– Sécurité offensive et contre-mesures –
(offensive security and countermeasures)

Academic year 2019-2020

Penetration test report for *This is the socks*

Under the supervision of M. Benjamin VAN DAMME, offensive security and countermeasures teacher.

Third year of bachelor review, in cybersecurity option, Hénallux.
January 24th, 2020 - Second version.

MOERYNCK Loïc & THOMAS Matis, 9th group, class A

Contents

1 Executive Summary

1.1 Contract

We, Matis Thomas and Loïc Moërynck, fictitiously contracted by N. Melchior, CEO of *This is the socks* to conduct a penetration test and to report any weaknesses of his infrastructure.

Furthermore, Mr. Melchior asked us to provide him with some information about one of his competitor, the www.spartoo.com website.

It goes without saying that every single thing we did in this report was done in a strictly legal and proper way.

1.2 Summary of results

Here is a list of the weaknesses we found on the infrastructure, and a classification of their risk :

- Password policy : **high risk**.

  Consequence : There is **no** password policy at all, which means that passwords are way more easy to crack.

  Mitigation : Setting up a strong password policy. Please confer to the recommendations at the end of this report.

- Network defense : **high risk**.

  Consequence : There is **no** network defense, such as firewalls or antivirus configured nor installed. That makes the act of hacking the network once in the internal network **really** easy.

  Mitigation : Installing and properly configuring firewalls and anti-viruses on every single computer of the network.

- Access rights management : **high risk**.

  Consequence : Every accounts is in the Administrators group for Windows OS, and every Linux users is in the sudoers group (a Linux equivalent of the Administrators).

  Mitigation : Groups must be created with their own rights, and users separated into them.

- Software and Operating Systems vulnerabilities : **medium risk**.

  Consequence : Some operating systems and applications are not up to date, despite the fact that updates protect from new vulnerabilities.

  Mitigation : Setting up updates policy, for instance updating the whole infrastructure once a week.

- SNMP agent misconfiguration : **medium risk**.

  Consequence : The SNMP agent is set to the default community name. An attacker could use this information to get more information about the remote host, or even change the configuration.

  Mitigation : Disable the SNMP service on the remote host if possible. If the service is needed, simply change the default community string or filter inbound UDP packets to this port.

1.3 Overall security of the infrastructure

It is important to realize that considering all the risks listed above, *This is the socks* is in a critical security status.
If the company were to come under attack, the consequences would be dreadful.
The company should patch every single high risk vulnerabilities above first, as they are critical.

2 Introduction

2.1 Contract explanation

We, Matis Thomas and Loïc Moërynck, fictitiously contracted by N. Melchior, CEO of *This is the socks* to conduct a penetration test and to report any weaknesses of his infrastructure.

Furthermore, Mr. Melchior asked us to provide him with some information about one of his competitor, the www.spartoo.com website.

It goes without saying that every single thing we did in this report was done in a strictly legal and proper way.

2.2 Baseline situation

This penetration test was done in a *gray box* testing manner : a combination of white-box and black-box.
Mr. Melchior gave us pieces of information and a full access to two computers in replica of his own internal network, for the purposes of simulating a malicious hacker that has gained internal access[1] and which is trying to obtain more access and to exploit vulnerabilities for personal reasons.

Here is a list of the information he gave to us :

- We are the 9th group :

Equipe	IPs	Site 1	Site 2
9	10.1.10.212-215	www.goodshopping-<groupe>09.com	www.moviescope-<groupe>09.com

  The IPs columns are the IP addresses that we have to statically address to our Windows 10 and kali virtual machines.[2]

- The credentials of an administrator on one of the computers in the internal network:
  - Username: Martin
  - Password : apple.

2.3 Our focus

The entire penetration test was done following the 2-7 CEHv10 modules.
Here are some of the points we focused on :

- Getting information about the competitor's website.
- Identifying vulnerabilities.
- Exploiting them to take over the control of the infrastructure.
- Doing all of this in a stealthy way.

[1] For instance with the help of fishing.
[2] There are 4 addresses available, 2 for each person of the group.

2.4 Summary of results

2.4.1 Classification of the risk

First of all, here is how we classified the levels of risk :

- **High risk** : The vulnerability should be fixed as soon as possible, and set as a top priority. Any exploitation could lead to critical damages.
- **Medium risk** : The vulnerability should be fixed in a reasonable time, after that every high risk vulnerability is fixed. Any exploitation could lead to harmful damages.
- **Low risk** : The vulnerability should be fixed if the schedule permits it. Any exploitation could not lead to any serious damage.

Here is a list of the weaknesses we found on the infrastructure, and a classification of their risk :

- Password policy : **high risk**.

  Consequence : There is **no** password policy at all, which means that passwords are way more easy to guess or bruteforce. For now, there is not a single strong password used for an account.

  Mitigation : Setting up a strong password policy[3] :

  For instance, here is a good password policy :
  Change the password every 90 to 180 days.
  Take wordlists used for dictionary attacks and use them as passwords blacklist.
  Do not use personal information in your passwords, they could be gathered and used to guess them.
  Never use your passwords multiple times.
  Use **at least** :

  - 8 characters,
  - 1 capital letter,
  - 1 lower-case letter,
  - 1 number,
  - one special character (!, #, &, etc.)[4].

  If you have troubles remembering your passwords, use a password keeper, such as keepass[5].

- Network defense : **high risk**.

  Consequence : There is **no** network defense, such as firewalls or antivirus configured nor installed. That makes the act of hacking the network once in the internal network **really** easy.

[3] Confer https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff741764(v=msdn.10)?redirectedfrom=MSDN

[4] confer https://docs.oracle.com/cd/E11223_01/doc.910/e11197/app_special_char.htm#MCMAD416

[5] https://keepass.info/

Mitigation : Installing and properly configuring firewalls and anti-viruses on every single computer of the network.

Installing and configuring these via the AD so that users can't disable the firewall and the anti-virus without the admin right.

- Access rights management : **high risk**.

