Wyliczenie

CELE KSZTAŁCENIA

01: Wyjaśnij pojęcia wyliczania

02: Zademonstruj różne techniki wyliczania NetBIOS

03: Zademonstruj różne techniki wyliczania SNMP

04: Użyj różnych technik wyliczania LDAP

05: Użyj różnych technik wyliczania NTP i NFS

06: Zademonstruj różne techniki wyliczania SMTP i DNS

07: Demonstracja wyliczania IPsec, VoIP, RPC, Unix/Linux, Telnet, FTP, TFTP, SMB, IPv6 i BGP

08: Wyjaśnij środki zaradcze wyliczania

Cele kształcenia

W poprzednich modułach nauczyłeś się o footprintingu i skanowaniu sieci. Ten moduł obejmuje następną fazę, wyliczanie. Zaczniemy od wprowadzenia do koncepcji wyliczania. Następnie moduł zapewnia wgląd w różne techniki Network Basic Input/Output System (NetBIOS), Simple Network Management Protocol (SNMP), Lightweight Directory Access Protocol (LDAP), Network Time Protocol (NTP), Network File System (NFS), Simple Mail Transfer Protocol (SMTP), Domain Name System (DNS), Internet Protocol Security (IPsec), Voice over Internet Protocol (VoIP), Remote Procedure Call (RPC), Linux/Unix, Telnet, File Transfer Protocol (FTP), Trivial FTP (TFTP), blok komunikatów serwera (SMB), protokół internetowy w wersji 6 (IPv6) i protokół Border Gateway Protocol (BGP). Moduł kończy się przeglądem środków zaradczych wyliczania. Pod koniec tego modułu będziesz w stanie:

• Opisać koncepcje wyliczania

• Wyjaśnić różne techniki wyliczania NetBIOS

• Wyjaśnić różne techniki wyliczania SNMP

• Wyjaśnić różne techniki wyliczania LDAP i Active Directory (AD).

• Wyjaśnić różne techniki wyliczania NTP

• Wyjaśnić różne techniki wyliczania NFS

• Wyjaśnić różne techniki wyliczania SMTP i DNS

• Wyjaśnić inne techniki wyliczania, takie jak IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, Wyliczanie TFTP, SMB, IPv6 i BGP

• Zastosować środki zaradcze polegające na wyliczaniu

Koncepcje wyliczania

Różne sekcje tego modułu dotyczą wyliczania różnych usług i portów. Przed omówieniem rzeczywistego procesu wyliczania wprowadzimy pojęcia związane z wyliczaniem.

Co to jest wyliczanie?

Wyliczanie to proces wyodrębniania nazw użytkowników, nazw komputerów, zasobów sieciowych, udziałów i usług z systemu lub sieci. W fazie wyliczania atakujący tworzy aktywne połączenia z systemem i wysyła ukierunkowane zapytania, aby uzyskać więcej informacji o celu. Atakujący wykorzystuje informacje zebrane za pomocą wyliczania, aby zidentyfikować luki w zabezpieczeniach systemu, które pomagają mu wykorzystać system docelowy. Z kolei wyliczanie umożliwia atakującemu przeprowadzanie ataków na hasła w celu uzyskania nieautoryzowanego dostępu do zasobów systemu informatycznego. Techniki wyliczania działają w środowisku intranetowym. W szczególności wyliczanie pozwala atakującemu na zebranie następujących informacji:

• Zasoby sieciowe

• Udziały sieciowe

• Tablice routingu

• Ustawienia audytu i serwisu

• Szczegóły SNMP iw pełni kwalifikowanej nazwy domeny (FQDN).

• Nazwy maszyn

• Użytkownicy i grupy

• Aplikacje i banery

Podczas wyliczania osoby atakujące mogą natknąć się na udział zdalnej komunikacji między procesami (IPC), taki jak IPC$ w systemie Windows, który mogą dalej sondować, aby połączyć się z udziałem administracyjnym przez brutalne wymuszenie poświadczeń administratora i uzyskać pełne informacje o pliku - lista systemowa, którą reprezentuje udział. W poprzednich modułach pokazano, w jaki sposób osoby atakujące zbierają niezbędne informacje o celu bez żadnych nielegalnych działań. Jednak działania związane z wyliczaniem mogą być nielegalne w zależności od zasad organizacji i obowiązujących przepisów. Etyczny haker lub pen tester powinien zawsze uzyskać odpowiednią autoryzację przed wykonaniem wyliczenia.

Techniki wyliczania

Poniższe techniki służą do wydobywania informacji o celu.

Wyodrębnij nazwy użytkowników za pomocą identyfikatorów e-mail

Każdy adres e-mail składa się z dwóch części, nazwy użytkownika i nazwy domeny, w formacie „nazwa_użytkownika@nazwa_domeny”.

Wyodrębnij informacje przy użyciu domyślnych haseł

Wiele zasobów internetowych zawiera listę domyślnych haseł przypisanych przez producentów do ich produktów. Użytkownicy często ignorują zalecenia dotyczące zmiany domyślnych nazw użytkownika i haseł dostarczonych przez producenta lub programistę produktu. Ułatwia to atakującemu zadanie wyliczenia i wykorzystania docelowego systemu.

Brute force usługi Active Directory

Usługa Microsoft Active Directory jest podatna na wyliczanie nazw użytkowników w czasie weryfikacji danych wprowadzonych przez użytkowników. Jest to błąd projektowy w implementacji usługi

Microsoft Active Directory. Jeżeli użytkownik włączy funkcję „godziny logowania”, to wszystkie próby autoryzacji usługi kończą się różnymi komunikatami o błędach. Atakujący wykorzystują to do wyliczania prawidłowych nazw użytkowników. Osoba atakująca, której uda się wydobyć prawidłowe nazwy użytkowników, może przeprowadzić atak siłowy w celu złamania odpowiednich haseł.

Wyodrębnij informacje za pomocą DNS Zone Transfer

Administrator sieci może użyć transferu stref DNS do replikacji danych DNS na kilku serwerach DNS lub tworzenia kopii zapasowych plików DNS. W tym celu administrator musi wykonać określone żądanie transferu strefy do serwera nazw. Jeśli serwer nazw zezwala na transfer stref, przekonwertuje wszystkie nazwy DNS i adresy IP hostowane przez ten serwer na tekst ASCII. Jeśli administratorzy sieci nie skonfigurowali poprawnie serwera DNS, transfer strefy DNS może być skuteczną metodą pozyskiwania informacji o sieci organizacji. Informacje te mogą obejmować listy wszystkich nazwanych hostów, stref podrzędnych i powiązanych adresów IP. Użytkownik może wykonać transfer strefy DNS za pomocą poleceń nslookup i dig.

Wyodrębnij grupy użytkowników z systemu Windows

Aby wyodrębnić grupy użytkowników z systemu Windows, osoba atakująca powinna mieć zarejestrowany identyfikator użytkownika w usłudze Active Directory. Osoba atakująca może następnie wyodrębnić informacje z grup, których członkiem jest użytkownik, korzystając z interfejsu systemu Windows lub metody wiersza poleceń.

Wyodrębnij nazwy użytkowników za pomocą SNMP

Atakujący mogą łatwo odgadnąć ciągi społeczności tylko do odczytu lub do odczytu i zapisu, używając interfejsu programowania aplikacji (API) SNMP do wyodrębniania nazw użytkowników.

Usługi i porty do wyliczenia

Protokół kontroli transmisji (TCP) i protokół datagramów użytkownika (UDP) zarządzają komunikacją danych między terminalami w sieci. TCP jest protokołem zorientowanym na połączenie, zdolnym do przesyłania wiadomości lub e-maili przez Internet. Zapewnia niezawodną usługę komunikacji wieloprocesowej w środowisku wielosieciowym. Cechy i funkcje protokołu TCP obejmują:

• Obsługuje potwierdzenie odbioru danych za pomocą systemu potwierdzania przesuwanego okna

• Oferuje automatyczną retransmisję utraconych lub potwierdzonych danych

• Umożliwia adresowanie i multipleksowanie danych

• Połączenie można nawiązać, zarządzać lub zakończyć

• Oferuje transmisję wysokiej jakości

• Oferuje zarządzanie zatorami i kontrolę przepływu

UDP to protokół bezpołączeniowy, który przesyła krótkie wiadomości przez sieć komputerową. Zapewnia nierzetelną obsługę. Zastosowania protokołu UDP obejmują:

• Strumieniowe przesyłanie dźwięku

• Wideokonferencje i telekonferencje

Usługi i porty TCP/UDP, które można wyliczyć, obejmują następujące.

TCP/UDP 53: Transfer strefy DNS

Proces rozpoznawania nazw DNS ustanawia komunikację między klientami DNS a serwerami DNS. Klienci DNS wysyłają wiadomości DNS do serwerów DNS nasłuchujących na porcie UDP 53. Jeśli rozmiar wiadomości DNS przekracza domyślny rozmiar UDP (512 oktetów), odpowiedź zawiera tylko dane, które może obsłużyć protokół UDP, a serwer DNS ustawia flagę wskazującą okrojoną odpowiedź. Klient DNS może teraz ponownie wysłać żądanie za pośrednictwem protokołu TCP przez port 53 do serwera DNS. W tym podejściu serwer DNS używa UDP jako protokołu domyślnego. W przypadku długich zapytań, w przypadku których UDP zawiedzie, protokół TCP jest używany jako rozwiązanie przełączania awaryjnego. Złośliwe oprogramowanie, takie jak robak ADM i trojan Bonk, wykorzystuje port 53 do wykorzystywania luk w serwerach DNS, pomagając intruzom przeprowadzać ataki.

TCP/UDP 135: mapowanie punktów końcowych Microsoft RPC

RPC to protokół używany przez system kliencki do żądania usługi od serwera. Punkt końcowy to port protokołu, na którym serwer nasłuchuje wywołań RPC klienta. Narzędzie RPC Endpoint Mapper umożliwia klientom RPC określenie numeru portu aktualnie przypisanego do określonej usługi RPC. W części RPC, która wymienia komunikaty przez TCP/IP, występuje luka. Nieprawidłowa obsługa zniekształconych komunikatów powoduje niepowodzenie. Ma to wpływ na narzędzie RPC Endpoint Mapper, które nasłuchuje na porcie TCP/IP 135. Ta luka może pozwolić osobie atakującej na wysyłanie komunikatów RPC do procesu RPC Endpoint Mapper na serwerze w celu przeprowadzenia ataku typu „odmowa usługi” (DoS).

UDP 137: Usługa nazw NetBIOS (NBNS)

Usługa NBNS, znana również jako Windows Internet Name Service (WINS), udostępnia usługę rozpoznawania nazw dla komputerów z systemem NetBIOS. Serwery nazw NetBIOS utrzymują bazę danych nazw NetBIOS dla hostów i odpowiadającego im adresu IP używanego przez hosta. NBNS ma na celu dopasowanie adresów IP do nazw i zapytań NetBIOS. Atakujący zazwyczaj najpierw atakują usługę nazw. Zazwyczaj NBNS używa UDP 137 jako protokołu transportowego. Może również używać protokołu TCP 137 jako protokołu transportowego dla kilku operacji, chociaż w praktyce może to nigdy nie wystąpić.

TCP 139: Usługa sesji NetBIOS (SMB przez NetBIOS)

TCP 139 jest prawdopodobnie najbardziej znanym portem systemu Windows. Służy do przesyłania plików przez sieć. Systemy używają tego portu zarówno do ustanawiania sesji zerowych, jak i udostępniania plików i drukarek. Administrator systemu rozważający ograniczenie dostępu do portów w systemie Windows powinien nadać ograniczeniu TCP 139 najwyższy priorytet. Nieprawidłowo skonfigurowany port TCP 139 może umożliwić intruzowi uzyskanie nieautoryzowanego dostępu do krytycznych plików systemowych lub całego systemu plików, co może skutkować kradzieżą danych lub innymi szkodliwymi działaniami.

TCP/UDP 445: SMB przez TCP (host bezpośredni)

System Windows obsługuje ruch związany z udostępnianiem plików i drukarek przy użyciu protokołu SMB hostowanego bezpośrednio w protokole TCP. We wcześniejszych systemach operacyjnych ruch SMB wymagał protokołu NetBIOS przez TCP (NBT) do pracy w transporcie TCP/IP. Bezpośrednio hostowany ruch SMB używa portu 445 (TCP i UDP) zamiast NetBIOS.

UDP 161: prosty protokół zarządzania siecią (SNMP)

SNMP jest szeroko stosowany w systemach zarządzania siecią do monitorowania urządzeń podłączonych do sieci, takich jak routery, przełączniki, zapory ogniowe, drukarki i serwery. Składa się z kierownika i agentów. Agent odbiera żądania na porcie 161 od menedżerów i odpowiada menedżerom na porcie 162.

TCP/UDP 389: Lekki protokół dostępu do katalogu (LDAP)

LDAP to protokół służący do uzyskiwania dostępu i obsługi rozproszonych usług informacyjnych katalogów w sieci IP. Domyślnie protokół LDAP używa protokołu TCP lub UDP jako protokołu transportowego przez port 389.

TCP 2049: Sieciowy system plików (NFS)

Protokół NFS jest używany do montowania systemów plików na zdalnym hoście przez sieć, a użytkownicy mogą wchodzić w interakcje z systemami plików tak, jakby były montowane lokalnie. Serwery NFS nasłuchują swoich systemów klienckich na porcie TCP 2049. Jeśli usługi NFS nie są odpowiednio skonfigurowane, osoby atakujące mogą wykorzystać protokół NFS do przejęcia kontroli nad zdalnym systemem, przeprowadzenia eskalacji uprawnień, wstrzyknięcia backdoorów lub złośliwego oprogramowania na zdalnym hoście itp.

TCP 25: Prosty protokół przesyłania poczty (SMTP)

SMTP to protokół dostarczania poczty TCP/IP. Przesyła pocztę e-mail przez Internet i sieci lokalne. Działa w oparciu o zorientowaną na połączenie usługę świadczoną przez protokół TCP i używa dobrze znanego portu numer 25. Poniższa tabela zawiera listę niektórych poleceń używanych przez protokół SMTP i ich odpowiednią składnię.

