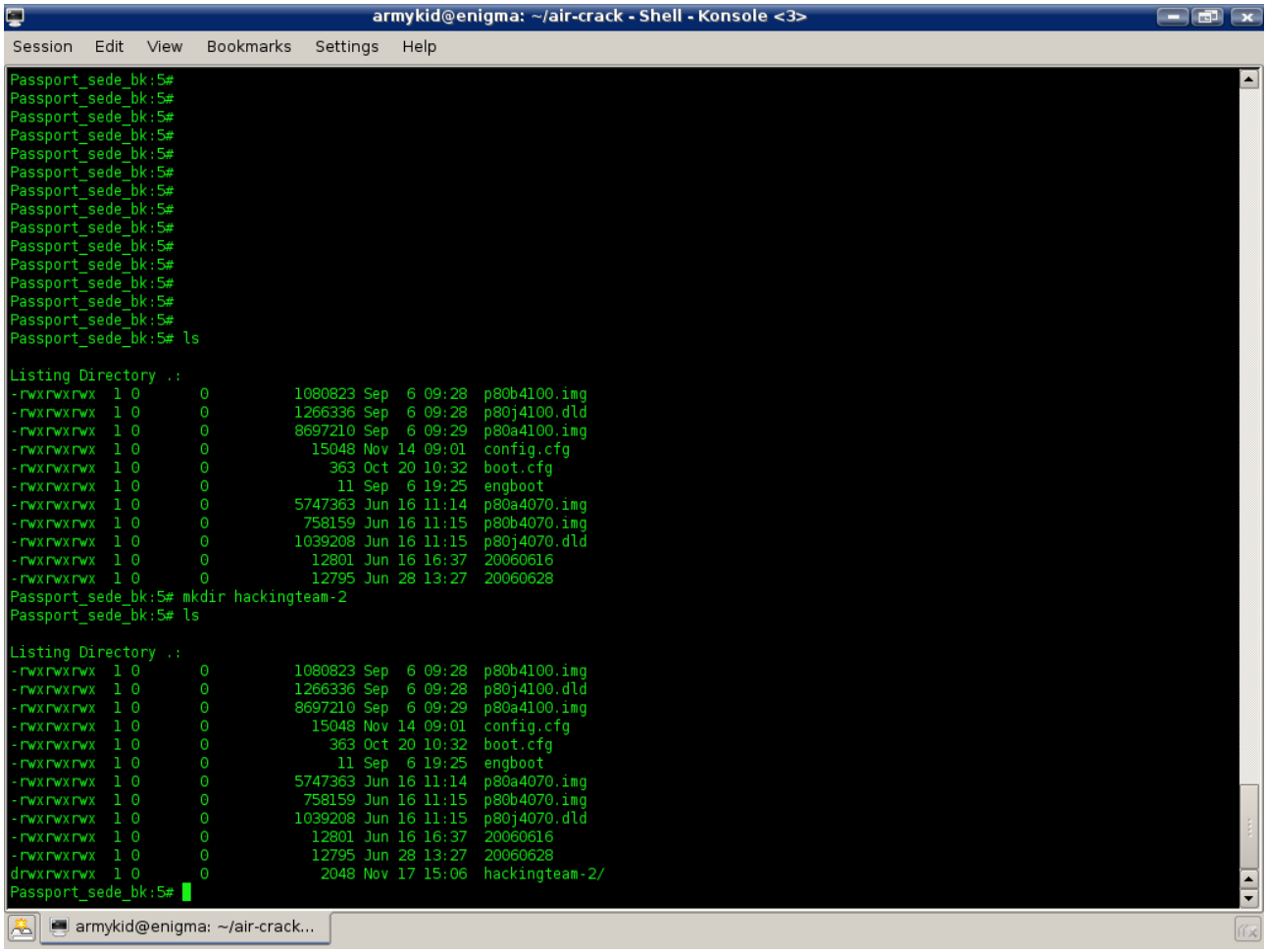
3) A directory listing in xxx.yy.zzz.65 after creating the hackingteam directory.



4) Inside xxx.yy.z.33



5) A directory listing in xxx.yy.z.33 after creating the hackingteam-2 directory.



4.4.5 Impersonation

Certain hardware WLAN security authentication devices are known to rely on matching user authentication credentials to the data link layer address of the user's machine. After a user has successfully authenticated the gateway adds the data link layer address of his machine to a dynamic list of authorized data link layer addresses. Upon receiving successive requests such a gateway only checks that the data link layer address in those packets is present in the dynamic list of authorized data link layer addresses, in which case the packets are successfully forwarded. With regard to the *home* service set identifier we used an attacking machine to intercept traffic for the purpose of identifying the data link layer address of the machine of an authenticated user. We assigned such data link layer address to the attacking machine and consequently acquired full access to the internet without using any credentials, i.e. without being preliminarily authenticated.

