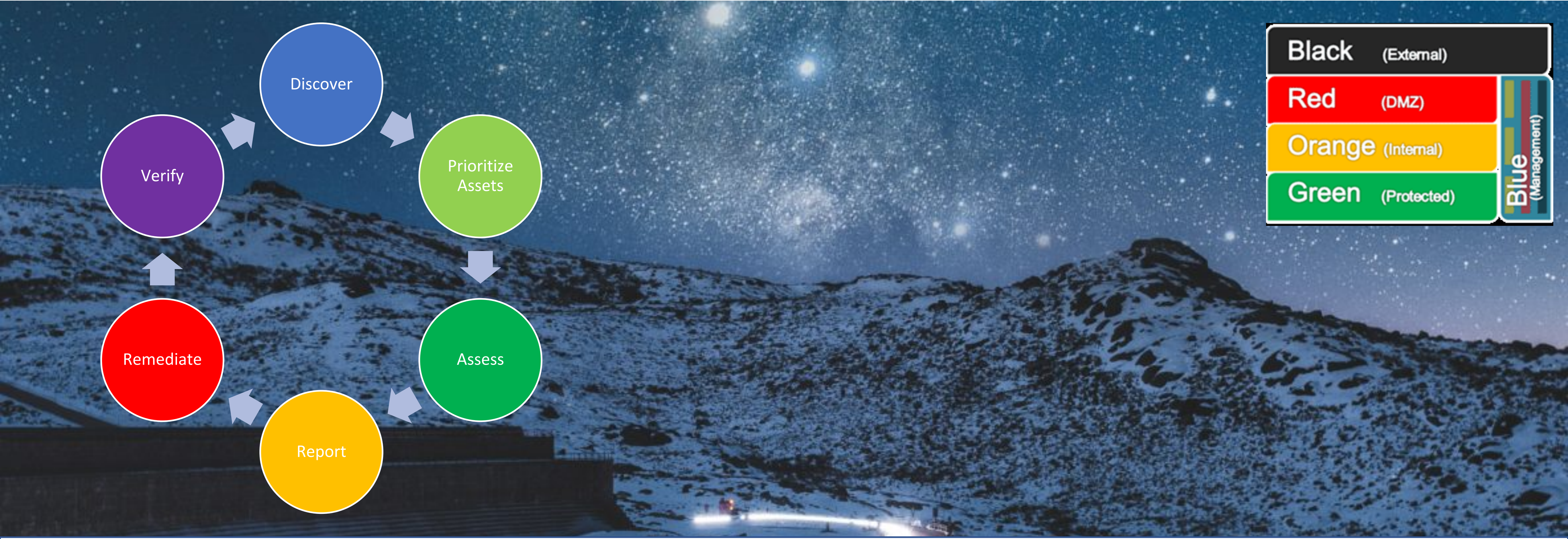
The art of Vulnerability Management

Vulnerability

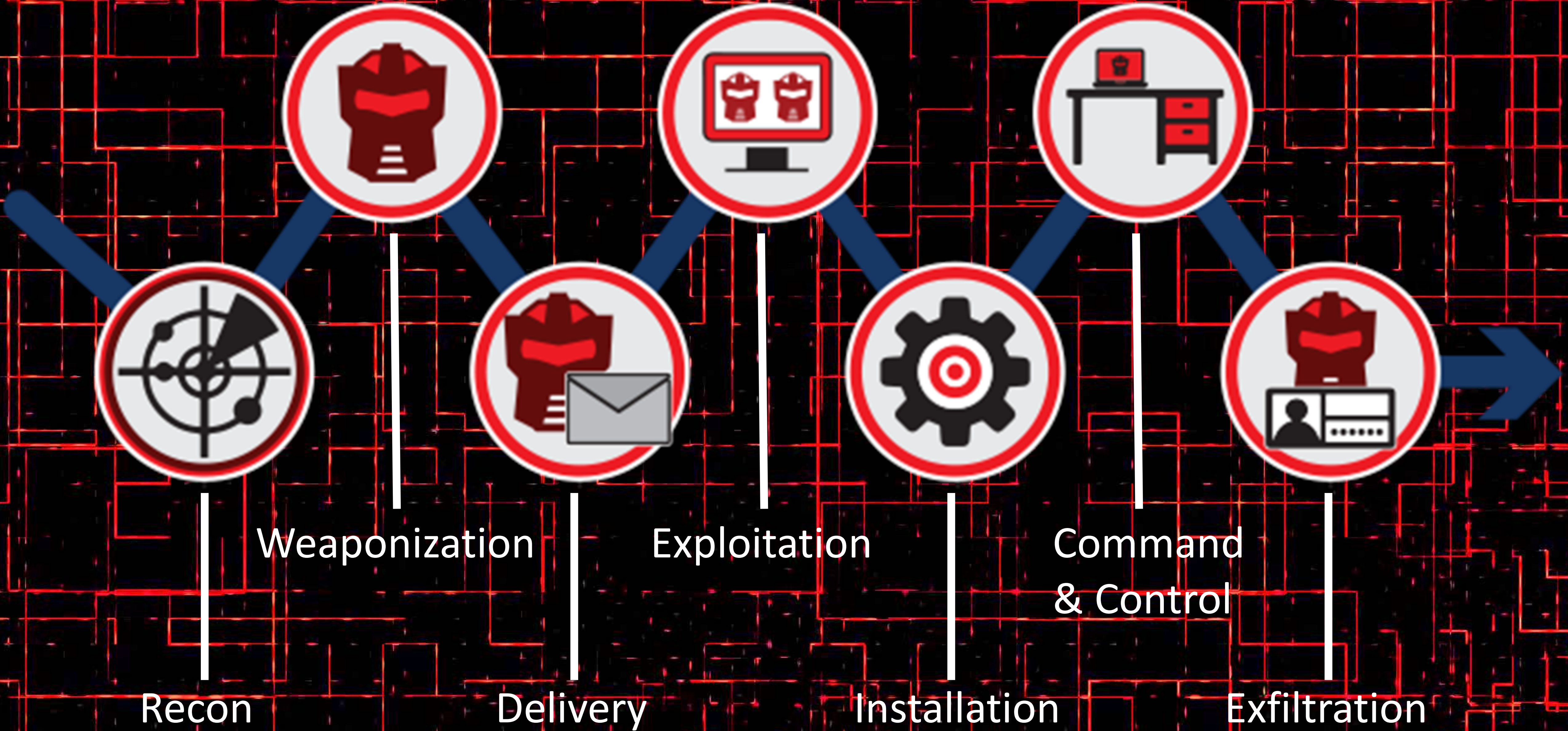
Days of age

0 → 1 → 5 → 10 → 15 → 20 → 25 → 30 → .....



	Prioriteit en oplostijd →	EEN direct	TWEE 2 weken	DRIE 1 maand	VIER 2 maanden	VIJF 6 maanden	ZES best effort
Scanner ↓	Zone ↓						
extern	zwart, rood	kritiek	hoog		middel		laag
intern	zwart, rood, blauw		kritiek	hoog	middel		laag
intern	oranje			kritiek	hoog	middel	laag
intern	groen				kritiek	hoog	mid-laag

