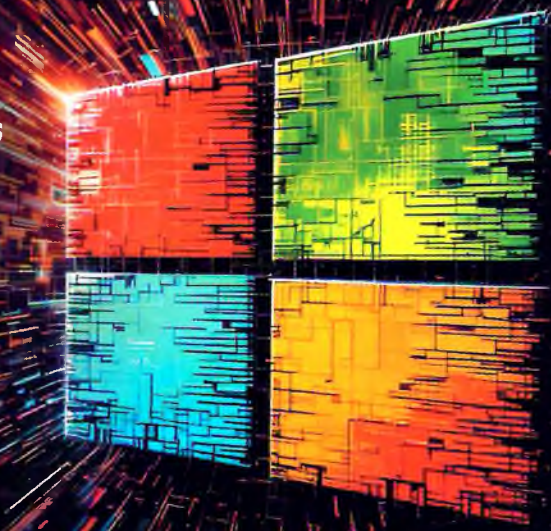
WINDOWS глазами ХАКЕРА

Михаил Жмайло

- Пентест Active Directory
- Поиск и эксплуатация уязвимостей в сетях Windows
- Трюки с групповыми политиками и привилегиями
- Kerberos и атаки на билеты
- Практические методы кражи учетных данных
- Инжекты и исполнение кода нестандартными способами
- Современные методы обхода средств защиты информации
- Практические техники пентеста Windows



bhv®

Оглавление

Предисловие **9**
От автора 9
От редакции 10

ЧАСТЬ I. ПЕНТЕСТ ACTIVE DIRECTORY **11**

Глава 1. Как работают атаки на доверенные отношения доменов и лесов AD **13**
Разведка 14
Леса 14
Домены 15
Trust Keys 17
Домены 17
Леса 19
Выдаем себя за контроллер домена 20
Неограниченное делегирование 20
Между доменами 21
Между лесами 21
Ограниченное делегирование 22
PAM Trust 23
Обнаружение 23
Проверка, не в бастионном лесе ли мы 24
Проверяем, не управляется ли текущий лес каким-то другим по PAM Trust 25
Дополнительные проверки и новые угрозы 26
Эксплуатация 27
Заключение 28

Глава 2. Эксплуатируем небезопасные групповые политики **29**
Структура 29
Обнаружение 30
Эксплуатация 35
mmc 35
Файл .ini 36
Создание GPO 37
Перемещение через GPO 38
Заключение 39

Глава 3. Пентестим Read-only Domain Controllers 40
Теория 40
Определения и особенности 40
Атрибуты 42
managedBy 42
msDS-RevealOnDemandGroup, msDS-NeverRevealGroup 42
msDS-AuthenticatedToAccountList 43
msDS-Revealed* 43
Аутентификация пользователей 43
Поиск RODC 44
Получение кешированных паролей с RODC 46
DSRM 48
Особенности работы Kerberos с RODC 48
Key List 50
Контроль над объектом RODC 52
Заключение 53

ЧАСТЬ II. СИСТЕМНОЕ ПРОГРАММИРОВАНИЕ ДЛЯ ХАКЕРОВ 55

Глава 4. Изучаем возможности WinAPI для пентестера 57
SID и токены 57
Токен и процесс 58
Приступаем к работе 59
Получаем токен 59
Проверка наличия привилегии в токене 60
Изменение информации токена 61
Выполнение кода с использованием токена 63
Создание процесса 63
Применение к потоку 65
Заимствование прав подключенного пользователя 65
Без установления соединения 65
Именованные каналы 66
Сокеты или другой механизм взаимодействия 67
Начало работы 67
Роль клиента 69
Роль сервера 73
Использование полного контекста 75
Имперсонация 75
RevertSecurityContext() 76
Получение токена из контекста 76
Заключение 76

Глава 5. Получаем билеты TGT методом GIUDA 77
Logon Session 77
Как LSA запрашивает билеты Kerberos 84
Крадем билет 85
TGT — это TGS 91
Заключение 92

Глава 6. Управляем привилегиями в Windows 93
Добавляем привилегии аккаунту 93
Запускаем процесс с привилегией 102
Удаляем привилегию из аккаунта 105
Ищем объекты с привилегией 107
Смотрим привилегии объекта 110
Заключение 111

Глава 7. Поставщик небезопасности. Как Windows раскрывает пароль пользователя 112
Компоненты безопасности 112
Security Package 113
SSP/AP (или же просто AP) 113
Security Providers 114
Credential Providers 115
Password Filters 115
Как происходит вход пользователя в систему 115
Инициализация LSA 119
Эксплуатация 123
Как дебажить? 123
Перехват пароля с помощью внедрения Security Package 125
Требования 125
Загрузка в систему 125
Проверка 126
Перехват пароля 126
Перехват пароля с помощью внедрения Password Filter 130
Требования 130
Загрузка в систему 130
Перехват пароля 130
Запрещаем пользователям менять пароль 132
Перехват пароля с помощью диспетчера учетных данных 133
Теория 133
Добавление в систему 133
Перехват пароля 135
Заключение 138

Глава 8. Долой Mimikatz! Инжектим тикеты своими руками 139
Получение тикета 139
Подключение к LSA 141
Обнаружение AP 143
Внедрение билета 144
Проверка 146
Заключение 146

