



# Cryptograghy And Cyber security risk analysis

## (CY702)

**Dr.Mohamed** **Saif**

***Project*** ***Part*** ***I*** ***(penetration*** ***testing)***

***-Information*** ***Gathering***

***-Exploitation***

Made by: ***Ahmed*** ***Elsayed*** ***Kareem*** ***Yasser***

**Phase** **one**

# Scan Report

- **Reconnaissance/** **Information** **Gathering** **Phase**

We begin with a network scan to examine the network and identify all available hosts and show the network topology:

**-sn:** Tell nmap to just scan available host with no port scan (ping scan) with ip range of 192.168.56.101 – 192.168.56.254

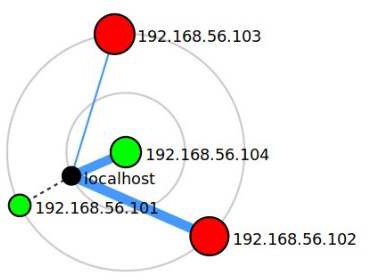
Nmap -sn 192.168.56.101-254

From this we see that the running hosts is on the following ip address’s

-192.168.56.102

-192.168.56.103

-192.168.56.104



Meanwhile IP: 192.168.56.101 shown in the topology Is the local machine

This topology design is from zenmap (nmap GUI)

* The green circle indicates that less than 3 ports open
* The red circle indicates more than 6 ports open

## We begin examining the ip and see the open port with service running and possibly their version and the OS using:

Nmap -A IPaddress

-A: Aggressive Scanning it combines OS Detection, Port Scanning and version Scanning, also provides better information

### - 192.168.56.102

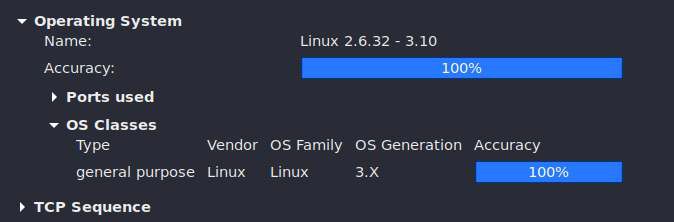
Open **ports** **Service**

|  |  |  |
| --- | --- | --- |
| - | 21 | FTP |
| - | 22 | SSH |
| - | 25 | SMTP |
| - | 139 | NETBIOS-SSN |
| - | 445 | NETBIOS-SSN |
| - | 993 | IMAPS |
| - | 995 | POP3S |

Machine name : SATURNA

Operating system

Linux kernel 3.0 on ubunto 12.04



### - 192.168.56.103

Nmap -A 192.168.56.103

We also use the same command as before to get information about the post OS, etc…

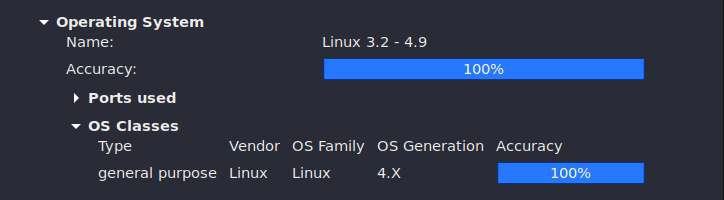
Open **ports** **Service**

|  |  |  |
| --- | --- | --- |
| - | 21 | FTP |
| - | 22 | SSH |
| - | 25 | SMTP |
| - | 53 | DOMAIN |
| - | 80 | HTTP |
| - | 110 | POP3 |
| - | 139 | NETBIOS-SSN |
| - | 143 | IMAP |
| - | 445 | NETBIOS-SSN |