CVSS	Score
kritiek	9 - 10
hoog	7 - 8.9
middel	4 - 6.9
laag	0 - 3.9



Recon

Weaponization

Delivery

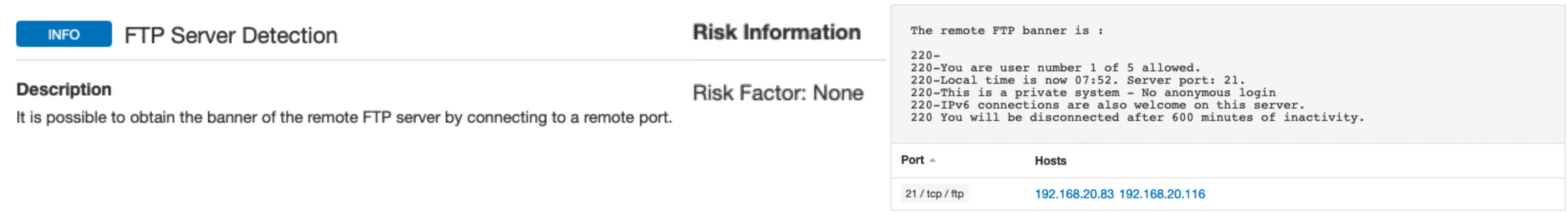
Exploitation

Installation

Command & Control

Exfiltration

Password Decryption



INFO **FTP Server Detection**

Description

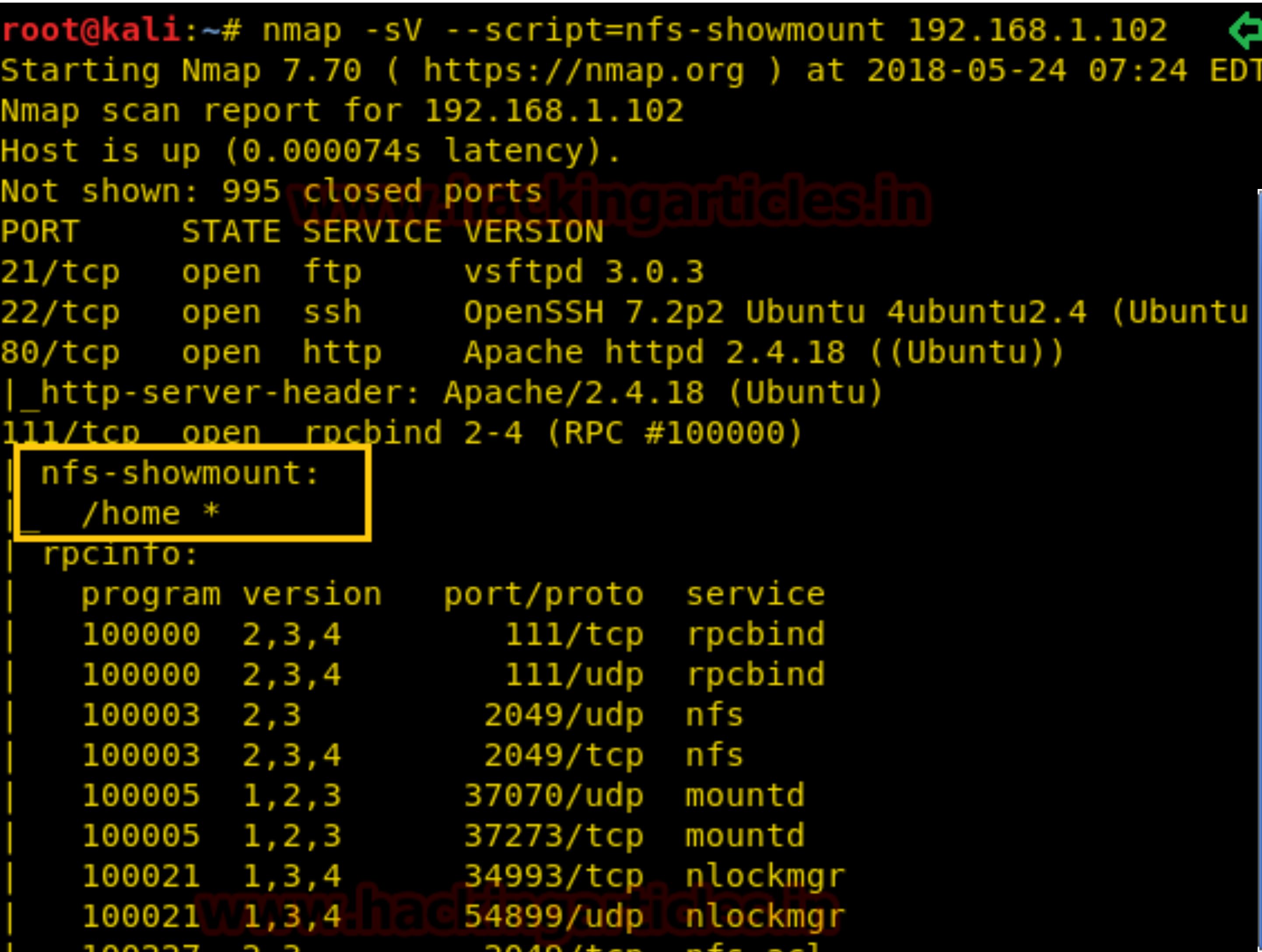