Глава 9. Как дампить тикеты Kerberos на C++ 149
Kerberos AP 149
Начало работы 150
Особенности дампа 155
Подключение к LSA 156
Получение ID 161

Перечисляем все LUID ... 162
Изучение кеша ... 166
Дамп тикета ... 171
Заключение ... 179

Глава 10. Как злоупотреблять хендлами в Windows ... 180
Интересные хендлы ... 180
Изучение хендлов процесса ... 181
Handle Duplicating ... 181
Leaked Handle ... 192
Handle Hijacking ... 193
Заключение ... 204

Глава 11. Достаем учетные данные Windows, не трогая LSASS ... 205
Реквизиты, контекст и блобы ... 206
Известные атаки ... 207
Внутренний монолог ... 209
Заключение ... 217

Глава 12. Ищем способы обращения к нативному коду из C# ... 218
Platform Invoke ... 218
Dynamic Invoke ... 221
Parasite Invoke ... 227
Dynamic PInvoke ... 230
Hash Invoke ... 234
Заключение ... 236

Глава 13. Как работает угон пользовательских сессий в Windows ... 237
Поиск сессий пользователей ... 237
- WinAPI ... 238
- Реестр ... 241
- Через SCCM ... 243
- Через RDP-сессии ... 244
- Логи ... 244
- Процессы ... 248

Кража сессий ... 248
- Воруем TGS ... 248
- Манипуляции с токенами ... 250
- RemotePotato0 ... 251
- Запрос чужих сертификатов ... 251
- SeMishaPrivilege ... 252
- Leaked Wallpaper ... 253

Заключение ... 255

Глава 14. Используем Named Pipes при атаке на Windows ... 256
Что такое Pipe ... 256
Пример клиента и сервера ... 258
Изучение доступных пайпов ... 259
- Process Hacker ... 259
- C++ ... 260
- PowerShell ... 262

IO Ninja 263
PipeViewer 263
Имперсонация клиентов 263
Чейн с SeImpersonate 268
Скрытое чтение данных 271
Гонка пайпов 272
Заключение 278

Глава 15. Исследуем обход UAC на примере Elevation Moniker 279
Моникеры 279
Подвиды моникеров 281
Регистрация Elevation Moniker 281
Использование Elevation Moniker 286
Примеры COM-объектов 287
ICMLuaUtil 287
IFileOperation 289
Заключение 290

Глава 16. Как работает кража сессии через механизм COM 291
Logon Sessions 291
Session Moniker 295
Запуск процесса в чужой сессии 301
Утечка хеша пароля при смене обоев 302
Заключение 304

ЧАСТЬ III. СПОСОБЫ ОБХОДА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ 305

Глава 17. Познаем анхукинг ntdll.dll 307
Снятие хука через чтение библиотеки с диска 308
Снятие хука через KnownDlls 321
Снятие хука через приостановленный процесс 329
Снятие хука через подгрузку ntdll.dll с удаленного веб-сервера 335
Заключение 345

Глава 18. Изучаем методы предотвращения подгрузки DLL 346
UpdateProcThreadAttribute 346
SetProcessMitigationPolicy 353
Включение ACG 355
Запуск процесса с DEBUG 359
Хук на NtCreateSection 362
Простой вариант 362
Модифицированный вариант 363
WMI 364
DLL Notification Callbacks 367
ETW (Kernel Provider) 370
Заключение 373

Глава 19. Ищем в Windows лазейки для исполнения стороннего кода 374
DLL Redirection 375
Для обычных исполняемых файлов 375
Сборки .NET 381

Image Path Name Spoofing ... 383
Теория ... 383
Реализация ... 384
WinSxS ... 387
svchost.exe ... 391
LSASS Driver ... 391
Заключение ... 392

Глава 20. Используем хардверные брейк-пойнты в пентестерских целях ... 393
Обработка исключений ... 394
Установка hardware breakpoint ... 402
Обход AMSI ... 406
Извлечение номеров сисколов ... 408
Анхукинг ... 412
Пишем кастомный GetThreadContext() ... 413
Ставим хуки ... 416
Заключение ... 416

Глава 21. Изучаем новый способ обхода AMSI в Windows ... 417
Становимся дебаггером ... 417
Избегаем использования функции DebugActiveProcess ... 423
Заключение ... 424

Глава 22. Замена для WinAPI. Пишем раннер для шелл-кода на чистом .NET ... 425
Синхронизация через Sleep ... 427
Поток без CreateThread() ... 429
Копируем память ручками ... 433
Выделяем исполняемую память без WinAPI ... 436
Делегаты ... 436
EmitAlloc() ... 437
Заключение ... 440

Глава 23. Обфусцируем вызовы WinAPI новыми способами ... 441
Проксирование вызовов ... 442
Теория ... 442
Обнаружение прокси-функций ... 443
Таблица экспортов/импортов ... 443
Бинарный анализ ... 443
Пример с DphCommitMemoryFromPageHeap ... 450
Через RPC ... 453
Используем альтернативные функции ... 455
Теория ... 455
Замена CRT ... 455
Через ссылки на структуры Windows ... 456
Изучаем COM ... 460
Замена ReadProcessMemory() ... 460
Замена WriteProcessMemory() ... 461
Где искать альтернативы ... 461
Заключение ... 461

Предметный указатель ... 462