NETWORKS AND TELECOMMUNICATIONS SERIES

Mobile Access Safety

Beyond BYOD

Dominique Assing
Stéphane Calé

ISTE

WILEY

Contents

Mobile Access Safety

Beyond BYOD

Dominique Assing
Stéphane Calé

ISTE WILEY

First published 2013 in Great Britain and the United States by ISTE Ltd and John Wiley & Sons, Inc.

ISTE Ltd

27-37 St George’s Road

London SW19 4EU

UK

www.iste.co.uk

John Wiley & Sons, Inc.

111 River Street

Hoboken, NJ 07030

USA

www.wiley.com

Library of Congress Control Number: 2012951550

British Library Cataloguing-in-Publication Data

A CIP record for this book is available from the British Library

ISBN: 978-1-84821-435-4

Printed and bound in Great Britain by CPI Group (UK) Ltd., Croydon, Surrey CR0 4YY

Introduction

> “With the Internet, to be competitive in the market is to communicate information to the outside world. It no longer consists of forbidding access to an organization’s data; it consists of mastering information exchange”.
>
> Jean-Philippe Jouas (president of LUSIF)
>
> Extract from *01 Informatique*, 4 September 1998

Remote access has helped realize one of mankind’s most ancient dreams: “ubiquity”, because with these new technologies, employees can now access all their company’s resources, anywhere, at any time and from any device (PC, PDA, etc.)

This development of “nomadism” is linked to a number of technological improvements, such as the “democratization” of the cost of laptops and the proliferation of Internet access, which is now available even in the remotest of places. However, it also has its roots in economic factors such as the globalization forcing companies to be more efficient and responsive in order to survive in a highly competitive environment. The gains arising from the implementation of mobility solutions are indeed many and varied:

– increases in the productivity of employees, who can continue to work while on the move (on trains, in airport lounges, in hotel rooms, etc.),with customers (online demonstration of in-house software use, etc.), and from home;

– increases in the flexibility of organizations and ways of working due to, for example, the development of teleworking, whether permanent (distributed call centers

allowing telephone operators to work from home) or casual;

– decreases in the emission of CO_2 into the atmosphere thanks to a reduction in the number of journeys (BT have estimated that the development of flexible working at their organization saves 12 million liters of gasoline per year);

– continuation of business operations in the case of major crises such as the destruction of the company's premises (by fire, water damage, etc.), epidemics (H1N1, etc.), strikes (rail employees, roads, airports), or any other event that prevents employees from reaching their place of work or to carry out their duties (power cut);

– decreases in the cost of business operations due to the reduction of costs related to the provision of office space (reduction in office space and therefore of rental costs, maintenance, security, insurance, etc.). BT has estimated savings in operating costs of £6,000 per year, per telecommuting employee;

– reduction in transport costs for employees, who can limit work-related travel because they have access to all necessary resources from any given location;

– reduction in employee turnover, by allowing them to adapt the way they perform their professional duties to their own requirements/personal wishes (e.g., childcare during school holidays, sports competitions, charity events, etc.). This improvement in working conditions can increase employee productivity and reduce the number of work stoppages;

– avoidance of fatigue and stress for employees by limiting the travel to the workplace (telecommuting).

Unfortunately, the exponential growth of remote access has completely called into question companies' security methods that have survived thus far. As in the Middle Ages,

this mainly consists of building high perimeter walls to protect against attacks from assailants, and to strictly limit and control incomings and exchanges with the outside. But today, organizations' physical boundaries are becoming more diffuse as the development of telework extends its geographical perimeter as well as the number of entry points. A veritable "Pandora's box" has been opened by the growing use of remote access. Thus, one employee can potentially inadvertently contaminate the entire information system of their company by connecting, for example, from home with their personal computer that has been contaminated by their children while surfing illegal download sites. The evolution of organizations' security policies is therefore vital.

Each security issue is unique, because such issues depend on the organization's intended use for its remote access, as well as on its own specific limitations and constraints (financial, technical, etc.) For this reason, it is not possible for us to provide, as part of this work, a universal "recipe". We will try, however, over the course of the following chapters, to give you some ideas, approaches, principles and techniques that will allow you to understand, on the one hand, the risks involved, and on the other, provide you with the means to build a security solution for your particular case.

Our aim is not to produce an exhaustive description of the various security issues and solutions concerning the mobile elements of companies, because as you will have gathered, such a task would require a much longer book. We have therefore chosen to adopt a didactic approach to make the reader aware of the various threats and protection solutions, by giving a concrete example based on an average user, and the various attacks suffered during a "typical day."