Hello HELO <sending-host>

From MAIL FROM:<from-address>

Recipient RCPT TO:<to-address>

Data DATA

Reset RESET

Verify VRFY<string>

Expand EXPN<string>

Help HELP[string]

Quit QUIT

TCP/UDP 162: Pułapka SNMP

Pułapka SNMP używa portu TCP/UDP 162 do wysyłania powiadomień, takich jak opcjonalne powiązania zmiennych i wartość sysUpTime, od agenta do menedżera.

UDP 500: Internet Security Association i protokół zarządzania kluczami

(ISAKMPj/Internetowa wymiana kluczy (IKE)

Internet Security Association and Key Management Protocol (ISAKMPj/Internet Key Exchange (IKE) to protokół używany do konfigurowania skojarzenia zabezpieczeń (SA) w zestawie protokołów IPsec.

Wykorzystuje port UDP 500 do ustanawiania, negocjowania, modyfikowania i usuwania SA i klucze kryptograficzne w środowisku wirtualnej sieci prywatnej (VPN).

TCP 22: Bezpieczna powłoka (SSH)

Secure Shell (SSH) to protokół na poziomie poleceń, używany głównie do bezpiecznego zarządzania różnymi urządzeniami sieciowymi. Jest powszechnie używany jako protokół alternatywny dla niezabezpieczonego protokołu Telnet. SSH wykorzystuje model komunikacji klient/serwer, a serwer SSH domyślnie nasłuchuje swojego klienta na porcie TCP 22. Atakujący mogą wykorzystać protokół SSH poprzez brutalne wymuszenie danych logowania SSH.

TCP/UDP 3268: usługa wykazu globalnego

Serwer Global Catalog firmy Microsoft, kontroler domeny, który przechowuje dodatkowe informacje, używa portu 3268. Jego baza danych zawiera wiersze dla każdego obiektu w całej organizacji, zamiast wierszy tylko dla obiektów w jednej domenie. Katalog Globalny pozwala zlokalizować obiekt z dowolnej domeny bez konieczności znajomości nazwy domeny. LDAP na serwerze wykazu globalnego używa portu 3268. Ta usługa nasłuchuje na porcie 3268 za pośrednictwem połączenia TCP. Administratorzy używają portu 3268 do rozwiązywania problemów w wykazie globalnym, łącząc się z nim za pomocą protokołu LDP.

TCP/UDP 5060, 5061: protokół inicjowania sesji (SIP)

Session Initiation Protocol (SIP) to protokół używany w telefonii internetowej do połączeń głosowych i wideo. Zwykle wykorzystuje port TCP/UDP 5060 (nieszyfrowany ruch sygnalizacyjny) lub 5061 (ruch szyfrowany z TLS) do SIP do serwerów i innych punktów końcowych.

TCP 20/21: Protokół przesyłania plików

FTP to zorientowany na połączenie protokół używany do przesyłania plików przez Internet i sieci prywatne. FTP jest kontrolowany na porcie TCP 21, a do transmisji danych FTP używa portu TCP 20 lub niektórych dynamicznych numerów portów w zależności od konfiguracji serwera. Jeśli osoby atakujące stwierdzą, że porty serwera FTP są otwarte, przeprowadzają wyliczanie na serwerze FTP w celu znalezienia informacji, takich jak wersja oprogramowania i stan istniejących luk, w celu przeprowadzenia dalszych działań, takich jak wąchanie ruchu FTP i ataki FTP typu brute-force.

TCP 23: Telnet

Protokół Telnet służy do zdalnego zarządzania różnymi urządzeniami sieciowymi. Jest to protokół niezabezpieczony, ponieważ przesyła dane logowania w formacie zwykłego tekstu. Dlatego jest najczęściej używany w sieciach prywatnych. Serwer Telnet nasłuchuje swoich klientów na porcie 23. Atakujący mogą wykorzystać protokół Telnet do przechwytywania banerów na innych protokołach, takich jak SSH i SMTP, ataków typu brute-force na dane logowania, ataków polegających na przekierowaniu portów itp.

UDP 69: trywialny protokół przesyłania plików (TFTP)

TFTP to bezpołączeniowy protokół używany do przesyłania plików przez Internet. TFTP zależy od bezpołączeniowego protokołu UDP; w związku z tym nie gwarantuje prawidłowej transmisji pliku do miejsca docelowego. Protokół TFTP jest używany głównie do aktualizacji lub aktualizacji oprogramowania i oprogramowania układowego na zdalnych urządzeniach sieciowych. Wykorzystuje port UDP 69 do przesyłania plików do zdalnego hosta. Atakujący mogą wykorzystywać protokół TFTP

do instalowania złośliwego oprogramowania lub oprogramowania układowego na urządzeniach zdalnych.

TCP 179: protokół bramy granicznej (BGP)

Protokół BGP jest szeroko stosowany przez dostawców usług internetowych (ISP) do utrzymywania ogromnych tablic routingu i wydajnego przetwarzania ruchu internetowego. Routery BGP ustanawiają sesje na porcie TCP 179. Błędna konfiguracja protokołu BGP może prowadzić do różnych ataków, takich jak ataki słownikowe, ataki polegające na wyczerpaniu zasobów, ataki typu flooding i hijacking.

Wyliczanie NetBIOS

W tej sekcji opisano wyliczanie NetBIOS, uzyskane informacje oraz różne narzędzia wyliczające NetBIOS. NetBIOS jest brany pod uwagę przy wyliczaniu jako pierwszy, ponieważ wyodrębnia dużą ilość poufnych informacji o sieci docelowej, takich jak użytkownicy i udziały sieciowe. Pierwszym krokiem w wyliczaniu systemu Windows jest skorzystanie z interfejsu API NetBIOS. NetBIOS został pierwotnie opracowany jako interfejs API dla oprogramowania klienckiego w celu uzyskania dostępu do zasobów sieci lokalnej (LAN). Windows używa NetBIOS do udostępniania plików i drukarek. Nazwa NetBIOS to unikatowy 16-znakowy ciąg znaków ASCII przypisywany do systemów Windows w celu identyfikacji urządzeń sieciowych za pośrednictwem protokołu TCP/IP; Nazwa urządzenia składa się z 15 znaków, a szesnasty jest zarezerwowany dla typu usługi lub rekordu. NetBIOS używa portu UDP 137 (usługi nazw), portu UDP 138 (usługi datagramowe) i portu TCP 139 (usługi sesji). Atakujący zwykle atakują usługę NetBIOS, ponieważ jest łatwa do wykorzystania i uruchamiana w systemach Windows, nawet gdy nie jest używana. Atakujący wykorzystują wyliczanie NetBIOS w celu uzyskania następujących informacji:

•Lista komputerów należących do domeny

•Lista udziałów na poszczególnych hostach w sieci

• Zasady i hasła

Osoba atakująca, która znajdzie system Windows z otwartym portem 139, może sprawdzić, do jakich zasobów można uzyskać dostęp lub które można przeglądać w systemie zdalnym. Jednak aby wyliczyć nazwy NetBIOS, system zdalny musi mieć włączone udostępnianie plików i drukarek. Wyliczanie NetBIOS może umożliwić atakującemu odczyt lub zapis w zdalnym systemie komputerowym, w zależności od dostępności udziałów, lub przeprowadzenie ataku DoS.

Name	NetBIOS Code	Type	Information Obtained
<host name>	<00>	UNIQUE	Hostname
<domain>	<00>	GROUP	Domain name
<host name>	<03>	UNIQUE	Messenger service running for the computer
<username>	<03>	UNIQUE	Messenger service running for the logged-in user
<host name>	<20>	UNIQUE	Server service running
<domain>	<1D>	GROUP	Master browser name for the subnet
<domain>	<1B>	UNIQUE	Domain master browser name, which identifies the primary domain controller (PDC) for the domain
<domain>	<1E>	GROUP	Browser service elections

Należy pamiętać, że firma Microsoft nie obsługuje rozpoznawania nazw NetBIOS dla protokołu IPv6.

Narzędzie Nbtstat

Nbtstat to narzędzie systemu Windows, które pomaga w rozwiązywaniu problemów z rozpoznawaniem nazw NETBIOS. Polecenie nbtstat usuwa i koryguje wstępnie załadowane wpisy za pomocą kilku przełączników rozróżniających wielkość liter. Atakujący używają Nbtstat do wyliczania informacji, takich jak statystyki protokołu NetBIOS przez TCP/IP (NetBT), tabele nazw NetBIOS dla komputerów lokalnych i zdalnych oraz pamięć podręczna nazw NetBIOS. Składnia polecenia nbtstat jest następująca:

nbtstat [-a Nazwa Zdalna] [-A Adres IP] [-c] [-n] [-r] [-R] [-RR] [-s][-S] [Interwał]

Poniższa tabela zawiera listę różnych parametrów Nbtstat i ich odpowiednich funkcji.

Nbtstat Parameter	Function
`-a RemoteName`	Displays the NetBIOS name table of a remote computer, where RemoteName is the NetBIOS computer name of the remote computer
`-A IP Address`	Displays the NetBIOS name table of a remote computer, specified by the IP address (in dotted decimal notation) of the remote computer
`-c`	Lists the contents of the NetBIOS name cache, the table of NetBIOS names and their resolved IP addresses
`-n`	Displays the names registered locally by NetBIOS applications such as the server and redirector
`-r`	Displays a count of all names resolved by a broadcast or WINS server
`-R`	Purges the name cache and reloads all #PRE-tagged entries from the Lmhosts file
`-RR`	Releases and re-registers all names with the name server
`-s`	Lists the NetBIOS sessions table converting destination IP addresses to computer NetBIOS names
`-S`	Lists the current NetBIOS sessions and their status with the IP addresses
`Interval`	Re-displays selected statistics, pausing at each display for the number of seconds specified in Interval

Poniżej przedstawiono kilka przykładów poleceń nbtstat.

* Polecenie nbtstat „nbtstat -a <adres IP maszyny zdalnej>” może

zostać wykonane w celu uzyskania tabeli nazw NetBIOS zdalnego komputera.

* Komenda nbtstat „nbtstat -c” może zostać wykonana w celu uzyskania zawartości pliku

Pamięć podręczna nazw NetBIOS, tabela nazw NetBIOS i ich rozwiązane adresy IP.

Narzędzia wyliczania NetBIOS

Narzędzia wyliczające NetBIOS eksplorują i skanują sieć w określonym zakresie adresów IP i list komputerów w celu zidentyfikowania luk w zabezpieczeniach lub wad systemów sieciowych. Narzędzia te wyliczają również systemy operacyjne (OS), użytkowników, grupy, identyfikatory zabezpieczeń (SID),

zasady haseł, usługi, dodatki Service Pack i poprawki, udziały NetBIOS, transporty, sesje, dyski i dzienniki zdarzeń bezpieczeństwa itp.

Moduł wyliczający NetBIOS

NetBIOS Enumerator to narzędzie wyliczające, które pokazuje, jak korzystać ze zdalnej obsługi sieci i radzić sobie z niektórymi innymi protokołami sieciowymi, takimi jak SMB. Jak pokazano na zrzucie ekranu, osoby atakujące używają narzędzia NetBIOS Enumerator do wyliczenia szczegółów, takich jak nazwy NetBIOS, nazwy użytkowników, nazwy domen i adresy MAC dla danego zakresu adresów IP.

Poniżej przedstawiono kilka dodatkowych narzędzi wyliczających NetBIOS:

- Inwentaryzacja globalnej sieci (http://www.mognetosoft.com)

- Zaawansowany skaner IP (https://www.odvanced-ip-sconner.com)

- Hiena (https://www.systemtools.com)

- Audytor bezpieczeństwa sieci Nsauditor (https://www.nsouditor.com)

Wyliczanie kont użytkowników

Wyliczanie kont użytkowników za pomocą pakietu PsTools pomaga w kontrolowaniu i zarządzaniu systemami zdalnymi z wiersza poleceń. Poniżej przedstawiono niektóre polecenia służące do wyliczania kont użytkowników.

PsExec

PsExec to lekki zamiennik Telnet, który może wykonywać procesy w innych systemach, wraz z pełną interaktywnością dla aplikacji konsolowych, bez konieczności ręcznego instalowania oprogramowania klienckiego. Najpotężniejszym przypadkiem użycia PsExec jest uruchamianie interaktywnych monitów poleceń w systemach zdalnych oraz narzędzi umożliwiających zdalne działanie, takich jak ipconfig, które w przeciwnym razie nie mogą wyświetlać informacji o systemach zdalnych. Składnia polecenia PsExec jest następująca:

psexec [\\komputer[,komputer2[,...] | @plik]][-u użytkownik [-p psswd][-

[sesja]][-c

psexec [-f|-v]][-w katalog][-d][-<priorytet>][-a n,n,...] cmd

[argumenty]

PsFile

PsFile to narzędzie wiersza polecenia, które wyświetla listę plików w systemie, który został otwarty zdalnie, i może zamykać otwarte pliki według nazwy lub identyfikatora pliku. Domyślnym zachowaniem PsFile jest wyświetlanie listy plików w systemie lokalnym otwieranych przez systemy zdalne. Wpisanie polecenia, po którym następuje ", wyświetla informacje o składni tego polecenia.

n s][-r nazwa_usługi][-h][-1][-s|-e][-x][-i

Składnia polecenia PsFile jest następująca:

psfile [\\Komputer zdalny [-u Nazwa użytkownika [-p Hasło]]] [[Id | ścieżka]

[-C]]

PsGetSid

PsGetSid tłumaczy identyfikatory SID na ich nazwy wyświetlane i odwrotnie. Działa na kontach wbudowanych, kontach domeny i kontach lokalnych. Wyświetla również identyfikatory SID kont użytkowników i tłumaczy identyfikator SID na nazwę, która go reprezentuje. Działa w całej sieci, zdalnie wysyłając zapytania o identyfikatory SID. Składnia polecenia PsGetSid jest następująca:

psgetsid [\\komputer[,komputer[,...] | @plik] [-u nazwa użytkownika [-p

hasło]]] [konto|SID]

PsKill

PsKill to narzędzie do zabijania, które może zabijać procesy w systemach zdalnych i kończyć procesy na komputerze lokalnym. Uruchomienie PsKill z identyfikatorem procesu nakazuje mu zabicie procesu o tym identyfikatorze na komputerze lokalnym. Jeśli zostanie określona nazwa procesu, PsKill zabije wszystkie procesy o tej nazwie. Nie trzeba instalować klienta na komputerze docelowym, aby użyć PsKill do zakończenia zdalnego procesu. Składnia polecenia PsKill jest następująca:

pskill [-] [-t] [\\komputer [-u nazwa użytkownika] [-p hasło]] <proces

nazwa | identyfikator procesu>

Pslnfo

Pslnfo to narzędzie wiersza poleceń, które gromadzi kluczowe informacje o lokalnych lub zdalnych starszych systemach Windows, w tym typ instalacji, kompilację jądra, zarejestrowaną organizację i właściciela, liczbę procesorów i ich typ, ilość pamięci fizycznej, datę instalacji systemu , oraz data wygaśnięcia w przypadku wersji próbnej. Domyślnie Pslnfo pokazuje informacje dla systemu lokalnego. Można określić nazwę komputera zdalnego w celu uzyskania informacji o systemie zdalnym. Składnia polecenia Pslnfo jest następująca:

informacje ps

[-p psswd]]] [-h] [-s] [-d] [-c [-t ogranicznik]] [filtr]

PsList

PsList to narzędzie wiersza poleceń, które wyświetla informacje o jednostce centralnej (CPU) i pamięci lub statystyki wątków. Narzędzia w zestawach Resource Kit, pstat i pmon, pokazują różne typy danych tylko dla procesów w systemie, w którym narzędzia są uruchomione.