Consequence : Every accounts is in the Administrators group for Windows OS, and every Linux users is in the sudoers group (a Linux equivalent of the Administrators).

Mitigation : Groups must be created with their own rights, and users separated into them.

Simple users should **not** have the Administrator right. Groups should be managed by GPO[6] to limit the impact users can have. Furthermore, Linux, critical folders, such as webpages, should have corrects rights assigned.

- Software and Operating Systems vulnerabilities : **medium risk**.

Consequence : Some operating systems and applications are not up to date, despite the fact that updates protect from new vulnerabilities.

Mitigation : Setting up updates policy, for instance updating the whole infrastructure once a week.

- SNMP agent misconfiguration : **medium risk**.

Consequence : The SNMP agent is set to the default community name. An attacker could use this information to get more information about the remote host, or even change the configuration.

Mitigation : Disable the SNMP service on the remote host if possible. If the service is needed, simply change the default community string or filter inbound UDP packets to this port.

2.5 What still need to be done

The infrastructure still needs to be tested upon these points :

- Denial-Of-Service resistance,
- Verify the unwanted connections over the network,
- Try to crack the wi-fi password : As the first one has a WEP password, it should be quite easy. The WPA2 should be way harder and more secured.

[6] Group Policy Object

3 Methodology

To conduct this penetration test, we used the 2-7 CEHv10 modules, which are :

3.1 Footprinting and Reconnaissance

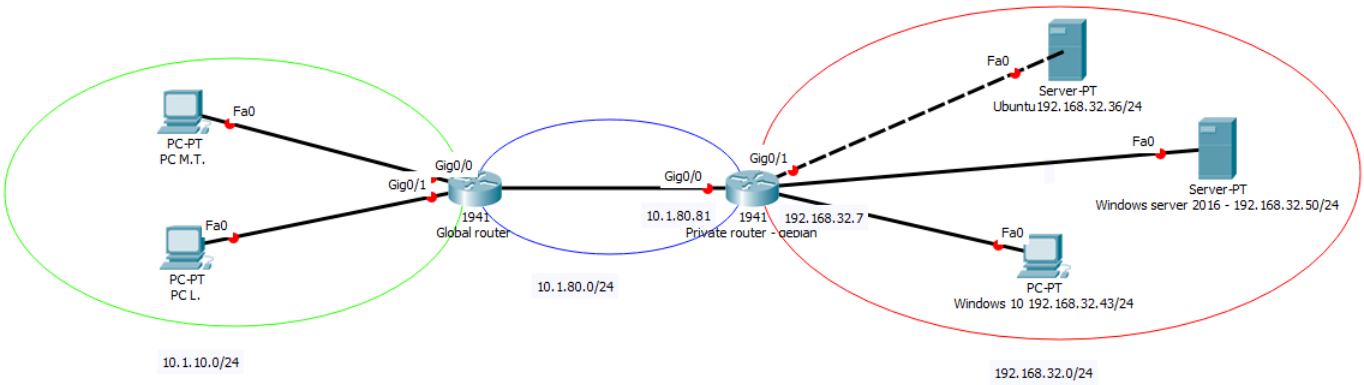
The purpose of this module is to gather pieces of information about a company and its employees. We applied this module to the concurent website of our client : spartoo.com, which was quite secured.

3.1.1 Tools used

- Sublist3r : Used to find subdomains.
- Whois website : A website that gives information about other websites.
- Netcraft : Looks like whois, but rates the risk.
- Spiderfoot : Used to find the ssl certificates.
- Recon-ng : Can find hosts and contacts. -> As recon-ng hasn't been successful, we used google search and linkedin.

3.2 Scanning Networks

The purpose of this module is to identify computers of the networks to be able to draw a draft of the infrastrucute. Here is our draft:



3.2.1 Tools used

- Command shell such as pings and tracert.
- Megaping : Runs scans on the network to get ip addresses, running services and hostnames.
- A proxy switcher : Hides our IP address.
- Cisco packet tracer : To draw the draft of the infrastructure.

3.3 Enumeration

This step consists in detection of open ports and their services. It aims to obtain the most accurate information to be able to exploit them in next module.

3.3.1 Tools used

- Angry IP scanner : scans the open ports if the given network.
- Zenmap (and nmap CLI for linux) : gives more information on the open ports, such as the version of the running services on it.

3.4 Vulnerability Analysis

The vulnerability analysis aims to seek for all vulnerabilities of the system, such as the OWASP top 10.[7]

3.4.1 Tools used

- Nessus : a fork of OpenVas, which is a vulnerability scanner.
- GFI LanGuard : another vulnerability scanner, which gave us the same results as Nessus.

3.5 Exploitation

The exploitation phase is simply to exploit the vulnerabilities found in the above section.

3.5.1 Tools used

- The reg command : to save SAM, SYSTEM and SECURITY files from the Windows 10 computer,
- Secretsdump python script : to extract the password's hashes,
- Hash Suite Free : to crack the hashes,
- Xhydra Linux's command : to extract the passwords.

3.6 Maintaining the access

Now that we gained the control over the infrastructure, we want to maintaining our access to it for further use.
It is important that this open door isn't noticed.

3.6.1 Tools used

- ProRat : setting up an open door to the infrastructure.

[7] https://owasp.org/www-project-top-ten/

4 Results

For more technical or precise explanation please confer to the annex at the end of this report.