Then, we place these attacks in the broader context of the different families of risk. This allows us to then present the

tools capable of countering these attacks or limiting their effects.

Finally, we finish with our average user by explaining the protection solutions that should have been put in place to protect him. As the field of security is not solely related to technical issues, we conclude by making the link between the various recommendations with one of the main methodological approaches in this area (ISO/IEC 27002).

Chapter 1

An Ordinary Day in the Life of Mr. Rowley, or the Dangers of Virtualization and Mobility

“Appearances can be deceiving”

Proverb

1.1. A busy day

The day promised to be busy for Mr. Rowley. Upon awakening that morning, he knew it would be punctuated by unexpected events – as usual – but what they would be he didn’t know.

It all started after breakfast, when, after his son had already been surfing the Web, he decided to get on with preparing his annual report by logging onto his company’s fileserver from his personal computer. Thanks to the VPN[1] Internet access solution which had been installed by his company, he could work from home as if he were in the office. What a gain in productivity! And it was so simple: all that he had needed to do was simply install a small software client on his PC and configure it appropriately.

Then, because his plane took off at 9am and he was worried there might be heavy traffic, Mr. Rowley hurried out of the house – and found himself at the airport more than

three quarters of an hour before boarding. It was not a waste of time, though, since with his business class ticket, he had access to the VIP lounge. He took advantage of the opportunity to download his latest emails on his laptop, using the free Wi-Fi[2] access to deal with them while he was travelling. These little desks for travelers to use were really useful. You could even leave your PC connected and downloading emails, and go to the café to enjoy a coffee and a pastry.

Two hours later, when he had arrived at his destination, Mr. Rowley had dealt with all his emails, and even slept for a little while.

It really was his lucky day. It took barely ten minutes from the airport by taxi to get to his client's workplace. As it wasn't the done thing to arrive at an appointment an hour early, he decided to wait in a small café at the foot of the building. This café also offered free Internet access via Wi-Fi, so our man took the opportunity to order, on an e-commerce site, a fashion doll that his daughter wanted for her birthday.

The meeting with his client went as hoped, and Mr. Rowley could finally close the deal on the new V91 model, which he had been working on for several weeks.

Back to the airport, and as he was early again, he made the most of the VIP lounge, and got on with some work. He took the opportunity to transfer the full list of contacts on his laptop to his new smartphone via Bluetooth[3].

Finally, back at home, he was able to celebrate signing the contract with his little family, with a bottle of champagne.

Just before going to sleep, wanting to check his emails using his smartphone, Mr. Rowley made the unpleasant discovery of the disappearance of his precious device. It had slipped from his pocket in the taxi that took him home, without him having noticed. This perfect day ended on a

negative note; he would have to replace it as soon as possible, and transfer his contacts from his PC again: a slight waste of time, but he thought no more of it.

1.2. The ups and downs of the day

Mr. Rowley was happy, because he had finally succeeded in convincing his client to sign the contract that was so important to his business, and which assured more than $50,000 of turnover in the coming months.

But he did not yet know, that on that day:

– his credit card details had been stolen;

– he had infected the corporate network with a worm, which effectively paralyzed the entirety of its information systems for nearly six hours;

– the detailed plans for the launch of the new V91 model had been stolen by a rival company;

– all the contact details for his clients and prospects had been stolen.

1.3. What actually happened?

While nothing in the eyes of Mr. Rowley could distinguish this day from so many others he had experienced in the course of his long business career, invisible and ill-intentioned individuals had made every effort to take advantage of his lack of knowledge of information security.

It all started when his son connected to a Website which had previously been attacked by a hacker. Upon visiting the

site, a worm[4] was automatically installed on Mr. Rowley's personal computer via vulnerability in the operating system. The worm then took advantage of the IP tunnel that had been established with the company network to propagate there, significantly disrupting the functioning of the information system.

Then, at the airport, when Mr. Rowley left his PC unattended, an employee of a competitor who had recognized him, piqued by curiosity, decided to glance at his laptop. It was then that he recognized the plan for the launch of the new V91 model. The opportunity to obtain valuable information that might hamper the launch of the new product was too good to miss. All it took was to use a USB key to copy all of the desktop files on Mr. Rowley's computer, in just a few seconds.