Machine name : UBS16

Operating system

Linux kernel 4.4 on ubunto 16.04



### - 192.168.56.104

Nmap -A 192.168.56.104

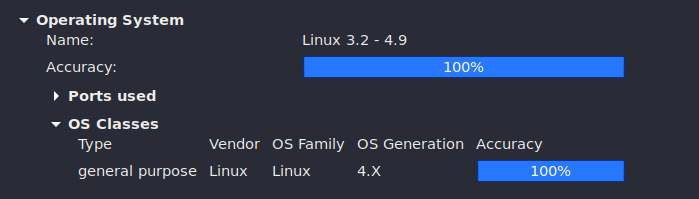
We also use the same command as before to get information about the post OS, etc…

Open **ports** **Service**

* 22 SSH
* 8080 HTTP-PROXY

Operating system

Linux kernel 4.4 on ubunto 16.04



**Phase** **two**

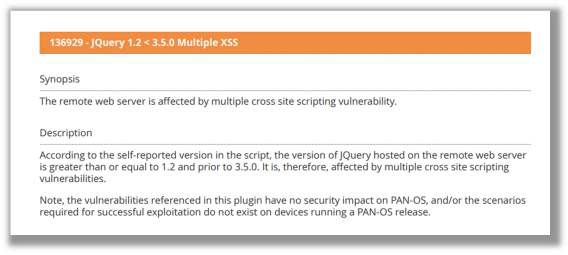
**- Exploitation**



Inspected the website, which is found on 192.168.56.104:8080 and managed to achieve a list of employee’s mail accounts: Enter the website -> Company’s tab

Now, we have a list of employees and potentially emails:

* + Peter Soell – [p.soell@saturn.com](mailto:p.soell@saturn.com)
  + Patrik Oliver Graf – [p.graf@saturn.com](mailto:p.graf@saturn.com)
  + Beate Dietrich – [b.dietrich@saturn.com](mailto:b.dietrich@saturn.com)
  + Jon Oberoi – [j.oberoi@saturn.com](mailto:j.oberoi@saturn.com)
  + Anaya Obaidat – [a.obaidat@saturn.com](mailto:a.obaidat@saturn.com)
  + Chester Kustarz – [c.kustarz@saturn.com](mailto:c.kustarz@saturn.com)



* + Joe Pesci – [j.pesci@saturn.com](mailto:j.pesci@saturn.com)
  + Arel – [l.arel@saturn.com](mailto:l.arel@saturn.com)
  + Wei Zhang – [w.zhang@saturn.com](mailto:w.zhang@saturn.com)
  + Abdulah Sahraoui – [a.sahraoui@saturn.com](mailto:a.sahraoui@saturn.com)
  + Ayesha Coulibaly – [a.coulibaly@saturn.com](mailto:a.coulibaly@saturn.com)

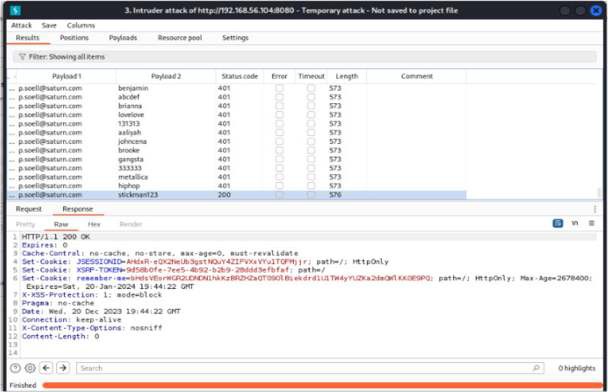
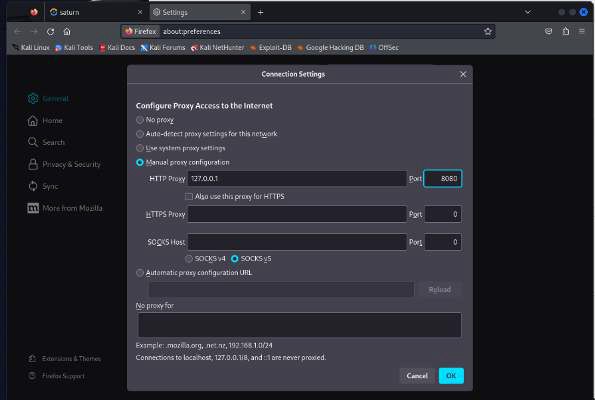
After we found the mail list it was more reasonable to