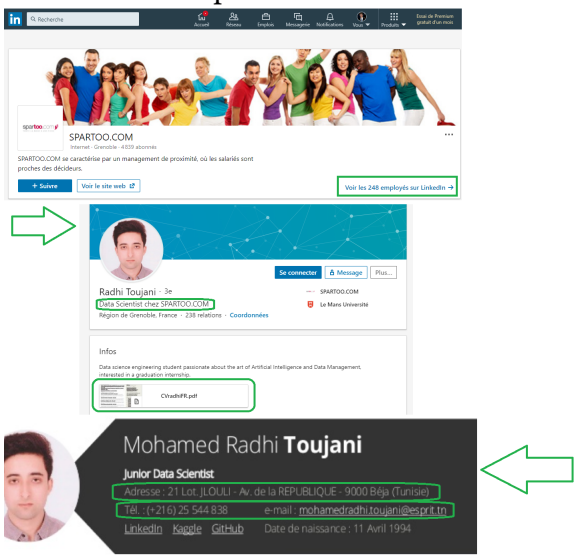
4.1 Competitor's website

According to the score given by Netcraft, the competitor's website spartoo.com is very secure : they assigned it the risk score of 0 out of 10.
Anyway, here is everything we could gather from the website :

Name	www.spartoo.com
IP address	185.28.232.10
IP location	France, Auvergne-rhone-alpes – Grenoble – Spartoo Sas
Registrant	TOUCHARD Jeremie
Registrant Organization	SPARTOO
Creation date	September 27th, 2005
Expiration date	September 27th, 2019
Nameserver	ns-01.ig-1.net
Last Reboot	142 days ago
Operating System	Linux
Web server	Apache
Contacts	N/A – none found
Netcraft Risk Rating	**0/10 : Safe**

As recon-ng hasn't been successful in its search for contacts, we did it manually by looking on LinkedIn.

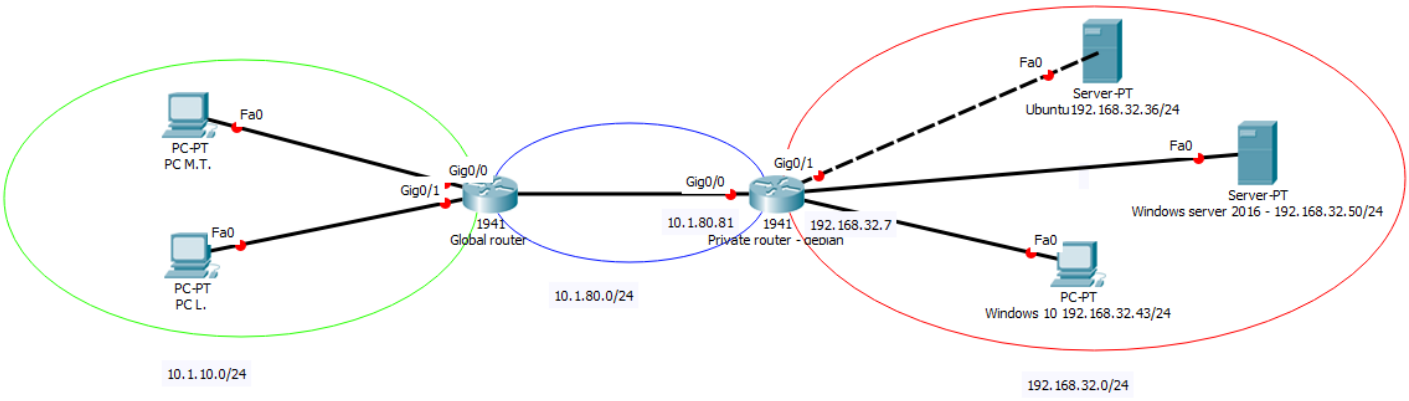
Here is an example of what kind of information could be obtained :



We could easily get the address, phone number and e-mail from an employee of the company.

4.2 Infrastructure's topology

Here is a draft illustrating the topology of the infrastructure :



4.3 Enumeration

The windows server 2016 is running multiple services. Some of them are known as high-risk ports if misconfigured. It is important to configure and test properly the FTP, HTTP, netbios-ssn, SNMP and ssh ports, for example.

IP Address	Operating System	Running Services
192.168.32.36	Ubuntu	22 : ssh (openssh), 53: domain (bind9), 80: http (apache2), 110 & 995 : pop3, 139 & 445: netbios-ssn (samba), 143 & 993 : imap.
192.168.32.50	Windows Server 2016	21 : ftp (ftpd), 22: ssh (openssh), 110 & 995: pop3, 123 = ntp, 139: netbios-ssn (samba),143 & 993: imap, 80: http (apache2), 53: domain (bind9), 88: kerberos, 161 : snmp (snmpv1), 389 & 3268 : LDAP, 445 : microsoft-ds (datacenter), 446: kpasswd5, 135 & 593 & 2103-5-7 : RPC, 3389: ms-wbt-server.
192.168.32.43	Windows 10	135 : RPC, 139 : netbios-ssn (samba), 445 : microsoft-ds (datacenter).
192.168.32.7	Debian	2 : ssh.

4.4 Vulnerabilities

Medium risk : Running Nessus on the system returned us a high risk vulnerability that drew our attention : an SNMP agent misconfiguration.
The SNMP agent is set to the default community name. An attacker could use this information to get more information about the remote host, or even change the configuration.

Severity	CVSS	Plugin	Name
HIGH	7.5	41028	SNMP Agent Default Community Name (public)

Mitigation : Disable the SNMP service on the remote host if possible. If the service is needed, simply change the default community string or filter inbound UDP packets to this port.

4.5 User Accounts

High risk : We have been able to discover every single password from the users.
Anyway, there is not even one password that matches the good practice code. For example, there is no account using any special character in its password.
This is an extremely easy attack point for the hacker that has internal access to the network of our client :

Operating System	Domain or Local	Username	Group	Password
W2k16 & W10	Domain	Administrator	Domain Administrators	123456a
W2k16 & W10	Domain	Jason	Administrators / Users	qwerty
W2k16 & W10	Domain	Martin	Administrators / Users	apple
W2k16 & W10	Domain	Shiela	Administrators / Users	test
W2k16 & W10	Domain	Guest	Guests	Guest
Windows 10	Local	Admin	Administrators	Tigrou007
Windows 10	Local	Melchior	Administrators	Melchior
Ubuntu	Local	user	user / sudoers	ChangeMe
Debian	Local	user	user / sudoers	123456

Furthermore, every account is in the administrator Group.
Groups seriously need to be created and user divided into them, so that GPOs can be applied to limit the risk coming from users.