As for the Internet access point used in the café, it was not provided for customers by the owner, but had been installed by a hacker who knew that by placing a Wi-Fi router in a busy place, many victims could be snared. Those who believed they were connecting to popular Websites (eBay, Amazon, etc.) were unknowingly automatically redirected to a server maintained by an attacker. Taking advantage of this middleman position (see Section 2.2.4 *Man in the middle*) between the user and the e-commerce site, the attacker profited by collecting confidential information, including payment card details.

When Mr. Rowley synchronized his address book between his smartphone and his laptop, he had to input a matching PIN on both devices. But a hacker had installed a PC with Bluetooth sniffing software in the VIP lounge. He knew that this kind of place necessarily attracted people holding positions of responsibility, and therefore having easily marketable, confidential information. By analyzing the traffic exchanged between the PC and the smartphone, he could obtain some of the information necessary for authentication

(IN_RAND[5]) and could determine the rest through a brute force attack (PIN[6], BD_ADDR[7]) (see section 2.3.4. *Cracking encrypted data*). Once the authentication key had thus been obtained, it was not difficult to retrieve the desired information from Mr. Rowley's mobile phone.

The bad luck of losing the smartphone in the taxi was the good luck of the next customer, who discovered it, and was even luckier to discover that no protection was in place to prevent access. Mr. Rowley had disabled his passcode protection, deciding that he was wasting too much time repeatedly typing it in.

Mr. Rowley's misfortunes did not end there. Whoever had got their hands on the smartphone quickly realized the value of his discovery: all the emails, business contacts, meeting notes, tender offers in email attachments, etc. He knew enough people who would be very interested to know all this information – the world of business is sometimes very small!

Unfortunately what happened to our fictional character during this "very ordinary day" is only a small example of the many types of attacks experienced every day by companies which use mobility solutions. In Chapter 2, we present in detail the main types of threats you might encounter, so that you can better understand the scope of potential attacks, and the inventiveness of hackers.

1 *Virtual Private Network*: virtual private networks typically exist over a public infrastructure such as the Internet, thanks to an encryption solution that ensures confidentiality of data exchange.

2 *Wireless Fidelity*: Wireless Ethernet local area network technology, standardized by IEEE (802.11a, 802.11b, 802.11g, 802.11n).

3 Wireless communication technology (2.4 Ghz) invented in 1994 by the Ericsson company to facilitate exchange of information between devices over short distances.

4 A program that spreads from computer to computer by reproducing (duplicating) each time, using means as diverse as email, instant messaging, P2P networks, etc.

5 Random number used when creating the key for pairing Bluetooth devices.

6 *Personal Identification Number*: numerical password used on mobile telephones.

7 Unique 48-bit address which identifies a Bluetooth device.

Chapter 2

Threats and Attacks

"Even the most improbable risk is possible"

Gérard Mestrallet (president of GDF-Suez)

It is impossible to list all the attacks with which mobile systems could one day be confronted because there are hundreds, with new ones appearing every week. We have therefore chosen to present the most important, to give you an idea of the techniques and methods that could be used by hackers against you, so that you can assess these threats and put in place appropriate protection measures.

To assist in your understanding, we have classed these threats into five broad categories:

– *reconnaissance phase:* a set of methods and techniques allowing a hacker to gather information about the target before launching his attack;

– *identity/authentication attack:* a set of methods and techniques which allow a hacker to steal the identity of a machine, a program or a user, in order to use existing authorizations;

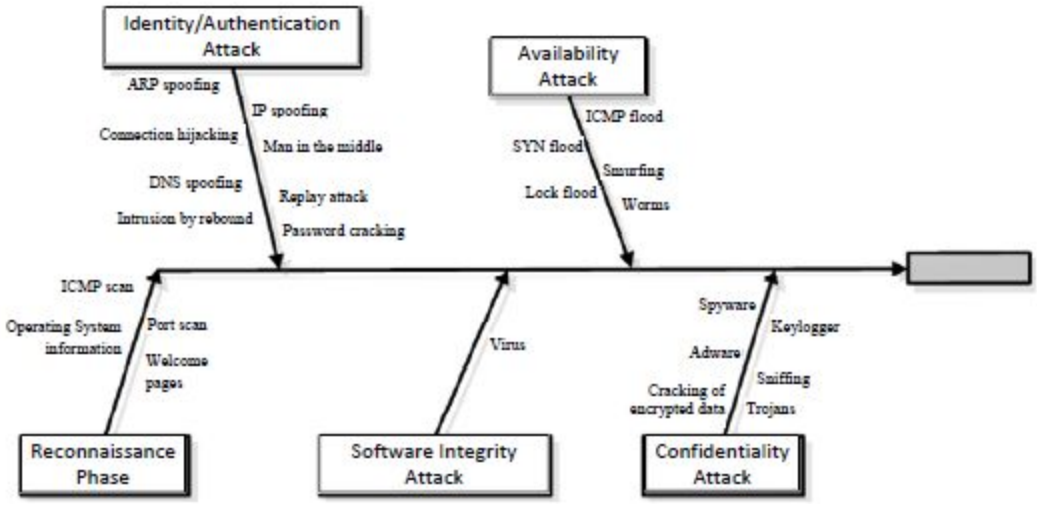
– *confidentiality attack:* a set of methods and techniques which allow a hacker to obtain information which is not freely available;