PsLoggedOn

PsLoggedOn to aplet, który wyświetla zarówno użytkowników zalogowanych lokalnie, jak i użytkowników zalogowanych za pośrednictwem zasobów komputera lokalnego lub zdalnego. Jeśli nazwa użytkownika jest określona zamiast komputera, PsLoggedOn przeszukuje komputery w sąsiedztwie sieci i ujawnia, czy użytkownik jest aktualnie zalogowany. PsLoggedOn definiuje, że użytkownik zalogowany lokalnie to taki, który ma profil załadowany do rejestru. Dlatego PsLoggedOn określa, kto jest zalogowany, skanując klucze pod kluczem HKEY_USERS. Dla każdego klucza, który ma nazwę lub identyfikator SID użytkownika, PsLoggedOn wyszukuje odpowiednią nazwę użytkownika i wyświetla ją. Aby określić, kto zalogował się do komputera za pośrednictwem udziałów zasobów, PsLoggedOn używa interfejsu API NetSessionEnum. Składnia polecenia PsLoggedOn jest następująca:

psloggedon [-] [-1] [-x] [\\

nazwakomputera|nazwaużytkownika]

PsLogList

Narzędzie elogdump zrzuca zawartość dziennika zdarzeń na komputer lokalny lub zdalny. PsLogList jest klonem elogdump, z wyjątkiem tego, że PsLogList może logować się do systemów zdalnych w sytuacjach, w których poświadczenia bezpieczeństwa użytkownika nie pozwalają na dostęp do dziennika zdarzeń, a PsLogList pobiera ciągi komunikatów z komputera, na którym przechowywany jest dziennik zdarzeń. Domyślną funkcją PsLogList jest wyświetlanie zawartości dziennika zdarzeń systemowych na komputerze lokalnym z przyjaznym wizualnie formatowaniem. Składnia polecenia PsLogList jest następująca:

psloglist [-] [\ \komputer [,komputer [,...] I @plik [-u nazwa_użytkownika [-

p hasło]]] [-s [-t ogranicznik]] [-m # | -n # | -h # |-d # | -w] [-c] [-

x][-r][-a mm/dd/rr][-b mm/dd/rr] [-f filtr] [-iID[,ID[, . . .] | -mi

ZROBIŁEM[, . . .]]] [-o źródło zdarzenia [,źródło zdarzenia] [,..]]] [-q zdarzenie

źródło [,źródło zdarzenia] [,..]]] [-1 plik dziennika zdarzeń] <dziennik zdarzeń>

PsPasswd

PsPasswd może zmienić hasło do konta w systemach lokalnych lub zdalnych, a administratorzy mogą tworzyć pliki wsadowe, które uruchamiają PsPasswd na komputerach, którymi zarządzają, w celu masowej zmiany hasła administratora. PsPasswd używa interfejsów API resetowania hasła systemu Windows; dlatego nie wysyła haseł przez sieć w postaci zwykłego tekstu. Składnia polecenia PsPasswd jest następująca:

pspasswd [[\\komputer[,komputer[,..] I @plik [-u użytkownik [-p psswd]]]

Nazwa użytkownika [NoweHasło]

PsShutdown

PsShutdown może zamknąć lub ponownie uruchomić komputer lokalny lub zdalny. Nie wymaga ręcznej instalacji oprogramowania klienckiego. Składnia polecenia PsShutdown jest następująca: psshutdown [[\\komputer[,komputer[,..] | gplik [-u użytkownik [-p

psswd]]] -s|-r|-h|-d|-k|-a|-11-o [-f] [-c] [-t nn|h:m] [-n s] [-v

nn] [-e [u|p]:xx:yy] [-m "wiadomość"]

Wyliczanie zasobów udostępnionych za pomocą widoku sieciowego

Net View to narzędzie wiersza polecenia, które wyświetla listę komputerów w określonej grupie roboczej lub udostępnionych zasobów dostępnych na określonym komputerze. Można go używać na następujące sposoby.

net view \\<computername>

W powyższym poleceniu <nazwa_komputera> to nazwa lub adres IP konkretnego komputera, którego zasoby mają zostać wyświetlone.

net view \\<computername> /ALL

Powyższe polecenie wyświetla wszystkie udziały na określonym komputerze zdalnym wraz z udziałami ukrytymi.

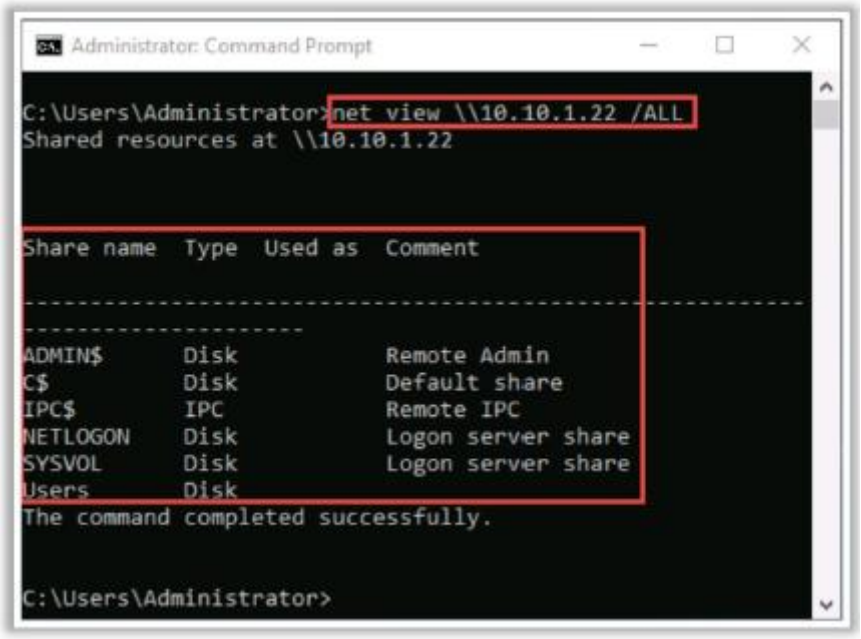
net view /domain

Powyższe polecenie wyświetla wszystkie udziały w domenie.

net view /domain:<domain name>

Powyższe polecenie wyświetla wszystkie udziały w określonej domenie.

Zrzut ekranu pokazuje udostępnione zasoby dostępne na określonym komputerze.



Wyliczanie SNMP

Simple Network Management Protocol (SNMP) umożliwia administratorom sieci zdalne zarządzanie urządzeniami sieciowymi. Jednak SNMP ma wiele luk w zabezpieczeniach, takich jak brak audytu. Atakujący mogą wykorzystać te luki do wyliczenia kont i urządzeń. Ta sekcja opisuje wyliczanie SNMP, informacje wyodrębniane za pomocą wyliczania SNMP oraz różne narzędzia wyliczania SNMP używane do wyliczania kont użytkowników i urządzeń w systemie docelowym. SNMP to protokół warstwy aplikacji, który działa na UDP i utrzymuje oraz zarządza routerami, koncentratorami i przełącznikami w sieci IP. Agenci SNMP działają w sieciach Windows i Unix na urządzeniach sieciowych. Wyliczanie SNMP to proces tworzenia listy kont użytkowników i urządzeń w miejscu docelowym komputerze za pomocą protokołu SNMP. SNMP wykorzystuje do komunikacji dwa rodzaje komponentów oprogramowania: agenta SNMP i stację zarządzającą SNMP. Agent SNMP znajduje się na urządzeniu sieciowym, a stacja zarządzająca SNMP komunikuje się z agentem. Prawie wszystkie urządzenia infrastruktury sieciowej, takie jak routery i przełączniki, zawierają agenta SNMP do zarządzania systemem lub urządzeniami. Stacja zarządzająca SNMP wysyła żądania do agenta; po otrzymaniu żądania agent odpowiada. Zarówno żądania, jak i odpowiedzi są zmiennymi konfiguracyjnymi dostępnymi dla oprogramowania agenta. Stacje zarządzające SNMP wysyłają żądania ustawienia wartości dla niektórych zmiennych. Pułapki informują stację zarządzającą o wystąpieniu nietypowego zdarzenia, takiego jak ponowne uruchomienie lub awaria interfejsu po stronie agenta. SNMP zawiera następujące dwa hasła do konfigurowania i uzyskiwania dostępu do agenta SNMP ze stacji zarządzającej.

Przeczytaj ciąg społeczności

o Za pomocą tego hasła można przeglądać konfigurację urządzenia lub systemu.

o Te łańcuchy są publiczne.

Odczyt/zapis ciągu społeczności

o Za pomocą tego hasła można zmienić lub edytować konfigurację urządzenia,

o Te łańcuchy są prywatne.

Gdy administratorzy pozostawią ciągi społeczności z ustawieniem domyślnym, osoby atakujące mogą użyć tych domyślnych ciągów społeczności (hasła) do zmiany lub przeglądania konfiguracji urządzenia lub systemu. Atakujący wyliczają SNMP, aby wyodrębnić informacje o zasobach sieciowych, takich jak hosty, routery, urządzenia i udziały, a także informacje o sieci, takie jak tabele ARP, tablice routingu, informacje specyficzne dla urządzeń i statystyki ruchu. Powszechnie używane narzędzia wyliczające SNMP obejmują OpUtils i Network Monitor wydajności.

Działanie SNMP

SNMP wykorzystuje zakłóconą architekturę zawierającą menedżerów SNMP, agentów SNMP i kilka powiązanych komponentów. Poniżej przedstawiono niektóre polecenia związane z SNMP.

• GetRequest: Używany przez menedżera SNMP do żądania informacji od agenta SNMP

• GetNextRequest: Używany przez menedżera SNMP w sposób ciągły do pobierania wszystkich zapisanych danych w tablicy lub tabeli

• GetResponse: Używany przez agenta SNMP do spełnienia żądania wysłanego przez menedżera SNMP

• SetRequest: Używany przez menedżera SNMP do modyfikowania wartości parametru w bazie informacji zarządzania agenta SNMP (MIB)

• Pułapka: używana przez agenta SNMP do informowania wstępnie skonfigurowanego menedżera SNMP o pewnym wydarzeniu

Proces komunikacji między menedżerem SNMP a agentem SNMP wygląda następująco.

• Menedżer SNMP (Host X, 10.10.2.1) używa polecenia GetRequest do wysłania żądania liczby aktywnych sesji do agenta SNMP (Host Y, 10.10.2.15). Aby wykonać ten krok, menedżer SNMP używa biblioteki usługi SNMP, takiej jak biblioteka Microsoft SNMP Management API (Mgmtapi.dll) lub biblioteka Microsoft WinSNMP API (Wsnmp32.dll).

• Agent SNMP (Host Y) odbiera komunikat i sprawdza, czy w jego bazie MIB znajduje się ciąg społeczności (Compinfo), porównuje żądanie z listą uprawnień dostępu dla tej społeczności i weryfikuje źródłowy adres IP.

• Jeśli agent SNMP nie znajdzie ciągu społeczności lub pozwolenia dostępu w bazie danych MIB hosta Y, a usługa SNMP jest ustawiona na wysyłanie pułapki uwierzytelniania, wysyła pułapkę niepowodzenia uwierzytelnienia do określonego miejsca docelowego pułapki, hosta Z.

• Komponent głównego agenta agenta SNMP wywołuje odpowiedniego agenta rozszerzeń i pobrać żądane informacje o sesji z bazy MIB.

• Korzystając z informacji o sesji pobranych z agenta rozszerzeń, usługa SNMP tworzy zwrotny komunikat SNMP zawierający liczbę aktywnych sesji i docelowy adres IP (10.10.2.1) menedżera SNMP, hosta X.

• Host Y wysyła odpowiedź do hosta X.