Mitigation : Setting up a strong password policy[8] :

For instance, here is a good password policy :
Change the password every 90 to 180 days.
Take wordlists used for dictionary attacks and use them as passwords blacklist.
Do not use personal information in your passwords, they could be gathered and used to guess them.
Never use your passwords multiple times.
Use **at least** :

- 8 characters,
- 1 capital letter,
- 1 lower-case letter,
- 1 number,
- one special character (!, #, &, etc.)[9].

[8] Confer https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff741764(v=msdn.10)?redirectedfrom=MSDN
[9] confer https://docs.oracle.com/cd/E11223_01/doc.910/e11197/app_special_char.htm#MCMAD416

If you have troubles remembering your passwords, use a password keeper, such as keepass[10].

Furthermore, Groups must be created with their own rights, and users separated into them.

Simple users should **not** have the Administrator right. Groups should be managed by GPO[11] to limit the impact users can have. Furthermore, Linux, critical folders, such as webpages, should have corrects rights assigned.

4.6 Malicious activity

High risk : With the help of the obtained credentials and the absence of any antivirus or firewall, we have been able to use what we call a *keylogger*, which is a software that save remotely every single key pressed on the computer.
We simply had to download a payload from the server to the client.
Now that the server can have access to the client, we will escalate the privilege and gain the administrator's right on the computer, using the metasploit bypassUAC exploit.

We now have access to everything that is written on the windows 10 computer : every single type of passwords (bank accounts, user accounts, etc.) and every conversation : the confidentiality is fully broken.
We set the software invisible to the naked human eye and to the anti-virus of the computer : it appears as an image file :

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
[-] stdapi_ui_start_keyscan: Operation failed: Incorrect function.
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><M
AJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ
><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><CR>
<CR>
administrator<CR>
easypassword<CR>
<CR>
bonjour,<CR>
voici les docuemnts secrtes de l'entreprise<CR>
<CR>
restez discret.

meterpreter >
```

Mitigation : Installing and properly configuring firewalls and anti-viruses on every single computer of the network.

Installing and configuring these via the AD so that users can't disable the firewall and the anti-virus without the admin right.

[10] https://keepass.info/
[11] Group Policy Object

5 Conclusion

To conclude, here is a summary of the results :
High risk : password policy, network defense, access rights management.
Medium risk : software and operating systems vulnerabilities, SNMP agent misconfiguration.
For more precise information please confer to the beginning of this report in summary of result in the introduction for any technical recommendation.

Considering all the risks listed above, *This is the socks* is in a critical security status.
If the company were to come under attack, the consequences would be dreadful.
The company should patch every single high risk vulnerabilities above first, as they are critical.

If any attacker could find an access point from the external network, the company's current security would literally hand the entire network over the attacker.

5.1 Recommendations

Please confer to the beginning of this report in summary of result in the introduction for any technical recommendation.

5.1.1 About setting priorities

- Fixing the high vulnerability first, then the medium ones.[12]

5.1.2 About following best practices

A "working' system is great but sadly not enough : good practices of security have to be followed to make sure the system is secured and is maintained that way.

For example, good practices of remote shell require to disable password authentication, change the port number, and limit the range of IP addresses that can connect to the server, which has probably not been done on this infrastructure.

For more information, please visit The National Cyber Security Centre.

[12] Confer Vulnerabilities part.

6 Annex

6.1 Discovery of the competitor's website

Here are some information that we could gather from the website using whois :

Domain Profile

Registrant	TOUCHARD Jeremie
Registrant Org	SPARTOO
Registrant Country	fr
Registrar	Safebrands SAS SafeBrands SAS IANA ID: 1290 URL: http://www.safebrands.com,http://safebrands.com Whois Server: whois.safebrands.com legal@safebrands.com (p) 33488662222
Registrar Status	clientTransferProhibited
Dates	5,142 days old Created on 2005-09-27 Expires on 2019-09-27 Updated on 2018-08-11
Name Servers	NS-01.IG-1.NET (has 528 domains) NS-02.IG-1.NET (has 528 domains) NS-03.IG-1.NET (has 528 domains)
Tech Contact	Host Master SafeBrands Pole Media de la Belle de Mai 37 rue Guibal, Marseille cedex 03, 13356, fr clientele@safebrands.com (p) 33488662222 (f) 33488662220
IP Address	185.28.232.10 - 57 other sites hosted on this server
IP Location	- Auvergne-rhone-alpes - Grenoble - Spartoo Sas
ASN	AS39605 IGUANESOLUTIONS, FR (registered Mar 24, 2006)

We can get the IP addresses, location and the day it was created.

Furthermore, we discovered the risk rating of the website, its nameserver and the last time the server has been rebooted :

Site title	Chaussures, sacs et vêtements | Livraison Gratuite | SPARTOO
Site rank	310992
Description	D\303\251couvrez plus de 552000 Chaussures, Bottes, Ballerines, V\303\252tements et Sacs \303\2
Keywords	spartoo, spartoo.com, vente en ligne, boutique en ligne, chaussures, sacs, v\303\252tements, mode
Netcraft Risk Rating [FAQ]	0/10

Netblock Owner	Spartoo Hosting Infrastructure
Nameserver	ns-01.ig-1.net
DNS admin	hostmaster@iguanesolutions.net
Reverse DNS	spo-webvip-01.ig-1.net
Nameserver organisation	whois.gandi.net
Hosting company	Iguane Solutions
DNS Security Extensions	*unknown*

Last Reboot (142 days ago)

Netblock owner	IP address
Spartoo Hosting Infrastructure	185.28.232.10

OS	Web server
Linux	Apache

ssl certificates issuers :

