

# Spis treści

|                                                                                          |    |
|------------------------------------------------------------------------------------------|----|
| O autorze .....                                                                          | 13 |
| O recenzentach .....                                                                     | 14 |
| Przedmowa .....                                                                          | 15 |
| ROZDZIAŁ 1.                                                                              |    |
| Przygotowanie laboratorium i atak na serwer Microsoft Exchange ....                      | 19 |
| Wymagania techniczne .....                                                               | 20 |
| Architektura i wdrożenie laboratorium .....                                              | 20 |
| Zabójczy łańcuch usługi Active Directory .....                                           | 22 |
| Dlaczego nie zajmiemy się dostępem początkowym<br>i tematami związanymi z hostami? ..... | 24 |
| Atakowanie serwera Exchange .....                                                        | 25 |
| Enumeracja użytkowników i rozsiewanie haseł .....                                        | 27 |
| Zrzut danych i eksfiltracja .....                                                        | 29 |
| Eksploity Zero2Hero .....                                                                | 33 |
| Zdobywanie przyciółka .....                                                              | 38 |
| Podsumowanie .....                                                                       | 40 |
| Więcej informacji .....                                                                  | 40 |
| ROZDZIAŁ 2.                                                                              |    |
| Unikanie obrony .....                                                                    | 43 |
| Wymagania techniczne .....                                                               | 43 |
| Interfejs AMSI, tryb PowerShell CLM i blokada AppLocker .....                            | 44 |
| Interfejs skanowania antymalware .....                                                   | 44 |
| Sposób 1 — wymuszanie błędów .....                                                       | 46 |
| Sposób 2 — zaciemnianie kodu .....                                                       | 47 |
| Sposób 3 — patchowanie pamięci .....                                                     | 48 |
| AppLocker i PowerShell CLM .....                                                         | 50 |
| Ulepszone rejestrowanie powłoki PowerShell i Sysmon .....                                | 54 |
| Usługa śledzenia zdarzeń dla systemu Windows (ETW) .....                                 | 60 |

## 6 Testy penetracyjne środowiska Active Directory

|                                                          |    |
|----------------------------------------------------------|----|
| Podsumowanie .....                                       | 63 |
| Bibliografia .....                                       | 64 |
| Więcej informacji .....                                  | 67 |
| ROZDZIAŁ 3.                                              |    |
| Rekonesans i odkrywanie domen .....                      | 68 |
| Wymagania techniczne .....                               | 68 |
| Enumeracja przy użyciu wbudowanych funkcjonalności ..... | 69 |
| Polecenie cmdlet PowerShell .....                        | 69 |
| WMI .....                                                | 70 |
| net.exe .....                                            | 71 |
| Protokół LDAP .....                                      | 73 |
| Narzędzia stosowane przy enumeracji .....                | 74 |
| SharpView/PowerView .....                                | 74 |
| BloodHound .....                                         | 77 |
| Enumeracja usług i polowanie na użytkowników .....       | 80 |
| SPN .....                                                | 80 |
| Serwer plików .....                                      | 81 |
| Polowanie na użytkownika .....                           | 81 |
| Unikanie wykrywania enumeracji .....                     | 82 |
| Microsoft ATA .....                                      | 82 |
| Tokeny-przynęty .....                                    | 82 |
| Podsumowanie .....                                       | 84 |
| Bibliografia .....                                       | 84 |
| Więcej informacji .....                                  | 86 |
| ROZDZIAŁ 4.                                              |    |
| Dostęp do poświadczeń w domenie .....                    | 87 |
| Wymagania techniczne .....                               | 88 |
| Poświadczenia w postaci czystego tekstu w domenie .....  | 88 |
| Sposoby stare, ale wciąż warte wypróbowania .....        | 88 |
| Hasło w polu opisu .....                                 | 89 |