Baza informacji zarządczej (MIB)

MIB to wirtualna baza danych zawierająca formalny opis wszystkich obiektów sieciowych zarządzanych przez SNMP. Jest to zbiór uporządkowanych hierarchicznie informacji. Zapewnia standardową reprezentację informacji i przechowywania agenta SNMP. Elementy MIB są rozpoznawane za pomocą identyfikatorów obiektów (OID). OID to numeryczna nazwa nadana obiektowi, rozpoczynająca się od korzenia drzewa MIB. OID może jednoznacznie identyfikować obiekt w hierarchii MIB. Obiekty zarządzane przez MIB obejmują obiekty skalarne, które definiują pojedynczą instancję obiektu, oraz obiekty tabelaryczne, które definiują grupę powiązanych instancji obiektu. Identyfikatory OID obejmują typ obiektu (taki jak licznik, ciąg znaków lub adres), poziom dostępu (taki jak odczyt lub odczyt/zapis), ograniczenia rozmiaru i informacje o zakresie. Menedżer SNMP konwertuje identyfikatory OID na czytelny dla człowieka wyświetlacz, używając MIB jako książki kodowej. Użytkownik może uzyskać dostęp do zawartości MIB za pomocą przeglądarki internetowej, wprowadzając adres IP i Lseries.mib lub wprowadzając nazwę biblioteki DNS i Lseries.mib. Na przykład http://IP.Address/Lseries.mib lub http://nazwa_biblioteki/Lseries.mib.Microsoft udostępnia listę baz MIB, które są instalowane z usługą SNMP w zestawie Windows Resource Kit. Główne bazy MIB są następujące:

DHCP.MIB: Monitoruje ruch sieciowy między serwerami DHCP a zdalnymi hostami

HOSTMIB.MIB: Monitoruje zasoby hosta i zarządza nimi

LNMIB2.MIB: Zawiera typy obiektów dla usług stacji roboczej i serwera

MIB_II.MIB: Zarządza Internetem opartym na protokole TCP/IP przy użyciu prostej architektury i systemu

WINS.MIB: dla usługi Windows Internet Name Service (WINS)

Wyliczanie SNMP za pomocą SnmpWalk

SnmpWalk to narzędzie wiersza poleceń, które umożliwia atakującym natychmiastowe skanowanie wielu węzłów protokołu SNMP (Simple Network Management Protocol) i identyfikowanie zestawu zmiennych, które są dostępne w celu uzyskania dostępu do sieci docelowej. Za pomocą tego narzędzia atakujący atakują węzeł główny, aby można było pobrać informacje ze wszystkich węzłów podrzędnych, takich jak routery i przełączniki. Informacje można pobrać w postaci identyfikatora obiektu (OID), który jest częścią bazy informacji zarządzania (MIB) powiązanej z urządzeniami z włączonym SNMP. Atakujący wykonują następujące polecenie, aby pobrać informacje SNMP z urządzenia docelowego:

snmpwalk -vl -c public <docelowy adres IP>

Powyższe polecenie umożliwia atakującym przeglądanie wszystkich identyfikatorów OID, zmiennych i innych powiązanych informacji. Za pomocą tego polecenia osoby atakujące mogą również pobrać wszystkie dane przesyłane do serwera SNMP z agenta SNMP, w tym używany serwer, poświadczenia użytkownika i inne parametry.

Inne polecenia SnmpWalk:

Polecenie wyliczenia SNMPv2 z łańcuchem społeczności public:

snmpwalk -v2c -c public <docelowy adres IP>

Polecenie wyszukania zainstalowanego oprogramowania:

snmpwalk -v2c -c public <docelowy adres IP> hrSWInstalledName

Polecenie do określenia ilości pamięci RAM na hoście:

snmpwalk -v2c -c public <docelowy adres IP> hrMemorySize

Polecenie zmiany OID na inną wartość:

snmpwalk -v2c -c public <Docelowy adres IP> <OID> <Nowa wartość>

Polecenie zmiany identyfikatora sysContact OID:

snmpwalk -v2c -c public <Docelowy adres IP> sysContact <Nowa wartość>

Wyliczanie SNMP za pomocą Nmap

Atakujący używają skryptu snmp-processes Nmap Scripting Engine (NSE) przeciwko zdalnemu serwerowi SNMP w celu pobrania informacji związanych z hostowanymi usługami SNMP.

nmap -sU -p 161 --script=snmp-processes <Docelowy adres IP>

Powyższe polecenie Nmap po wykonaniu pobiera listę wszystkich uruchomionych procesów SNMP wraz z powiązanymi portami na hoście docelowym. Inne polecenia Nmap do wykonywania wyliczania SNMP:

nmap -sU -p 161 --script=snmp-sysdescr <Docelowy adres IP> Pobiera informacje dotyczące typu serwera SNMP i szczegółów systemu operacyjnego.

nmap -sU -p 161 --script=snmp-win32-software <docelowy adres IP>

-> Pobiera listę wszystkich aplikacji uruchomionych na komputerze docelowym.

Narzędzia wyliczania SNMP

Narzędzia wyliczające SNMP służą do skanowania pojedynczego adresu IP lub zakresu adresów IP urządzeń sieciowych obsługujących protokół SNMP w celu monitorowania, diagnozowania i rozwiązywania problemów związanych z zagrożeniami bezpieczeństwa.

snmp-check (moduł snmp_enum)

snmp-check to narzędzie typu open source rozpowszechniane na licencji GNU General Public License (GPL). Jego celem jest automatyzacja procesu zbierania informacji na dowolnym urządzeniu z obsługą SNMP (Windows, Unix, urządzenia sieciowe, drukarki itp.), snmp-check umożliwia wyliczanie urządzeń SNMP i umieszcza dane wyjściowe w postaci czytelnej dla człowieka i przyjazny dla użytkownika format. Może być przydatny do testów penetracyjnych lub monitorowania systemów. Atakujący używają tego narzędzia do zbierania informacji o celu, takich jak kontakt, opis, dostęp do zapisu, urządzenia, domena, informacje o sprzęcie i pamięci masowej, nazwa hosta, statystyki Internet Information Services (IIS), przekazywanie IP, nasłuchiwanie portów UDP, lokalizacja, punkty

montowania, interfejsy sieciowe, usługi sieciowe, informacje o trasach, komponenty oprogramowania, czas pracy systemu, połączenia TCP, łączna pamięć, czas pracy bez przestojów i konta użytkowników.

Skaner sieciowy SoftPerfect

SoftPerfect Network Scanner może pingować komputery, skanować porty, wykrywać udostępnione foldery i pobierać praktycznie dowolne informacje o urządzeniach sieciowych za pośrednictwem Windows Management Instrumentation (WMI), SNMP, Hypertext Transfer Protocol (HTTP), SSH i PowerShell. Skanuje również w poszukiwaniu usług zdalnych, rejestru, plików i liczników wydajności; oferuje elastyczne opcje filtrowania i wyświetlania; i eksportuje wyniki NetScan do różnych formatów, od Extensible Markup Language (XML) do JavaScript Object Notation (JSON). Co więcej, SoftPerfect Network Scanner może sprawdzić port zdefiniowany przez użytkownika i zgłosić, czy jest on otwarty. Ponadto może rozpoznawać nazwy hostów i automatycznie wykrywać lokalny i zewnętrzny zakres adresów IP. Obsługuje zdalne wyłączanie i funkcję Wake-on-LAN. Atakujący używają tego narzędzia do zbierania informacji o udostępnionym folderze i urządzeniach sieciowych.

Poniżej przedstawiono kilka dodatkowych narzędzi wyliczających SNMP:

- Monitor wydajności sieci (https://www.solarwinds.com)

- OpUtils (https://www.manageengine.com)

- Monitor sieci PRTG (https://www.paessler.com)

- Zestaw narzędzi inżyniera (https://www.solarwinds.com)

Wyliczanie LDAP

Różne protokoły umożliwiają komunikację i zarządzanie transferem danych pomiędzy zasobami sieciowymi. Wszystkie te protokoły przenoszą wraz z danymi cenne informacje o zasobach sieciowych. Użytkownik zewnętrzny, któremu uda się wyliczyć te informacje, manipulując protokołami, może włamać się do sieci i niewłaściwie wykorzystać zasoby sieciowe. Protokół LDAP (Lightweight Directory Access Protocol) jest jednym z takich protokołów, który uzyskuje dostęp do list katalogów. Ta sekcja koncentruje się na wyliczaniu LDAP, informacjach wyodrębnionych za pomocą wyliczania LDAP oraz narzędziach wyliczania LDAP. LDAP to protokół internetowy umożliwiający dostęp do rozproszonych usług katalogowych. LDAP uzyskuje dostęp do list katalogów w usłudze Active Directory lub z innych usług katalogowych. LDAP to hierarchiczna lub logiczna forma katalogu, podobna do schematu organizacyjnego firmy. Usługi katalogowe mogą zapewniać dowolny zorganizowany zestaw rekordów, często w strukturze hierarchicznej i logicznej, taki jak firmowy katalog poczty e-mail. Używa DNS do szybkiego wyszukiwania i szybkiego rozwiązywania zapytań. Klient rozpoczyna sesję LDAP, łącząc się z agentem systemu katalogowego (DSA), zazwyczaj na porcie TCP 389, i wysyła żądanie operacji do agenta DSA. Do transmisji używany jest format Basic Encoding Rules (BER). Osoba atakująca może anonimowo wysłać zapytanie do usługi LDAP w celu uzyskania poufnych informacji, takich jak nazwy użytkowników, adresy, szczegóły działów i nazwy serwerów, których osoba atakująca może użyć do przeprowadzenia ataków.

Ręczne i automatyczne wyliczanie LDAP

Atakujący mogą stosować zarówno ręczne, jak i automatyczne podejście do wyliczania LDAP. Oto niektóre z poleceń, których można użyć do wyliczenia LDAP.

Ręczne wyliczanie LDAP

Atakujący mogą wykonać ręczne wyliczanie LDAP przy użyciu języka Python. Wykonaj czynności podane poniżej, aby wykonać ręczne wyliczanie LDAP przy użyciu języka Python.

1. Za pomocą Nmap sprawdź, czy docelowy serwer LDAP nasłuchuje na porcie 389 dla LDAP i na porcie 636 dla bezpiecznego LDAP.

2. Jeśli serwer docelowy nasłuchuje na określonych portach, zainicjuj proces wyliczania, instalując LDAP za pomocą następującego polecenia:

pip3 install ldap3

3. Jak pokazano w kodzie podanym poniżej, utwórz obiekt serwera (serwer), określ docelowy adres IP lub nazwę hosta i numer portu. Jeśli serwer docelowy nasłuchuje na bezpiecznym LDAP, podaj use_ssl = True.

4. Pobierz konteksty nazewnictwa wpisów (DSE) agenta systemu katalogowego (DSA), określając get_info = ldap3.ALL.

5. Teraz utwórz obiekt połączenia, connection i zainicjuj wywołanie metody bind().

6. Jeśli połączenie się powiedzie, na ekranie zostanie wyświetlona prawda w następujący sposób:

»> import ldap3

»> server = ldap3.Server('Target IP Address ', get_info =

ldap3.ALL, port =389)

»> connection = ldap3.Connection(server)

»> connection.bind()

True

7. Teraz można pobrać informacje, takie jak nazwa domeny i kontekst nazewnictwa za pomocą

następujący skrypt:

»> serwer.info

8. Po uzyskaniu kontekstu nazewnictwa pobierz wszystkie obiekty katalogu, używając podanego skryptu

poniżej:

»> connection.search(search_base='DC=DOMAIN,DC=DOMAIN',

search_filter='(&(objectClass=*))', search_scope='SUBTREE',

attributes='*')

True

» connection.entries

9. Teraz użyj następującego skryptu, aby zrzucić cały LDAP:

» connection.search(search_base='DC=DOMAIN,DC=DOMAIN' ,

search_filter='(&(objectClass=person))', search_scope='SUBTREE',

attributes='userPassword')

True

»> connection.entries

Narzędzia wyliczania LDAP

Istnieje wiele narzędzi do wyliczania LDAP, które uzyskują dostęp do list katalogów w usłudze Active Directory (AD) lub innych usługach katalogowych. Korzystając z tych narzędzi, osoby atakujące mogą wyliczyć informacje, takie jak prawidłowe nazwy użytkowników, adresy i szczegóły działów z różnych serwerów LDAP.

Softerra Administrator LDAP

Softerra LDAP Administrator to narzędzie administracyjne LDAP, które współpracuje z serwerami LDAP, takimi jak Active Directory (AD), Novell Directory Services i Netscape/iPlanet. Przegląda i zarządza katalogami LDAP. Jak pokazano na zrzucie ekranu, atakujący używają Softerra LDAP Administrator do wyliczania szczegółów użytkownika, takich jak nazwa użytkownika, adres e-mail i dział.

Idapsearch

idapsearch jest interfejsem dostępnym dla powłoki dla wywołania biblioteki idap_search_ext(3), idapsearch otwiera połączenie z serwerem LDAP, wiąże go i przeprowadza wyszukiwanie przy użyciu określonych parametrów. Filtr powinien być zgodny z łańcuchową reprezentacją filtrów wyszukiwania, zgodnie z definicją w dokumencie RFC 4515. Jeśli nie zostanie podany, używany jest filtr domyślny (objectClass=*). Jeśli idapsearch znajdzie jeden lub więcej wpisów, zwracane są atrybuty określone przez attrs. Jeśli na liście znajduje się *, zwracane są wszystkie atrybuty użytkownika. Jeśli na liście znajduje się znak +, zwracane są wszystkie atrybuty operacyjne. Jeśli na liście nie ma atrybutów, zwracane są wszystkie atrybuty użytkownika. Jeśli na liście jest tylko 1.1, nie są zwracane żadne atrybuty. Wyniki wyszukiwania są wyświetlane przy użyciu rozszerzonej wersji formatu wymiany danych LDAP (LDIF). Opcja -L steruje formatem wyjściowym. Atakujący używają idapsearch do wyliczania użytkowników AD. Umożliwia to atakującym nawiązanie połączenia z serwerem LDAP w celu przeprowadzenia różnych wyszukiwań przy użyciu określonych filtrów. Następującego polecenia można użyć do wyszukiwania LDAP przy użyciu prostego uwierzytelniania:

Idapsearch -h <docelowy adres IP> -x

Jeśli powyższe polecenie zostanie wykonane pomyślnie, można wykonać następujące polecenie, aby uzyskać dodatkowe szczegóły związane z kontekstami nazewnictwa:

ldapsearch -h <docelowy adres IP> -x -s podstawowe konteksty nazw

Na przykład z danych wyjściowych powyższego polecenia, jeśli składnik domeny podstawowej można zidentyfikować jako DC=htb,DC=local, można użyć następującego polecenia, aby uzyskać więcej informacji o domenie podstawowej:

ldapsearch -h <docelowy adres IP> -x -b "DC=htb,DC=local"

Poniższych poleceń można użyć do pobrania informacji o określonym obiekcie lub wszystkich obiektach w drzewie katalogów:

ldapsearch -h <docelowy adres IP> '(objectClass=Employee)' -> pobiera informacje związane z klasą obiektu Pracownik.

ldapsearch –x -h <Docelowy adres IP> -b „DC=htb, DC=local” objectciass=*u -> pobiera informacje dotyczące wszystkich obiektów w drzewie katalogu.