```
Updated,Type,Module,Source,F/P,Data
2019-10-23 07:54:20,SSL_CERTIFICATE_ISSUER,sfp_sslcert,http://photos6.spartoo.com,0,"C=FR,ST=Paris,L=Paris,O=Gandi,CN=Gandi Standard SSL CA 2"
2019-10-23 07:54:29,SSL_CERTIFICATE_ISSUER,sfp_ssltools,photos6.spartoo.com,0,"C=FR,ST=Paris,L=Paris,O=Gandi,CN=Gandi Standard SSL CA 2"
2019-10-23 07:26:15,SSL_CERTIFICATE_ISSUER,sfp_sslcert,http://nvaxcb.spartoo.com,0,"C=US,O=DigiCert Inc,CN=DigiCert ECC Secure Server CA"
2019-10-23 07:28:40,SSL_CERTIFICATE_ISSUER,sfp_sslcert,74.119.119.139,0,"C=US,O=DigiCert Inc,CN=DigiCert ECC Secure Server CA"
2019-10-23 07:28:44,SSL_CERTIFICATE_ISSUER,sfp_ssltools,74.119.119.139,0,"C=US,O=DigiCert Inc,CN=DigiCert ECC Secure Server CA"
2019-10-23 07:28:52,SSL_CERTIFICATE_ISSUER,sfp_ssltools,nvaxcb.spartoo.com,0,"C=US,O=DigiCert Inc,CN=DigiCert ECC Secure Server CA"
2019-10-23 07:33:36,SSL_CERTIFICATE_ISSUER,sfp_sslcert,178.250.2.146,0,"C=US,O=DigiCert Inc,CN=DigiCert ECC Secure Server CA"
2019-10-23 07:33:41,SSL_CERTIFICATE_ISSUER,sfp_ssltools,178.250.2.146,0,"C=US,O=DigiCert Inc,CN=DigiCert ECC Secure Server CA"
```

We scanned their hosts :

```
[*] z.spartoo.com => No record found.
[*] zlog.spartoo.com => No record found.
[*] yu.spartoo.com => No record found.
[*] z-log.spartoo.com => No record found.
[*] zeus.spartoo.com => No record found.
[*] zera.spartoo.com => No record found.
[*] zulu.spartoo.com => No record found.
[*] zw.spartoo.com => No record found.
[*] zm.spartoo.com => No record found.
[*] vend.spartoo.com => No record found.

-------
SUMMARY
-------
[*] 48 total (36 new) hosts found.
```

We tried to get contacts from the websites, but it was impossible : the security team did a great job :

```
[recon-ng][matis][whois_pocs] > run

-----------
SPARTOO.COM
-----------
[*] URL: http://whois.arin.net/rest/pocs;domain=spartoo.com
[*] No contacts found.
```

6.2 Information about the infrastructure

We will now probe the network of our client. We are pinging his website to get its ip address :

```
C:\Users\kirikou>ping www.goodshopping-A09.com

Pinging www.goodshopping-a09.com [192.168.32.50] with 32 bytes of data:
Reply from 192.168.32.50: bytes=32 time=2ms TTL=126
Reply from 192.168.32.50: bytes=32 time<1ms TTL=126
Reply from 192.168.32.50: bytes=32 time=1ms TTL=126
Reply from 192.168.32.50: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.32.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 1ms
```

Now we know that the website has the 192.168.32.50 ip address.
Next, we found the maximum frame size on the network :

```
C:\Users\kirikou>ping www.goodshopping-A09.com -f -l 1473

Pinging www.goodshopping-a09.com [192.168.32.50] with 1473 bytes of data:
Packet needs to be fragmented but DF set.
Packet needs to be fragmented but DF set.

Ping statistics for 192.168.32.50:
    Packets: Sent = 2, Received = 0, Lost = 2 (100% loss),
Control-C
^C
C:\Users\kirikou>ping www.goodshopping-A09.com -f -l 1472

Pinging www.goodshopping-a09.com [192.168.32.50] with 1472 bytes of data:
Reply from 192.168.32.50: bytes=1472 time=1ms TTL=126
Reply from 192.168.32.50: bytes=1472 time=4ms TTL=126
Reply from 192.168.32.50: bytes=1472 time=1ms TTL=126

Ping statistics for 192.168.32.50:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 4ms, Average = 2ms
```

We can see here that the maximum frame size of the ping must be 1472, otherwise the pings won't reach their destination, so they need to be fragmented.
Same thing for the TTL :

```
C:\Users\kirikou>ping www.goodshopping-A09.com -i 3

Pinging www.goodshopping-a09.com [192.168.32.50] with 32 bytes of data:
Reply from 192.168.32.50: bytes=32 time<1ms TTL=126
Reply from 192.168.32.50: bytes=32 time<1ms TTL=126
Reply from 192.168.32.50: bytes=32 time<1ms TTL=126
Reply from 192.168.32.50: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.32.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\kirikou>ping www.goodshopping-A09.com -i 2

Pinging www.goodshopping-a09.com [192.168.32.50] with 32 bytes of data:
Reply from 10.1.80.81: TTL expired in transit.
Reply from 10.1.80.81: TTL expired in transit.
Reply from 10.1.80.81: TTL expired in transit.
Reply from 10.1.80.81: TTL expired in transit.

Ping statistics for 192.168.32.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

Using the traceroute command, we will be able to check the route of the ping.

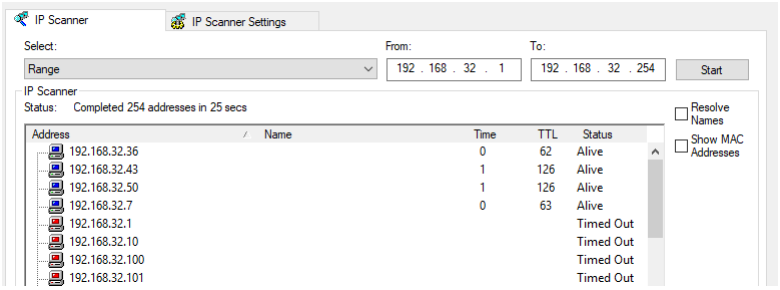
```
C:\Users\kirikou>tracert www.goodshopping-A09.com

Tracing route to www.goodshopping-a09.com [192.168.32.50]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.1.10.248
  2     1 ms     4 ms    <1 ms  10.1.80.81
  3     1 ms     1 ms     1 ms  192.168.32.50

Trace complete.
```

These ips will be used later on this section to draw the topology of the network.