|                                                                                                 |     |
|-------------------------------------------------------------------------------------------------|-----|
| Rozsiewanie haseł .....                                                                         | 90  |
| Przechwytywanie hasha .....                                                                     | 91  |
| Wymuszone uwierzytelnianie .....                                                                | 95  |
| Użycie do ataków protokołu MS-RPRN (eksploit PrinterBug) .....                                  | 95  |
| Użycie do ataków protokołu MS-EFSR (PetitPotam) .....                                           | 95  |
| Użycie do ataków protokołu WebDAV .....                                                         | 96  |
| Użycie do ataków protokołu MS-FSRVP (ShadowCoerce) .....                                        | 96  |
| Użycie do ataków protokołu MS-DFSNM (DFSCoerce) .....                                           | 97  |
| Atak roasting na protokół Kerberos .....                                                        | 97  |
| Kerberos 101 .....                                                                              | 97  |
| Atak ASREQRoast .....                                                                           | 99  |
| Atak roasting KRB_AS_REP (ASREPRoast) .....                                                     | 99  |
| Atak Kerberoasting .....                                                                        | 102 |
| Automatyczne zarządzanie hasłami w domenie .....                                                | 105 |
| LAPS .....                                                                                      | 105 |
| gMSA .....                                                                                      | 107 |
| Hasła zamaskowane NTDS .....                                                                    | 109 |
| Atak DCSync .....                                                                               | 110 |
| Zrzucanie danych uwierzytelniających użytkownika<br>w postaci czystego tekstu przez DPAPI ..... | 112 |
| Podsumowanie .....                                                                              | 114 |
| Bibliografia .....                                                                              | 114 |
| Więcej informacji .....                                                                         | 116 |
| ROZDZIAŁ 5.                                                                                     |     |
| Ruch boczny w obrębie domeny i pomiędzy lasami domen .....                                      | 117 |
| Wymagania techniczne .....                                                                      | 118 |
| Wykorzystanie protokołów administracyjnych w domenie .....                                      | 118 |
| PSRemoting i JEA .....                                                                          | 118 |
| Protokół RDP .....                                                                              | 120 |
| Inne protokoły z klasami Impacket .....                                                         | 122 |
| Przekazywanie hasha .....                                                                       | 123 |

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| Atak pass-the-whatever .....                                    | 129 |
| Atak pass-the-hash .....                                        | 129 |
| Ataki pass-the-key i overpass-the-hash .....                    | 132 |
| Atak pass-the-ticket .....                                      | 135 |
| Delegowanie protokołu Kerberos .....                            | 136 |
| Delegowanie nieograniczone .....                                | 136 |
| Ograniczone delegowanie oparte na zasobach .....                | 139 |
| Delegowanie ograniczone .....                                   | 141 |
| Atak Bronze Bit alias CVE-2020-17049 .....                      | 146 |
| Wykorzystywanie przy atakach relacji zaufania                   |     |
| do wykonywania ruchu bocznego .....                             | 147 |
| Podsumowanie .....                                              | 152 |
| Bibliografia .....                                              | 153 |
| Więcej informacji .....                                         | 154 |
| ROZDZIAŁ 6.                                                     |     |
| Eskalacja przywilejów w domenie .....                           | 155 |
| Wymagania techniczne .....                                      | 156 |
| Eksploity Zero2Hero .....                                       | 156 |
| Podatność MS14-068 .....                                        | 156 |
| Podatność Zerologon (CVE-2020-1472) .....                       | 157 |
| Podatność PrintNightmare (CVE-2021-1675 & CVE-2021-34527) ..... | 159 |
| Spoofing sAMAccountName i noPac                                 |     |
| (CVE-2021-42278/CVE-2021-42287) .....                           | 160 |
| Podatność RemotePotato0 .....                                   | 162 |
| Wykorzystywanie do ataków list ACL .....                        | 166 |
| Grupa .....                                                     | 167 |
| Komputer .....                                                  | 169 |
| Użytkownik .....                                                | 170 |
| Atak DCSync .....                                               | 173 |
| Naruszanie bezpieczeństwa zasad grupy .....                     | 175 |
| Pozostałe wektory eskalacji przywilejów .....                   | 179 |