It is possible to obtain the banner of the remote FTP server by connecting to a remote port.

Risk Information

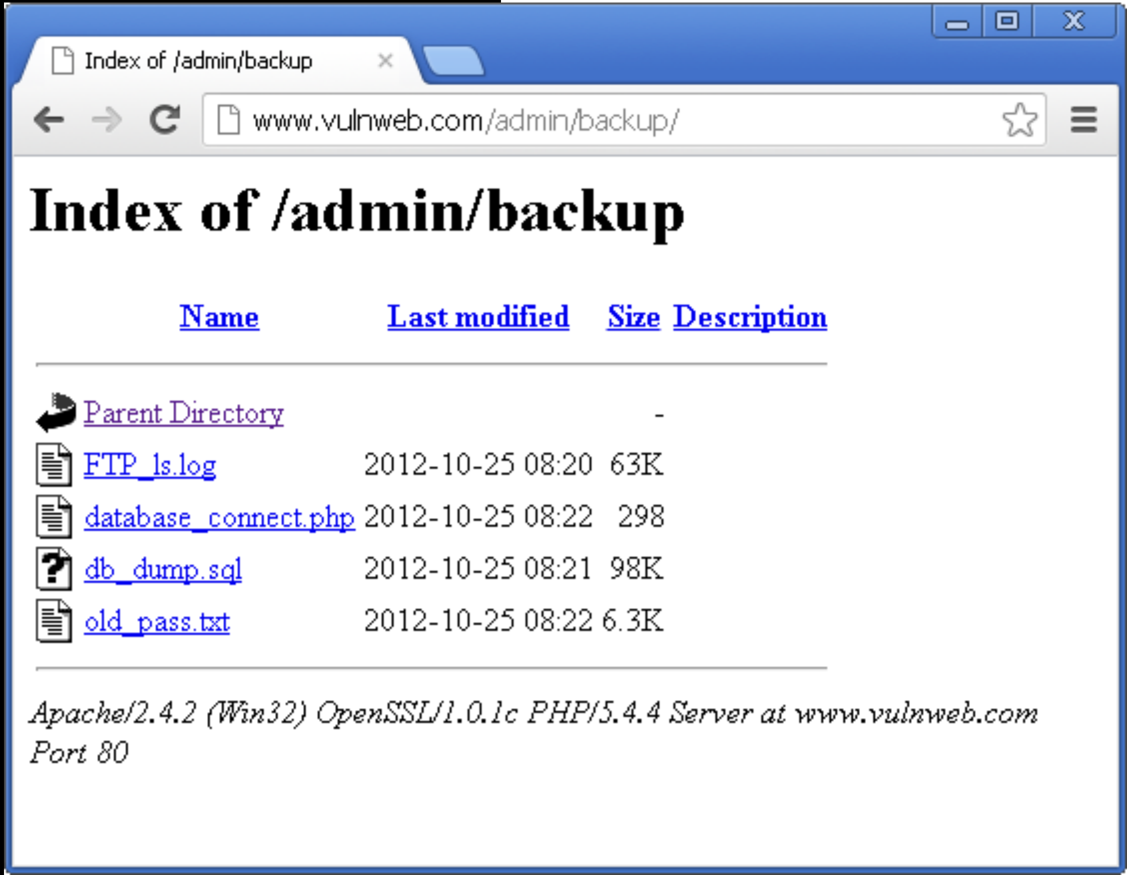
Risk Factor: None

```
The remote FTP banner is :

220-
220-You are user number 1 of 5 allowed.
220-Local time is now 07:52. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 600 minutes of inactivity.
```