Nslookup gives us the ip address, the dns and the mail server address of the server.

```
C:\Users\kirikou>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  10.1.10.248

> set type=a
> www.goodshopping-A09.com
Server:  UnKnown
Address:  10.1.10.248

Name:    www.goodshopping-a09.com
Address:  192.168.32.50

> set type=cname
> www.goodshopping-A09.com
Server:  UnKnown
Address:  10.1.10.248

goodshopping-a09.com
        primary name server = dns.goodshopping-a09.com
        responsible mail addr = root.goodshopping-a09.com
        serial  = 20191105
        refresh = 3600 (1 hour)
        retry   = 1800 (30 mins)
        expire  = 604800 (7 days)
        default TTL = 86400 (1 day)
>
```

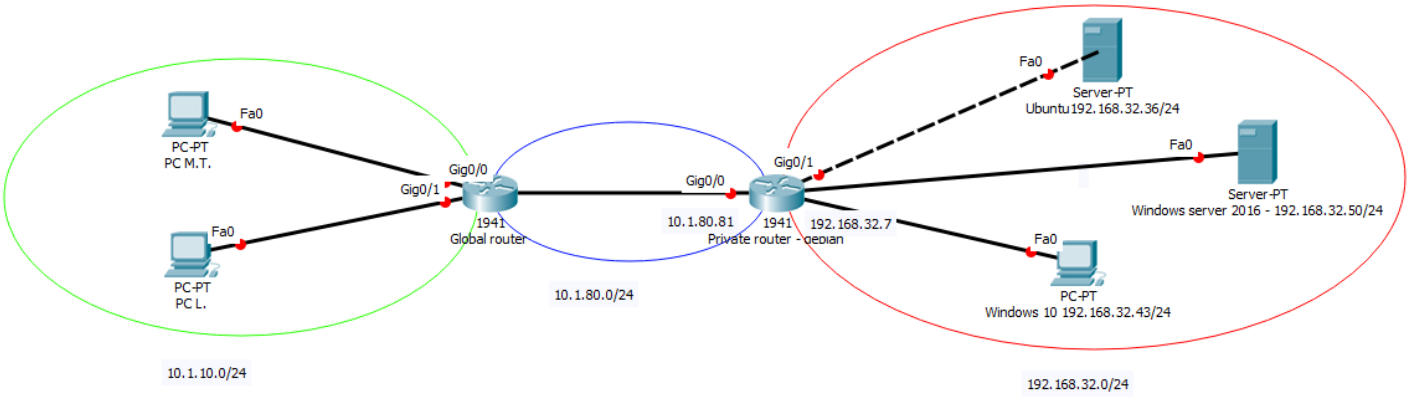
We pinged the entire network and here are the 4 computers we discovered :



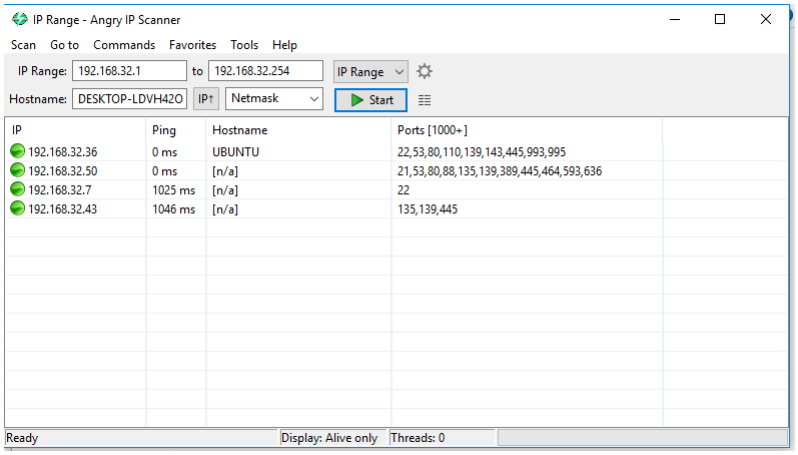
Results

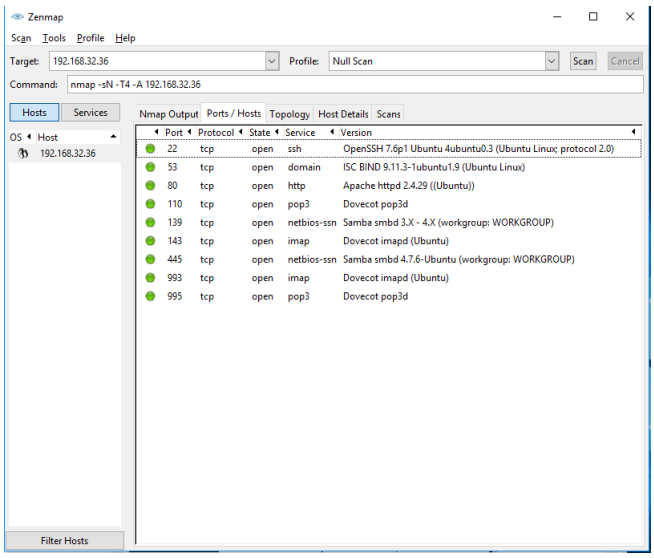
Hop	Time	Name	Details
3		[192.168.32.50]	Complete.
1	16	10.1.10.248	11/07/19 05:29:41
2	15	10.1.80.81	11/07/19 05:29:41
3	0	192.168.32.50	11/07/19 05:29:41
3		[192.168.32.43]	Complete.
1	31	10.1.10.248	11/07/19 05:31:29
2	16	10.1.80.81	11/07/19 05:31:30
3	0	192.168.32.43	11/07/19 05:31:30
3		[192.168.32.36]	Complete.
1	16	10.1.10.248	11/07/19 05:31:47
2	31	10.1.80.81	11/07/19 05:31:48
3	1	192.168.32.36	11/07/19 05:31:48
2		[192.168.32.7]	Complete.
1	16	10.1.10.248	11/07/19 05:31:53
2	0	192.168.32.7	11/07/19 05:31:53