|                                                                                        |     |
|----------------------------------------------------------------------------------------|-----|
| Wbudowane grupy bezpieczeństwa .....                                                   | 181 |
| Wykorzystanie do ataków grupy DNSAdmins (CVE-2021-40469) .....                         | 183 |
| Eskalacja domeny podrzędnej/potomnej .....                                             | 185 |
| Zarządzanie dostępem uprzywilejowanym .....                                            | 185 |
| Podsumowanie .....                                                                     | 188 |
| Bibliografia .....                                                                     | 189 |
| Więcej informacji .....                                                                | 190 |
| ROZDZIAŁ 7.                                                                            |     |
| Przetwarzanie na poziomie domeny .....                                                 | 191 |
| Wymagania techniczne .....                                                             | 192 |
| Przetwarzanie na poziomie domeny .....                                                 | 192 |
| Sfałszowane bilety .....                                                               | 192 |
| Manipulacje listami ACL i atrybutami obiektu domeny .....                              | 203 |
| Atak DCSshadow .....                                                                   | 212 |
| Atak Golden gMSA .....                                                                 | 216 |
| Przetwarzanie na poziomie kontrolera domeny .....                                      | 218 |
| Atak typu Skeleton Key .....                                                           | 218 |
| Złośliwy dostawca usług wsparcia w zakresie zabezpieczeń (SSP) .....                   | 221 |
| Konto DSRM .....                                                                       | 223 |
| Zmiana deskryptora zabezpieczeń .....                                                  | 225 |
| Podsumowanie .....                                                                     | 227 |
| Bibliografia .....                                                                     | 227 |
| ROZDZIAŁ 8.                                                                            |     |
| Używanie do ataków usług certyfikatów w Active Director .....                          | 228 |
| Wymagania techniczne .....                                                             | 229 |
| Teoria infrastruktury klucza publicznego .....                                         | 229 |
| Kradzież certyfikatów .....                                                            | 232 |
| Kradzież THEFT1 — eksportowanie certyfikatów<br>przy użyciu interfejsu CryptoAPI ..... | 232 |
| Kradzież THEFT2 — kradzież certyfikatu użytkownika<br>poprzez DPAPI .....              | 233 |

|                                                                                                                          |     |
|--------------------------------------------------------------------------------------------------------------------------|-----|
| Kradzież THEFT3 — kradzież certyfikatu maszyny<br>za pośrednictwem DPAPI .....                                           | 235 |
| Kradzież THEFT4 — zbieranie plików certyfikatów .....                                                                    | 236 |
| Kradzież THEFT5 — kradzież danych uwierzytelniających NTLM<br>poprzez mechanizm PKINIT (nPAC-the-hash) .....             | 237 |
| Przetrwanie na poziomie konta .....                                                                                      | 238 |
| Przetrwanie PERSIST1 — kradzież danych uwierzytelniających<br>aktywnych użytkowników za pośrednictwem certyfikatów ..... | 239 |
| Przetrwanie PERSIST2 — przetrwanie na poziomie maszyny<br>za pomocą certyfikatów .....                                   | 240 |
| Przetrwanie PERSIST3 — przetrwanie na poziomie konta<br>poprzez odnowienie certyfikatu .....                             | 241 |
| Poświadczenia-cienie (Shadow Credentials) .....                                                                          | 241 |
| Eskalacja przywilejów domeny .....                                                                                       | 243 |
| Podatność Certifried (CVE-2022-26923) .....                                                                              | 243 |
| Błędne konfiguracje szablonów i rozszerzeń .....                                                                         | 245 |
| Niewłaściwa kontrola dostępu .....                                                                                       | 255 |
| Błędna konfiguracja urzędu certyfikacji (CA) .....                                                                       | 264 |
| Ataki przekaźnikowe .....                                                                                                | 265 |
| Przetrwanie na poziomie domeny .....                                                                                     | 268 |
| Przetrwanie DPERSIST1 — fałszowanie certyfikatów<br>przy użyciu skradzionego certyfikatu urzędu certyfikacji (CA) .....  | 269 |
| Przetrwanie DPERSIST2 — ufać fałszywym certyfikatom<br>wystawionym przez urzędy certyfikacji .....                       | 270 |
| Przetrwanie DPERSIST3 — złośliwa błędna konfiguracja .....                                                               | 271 |
| Podsumowanie .....                                                                                                       | 271 |
| Bibliografia .....                                                                                                       | 271 |
| ROZDZIAŁ 9.                                                                                                              |     |
| Naruszanie zabezpieczeń serwera Microsoft SQL .....                                                                      | 274 |
| Wymagania techniczne .....                                                                                               | 274 |
| Wprowadzenie, odkrywanie i enumeracja .....                                                                              | 275 |