Port	Hosts
21 / tcp / ftp	192.168.20.83 192.168.20.116



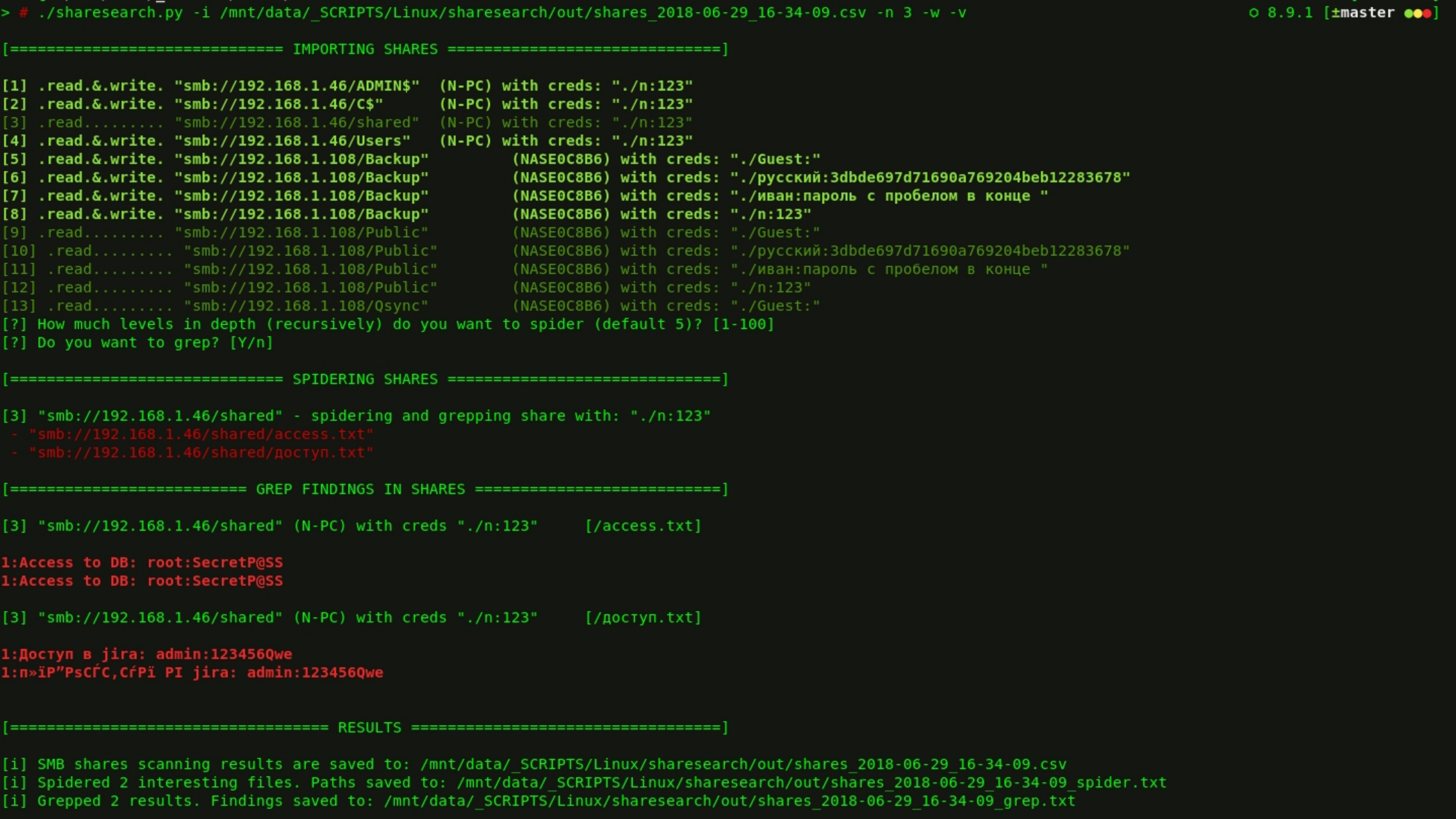
```
root@kali:~# nmap -sV --script=nfs-showmount 192.168.1.102
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-24 07:24 EDT
Nmap scan report for 192.168.1.102
Host is up (0.000074s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind 2-4 (RPC #100000)
| nfs-showmount:
|_  /home *
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  2,3         2049/udp  nfs
|   100003  2,3,4       2049/tcp  nfs
|   100005  1,2,3      37070/udp  mountd
|   100005  1,2,3      37273/tcp  mountd
|   100021  1,3,4      34993/tcp  nlockmgr
|   100021  1,3,4      54899/udp  nlockmgr
|   100227  2,3         2049/tcp  nfs_acl
```