Następujące polecenie pobiera listę użytkowników należących do określonej klasy obiektów:

ldapsearch -h <Docelowy adres IP> ’(objectClass=Pracownik) -x -b ”DC=htb,DC=local” ,(objectClass=Employee)’sAMAccountName sAMAccountType

Poniżej przedstawiono kilka dodatkowych narzędzi do wyliczania LDAP:

• Eksplorator AD (https://docs.microsoft.com)

• Narzędzie administratora LDAP (https://www.ldapsoft.com)

• Menedżer kont LDAP (https://www.ldap-account-manager.org)

• Wyszukiwanie LDAP (https://securityxploded.com)

Wyliczanie NTP i NFS

Rozważając kwestie bezpieczeństwa, administratorzy często pomijają serwer Network Time Protocol (NTP). Jednakże, jeśli zostanie poprawnie zapytany, może dostarczyć atakującemu cenne informacje o sieci. Dlatego konieczne jest, aby wiedzieć, jakie informacje o sieci atakujący może uzyskać za pomocą wyliczenia NTP. Sieciowy system plików (NFS) służy do zarządzania zdalnym dostępem do plików. Wyliczanie NFS pomaga atakującym zebrać informacje, takie jak lista klientów podłączonych do serwera NFS wraz z ich adresami IP oraz wyeksportowane katalogi. Ta sekcja opisuje wyliczanie NTP, informacje wyodrębniane za pomocą wyliczania NTP, różne polecenia wyliczania NTP, narzędzia wyliczania NTP oraz techniki i narzędzia wyliczania NFS.

Wyliczanie NTP

NTP jest przeznaczony do synchronizacji zegarów komputerów w sieci. Używa portu UDP 123 jako podstawowego środka komunikacji. NTP może utrzymywać czas z dokładnością do 10 ms w publicznym Internecie. Co więcej, w idealnych warunkach może osiągnąć dokładność 200 ps lub lepszą w sieciach LAN. Poniżej przedstawiono niektóre informacje, które osoba atakująca może uzyskać, wysyłając zapytanie do serwera NTP:

* Lista hostów podłączonych do serwera NTP

* Adresy IP klientów w sieci, ich nazwy systemowe i systemy operacyjne

* Wewnętrzne adresy IP, jeśli serwer NTP znajduje się w strefie zdemilitaryzowanej (DMZ)

Polecenia wyliczania NTP

Polecenia wyliczania NTP, takie jak ntpdate, ntptrace, ntpdc i ntpq, służą do wysyłania zapytań do serwera NTP w celu uzyskania cennych informacji.

ntpdata

To polecenie zbiera liczbę próbek czasu z kilku źródeł czasu. Jego składnia

następująco:

ntpdate [-46bBdqsuv] [-a key] [-e authdelay] [-k keyfile] [-o

version] [-p samples] [-t timeout] [-U user_name] server [...]

-4 Wymuś rozpoznawanie DNS podanych nazw hostów na przestrzeń nazw IPv4

-6 Wymuś rozpoznawanie nazw DNS podanych nazw hostów na przestrzeń nazw IPv6

Włącz funkcję uwierzytelniania/określ identyfikator klucza, który ma być używany do uwierzytelniania -a klucz

-B Wymuś zawsze obracanie czasu

-b Wymuś stopniowanie czasu

-d Włącz tryb debugowania

-e authdelay Określ opóźnienie przetwarzania w celu wykonania funkcji uwierzytelniania

-k plik-klucz Określa ścieżkę do pliku klucza uwierzytelniającego jako ciąg "plik-klucza"; wartością domyślną jest /etc/ntp/keys

- o wersja Określ wersję NTP dla wychodzących pakietów jako wersję całkowitą, która może wynosić 1 lub 2; wartość domyślna to 4

-p próbki

-q Tylko zapytanie; nie ustawiaj zegara

-s Przekierowuje wyjście rejestrowania ze standardowego wyjścia (domyślnie) do systemu syslog

-t timeout Określ maksymalny czas oczekiwania na odpowiedź serwera; wartość domyślna to 1s

-u Użyj nieuprzywilejowanego portu dla pakietów wychodzących

-v Bądź gadatliwy; rejestruje łańcuch identyfikacyjny wersji ntpdate

ntptrace

To polecenie określa, skąd serwer NTP uzyskuje czas i śledzi łańcuch serwerów NTP z powrotem do głównego źródła czasu. Atakujący używają tego polecenia do śledzenia listy serwerów NTP podłączonych do sieci. Jego składnia jest następująca:

ntptrace [-n] [-m maxhosts] [nazwa_serwera/adres_IP]

- n Nie drukuj nazw hostów i pokazuj tylko adresy IP; może być przydatne, jeśli serwer nazw nie działa

-m maxhosts Ustawia maksymalną liczbę poziomów w górę łańcucha, które mają być przestrzegane

Przykład:

ntptrace

localhost: stratum 4, offset 0.0019529, synch distance 0.143235

10.10.0.1: stratum 2, offset 0.01142

73, synch distance 0.115554

10.10.1.1: stratum 1, offset 0.0017698, synch distance 0.01119

ntpdc

To polecenie wysyła zapytanie do demona ntpd dotyczące jego bieżącego stanu i żąda zmian w tym stanie. Atakujący używają tego polecenia, aby pobrać stan i statystyki każdego serwera NTP podłączonego do sieci docelowej. Jego składnia jest następująca:

ntpdc [-46dilnps] [-c command] [hostname/IP_address]

-4 Wymuś rozpoznawanie DNS podanej nazwy hosta na przestrzeń nazw IPv4

-6 Wymuś rozpoznawanie DNS podanej nazwy hosta na przestrzeń nazw IPv6

-d Włącz tryb debugowania

-c Poniższy argument jest interpretowany jako interaktywne polecenie formatowania; można podać wiele opcji -c

-i Wymuś działanie ntpdc w trybie interaktywnym

-l Uzyskaj listę peerów znanych serwerowi (serwerom); ten przełącznik jest odpowiednikiem opcji -c listpeers

-n Wypisuje wszystkie adresy hostów w formacie numerycznym z kropkami i czterema kropkami, zamiast nazw hostów

-p Wydrukuj listę peerów oraz podsumowanie ich stanów; jest to równoważne opcji -c rówieśnicy

-s Wypisuje listę peerów oraz podsumowanie ich stanów, ale w nieco innym formacie niż dla przełącznika -p; jest to równoważne opcji -c dmpeers

ntpq

To polecenie monitoruje działanie demona NTP ntpd i określa jego wydajność. Jego składnia jest następująca:

ntpq [-46dinp] [-c polecenie] [host/adres_IP]

-4 Wymuś rozpoznawanie DNS podanej nazwy hosta na przestrzeń nazw IPv4

-6 Wymuś rozpoznawanie DNS podanej nazwy hosta na przestrzeń nazw IPv6

-c Następujący argument jest interaktywnym poleceniem formatującym; można podać wiele opcji -c

-d Tryb debugowania

-i Wymuś działanie ntpq w trybie interaktywnym

-n Wypisuje wszystkie adresy hostów w formacie numerycznym z kropkami i czterema kropkami, zamiast nazw hostów

-P Wydrukuj listę peerów oraz podsumowanie ich stanów

Przykład:

ntpq> wersja

ntpq 4.2.8pl5@l.3728-0

ntpq> host

obecny host to localhost

Uwaga: W wielu dystrybucjach Linuksa demon NTP został połączony z Chrony,chronyd. Oba demony synchronizują czas lokalnego systemu ze zdalnym serwerem czasu.

Narzędzia wyliczania NTP

Narzędzia wyliczeniowe NTP służą do monitorowania pracy serwerów NTP i SNTP w sieci oraz pomagają w konfiguracji i weryfikacji łączności od klienta czasu do serwerów NTP.

Monitor sieci PRTG

PRTG monitoruje wszystkie systemy, urządzenia, ruch i aplikacje infrastruktury IT za pomocą różnych technologii, takich jak SNMP, WMI i SSH. Atakujący wykorzystują Monitor sieci PRTG do pobierania szczegółowych informacji o serwerze SNTP, takich jak czas odpowiedzi z serwera, aktywne czujniki z serwerem i czas synchronizacji.

Oto niektóre narzędzia do wyliczania NTP:

- Nmap (https://nmop.org)

-Wireshark (https://www.wireshork.org)

- udp-proto-scanner (https://lobs.portcullis.co.uk)

- Skaner serwera NTP (http://www.bytefusion.com)

Wyliczanie NFS

NFS to rodzaj systemu plików, który umożliwia użytkownikom dostęp, przeglądanie, przechowywanie i aktualizowanie plików za pośrednictwem zdalnego serwera. Klient może uzyskiwać dostęp do tych zdalnych danych w taki sam sposób, jak w systemie lokalnym. W zależności od uprawnień przypisanych klientom, mogą oni albo tylko odczytywać, albo jednocześnie odczytywać i zapisywać dane. System NFS jest zwykle wdrażany w sieci komputerowej, w której wymagana jest centralizacja danych dla zasobów krytycznych. Zdalne wywołanie procedury (RPC) służy do kierowania i przetwarzania żądania między klientami a serwerami. Aby wykonać zadanie udostępniania plików i katalogów w sieci, używany jest proces „eksportowania". Niezależnie od tego, klient najpierw próbuje udostępnić plik do udostępniania, korzystając z procesu „montowania". Lokalizacja /etc/exports na serwerze NFS zawiera listę klientów, którym wolno udostępniać pliki na serwerze. W tym podejściu, aby uzyskać dostęp do serwera, jedynym używanym poświadczeniem jest adres IP klienta. Wersje NFS przed wersją 4 działają w oparciu o tę samą specyfikację zabezpieczeń. Wyliczanie usług NFS umożliwia atakującym identyfikację wyeksportowanych katalogów, listy klientów podłączonych do serwera NFS wraz z ich adresami IP oraz współdzielonych danych powiązanych z adresami IP. Po zebraniu tych informacji osoby atakujące mogą sfałszować swoje adresy IP, aby uzyskać pełny dostęp do udostępnionych plików na serwerze. Jak pokazano na zrzucie ekranu, osoba atakująca uruchamia następujące polecenie rpcinfo, aby przeskanować docelowy adres IP w poszukiwaniu otwartego portu NFS (port 2049) i działających na nim usług NFS:

rpcinfo -p <docelowy adres IP>

Jak pokazano na zrzucie ekranu, osoba atakująca uruchamia następujące polecenie, aby wyświetlić listę udostępnionych plików i katalogów:

showmount -e <Docelowy adres IP>

Ponadto osoba atakująca może użyć różnych innych poleceń i narzędzi, aby uzyskać dostęp do serwera NFS i przesłać złośliwe pliki na serwer w celu przeprowadzenia dalszych ataków.

Narzędzia wyliczające NFS

Narzędzia wyliczające NFS skanują sieć w określonym zakresie adresów IP lub pojedynczym adresie IP, aby zidentyfikować uruchomione w niej usługi NFS. Narzędzia te pomagają również uzyskać listę usług RPC przy użyciu portmap, listę udziałów NFS oraz listę katalogów dostępnych przez NFS; ponadto umożliwiają pobieranie pliku udostępnionego przez serwer NFS. Atakujący używają narzędzi takich jak RPCScan i SuperEnum do wyliczania NFS.

RPCScan

RPCScan komunikuje się z usługami RPC i sprawdza błędne konfiguracje udziałów NFS. Jak pokazano na zrzucie ekranu, osoba atakująca uruchamia następujące polecenie w celu wyliczenia docelowego adresu IP dla aktywnych usług NFS:

python3 rpc-scan.py <docelowy adres IP> --rpc

SuperEnum

SuperEnum zawiera skrypt, który wykonuje podstawowe wyliczanie dowolnego otwartego portu. Jak pokazano na zrzucie ekranu, atakujący używa skryptu ./superenum, a następnie wprowadza nazwę pliku tekstowego „Target.txt" zawierającego docelowy adres IP lub listę adresów IP do wyliczenia.

r- n - Parrot Tei

Po przeskanowaniu docelowego adresu IP skrypt wyświetla wszystkie otwarte porty, jak pokazano na poniższym zrzucie ekranu. Port 2049 ma uruchomioną usługę NFS.

Wyliczanie SMTP i DNS

W tej sekcji opisano techniki wyliczania w celu wyodrębnienia informacji związanych z zasobami sieciowymi. Obejmuje również techniki wyliczania DNS, które dostarczają informacji o serwerach DNS i infrastrukturze sieciowej docelowej organizacji. W tej sekcji omówiono techniki wyliczania MTP i DNS, obejmujące wyliczanie SMTP, proces uzyskiwania listy prawidłowych użytkowników na serwerze SMTP, narzędzia wyliczania SMTP, wyliczanie transferu stref DNS, szpiegowanie pamięci podręcznej DNS i chodzenie po strefach DNS.

Wyliczanie SMTP

Systemy pocztowe zwykle używają protokołu SMTP z protokołami POP3 i IMAP, które umożliwiają użytkownikom zapisywanie wiadomości w skrzynce pocztowej serwera i pobieranie ich z serwera w razie potrzeby. SMTP używa serwerów wymiany poczty (MX) do kierowania poczty przez DNS. Działa na porcie TCP 25, 2525 lub 587 SMTP udostępnia następujące trzy wbudowane polecenia.

VRFY: Validates users

$ telnet 192.168.168.1 25

Trying 192.168.168.1...

Connected to 192.168.168.1.

Escape character is

220 NYmailserver ESMTP Sendmail 8.9.3

HELO

501 HELO requires domain address

HELO x

250 NYmailserver Hello [10.0.0.86], pleased to meet you

VRFY Jonathan

250 Super-User <Jonathan@NYmailserver>

VRFY Smith

550 Smith... User unknown

EXPN: Wyświetla rzeczywiste adresy dostawy aliasów i list mailingowych

$ telnet 192.168.168.1 25

Trying 192.168.168.1...

Connected to 192.168.168.1.