Exploit the HTTP vulnerability which was scanned by Nessus since that was the most valuable info we had

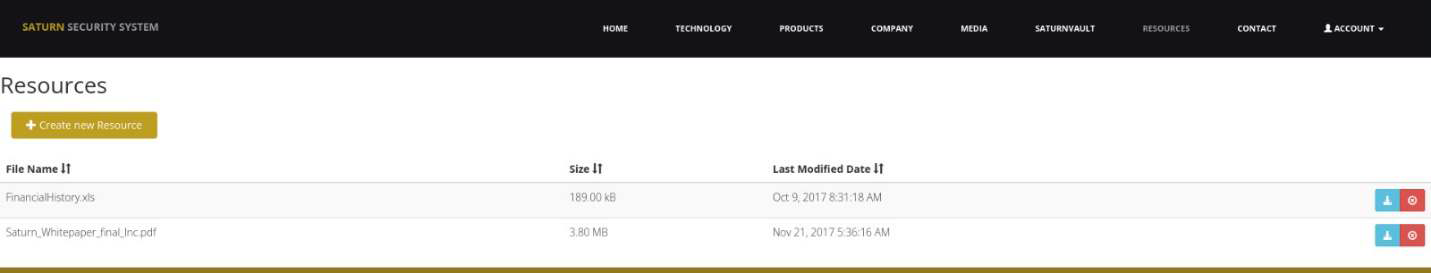
As a start

After Gaining this Information, we hoped to crack every password from this list, Starting by Peter Soell the founder, now let us go over burpsuite, we have the email and also have a password list provided by Dr. Mohammed

We split the 50,000+ password ﬁle and each begin to crack the ﬁrst email: [p.soell@saturn.com](mailto:p.soell@saturn.com)



After setting up the conﬁguration needed to start burpsuite such as Changing proxy settings and etc…



After days of running burpsuite, we ﬁnally found the password: ‘stickman123’ and we found 2 of the 4 ﬁles required: (Resources tap showed up directly after successful log in)

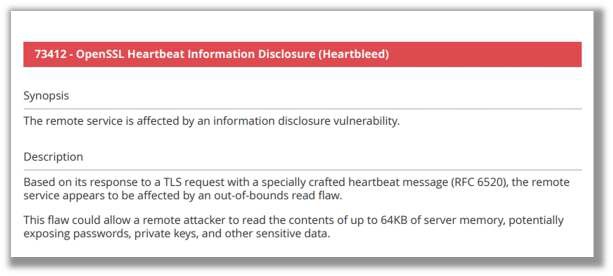


- Other exploitation

While the burpsuite was running we tried to exploit other vulnerabilities To speed up the process and save time.

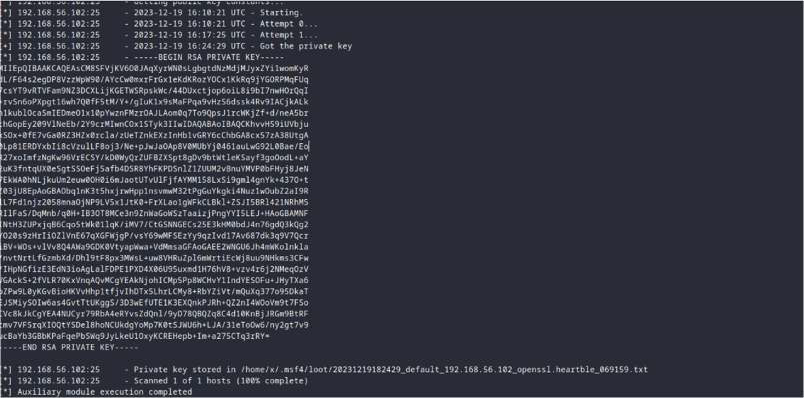
So, we decided to Focus for vulnerabilities that would comeback with valuable information To help us

Heartbleed on 192.168.56.102(SATURNA) was a good option for many



Reasons

* Potentially exposing passwords, private keys, and other sensitive data.
* Could be run in repeat until achieving that info.