Index of /admin/backup

Name	Last modified	Size	Description
Parent Directory		-	
FTP_ls.log	2012-10-25 08:20	63K	
database_connect.php	2012-10-25 08:22	298	
db_dump.sql	2012-10-25 08:21	98K	
old_pass.txt	2012-10-25 08:22	6.3K	

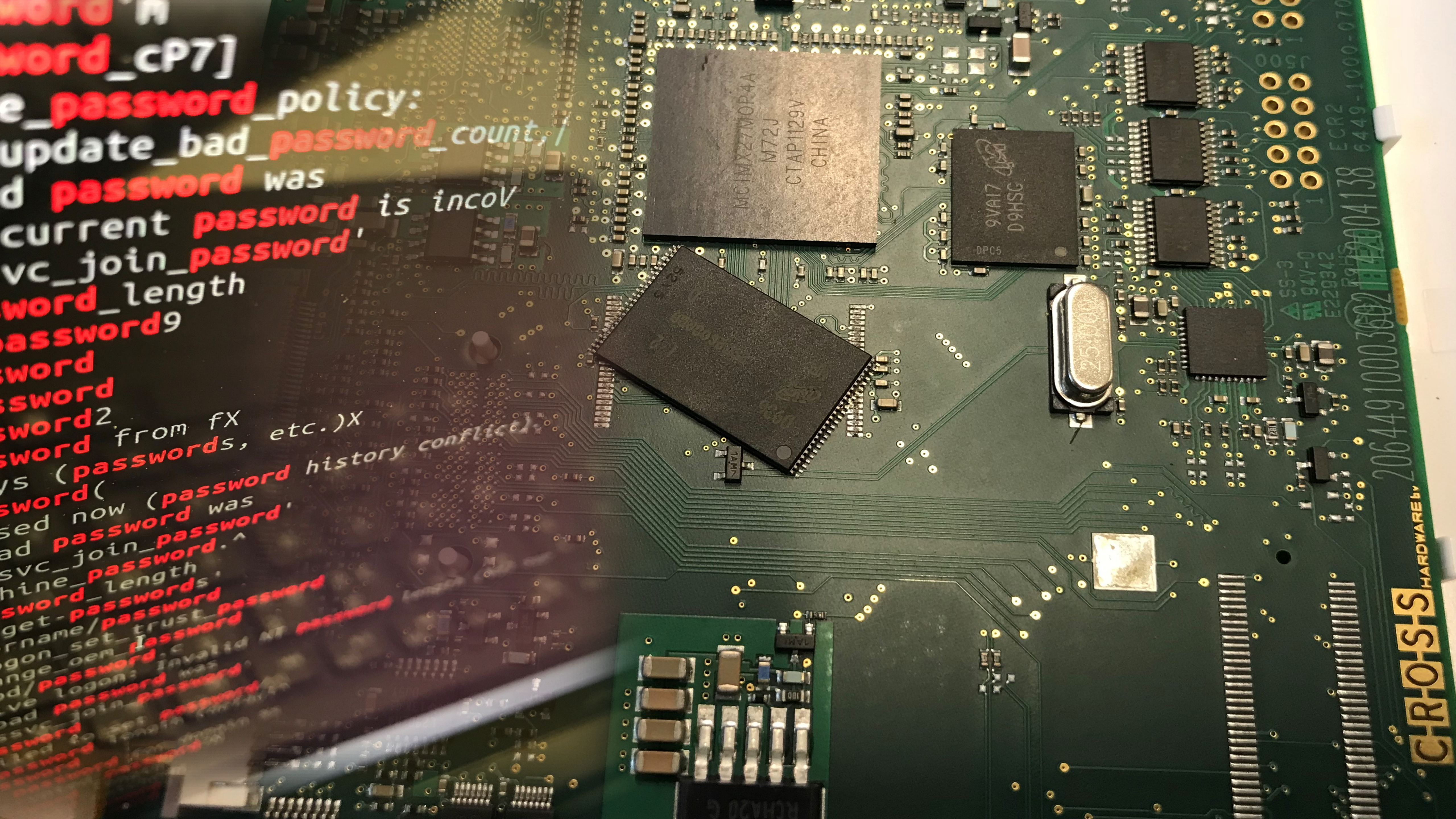
Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4 Server at www.vulnweb.com Port 80