Escape character is I A] ' •

220 NYmailserver ESMTP Sendmail 8.9.3

HELO

501 HELO requires domain address

HELO x

250 NYmailserver Hello [10.0.0.86], pleased to meet you

EXPN Jonathan

250 Super-User <Jonathan@NYmailserver>

EXPN Smith

550 Smith... User unknown

RCPT TO: Określa odbiorców wiadomości

$ telnetl 192.168.168.1 25

Trying 192.168.168.1 ...

Connected to 192.168.168.1.

Escape character is , A]'.

220 NYmailserver ESMTP Sendmail 8.9.3

HELO

501 HELO requires domain address

HELO x

250 NYmailserver Hello [10.0.0.86], pleased to meet you

MAIL FROM:Jonathan

250 Jonathan... Sender ok

RCPT TO:Ryder

250 Ryder... Recipient ok

RCPT TO: Smith

550 Smith... User unknown

Serwery SMTP różnie reagują na polecenia VRFY, EXPN i RCPT TO dla prawidłowych i nieprawidłowych użytkowników; w związku z tym można określić prawidłowych użytkowników na serwerze SMTP. Atakujący mogą bezpośrednio wchodzić w interakcje z SMTP za pośrednictwem polecenia Telnet i gromadzić listę prawidłowych użytkowników na serwerze SMTP. Administratorzy i testerzy piór mogą przeprowadzać wyliczanie SMTP za pomocą narzędzi wiersza poleceń, takich jak Telnet i netcat, lub za pomocą narzędzi, takich jak Metasploit, Nmap, NetScanTools Pro i smtp-user-enum w celu zebrania listy prawidłowych użytkowników, adresów dostawy, odbiorców wiadomości itp.

Wyliczanie SMTP za pomocą Nmap

Atakujący używają Nmap do wyliczania informacji z docelowego serwera SMTP. Wyliczają docelowy serwer SMTP za pomocą różnych poleceń SMTP dostępnych w Nmap Scripting Engine (NSE).

* Wykonanie następującego polecenia wyświetla listę wszystkich poleceń SMTP dostępnych w katalogu Nmap:

nmap -p 25, 365, 587 -script=smtp-commands <docelowy adres IP>

* Uruchom następujące polecenie, aby zidentyfikować otwarte przekaźniki SMTP:

nmap -p 25 -script=smtp-open-relay <Docelowy adres IP>

* Uruchom następujące polecenie, aby wyliczyć wszystkich użytkowników poczty na serwerze SMTP:

nmap -p 25 -script=smtp-enum-users <docelowy adres IP>

Serwery SMTP różnie reagują na polecenia VRFY, EXPN i RCPT TO dla prawidłowych i nieprawidłowych użytkowników; w związku z tym można określić prawidłowych użytkowników na serwerze SMTP. Atakujący mogą bezpośrednio wchodzić w interakcje z SMTP za pośrednictwem polecenia Telnet i gromadzić listę prawidłowych użytkowników na serwerze SMTP. Administratorzy i testerzy piór mogą przeprowadzać wyliczanie SMTP za pomocą narzędzi wiersza poleceń, takich jak Telnet i netcat, lub za pomocą narzędzi, takich jak Metasploit, Nmap, NetScanTools Pro i smtp-user-enum w celu zebrania listy prawidłowych użytkowników, adresów dostawy, odbiorców wiadomości itp.

Wyliczanie SMTP przy użyciu Metasploit

Atakujący wykorzystują platformę Metasploit do wyliczania użytkowników SMTP. Struktura zawiera moduł wyliczania SMTP, który umożliwia atakującym łączenie się z docelowym serwerem SMTP i wyliczać nazwy użytkowników za pomocą predefiniowanych list słów. Serwer SMTP wykorzystuje swoją wbudowaną metodę VRFY do sprawdzania poprawności nazw użytkowników w pliku listy słów z użytkownikami obecnymi na serwerze i wyświetla dopasowaną listę użytkowników.

Kroki, aby wyliczyć użytkowników SMTP za pomocą Metasploit

Krok 1: Uruchom Metasploit msfconsole i przełącz się na odpowiedni skaner pomocniczy, aby zainicjować proces:

/smtp/smtp_enum.

msf > use auxiliary/scanner/smtp/smtp_enuin

msf auxiliary(smtp_enum) >

Krok 2: Użyj polecenia pokaż opcje, aby wyświetlić całą listę opcji wymaganych do wykonania tego zadania. Alternatywnie można użyć polecenia show evasion, aby wyświetlić listę opcji umożliwiających obejście rozwiązań bezpieczeństwa.

Krok 3: Użyj opcji zestawu RHOST, aby ustawić adres IP docelowego serwera SMTP lub zakres adresów IP.

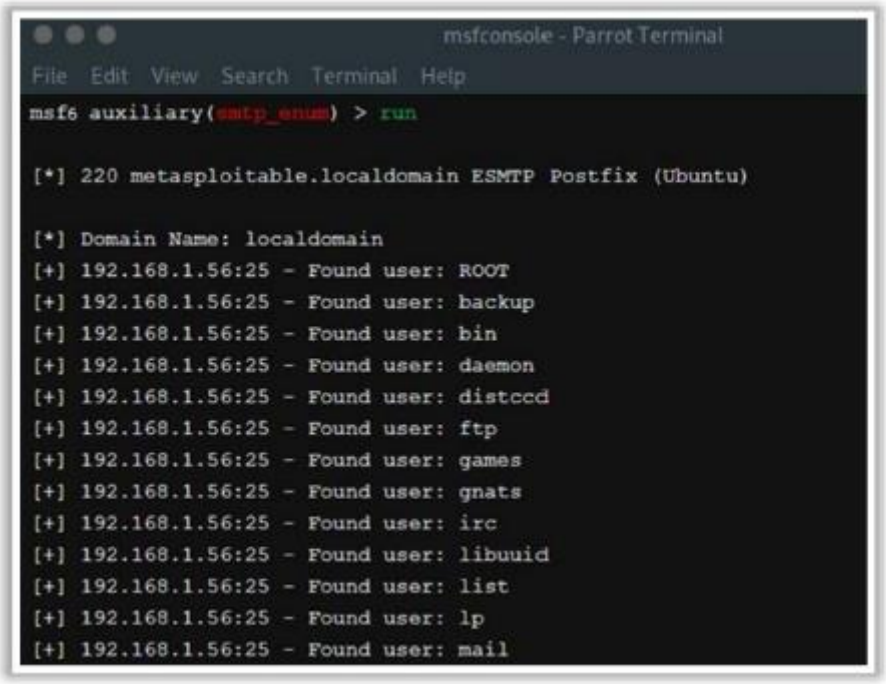
Krok 4: Domyślnie platforma Metasploit używa domyślnych list słów znajdujących się pod adresem

/usr/share/64etasploit-framework/data/wordlists/unix_users.txt aby wyliczyć użytkowników SMTP. Opcję USER_FILE można ustawić tak, aby korzystała z niestandardowych list słów.

msf auxiliary(smtp_enum) > set USER_FILE <location of wordlists file>

Krok 5: Użyj polecenia show advanced, aby wyświetlić pełną listę dostępnych opcji w module wyliczania użytkowników SMTP.

Krok 6: Wykonaj polecenie uruchomienia, aby rozpocząć proces wyliczania. Skanuje podane listy słów z użytkownikami serwera SMTP i wyświetla listę wszystkich pasujących nazw użytkowników.



Jak pokazano na zrzucie ekranu, osoby atakujące uzyskują listę prawidłowych użytkowników SMTP z docelowego serwera SMTP i mogą wykorzystać te informacje do zainicjowania ataków ukierunkowanych.

Narzędzia wyliczania SMTP

Narzędzia wyliczające SMTP służą do wyliczania nazw użytkowników. Atakujący mogą wykorzystać nazwy użytkowników uzyskane z tego wyliczenia do przeprowadzania dalszych ataków na inne systemy w sieci.

NetScanTools Pro

Narzędzie SMTP Email Generator NetScanTools Pro testuje proces wysyłania wiadomości e-mail przez serwer SMTP. Atakujący używają NetScanTools Pro do wyliczania SMTP i wyodrębniają wszystkie parametry nagłówka wiadomości e-mail, w tym flagi potwierdzenia/pilności. Atakujący mogą również rejestrować sesję e-mail w pliku dziennika, a następnie przeglądać komunikację między programem NetScanTools Pro a serwerem SMTP w pliku dziennika.

smtp-user-enum

smtp-user-enum to narzędzie do wyliczania kont użytkowników na poziomie systemu operacyjnego w systemie Solaris za pośrednictwem usługi SMTP (sendmail). Wyliczanie odbywa się poprzez sprawdzanie odpowiedzi na polecenia VRFY, EXPN i RCPT TO. Jak pokazano na zrzucie ekranu, smtp-user-enum należy przekazać do listy użytkowników i co najmniej jednego celu z uruchomioną usługą SMTP. Składnia używania smtp-user-enum jest następująca:

smtp-user-enum.pl [opcje] (-u username|-U file-of-usernames) (-t host|-T plik-celów)

smtp-user-enum ma następujące opcje:

o -m n: Maksymalna liczba procesów (domyślnie: 5)

o Tryb -M: Określ polecenie SMTP, które ma być używane do odgadywania nazwy użytkownika

EXPN, VRFY i RCPT TO (domyślnie: VRFY)

o -u użytkownik: Sprawdź, czy użytkownik istnieje w systemie zdalnym

o -f adres: Określ adres e-mail nadawcy, który ma być używany do zgadywania „RCPT TO” (domyślnie:

użytkownik@example.com)

-D dom: Określ domenę, która ma zostać dołączona do podanej listy użytkowników w celu utworzenia wiadomości e-mail

adresy (domyślnie: brak)

-U plik: Wybierz plik zawierający nazwy użytkowników do sprawdzenia za pośrednictwem usługi SMTP

-t host: Określ host serwera, na którym działa usługa SMTP

-T plik: Wybierz plik zawierający nazwy hostów, na których działa usługa SMTP

-p port: Określ port TCP, na którym działa usługa SMTP (domyślnie: 25)

-d: wyjście debugowania

-t n: Poczekaj na odpowiedź maksymalnie n sekund (domyślnie: 5)

-v: pełne

-h: komunikat pomocy

Wyliczanie DNS przy użyciu transferu strefy

Transfer strefy DNS to proces przesyłania kopii pliku strefy DNS z podstawowego serwera DNS na pomocniczy serwer DNS. W większości przypadków podstawowy serwer DNS utrzymuje zapasowy lub pomocniczy serwer zapewniający nadmiarowość, na którym przechowywane są wszystkie informacje przechowywane w główny serwer. Serwer DNS używa transferu stref do dystrybucji zmian wprowadzonych na serwerze głównym do serwerów pomocniczych. Osoba atakująca przeprowadza wyliczanie transferu stref DNS w celu zlokalizowania serwera DNS i uzyskania dostępu do rekordów docelowej organizacji. Jeśli serwer DNS docelowej organizacji zezwala na transfery stref, osoby atakujące mogą wykonać transfer stref DNS w celu uzyskania nazw serwerów DNS, nazw hostów, nazw maszyn, nazw użytkowników, adresów IP, aliasów itp. przypisanych w domenie docelowej. Podczas wyliczania DNS przy użyciu transferu stref osoba atakująca próbuje pobrać kopię całego pliku strefy dla domeny z serwera DNS. Atakujący mogą wykonać transfer strefy DNS za pomocą narzędzi, takich jak nslookup, komenda dig i DNSRecon. Jeśli ustawienie transferu DNS jest włączone na docelowym serwerze nazw, dostarczy informacje DNS; w przeciwnym razie zwróci błąd informujący o niepowodzeniu lub odrzuceniu transferu strefy. Aby wykonać transfer strefy DNS, atakujący wysyła żądanie przeniesienia strefy do serwera DNS, podszywając się pod klienta; następnie serwer DNS wysyła atakującemu część swojej bazy danych jako strefę. Ta strefa może zawierać dużą ilość informacji o sieci strefy DNS.

Komenda dig

Atakujący używają polecenia dig w systemach opartych na systemie Linux, aby wysyłać zapytania do serwerów nazw DNS i pobierać informacje o docelowych adresach hostów, serwerach nazw, wymianach poczty itp. Jak pokazano na zrzucie ekranu, osoby atakujące używają następującego polecenia do wykonania transferu strefy DNS:

dig ns <domena docelowa>

Powyższe polecenie pobiera wszystkie serwery nazw DNS domeny docelowej. Następnie atakujący używają jednego z serwerów nazw z danych wyjściowych powyższego polecenia, aby sprawdzić, czy docelowy DNS zezwala na transfery stref. Używają w tym celu następującego polecenia:

dig @<domena serwera nazw> <domena docelowa> axfr

Polecenie nslookup

Atakujący używają polecenia nslookup w systemach Windows do wysyłania zapytań do serwerów nazw DNS i pobierania informacji o docelowych adresach hostów, serwerach nazw, wymianach poczty itp. Jak pokazano na zrzucie ekranu, osoby atakujące używają następującego polecenia do wykonania transferu strefy DNS:

nslookup

ustaw typ zapytania=soa

<domena docelowa>

Powyższe polecenie ustawia typ zapytania na rekord Start of Authority (SOA) w celu pobrania informacji administracyjnych o strefie DNS domeny docelowej Certifiedhacker.com. Następujące polecenie służy do próby przeniesienia strefy określonego serwera nazw:

/ls -d <domena serwera nazw>

DNSRecon

Atakujący używają DNSRecon do sprawdzenia wszystkich rekordów NS domeny docelowej pod kątem transferów stref. Jak pokazano na zrzucie ekranu, atakujący używają następującego polecenia do transferu strefy DNS: dnsrecon -t axfr -d <domena docelowa>

W powyższym poleceniu opcja -t określa typ wyliczenia, które ma zostać wykonane, axfr to typ wyliczenia, w którym wszystkie serwery NS są testowane pod kątem transferu strefy, a opcja -doption określa domenę docelową.