**Action** **done**

Metasploit

Set action KEYS

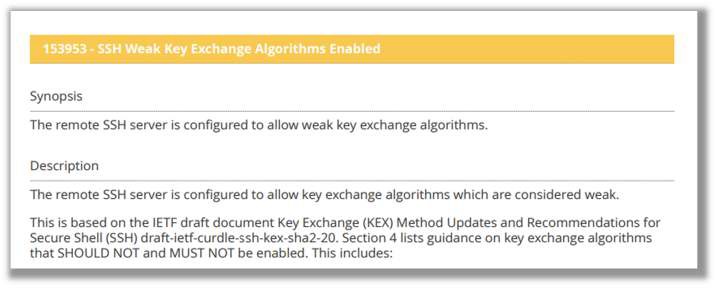
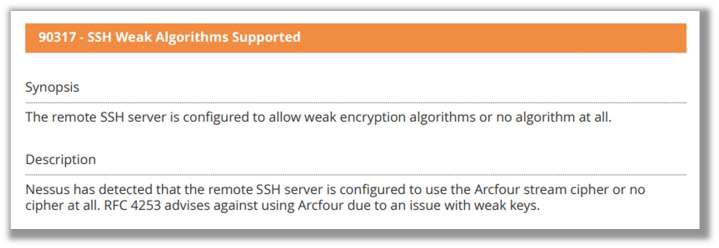
Set RHOSTS 192.168.56.102

Set RPORT 25

And after a short while private key was captured

### These attempts were done before achieving the password for the account [p.soell@saturna.com](mailto:p.soell@saturna.com)

Since there’s nothing else on the Website we aimed



To gain remote access to 192.168.56.102 Specially because

The vulnerability Nessus caught on port 22 and also, we got a key that could be useful passing the encryption algorithms via login.

Only thing we know about account that it could be one or more of the

Members we have their emails.

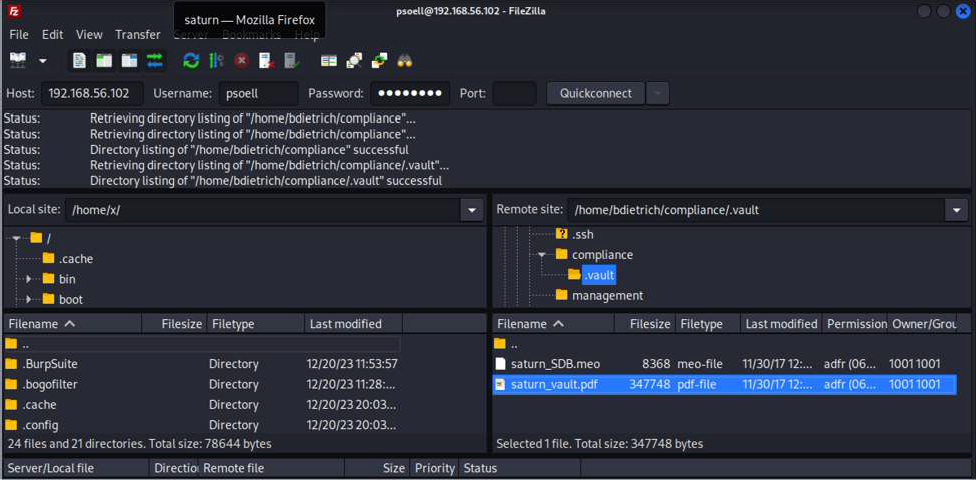
Removed the dots and mail extension from Peter Soell Mail (psoell) luckily, the same credentials is used on 1 of the machines