We have then been able to produce a draft of the infrastructure :



Using the account's credentials Mr. MELCHIOR provided us, we have been able to scan the services running on the infrastructure :





Same thing for the snmp server :

```
root@kali:~# nmap -sU -p 161 192.168.32.*
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-07 10:39 EST
Nmap scan report for 192.168.32.7
Host is up (0.00085s latency).

PORT    STATE         SERVICE
161/udp open|filtered snmp

Nmap scan report for 192.168.32.36
Host is up (0.00091s latency).

PORT    STATE  SERVICE
161/udp closed snmp

Nmap scan report for 192.168.32.43
Host is up (0.00071s latency).

PORT    STATE  SERVICE
161/udp closed snmp

Nmap scan report for 192.168.32.50
Host is up (0.00079s latency).

PORT    STATE         SERVICE
161/udp open|filtered snmp

Nmap done: 256 IP addresses (4 hosts up) scanned in 3.97 seconds
```

6.3 Vulnerabilities

As the main machines and services have been exposed, we can use tools to determine if those services can be exploited.
One of these tools is called Nessus (OpenVAS is a fork of Nessus).

With Nessus, we discoverd one 'High' vulnerability on host 192.168.32.50. Nessus describes it as follows:
"The community name of the remote SNMP server can be guessed. An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications)".

192.168.32.50

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	1	6	1	50

Severity	CVSS	Plugin	Name
HIGH	7.5	41028	SNMP Agent Default Community Name (public)
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	12217	DNS Server Cache Snooping Remote Information Disclosure
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	4.3	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only

Using an other tool might reveal other vulnerabilities that the other one did not spot. We double-checked our results with GFI-Languard.

On the other computers, we only found a few medium vulnerabilities, which are the same[13] as the .50 computer :

192.168.32.43

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	21

Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)

192.168.32.36

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	3	0	51

Severity	CVSS	Plugin	Name
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	57608	SMB Signing not required

192.168.32.7

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	0	0	15

[13] Except for the SMB Signing not required

6.4 Exploitation of the vulnerabilities

6.4.1 From hashes to passwords

With the password of user Martin, we were able to "steal" some registry files from the Windows 10 machine: SAM, SYSTEM and SECURITY.

With the tool "impacket", we were able to decode the files and display it as a list of usernames and hashes:

```
root@kali:~/Documents/Win10# secretsdump.py -sam sam -security security -system system LOCAL
Impacket v0.9.21-dev - Copyright 2019 SecureAuth Corporation

[*] Target system bootKey: 0xe7c71ce802841290ae3f01f2ac15f04c
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:93d84d6712df4366ce6d48f60889fbc8:::
Martin:1003:aad3b435b51404eeaad3b435b51404ee:5ebe7dfa074da8ee8aef1faa2bbde876:::
Jason:1004:aad3b435b51404eeaad3b435b51404ee:2d20d252a479f485cdf5e171d93985bf:::
Shiela:1005:aad3b435b51404eeaad3b435b51404ee:0cb6948805f797bf2a82807973b89537:::
Admin:1006:aad3b435b51404eeaad3b435b51404ee:944f97c19a6d1d3b51a073b1746df642:::
Melchior:1007:aad3b435b51404eeaad3b435b51404ee:9972e2ead35ae1f1226459ea2433d826:::
```

After going through hashkiller, a website that looks up strings from hashes, we were able to find the link between several hashes and passwords (3rd line is Martin, 4th line is Jason, ...etc).

Cracker Results:

```
31d6cfe0d16ae931b73c59d7e0c089c0 [No Match]
93d84d6712df4366ce6d48f60889fbc8 [No Match]
5ebe7dfa074da8ee8aef1faa2bbde876 NTLM apple
2d20d252a479f485cdf5e171d93985bf NTLM qwerty
0cb6948805f797bf2a82807973b89537 NTLM test
944f97c19a6d1d3b51a073b1746df642 NTLM Tigrou007
9972e2ead35ae1f1226459ea2433d826 NTLM Melchior
```

Doing the same with the Windows server machine, we got this:

Cracker Results:

```
Administrator: [Invalid ]
e5df2c988f0d77ef35aa949be5dc95b5 NTLM 123456a.
Guest: [Invalid ]
31d6cfe0d16ae931b73c59d7e0c089c0 [No Match]
Martin: [Invalid ]
5ebe7dfa074da8ee8aef1faa2bbde876 NTLM apple
Jason: [Invalid ]
2d20d252a479f485cdf5e171d93985bf NTLM qwerty
Shiela: [Invalid ]
0cb6948805f797bf2a82807973b89537 NTLM test
```

6.4.2 Weak SSH policy is not good

The tool "xhydra" allows its user to try to connect to an SSH server with a dictionary or generated list of usernames and passwords. Because we knew the SSH user was named "user", it made our task easier and we were able to quickly find the passwords.
192.168.32.7 machine:

```
[STATUS] 241.50 tries/min, 2898 tries in 00:12h, 663 to do in 00:03h, 16 active
[22][ssh] host: 192.168.32.7   login: user   password: 123456
1 of 1 target successfully completed, 1 valid password found
```

192.168.32.36 machine:

```
[STATUS] 221.50 tries/min, 2658 tries in 00:12h, 903 to do in 00:05h, 16 active
[22][ssh] host: 192.168.32.36   login: user   password: ChangeMe
1 of 1 target successfully completed, 1 valid password found
```

Obviously these passwords have to be changed, and the SSH server settings need updating.