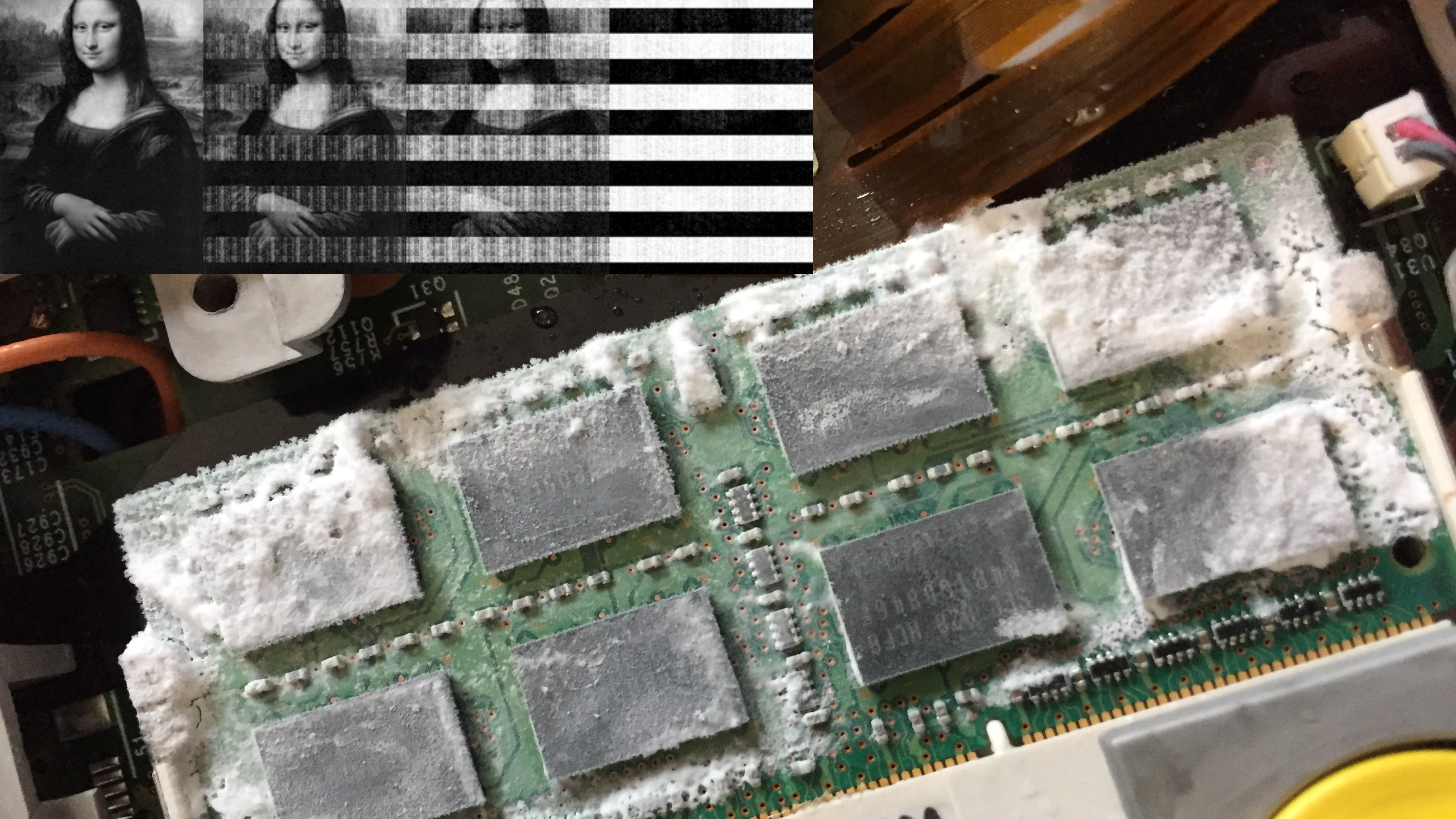
```
> # ./sharesearch.py -i /mnt/data/_SCRIPTS/Linux/sharesearch/out/shares_2018-06-29_16-34-09.csv -n 3 -w -v                              ○ 8.9.1 [±master ●●●]

[============================== IMPORTING SHARES ==============================]

[1] .read.&.write. "smb://192.168.1.46/ADMIN$"  (N-PC) with creds: "./n:123"
[2] .read.&.write. "smb://192.168.1.46/C$"      (N-PC) with creds: "./n:123"
[3] .read......... "smb://192.168.1.46/shared"  (N-PC) with creds: "./n:123"
[4] .read.&.write. "smb://192.168.1.46/Users"   (N-PC) with creds: "./n:123"
[5] .read.&.write. "smb://192.168.1.108/Backup"         (NASE0C8B6) with creds: "./Guest:"
[6] .read.&.write. "smb://192.168.1.108/Backup"         (NASE0C8B6) with creds: "./русский:3dbde697d71690a769204beb12283678"
[7] .read.&.write. "smb://192.168.1.108/Backup"         (NASE0C8B6) with creds: "./иван:пароль с пробелом в конце "
[8] .read.&.write. "smb://192.168.1.108/Backup"         (NASE0C8B6) with creds: "./n:123"
[9] .read......... "smb://192.168.1.108/Public"         (NASE0C8B6) with creds: "./Guest:"
[10] .read......... "smb://192.168.1.108/Public"        (NASE0C8B6) with creds: "./русский:3dbde697d71690a769204beb12283678"
[11] .read......... "smb://192.168.1.108/Public"        (NASE0C8B6) with creds: "./иван:пароль с пробелом в конце "
[12] .read......... "smb://192.168.1.108/Public"        (NASE0C8B6) with creds: "./n:123"
[13] .read......... "smb://192.168.1.108/Qsync"         (NASE0C8B6) with creds: "./Guest:"
[?] How much levels in depth (recursively) do you want to spider (default 5)? [1-100]
[?] Do you want to grep? [Y/n]

[============================== SPIDERING SHARES ==============================]

[3] "smb://192.168.1.46/shared" - spidering and grepping share with: "./n:123"
 - "smb://192.168.1.46/shared/access.txt"
 - "smb://192.168.1.46/shared/доступ.txt"

[========================== GREP FINDINGS IN SHARES ==========================]

[3] "smb://192.168.1.46/shared" (N-PC) with creds "./n:123"     [/access.txt]

1:Access to DB: root:SecretP@SS
1:Access to DB: root:SecretP@SS

[3] "smb://192.168.1.46/shared" (N-PC) with creds "./n:123"     [/доступ.txt]

1:Доступ в jira: admin:123456Qwe
1:п»їР”РѕСЃС‚СѓРї РІ jira: admin:123456Qwe


[==================================== RESULTS ===================================]

[i] SMB shares scanning results are saved to: /mnt/data/_SCRIPTS/Linux/sharesearch/out/shares_2018-06-29_16-34-09.csv
[i] Spidered 2 interesting files. Paths saved to: /mnt/data/_SCRIPTS/Linux/sharesearch/out/shares_2018-06-29_16-34-09_spider.txt
[i] Grepped 2 results. Findings saved to: /mnt/data/_SCRIPTS/Linux/sharesearch/out/shares_2018-06-29_16-34-09_grep.txt
```