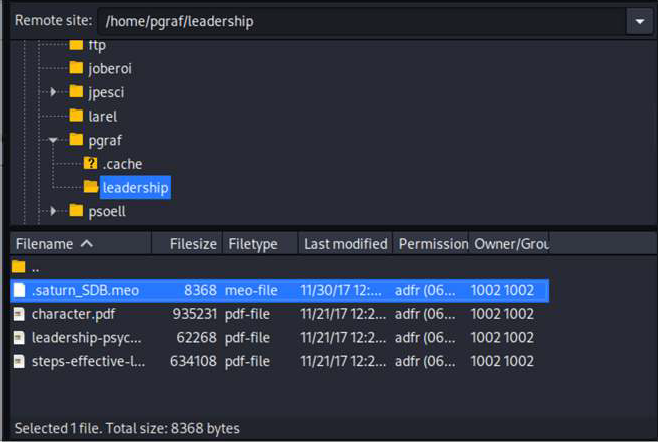
#### Code used.

Ssh [psoell@192.168.56.102](mailto:psoell@192.168.56.102)

Then we used SFTP (**FILE** **ZILLA**)

to transfer ﬁles to our local machine.

Found ﬁle Saturn\_vault.pdf (which contains company online banking account information) and Saturn\_SDB in bdietrich directory

**Saturn\_SDB** (safety deposit Box)

* Encrypted with

meo encryption software (NCH)

* File located in two proﬁles

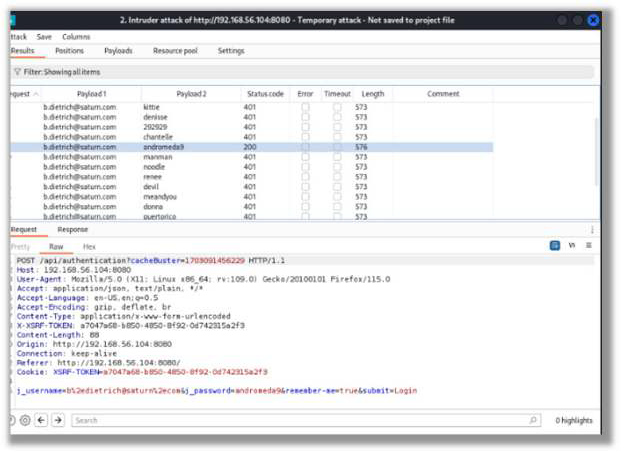
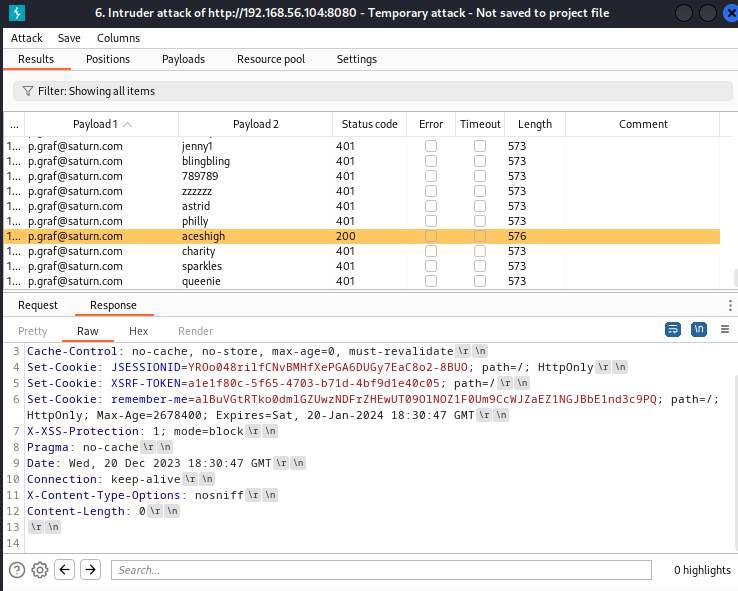
-(pgraf) CEO in leadership director