5 Countermeasures

With regard to the weak authentication applied by the service set identifier *voip* we suggest changing it to a stronger authentication system. The MAC based authentication is known to be extremely weak and easily breakable. In order to prevent unauthorized access to network switches of XXXXXX Banca we suggest changing the default password of the *rw* account from the default value to a security suitable one. Furthermore, the gateways should be configured not to allow clients authenticated to the service set identifier *voip* to reach network resources intended to be exclusively accessed by clients authenticated to the service set identifier *office*. Te de-authentication of clients alone is not serious from the security point of view. Nevertheless, in case of necessity such attacks are easily detected by a aireless network intrusion detection system.
We did not have access to information related to the kind of technology used for the gateways and their actual configuration, thus we are not sure whether the vulnerability which consists in allowing network access using a dynamic list of MAC addresses is a technology limitation or a security misconfiguration. In the former case one would think about changing technology, and in the later simply harden the gateway configuration. In any case, we suggest the use of virtual private networks which require valid cryptographic information for routing packets.

Vulnerability	***Description***	***Severity***	***Countermeasures***
Weak authentication	*voip* authenticates a wireless client through its data link layer address	Medium	Switch to a stronger authentication system
Network security misconfiguration	It has been possible to switch from *voip* to *office*	Medium	Review routing rules in the gateways
System security misconfiguration	in two switches the default account rw/rw has been found active	Medium	Change the default password to a secure one (already fixed)
Denial of service	it is possible to de-authenticate legitimate clients	Low	If necessary employ an intrusion detection to reveal the presence of malicious activity
Weak authentication	gateways use the data link layer to identify an already authenticated client	Medium	Switch to more secure technology or review the security configuration of the gateways

The WiFi network of XXXXXX Banca is protected by WPA which currently represents one of the best security protocols suitable for such a purpose. Nevertheless, we deem the actual WPA pass phrase used to protect the WiFi network of XXXXXX Banca is relatively weak as it is just 9 bytes long and is composed of lower case letters only. This would open the way to a brute force attack or a dictionary one. A determined attacker may use entire clusters of computers to break the WPA pass phrase. Furthermore, such an attack is not detectable since it is performed off line.

The service set identifier *voip* authenticates a wireless client through its data link layer address. By intercepting radio traffic it is possible to acquire a list of data link layer addresses of legitimate wireless clients. Consequently by assigning an authorized data link layer address to the wireless network card of our attacking machine it has been possible to bypass such authentication.

There was found a network security misconfiguration which allows for switching from the service set identifier *voip* to the service set identifier *office*. Thus, any wireless client who connects to *voip* anyhow, subsequently could reach *office* resources.

Two Ethernet Routing Switches 8010 release 4.1.0.0 manufactured by Northern Telecom, namely xxx.yy.zzz.65 and xxx.yy.z.33, were found to be accessible via telnet through a default account.

The WLAN security authentication devices of *home* bind an authenticated user with the data link layer address of his machine. By spoofing the data link layer of the machine of an authenticated user it is possible to bypass the authentication routine.

6 Conclusions

In order to understand the real threats of the XXXXXX Bank's wireless and better evaluate the associated business risk is useful to read the following table that shows the vulnerabilities impact.

Code	*Vulnerability*	*Difficult/Skill level*	*Impact*
V1	Weak authentication (voip)	Low to Medium	Grants unauthorized access to *voip*. Every one who can sniff the target WiFi may carry out the attack.
V2	Network security misconfiguration (already fixed)	Low to Medium	Allows unauthorized access to *office*. May be performed by someone who may access *voip*.
V3	System security misconfiguration (already fixed)	Low	Gives away full access to the underlying operating system. Could be carried out by every one who either has already or acquires access to the XXXXXX Bank's network.
V4	Denial of service	Low to Medium	Causes a temporary connection break to legitimate clients. Every one who could place himself within the coverage area of the WiFi network of XXXXXX Bank could send malicious packets necessary for carrying out such an attack.
V5	Weak authentication (gateways)	Medium	Allows unauthenticated access to the network. May be performed by someone who can sniff the target WiFi. The impact for XXXXXX Bank is that someone could have the same privileges of *home* users without any authentication.

The result of the entire security analysis is good and all vulnerabilities could be exploited only knowing the access point pass phrase. Therefore the vulnerabilities coverage is done deployng the following activities:

- to secure the pass phrase using more byte
- to secure the pass phrase using also numbers anc special characters
- to secure the passphrase changing it periodically

Having the possibility to cover also each vulnerabilities, we list below our considerations:

- V1: actually voip devices support only this kind of authentication; there are advanced devices with a more secure authentication mechanism implemented but they are much less performance level. In our honest opinion and experience, this kind of service is not ripe yet in companies with a high level of security provided.

- V2: already fixed by XXXXXX Bank's IT staff.
- V3: already fixed by XXXXXX Bank's IT staff.
- V4: it needs to evaluate the possibility to provide configurations/mechanisms on wireless access points that allow them to detect this kind of anomalies and to alarm in case of happening.
- V5: it needs to investigate the gateways configuration in order to define another way to authenticate this kind of traffic. It could be a configuration question or a product question.

With the exclusion of V2 (already fixed) there is no way to reach *office* sector from *home* sector. In fact the WPA authentication with certificates is the more secure technology available today; it allows neither to try to use the most part of wireless attacks technics.