– *availability attack*: a set of methods and techniques which allow a hacker to impair the performance of – or even completely disrupt – a service provided by the target;

– *software integrity attack:* a set of methods and techniques which allows an hacker to hijack or modify

the normal functioning of a piece of software, so that it performs functions which benefit the hacker.

Figure 2.1. *Classification of the different types of attack*



But as you will gather from reading the various paragraphs which return in more detail to these attacks, these five groups are not necessarily set in stone. Indeed, an attack could belong to several of these families. For instance, a “Trojan horse” may obtain information about the system on which it is installed (recognition phase), before stealing the administrator passwords (confidentiality attack) and using them (identity attack) to reformat the hard drive (availability attack).

Equally, you will realize that the types of threats that may affect a laptop also concern smartphones, which increasingly have the disadvantage, due to their small size, of being easily stolen or lost. It is estimated that in France alone, 500 smartphones are “lost” every day. Moreover, in general they have several wireless communication interfaces (Bluetooth, infrared, GPRS, UMTS, etc.), that provide the hacker with many channels of attack.

You will also note that the broad categories of attack we present (except the last, which is specific to new technologies) borrow all of the numerous elements of

military strategies that have historically been developed by generals during their campaigns.

In the Chinese strategy treatise, “The Thirty-Six Stratagems”, which probably dates from the Ming Dynasty (1368-1644), it is recommended that you conduct a reconnaissance phase with respect to the enemy you intend to attack (knowledge of the terrain, identification of positions, evaluation of strengths, etc.), in order to develop a strategy (打草惊蛇, *beat the grass to startle the snake*). This strategy then consists of causing confusion and disorder in enemy ranks, so that it becomes easy prey (打草惊蛇, *muddy the water to catch the fish*).

Another trick can be used, wherein the attacker takes on the guise of another person in order to cross lines of defense (金蝉脱壳, *the Golden Scarab sheds its shell*). Alternatively, the subterfuge exists not to hide the attacker’s identity, but rather to disguise their true intentions as initially innocent, to lull the victim into a false sense of security (笑里藏刀, *conceal a sword in a smile*).

2.1. Reconnaissance phase

In order to prepare an attack, the hacker will use a number of techniques, that will be described further here, to better understand the architecture of the remote access infrastructure and find potential vulnerabilities. In order for mobile devices to be able to access an organization’s resources, the organization must provide its users with an infrastructure to process their connection requests. Since, by definition, this infrastructure is located between the outside world (e.g., Internet) and the organization’s network, it is a primary target for hackers.

Attackers can collect information via *passive mode* or, equally, *active mode* information-gathering techniques. A combined use of both approaches is common. The use of

the term “passive” indicates all technical information gathering where the attacker does not interact directly with the target’s information system. In the active mode, direct action on the part of the hacker is required to obtain the desired information.

2.1.1. *Passive mode information gathering techniques*

As in military tactics, the passive reconnaissance phase consists of collecting as much information as possible about the target without being detected. In the Middle Ages, a spy disguised as a simple merchant, positioned in front of the castle, could note all the comings and goings of the garrison, analyze how the fortress was built, and listen to conversations, in order to collect all relevant data.

The approach with respect to a target information system is identical. The great advantage of this passive mode reconnaissance phase is that it is absolutely imperceptible by the target. No special attempt to access systems, and no abnormal or different activity in daily traffic, will be found on any of the target’s detection systems.

In the context of a passive mode reconnaissance phase, the attacker can:

1) collect information about the observed subject (an individual, a business, etc.);

2) look for direct vulnerabilities or critical information on the target’s information system;

3) listen to network traffic;

4) collect data relating to Web domains.

It should be noted that all the passive mode reconnaissance techniques described here are publicly available, in terms of both tools and services.