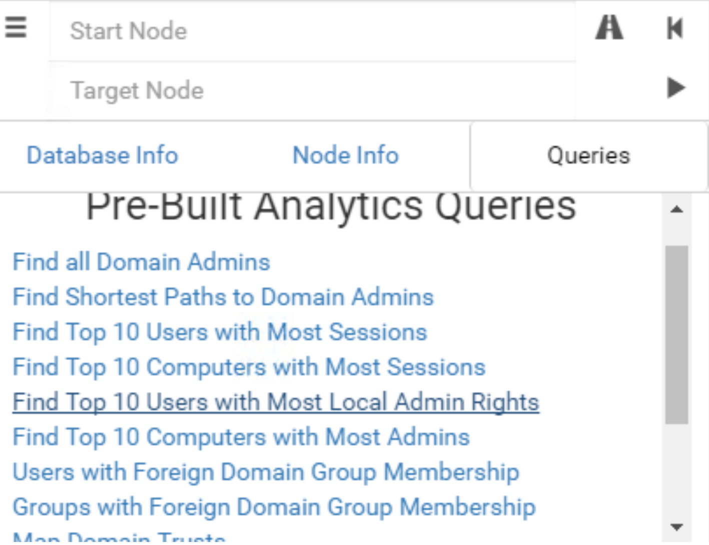
50137
479Z

EUGEN MÆRSK
MAERSK LINE
MAERSK
SEALAND
P&O



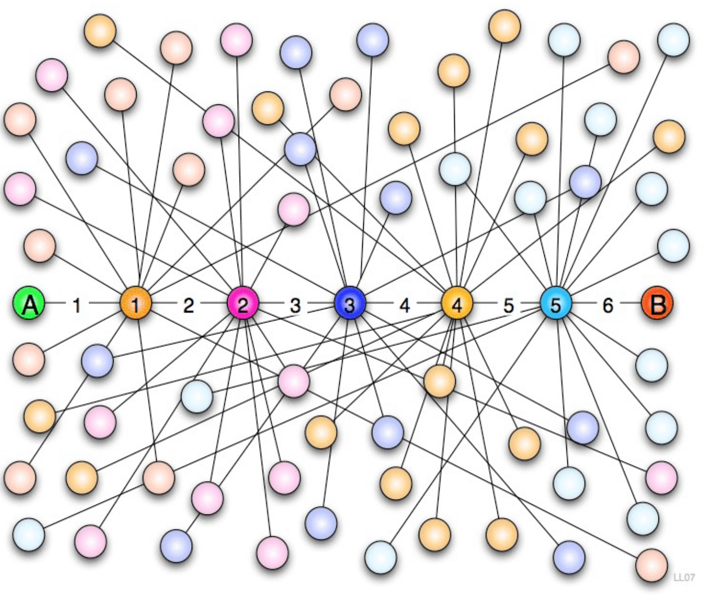
word_cP7]
e_password_policy:
update_bad_password_count
d password was
current password is incoV
vc_join_password'
word_length
password9
sword
ssword
sword2
sword from fX
ys (passwords, etc.)X
sword(
sed now (password history conflict
ad password was
svc_join_password'
hine_password.^
sword_length
get-passwords
rname/password
ogon_set_trust_password
MCIMX27VJOP4A
M72J
CTAP1129V
CHINA
9VA17
D9HSC
DPC5
CHROHS HARDWARE