|                                                             |     |
|-------------------------------------------------------------|-----|
| Wprowadzenie do serwera SQL .....                           | 275 |
| Odkrywanie .....                                            | 276 |
| Brute force .....                                           | 277 |
| Enumeracja bazy danych .....                                | 280 |
| Eskalacja przywilejów .....                                 | 282 |
| Podszywanie się pod innego użytkownika .....                | 282 |
| Błędna konfiguracja właściwości TRUSTWORTHY .....           | 283 |
| Wstrzykiwanie ścieżki UNC .....                             | 285 |
| Z konta usługi na konto systemowe (SYSTEM) .....            | 285 |
| Od administratora lokalnego do administratora systemu ..... | 287 |
| Wykonywanie poleceń systemu operacyjnego .....              | 289 |
| Procedura składowana xp_cmdshell .....                      | 289 |
| Niestandardowa rozszerzona procedura składowana .....       | 290 |
| Niestandardowe zestawy CLR .....                            | 291 |
| Procedury automatyzacji OLE .....                           | 294 |
| Zadania wykonywane przez agenta zadań .....                 | 295 |
| Skrypty zewnętrzne .....                                    | 296 |
| Ruch boczny .....                                           | 297 |
| Konta usług współdzielonych .....                           | 297 |
| Łączy do baz danych .....                                   | 297 |
| Przetwarzanie .....                                         | 301 |
| Automatyczne uruchamianie plików i rejestru .....           | 301 |
| Startowe procedury składowane .....                         | 302 |
| Złośliwe wyzwalacze .....                                   | 304 |
| Podsumowanie .....                                          | 305 |
| Więcej informacji .....                                     | 305 |
| ROZDZIAŁ 10.                                                |     |
| Przejmowanie usługi WSUS i menedżera SCCM .....             | 308 |
| Wymagania techniczne .....                                  | 309 |
| Wykorzystywanie do ataków usługi WSUS .....                 | 309 |
| Wprowadzenie do menedżera MECM/SCCM .....                   | 311 |

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| Wdrożenie .....                                                 | 312 |
| Rozpoznanie .....                                               | 315 |
| Eskalacja przywilejów .....                                     | 317 |
| Wymuszenie client push przy uwierzytelnianiu .....              | 317 |
| Pozyskiwanie (harvesting) poświadczeń .....                     | 319 |
| Ruch boczny .....                                               | 321 |
| Atak przekaźnikowy typu client push przy uwierzytelnianiu ..... | 321 |
| Przejęcie struktury fizycznej .....                             | 322 |
| Wykorzystywanie do ataków serwera Microsoft SQL .....           | 323 |
| Wdrażanie aplikacji .....                                       | 324 |
| Zalecenia obronne .....                                         | 327 |
| Podsumowanie .....                                              | 328 |
| Bibliografia .....                                              | 328 |
| Więcej informacji .....                                         | 330 |
| Skorowidz .....                                                 | 331 |