Podsłuchiwanie pamięci podręcznej DNS

Podsłuchiwanie pamięci podręcznej DNS to rodzaj techniki wyliczania DNS, w której osoba atakująca wysyła zapytanie do serwera DNS w celu uzyskania określonego zapisanego w pamięci podręcznej rekordu DNS. Korzystając z tego zapisanego w pamięci podręcznej rekordu, osoba atakująca może określić witryny ostatnio odwiedzane przez użytkownika. Informacje te mogą dodatkowo ujawniać ważne informacje, takie jak nazwa właściciela serwera DNS, jego usługodawcy, nazwa jego dostawcy i dane bankowe. Korzystając z tych informacji, osoba atakująca może przeprowadzić atak socjotechniczny na docelowego użytkownika. Atakujący wykonują szpiegowanie w pamięci podręcznej DNS za pomocą różnych narzędzi, takich jak polecenie dig i DNSRecon. Atakujący używają następujących dwóch metod szpiegowania pamięci podręcznej DNS, aby szpiegować domenę docelową.

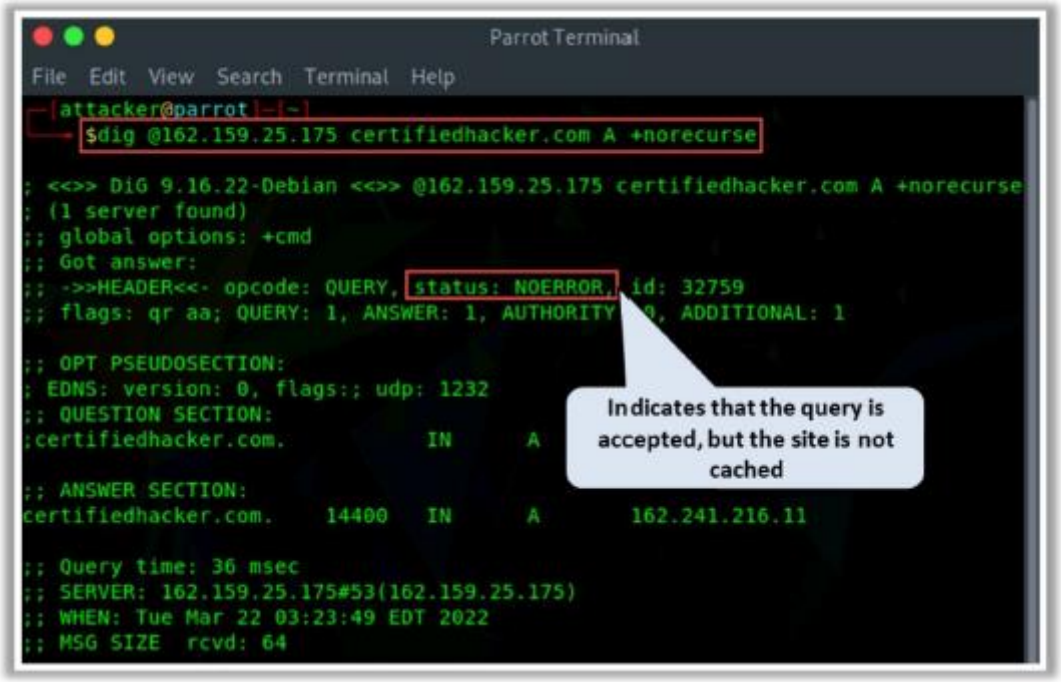
Metoda nierekurencyjna

W tej metodzie, aby szpiegować serwer DNS, atakujący wysyłają zapytanie nierekurencyjne, ustawiając bit Recursion Desired (RD) w nagłówku zapytania na zero. Atakujący wysyłają zapytanie do pamięci

podręcznej DNS pod kątem określonego rekordu DNS, takiego jak A,CNAME, PTR, CERT, SRV i MX. Jeśli żądany rekord znajduje się w pamięci podręcznej DNS, serwer DNS odpowiada informacją wskazującą, że jakiś użytkownik w systemie odwiedził określoną domenę. W przeciwnym razie serwer DNS prześle w odpowiedzi informacje o innym serwerze DNS, który może zwrócić odpowiedź na zapytanie, lub prześle odpowiedź w postaci pliku root.hints zawierającego informacje o wszystkich głównych serwerach DNS. Atakujący używają polecenia dig, po którym następuje nazwa/adres IP serwera DNS, nazwa domeny i typ pliku rekordu DNS. Opcja tnorecurse służy do ustawiania zapytania jako nierekurencyjnego.

dig @<adres IP serwera DNS> <domena docelowa> A +norecurse

Jak pokazano na zrzucie ekranu, status NOERROR oznacza, że zapytanie zostało zaakceptowane, ale nie została zwrócona żadna odpowiedź, co oznacza, że żaden użytkownik z systemu nie odwiedził żądanej witryny

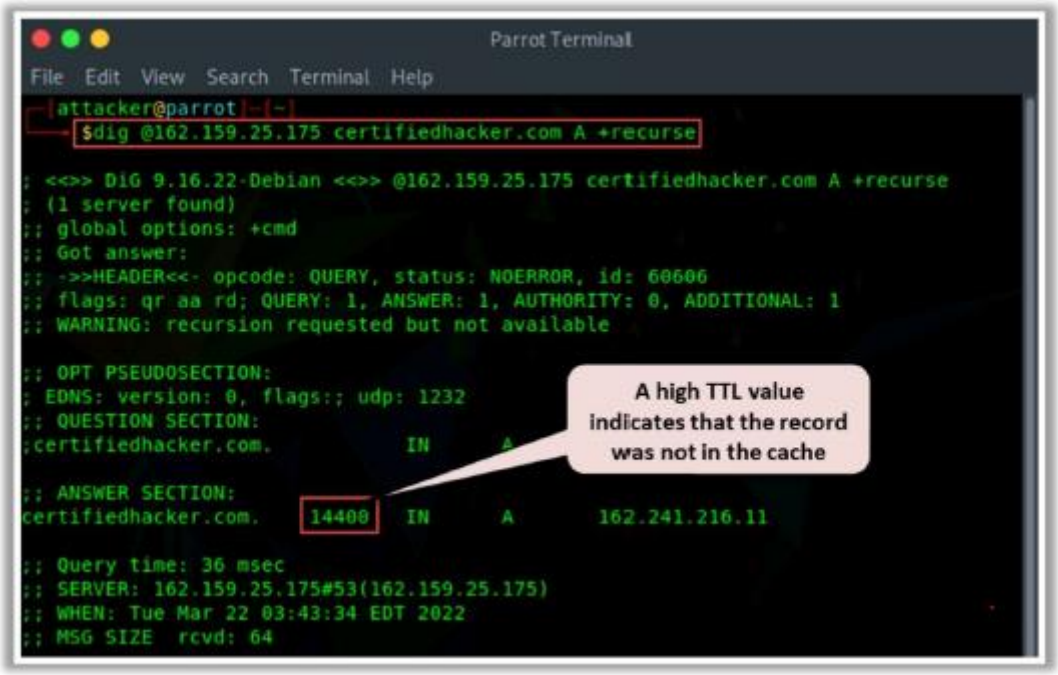


Metoda rekurencyjna

W tej metodzie, aby szpiegować serwer DNS, osoby atakujące wysyłają zapytanie rekurencyjne, ustawiając opcję trscurse zamiast opcji +norecurse. Podobnie jak w przypadku metody nierekurencyjnej, osoby atakujące wysyłają zapytanie do pamięci podręcznej DNS w celu uzyskania określonego rekordu DNS, takiego jak A, CNAME, PTR, CERT, SRV i MX. W tej metodzie sprawdzane jest pole czasu życia (TTL) w celu określenia czasu, przez który rekord DNS pozostaje w pamięci podręcznej. W tym przypadku wartość TTL uzyskana z wyniku jest porównywana z wartością TTL, która została pierwotnie ustawiona w polu TTL. Jeśli wartość TTL w wyniku jest mniejsza niż początkowa wartość TTL, rekord jest zapisywany w pamięci podręcznej, wskazując, że ktoś w systemie odwiedził tę witrynę. Jeśli jednak żądany rekord nie znajdował się w pamięci podręcznej, zostanie on dodany do pamięci podręcznej po wysłaniu pierwszego zapytania. Atakujący używają tego samego polecenia Dig, co w metodzie nierekurencyjnej, ale z opcją +recurse zamiast opcji +norecurse:

dig @<adres IP serwera DNS> <domena docelowa> A +recurse

Jak pokazano na zrzucie ekranu, wartość TTL dla domeny Certifiedhacker.com jest znacznie wysoka, co zdecydowanie sugeruje, że rekord domeny nie znajdował się w pamięci podręcznej w momencie wysłania zapytania.



Spacer po strefie DNSSEC

Zwiedzanie stref DNSSEC (Domain Name System Security Extensions) to rodzaj DNS — technika wyliczania, w której osoba atakująca próbuje uzyskać wewnętrzne rekordy, jeśli strefa DNS nie jest prawidłowo skonfigurowana. Wyliczone informacje o strefie mogą pomóc atakującemu w zbudowaniu mapy sieci hosta. Organizacje używają DNSSEC, aby dodać funkcje bezpieczeństwa do danych DNS i zapewnić ochronę przed znanymi zagrożeniami dla DNS. Ta funkcja zabezpieczeń wykorzystuje podpisy cyfrowe oparte na kryptografii klucza publicznego w celu wzmocnienia uwierzytelniania w DNS. Te podpisy cyfrowe są przechowywane na serwerach nazw DNS wraz z typowymi rekordami, takimi jak MX, A, AAAA i CNAME. Chociaż DNSSEC zapewnia bezpieczeństwo w Internecie, jest również podatny na lukę zwaną wyliczaniem stref lub chodzeniem po strefach. Wykorzystując tę lukę, osoby atakujące mogą uzyskać informacje o sieci domeny docelowej, na podstawie których mogą przeprowadzać ataki internetowe. Aby przezwyciężyć lukę w zabezpieczeniach związaną z wyliczaniem stref, używana jest nowa wersja DNSSEC, która korzysta z Next Secure w wersji 3 (NSEC3). Rekord NSEC3 zapewnia te same funkcje, co rekordy NSEC, z tą różnicą, że zapewnia zaszyfrowane kryptograficznie nazwy rekordów, które mają na celu zapobieganie wyliczaniu nazw rekordów znajdujących się w strefie. Aby przeprowadzić wyliczanie stref, osoby atakujące mogą użyć różnych modułów wyliczających strefy DNSSEC, takich jak LDNS, DNSRecon, nsec3map, nsec3walker i DNSwalk.

Narzędzia do chodzenia po strefie DNSSEC

Narzędzia do chodzenia po strefie DNSSEC służą do wyliczania plików rekordów DNS domeny docelowej. Narzędzia te mogą również wykonywać wyliczanie stref w plikach rekordów NSEC i NSEC3, a następnie wykorzystywać zebrane informacje do przeprowadzania ataków, takich jak ataki typu „odmowa usługi” (DoS) i ataki phishingowe.

LDNS

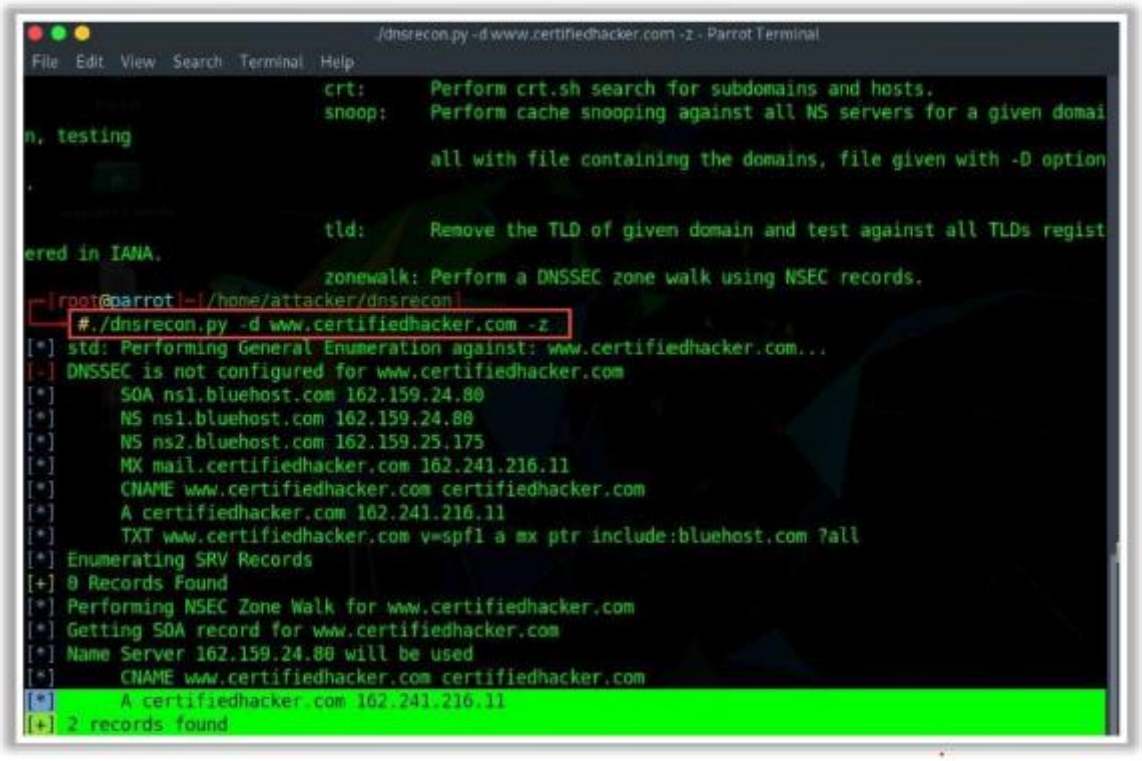
LDNS-walk wylicza strefę DNSSEC i uzyskuje wyniki w plikach rekordów DNS. Jak pokazano na zrzucie ekranu, osoby atakujące używają następującego zapytania do wyliczenia domeny docelowej iana.org przy użyciu serwera DNS 8.8 .8.8 w celu uzyskania plików rekordów DNS:

ldns-walk @<adres IP serwera DNS> <domena docelowa>

DNSRecon

DNSRecon to narzędzie do wyliczania stref, które pomaga użytkownikom w wyliczaniu rekordów DNS, takich jak A, AAAA i CNAME. Wykonuje również wyliczanie stref NSEC w celu uzyskania plików rekordów DNS domeny docelowej. Jak pokazano na zrzucie ekranu, osoby atakujące używają następującego zapytania do wyliczenia strefy w domenie docelowej Certifiedhacker.com:

dnsrecon -d <domena docelowa> -z



Wyliczanie DNS i DNSSEC za pomocą Nmap

Wyliczanie DNS za pomocą Nmap

Atakujący używają Nmap do skanowania domen i uzyskiwania listy subdomen, rekordów, adresów IP i innych cennych informacji od docelowego hosta. Uruchom następujące polecenie, aby wyświetlić listę wszystkich dostępnych usług na hoście docelowym:

nmap --script=broadcast-dns-service-discovery CDomena docelowa>

Wykonaj następujące polecenie, aby pobrać wszystkie subdomeny powiązane z hostem docelowym:

nmap -T4 -p 53 --script dns-brute <domena docelowa>

Powyższe polecenie udostępnia listę subdomen wraz z ich adresami IP. Jeśli rejestrowane są jakiekolwiek wpisy z symbolami wieloznacznymi, są one reprezentowane jako *A* dla adresów IPv4 i *AAAA* dla adresów IPv6.