6.4.3 A foot in the door: privilege escalation

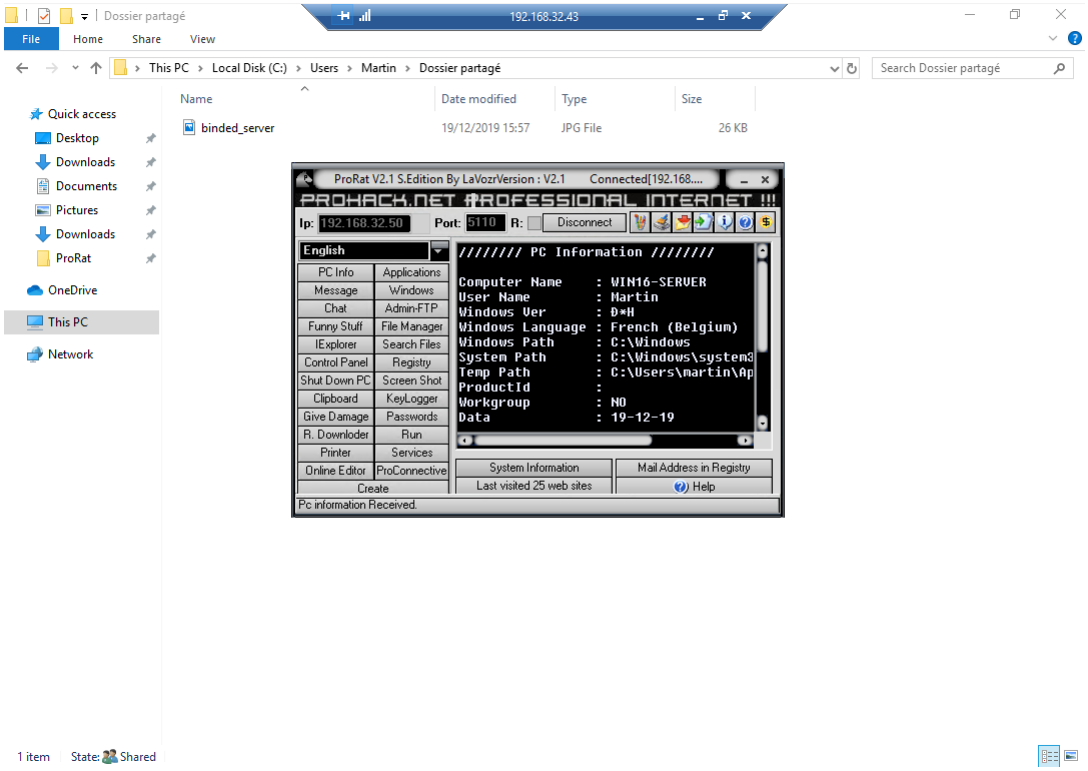
As a proof of concept, we then simulated what could happen if a simple malware (we used a key-logger) were to be executed on the machine. This kind of malware can be used to catch credentials, and help the hackers slowly becoming the super user. We used the Metasploit Framework as our primary tool.
As the following illustration shows, we were able to retrieve sensible information from the distant computer:

```
meterpreter > keyscan_start
Starting the keystroke sniffer ...
[-] stdapi_ui_start_keyscan: Operation failed: Incorrect function.
meterpreter > keyscan_dump
Dumping captured keystrokes ...
<MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><M
AJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ
><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><MAJ><CR>
<CR>
administrator<CR>
easypassword<CR>
<CR>
bonjour,<CR>
voici les docuemnts secrtes de l'entreprise<CR>
<CR>
restez discret.

meterpreter >
```

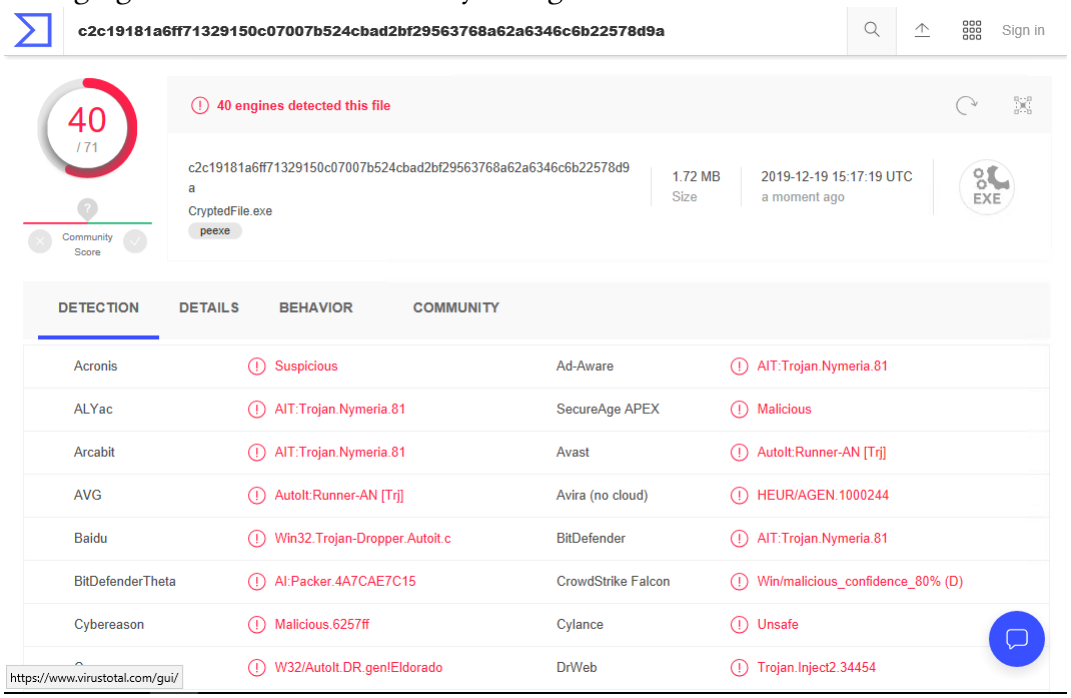
6.4.4 Forever and ever: maintaining access

A malware file isn't always easy to spot, and making it invisible is in the hacker's best interest:

Executables can be hidden as image files (ProRat is an example of that):



Tools can modify the source code so it is not detected by some of the anti-virus : these simply use the hash to compare the software to known viruses.
Changing the source code obviously changes the hash :



7 References

- Our reference : Offensive Security Penetration Test Report.
- Documents we followed to proceed with the penetration test.
- Special characters in passwords.
- Strong passwords policy.
- Tcp and UDP ports list.
- The National Cyber Security Centre