2.1.1.1. *Collection of information about the target*

Passive mode information gathering aims to find out all information about the target by querying search engines such as Google, using keywords such as the target's name, email addresses, etc. Very often, valuable data are available in the public domain without the target knowing, or being able to perceive this opportunity from the point of view of the attacker.

Thus, an employee using an Internet forum to post technical questions on issues related to a version of hardware could provide valuable information about the architecture of their information system (potential vulnerabilities, development in progress, etc.).

A simple email address can also be informative about the way in which email addresses are constructed. This then allows fake emails to be forged for use in *phishing* campaigns.

This type of information gathering is often classified as part of the business intelligence domain, but from the attacker's point of view it is primarily to discover all information, clues and weaknesses inside the company, which can then be exploited in order to carry out the attack.

Too often this research phase is dismissed by security services, who forget that apparently innocuous public information can be used to "penetrate the fortress". In this way, by simply conducting an Internet search for the name of Paris Hilton's dog, a hacker was able to recover the entire address book of her smartphone, because the password that protected access to her mobile phone was none other than the name of her favorite pet.

2.1.1.2. *Google Hacking*

Google has established itself as the most popular and most widely used search engine. For most Internet users the use of Google is limited to entering keywords. However, Google has advanced functions that can find information that is sensitive from a security point of view; this is known as *Google Hacking.*

In August 2011, the researcher Tom Parker was able to obtain the SCADA[1] functionality for the administration of certain power plants, accessible on the Internet via Google, by targeting the name of a specific *driver* contained in the headers of HTML pages from Websites referenced by Google.

Although for the layman, the following functions:

– *example 1*:

inurl:“editor/list.asp” | inurl:“database_editor.asp” | inurl:”login.asa” “are set”

or indeed:

– *example 2:* inurl:-cfgintext:”enable password”

are not particularly expressive, they form part of a hacker’s basic knowledge. Getting to know their target very often forms a major part of a hacker’s capacity to gain access to your systems.

The first example asks Google to search in the URL content for the keywords “editor/list.asp”or “database_editor.asp”or “login.asa” “are set”. The symbol | is the equivalent of the logical operator OR.

This search focuses on finding pages of sites where the *login* (username) and *password* are directly accessible in plain text.

The second example conducts a Google search for the keyword “cfg” in URLs and the term *enable password* in the text of indexed pages. This search aims to find the “clear passwords”of network equipment, identified by the “cfg”of URLs.

2.1.1.3. *Listening to traffic network (sniffing)*

Formerly, before the mass deployment of Wi-Fi networks, listening to network traffic required access to the target's premises. The reconnaissance phase was therefore not in passive mode, since it was necessary to obtain physical access in order to connect listening devices. But now, thanks to the rise in Wi-Fi networks, all this can be done from outside your premises, without any need for forced entry. The reconnaissance phase can be accomplished in passive mode from any location offering Wi-Fi access.

Wi-Fi hotspots that offer easy connection to the Internet from a public place often present security risks. Specifically, access through an unprotected public hotspot to messaging facilities that do not incorporate encryption features allow the transmission of identifiers and passwords in plain text.

However, the same problem can occur with Wi-Fi networks which are inadequately protected, and therefore, in the most extreme cases, allow an attacker to record communications and extract sensitive information. And even if the Wi-Fi network has integrated protection mechanisms, a hacker can discover, while remaining perfectly clandestine:

– hardware addresses of devices that pass through this network. On this basis, the attacker can perform a search for the type and manufacturer of the pieces of equipment to check whether vulnerabilities exist and subsequently exploit them;

– the structure of the network. This allows the hacker to manipulate or exploit the addressing scheme;

– the habits of the people who connect (frequency of use, connection times, etc.). The attacker can then use this information to plan the moment when their attack will have the best chance of going unnoticed: the time a

given person is away from the network, or conversely, the time when they are present, to avoid raising suspicions.

And even if the network itself is secure, a poorly configured wireless printer is sufficient for all documents sent to it to be captured.

As with military tactical planning, the attacker will collect all possible information to be sorted afterwards, because it is difficult to determine in advance which data will be critical. To assist in this task, there is a broad spectrum of tools, ranging from the most trivial solutions (such as switching the network card to the mode known as *promiscuous* to allow their computer to listen to traffic), to dedicated *open source* software, created by the hacker community.