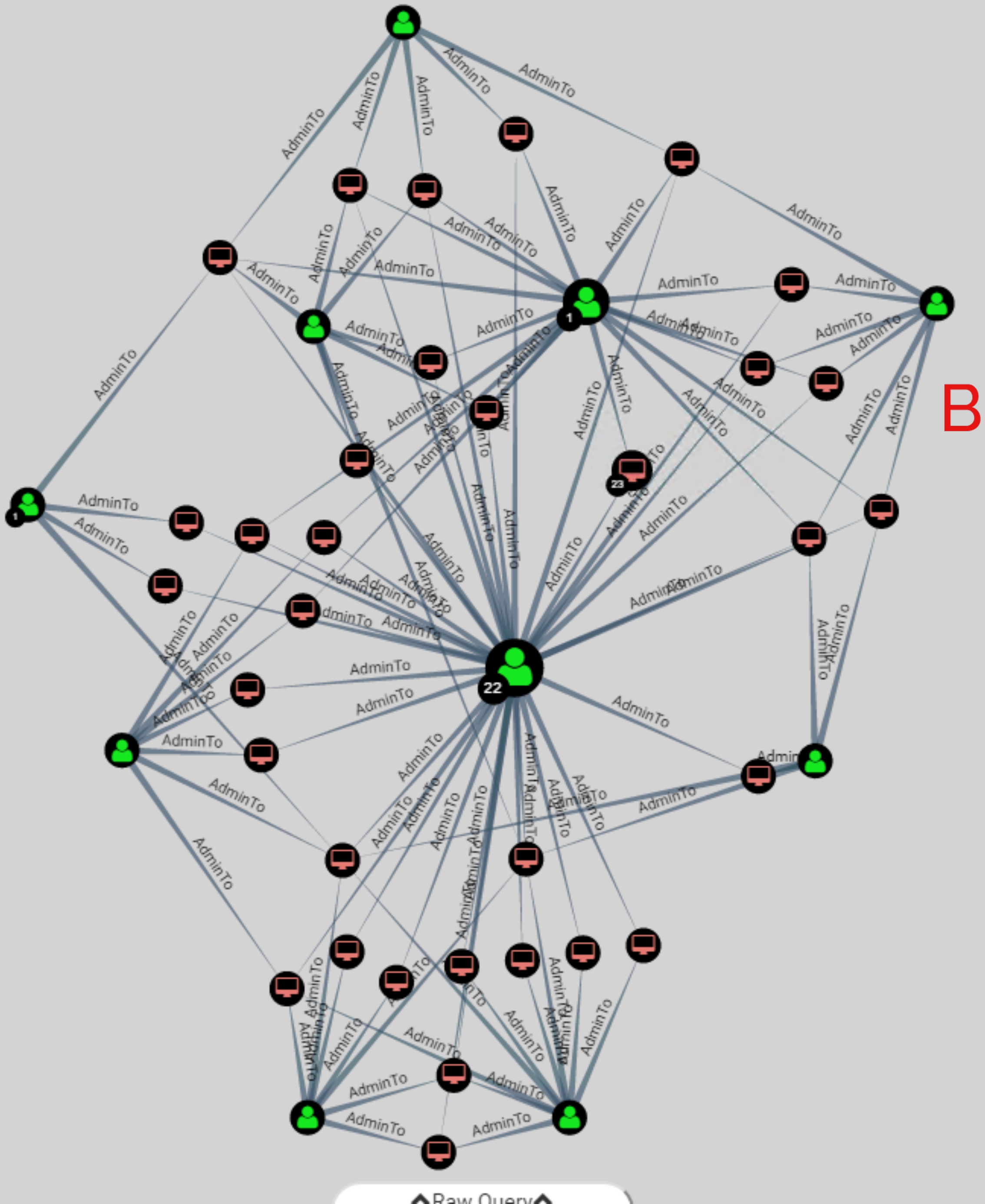




Pre-Built Analytics Queries

- Find all Domain Admins
- Find Shortest Paths to Domain Admins
- Find Top 10 Users with Most Sessions
- Find Top 10 Computers with Most Sessions
- Find Top 10 Users with Most Local Admin Rights
- Find Top 10 Computers with Most Admins
- Users with Foreign Domain Group Membership
- Groups with Foreign Domain Group Membership
- Map Domain Trusts





BLOODHOUND

WORLD CHAMPIONS
EUROPE
GLOBAL CYBERLYMPICS
EUROPE
WORLD FINALS
CHAMPIONS

Mark de Groot
Teamlead KPN REDteam
markdegroot@kpn.com
+31 6 10 27 70 87