-(bdietrich) CFO in a hidden folder in

Compliance directory

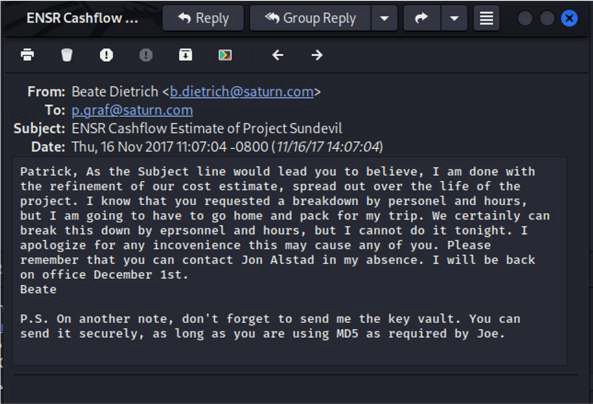
So most probably they shared it using Mail since it’s encrypted.

We cracked both their passwords using the previous method (burpsuite)

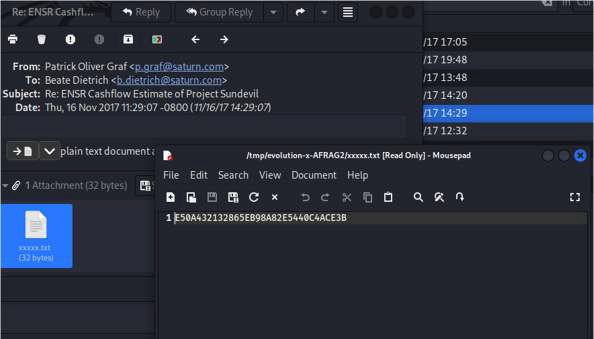


Credentials [p.graf@saturn.com](mailto:p.graf@saturn.com) : aceshigh

[b.dietrich@saturn.com](mailto:b.dietrich@saturn.com) : andromeda9

From this mail we understand that the ﬁle we

Found earlier is encrypted by a password that’s encrypted by a hash function (MD5)

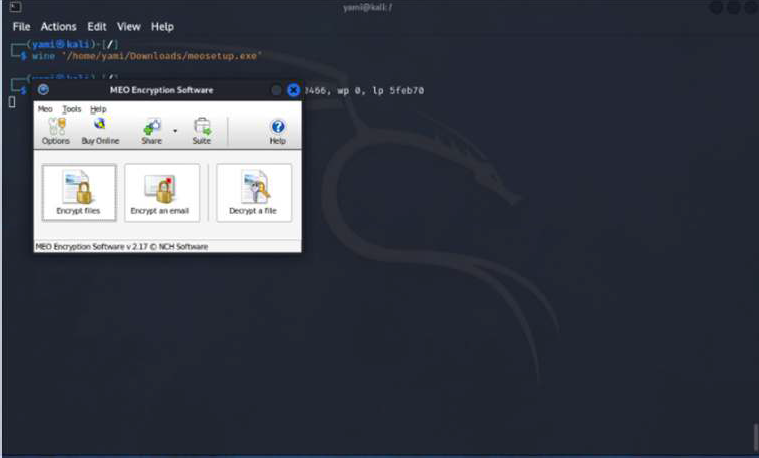
And the hash we retrieved from the sent mail

We can use (john) to match the hash with all Hash passwords that uses MD5

As you see the hashed password Is ( **letthemin** )



Now download NCH software and run with wine to decrypt the ﬁle

Now select the encrypted ﬁle Then type the password :

**letthemin**

**Safe** **Deposit** **Box** **Passcode:** **Abrac@d@bra**

**Master** **Key:** **XFTR@!!12YRT91VUT45R@L!ED@F0R!T**

#### Applications used

* Nmap
* nessus
* burpsuite
* evolution
* Metasploit
* SFTP using FILEZILLA
* John
* Wine
* NCH software