2.1.1.4. *DNS Analysis*

The DNS (*Domain Name System*) constitutes one of the pillars necessary for the proper functioning of the Internet. To connect clients and servers on the Internet, communication protocols use IP addresses. These addresses, made up of series of numbers, are not the easiest for a person to remember, unlike names. The requirement of establishing an association between these numerical addresses and names has therefore been imposed to allow for easier memorization of sites' addresses. For this reason, we type www.google.com instead of 173.194.34.56.

When you administer a domain name it is in your interest to configure a DNS server, so that you know, for example, how to contact your site or send emails to the administrator. However, in doing so, you provide information to potential attackers. If the DNS server is configured correctly, the information distributed indicates nothing more than how to contact you. But conversely, if poorly configured, poorly

monitored, poorly secured, etc., the information stored in the DNS server may reveal:

– the IP addresses of your test servers;

– the totality of your domain information, including internal information, in the case of a configuration error;

– the version of your DNS server. This therefore allows the hacker to establish if this is up-to-date, and if not, to discover opportunities for an attack.

The DNS is a directory, and as for any burglar who targets a given person, the more information available on the target, the more opportunities for burglary. Clearly, it would not cross anyone's mind to enter into a directory "Mr. X lives at Y, entrance extremely overlooked but backyard allowing easy access for entry through the bathroom window"! A poorly configured DNS server provides just such information.

The approaches presented at this stage are only those carried out in *passive mode*, and leave few, if any, traces of information gathering. However, information obtained by these means are not always sufficient for an attack to be prepared, so the attacker moves to a reconnaissance phase known as *active*, in order to confirm his initial findings, or to obtain more data.

2.1.2. *Active mode information gathering techniques*

Active mode reconnaissance is very different, and can be minimally or extremely intrusive upon the target's systems. Several broad categories of active reconnaissance can be distinguished:

– network discovery;

– port scanning;

– homepage analysis;

– vulnerability scans;
– collection of information on the operating system;
– social engineering, too often overlooked;
– analysis of garbage.

The reconnaissance phase therefore begins with OSI layer 3 analysis, to detect the IP addresses of active machines, and continues with a layer 4 analysis to determine which ports (UDP/TCP) are open. We therefore know which applications are available on the identified machines, possibly even if they are protected by a *firewall* or filtering router. The reconnaissance phase then continues with a layer 7 analysis, which attempts to determine which operating systems are being used, and what these machines are for. We finally finish with two reconnaissance methods, which are sometimes overlooked, but are nonetheless relevant: social engineering and analysis of garbage.

2.1.2.1. *Network discovery*

This reconnaissance phase is dedicated to discovering the IP addresses of the target's active machines. Several methods exist, and we present below the most well-known: *Ping sweep* and *Scan arp.*

Ping sweep relies on the ICMP protocol. It consists of sending *echo* requests to all IP addresses of a local subnet. Each active machine, in the absence of a *firewall*-type filter system for example, responds to this request by sending back a return ICMP *echo reply* packet.

This method allows the initial discovery of machines present on a subnet to be achieved quickly and very simply, and also exhaustively, as each possible IP on a subnet will be queried. However, this approach is very "noisy", and with the proliferation of protection such as *firewalls* or antivirus software which integrates alerts for this type of discovery

method, the attacker can be speedily identified, and their attempt blocked. Spacing queries over time and the use of a non-sequential ordering of the IP addresses queried are some of the possibilities that the attacker can implement to circumvent protection mechanisms.

NOTE.– In addition to this phase of the investigation *via* ICMP, the attacker can also use the *traceroute* utility, which generates a list of all the equipment that must be passed through in order for two machines to communicate. The structure of a network can therefore be determined, and as a result, the IP addresses of the principal interconnection nodes can be established and used in a Denial of Service attack, for example.

Because *ping sweep* is a “noisy” approach, the attacker may prefer a network discovery technique based on the ARP protocol. ARP scanning consists of sending an ARP request for each IP address in a given subnet. Here we rely on the principles of operation of the OSI layer 2. Each machine uses at least one network adapter to communicate, and each card contains information that uniquely identifies a hardware address. On a given subnet, before beginning to interact via the IP protocol, each machine needs to know the hardware address of its correspondent. The ARP protocol facilitates this dialogue and the correspondence between an IP address and a hardware address.

The ARP scan relies on this mechanism to discover who is present on a specific subnet. This type of scan is carried out much more discreetly, because the tools that implement it never go back up to OSI layer 3 (IP), and do not generate alerts in the majority of protection tools on users’ workstations. Furthermore, this type of query is not blocked.

This type of scan works on both Ethernet and Wi-Fi networks; its only limitation is that it can only scan the network on which the rogue machine is connected.