Uruchom następujące polecenie, aby sprawdzić, czy rekurencja DNS jest włączona na serwerze docelowym:

nmap -Pn -sU -p 53 --script=dns-recursion 192.168.1.150

Wyliczanie rozszerzeń zabezpieczeń DNS (DNSSEC) za pomocą Nmap

DNSSEC zapewnia bezpieczeństwo zapytań i odpowiedzi DNS. Atakujący wyliczają DNSSEC za pomocą skryptów NSE dns-nsec-enum.nse lub dns-nsec3-enum.nse w celu uzyskania informacji związanych z domenami i ich subdomenami.

Wykonaj następujące polecenie, aby pobrać listę subdomen powiązanych z domeną docelową:

nmap -sU -p 53 --script dns-nsec-enum --script-args dns-nsecenum.

domains= eccouncil.org <cel>

Oto niektóre z dodatkowych narzędzi wyliczania DNS:

KnockZapukaj (https://github.com)

Raccon (https://github.com)

Subfinder (https://github.com)

Turbolist3r (https://github.com)

Inne techniki wyliczania

W tej sekcji omówiono wyliczanie użytkowników IPsec, VoIP, RPC, użytkowników Unix/Linux, Telnet, użytkowników SSH, FTP, TFTP, SMB, IPv6 i BGP.

Wyliczanie IPsec

IPsec to najczęściej wdrażana technologia zarówno w rozwiązaniach VPN typu brama-brama (LAN-to-LAN), jak i host-brama (dostęp zdalny). IPsec zapewnia bezpieczeństwo danych, wykorzystując różne składniki, takie jak Encapsulating Security Payload (ESP), Authentication Header (AH) i Internet Key Exchange (IKE) w celu zabezpieczenia komunikacji między punktami końcowymi VPN. Większość sieci VPN opartych na protokole IPsec używa protokołu ISAKMP (Internet Security Association Key Management Protocol), który jest częścią IKE, do ustanawiania, negocjowania, modyfikowania i usuwania powiązań zabezpieczeń (SA) i kluczy kryptograficznych w środowisku VPN. Atakujący mogą wykonać proste bezpośrednie skanowanie w poszukiwaniu ISAKMP na porcie UDP 500 za pomocą narzędzi takich jak Nmap w celu uzyskania informacji związanych z obecnością bramy VPN. Następującego polecenia można użyć do wykonania skanowania Nmap w celu sprawdzenia stanu ISAKMP na porcie 500:

nmap -sU -p 500 <docelowy adres IP>

Atakujący mogą dalej sondować za pomocą narzędzi do pobierania odcisków palców, takich jak ike-scan, w celu wyliczenia poufnych informacji, w tym algorytmu szyfrowania i mieszania, typu uwierzytelniania, algorytmu dystrybucji kluczy i SA LifeDuration. W tym typie skanowania specjalnie spreparowane pakiety IKE z nagłówkiem ISAKMP są wysyłane do docelowej bramy, a odpowiedzi są

rejestrowane. Następujące polecenie służy do wstępnego wykrywania sieci VPN IPsec za pomocą narzędzia ike-scan:

ike-scan -M <adres IP docelowej bramy>

ike-scan

ike-scan wykrywa hosty IKE i może ich odciski palców przy użyciu wzorca wycofywania retransmisji, ike-scan może wykonywać następujące funkcje.

Wykrywanie: hosty z uruchomionym IKE w danym zakresie adresów IP można określić, wyświetlając hosty, które odpowiadają na żądania IKE wysyłane przez ike-scan.

Odcisk palca: można określić implementację IKE używaną przez hosty, aw niektórych przypadkach można określić wersję oprogramowania, z którego korzystają. Odbywa się to na dwa sposoby: odcisk palca UDP, który obejmuje rejestrowanie czasów nadejścia pakietów odpowiedzi IKE z hostów docelowych i porównanie zaobserwowanego wzorca wycofywania retransmisji ze znanymi wzorcami, oraz odcisk palca identyfikatora dostawcy, który porównuje ładunki identyfikatora dostawcy z Serwery VPN pod kątem znanych wzorców identyfikatorów dostawców.

Wyliczanie transformacji: Można określić atrybuty transformacji obsługiwane przez serwer VPN dla fazy IKE 1 (np. algorytm szyfrowania i algorytm mieszania).

Wyliczanie użytkowników: w przypadku niektórych systemów VPN można wykryć prawidłowe nazwy użytkowników VPN.

Łamanie klucza wstępnego: Łamanie hasła w trybie offline lub metodą brute-force można przeprowadzić w trybie agresywnym IKE z uwierzytelnianiem za pomocą klucza wstępnego. Wykorzystuje ikescan do uzyskania skrótu i innych parametrów, a także psk-crack, który jest częścią pakietu ike-scan, do przeprowadzenia crackowania.

Wyliczanie VoIP

VoIP to zaawansowana technologia, która zastąpiła konwencjonalną publiczną komutowaną sieć telefoniczną (PSTN) zarówno w środowiskach korporacyjnych, jak i domowych. VoIP wykorzystuje infrastrukturę internetową do nawiązywania połączeń dla połączeń głosowych; dane są również przesyłane w tej samej sieci. Jednak VoIP jest podatny na wektory ataków TCP/IP. Session Initiation Protocol (SIP) jest jednym z protokołów używanych przez VoIP do wykonywania połączeń głosowych, połączeń wideo itp. przez sieć IP. Ta usługa SIP zazwyczaj wykorzystuje porty UDP/TCP 2000, 2001, 5060 i 5061. Atakujący używają narzędzi Svmap i Metasploit do wyliczania VoIP. Poprzez wyliczanie VoIP osoby atakujące mogą gromadzić poufne informacje, takie jak bramy/serwery VoIP, systemy PBX (IP-Private Branch Exchange) oraz adresy IP User-Agent i rozszerzenia użytkownika oprogramowania klienckiego (softphones) lub telefonów VoIP. Informacje te mogą być wykorzystywane do przeprowadzania różnych ataków VoIP, takich jak ataki DoS, przejmowanie sesji, fałszowanie identyfikatora dzwoniącego, podsłuchiwanie, spam przez telefonię internetową (SPIT) i phishing VoIP (Vishing).

Svmap

Svmap to skaner typu open source, który identyfikuje urządzenia SIP i serwery PBX w sieci docelowej. Może być pomocny dla administratorów systemu, gdy jest używany jako narzędzie do inwentaryzacji sieci.

Atakujący używają Svmap do wykonywania następujących czynności:

o Zidentyfikuj urządzenia SIP i serwery PBX na portach domyślnych i innych niż domyślne

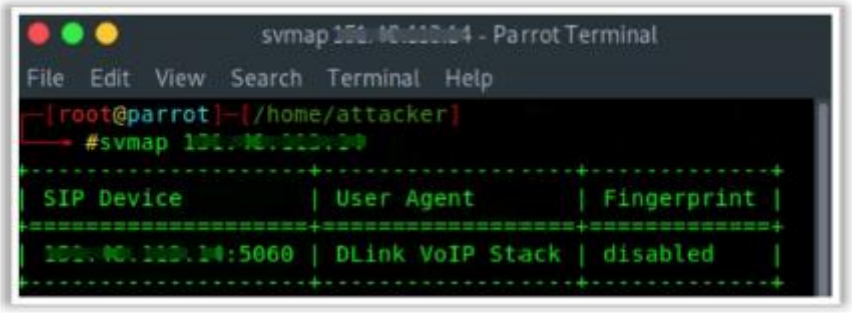
o Skanuj duże zakresy sieci

o Skanuj jednego hosta na różnych portach w poszukiwaniu usługi SIP na tym hoście lub wielu hostach na wielu portach

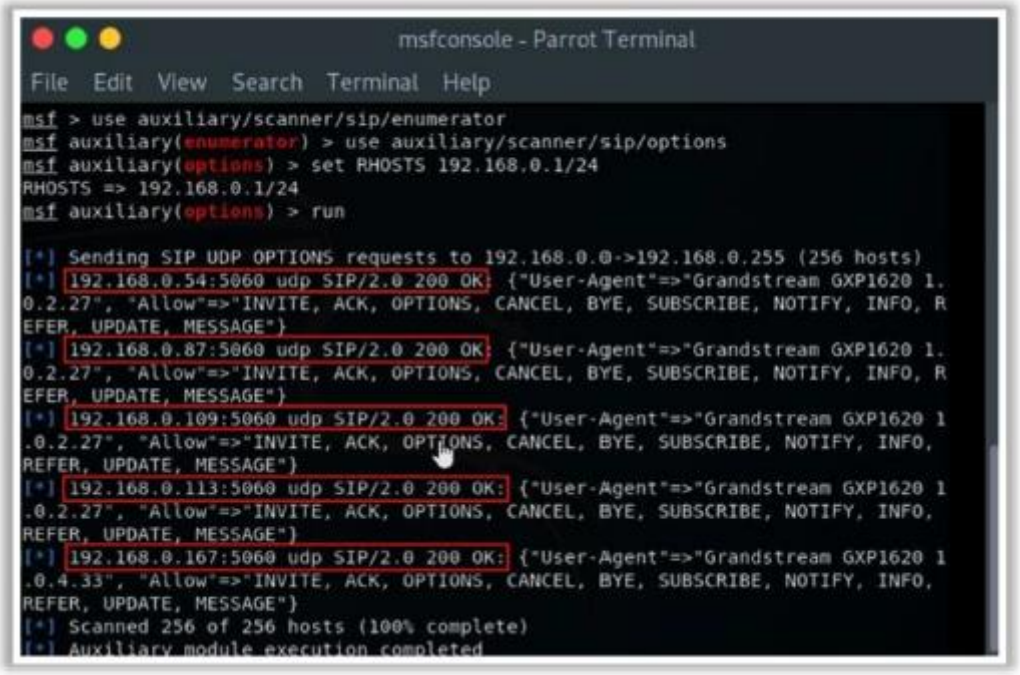
o Zadzwoń jednocześnie na wszystkie telefony w sieci, korzystając z metody ZAPROSZENIA

Poniższy zrzut ekranu pokazuje przykład wyliczania szczegółów urządzenia SIP za pomocą narzędzia Svmap za pomocą następującego polecenia:

svmap <docelowy zakres sieci/adres IP>



Atakujący używają narzędzia SIP Username Enumerator Metasploit do skanowania numerycznych nazw użytkowników/rozszerzeń telefonów VoIP. Poniższy zrzut ekranu pokazuje przykład wyliczania SIP przy użyciu Metasploit.



Wyliczanie RPC

Zdalne wywołanie procedury (RPC) to technologia używana do tworzenia rozproszonych programów typu klient/serwer. RPC umożliwia klientom i serwerom komunikację w rozproszonych programach klient/serwer. Jest to mechanizm komunikacji międzyprocesowej, który umożliwia wymianę danych

pomiędzy różnymi procesami. Ogólnie rzecz biorąc, RPC składa się z komponentów, takich jak klient, serwer, punkt końcowy, program odwzorowujący punkty końcowe, kod pośredniczący klienta i kod pośredniczący serwera, a także różne zależności. Usługa portmapper nasłuchuje na porcie TCP i UDP 111 w celu wykrycia punktów końcowych i przedstawienia klientów wraz ze szczegółami nasłuchiwania usług RPC. Wyliczanie punktów końcowych RPC umożliwia atakującym zidentyfikowanie wszelkich wrażliwych usług na tych portach usług. W sieciach chronionych zaporami ogniowymi i innymi zabezpieczeniami ten portmapper jest często filtrowany. Dlatego osoby atakujące skanują szerokie zakresy portów, aby zidentyfikować usługi RPC, które są otwarte na bezpośredni atak.

Atakujący używają następujących poleceń skanowania Nmap, aby zidentyfikować usługę RPC działającą w sieci:

nmap -sR <docelowy adres IP/sieć>

nmap -T4 -A <docelowy adres IP/sieć>

Ponadto osoby atakujące używają narzędzi, takich jak NetScanTools Pro, do przechwytywania informacji RPC sieci docelowej. Narzędzie NetScanTools Pro RPC Info pomaga atakującym wykryć i uzyskać dostęp do demona/usługi mapowania portów, która zazwyczaj działa na porcie 111 maszyn z systemem Unix lub Linux.

Wyliczanie użytkowników systemu Unix/Linux

Jednym z ważnych kroków do wyliczenia jest wykonanie wyliczenia użytkowników systemu Unix/Linux. Wyliczanie użytkowników systemów Unix/Linux zapewnia listę użytkowników wraz ze szczegółami, takimi jak nazwa użytkownika, nazwa hosta oraz data i godzina rozpoczęcia każdej sesji. Następujące narzędzia wiersza polecenia mogą być używane do wykonywania wyliczania użytkowników systemów Unix/Linux.

rusers

rusers wyświetla listę użytkowników zalogowanych na komputerach zdalnych lub komputerach w sieci lokalnej. Wyświetla dane wyjściowe podobne do polecenia who, ale dla hostów/systemów w sieci lokalnej. Jego składnia jest następująca:

/usr/bin/rusers [-a] [-1] [-u| -h| -ja gospodarzę ...]

Opcje są następujące.

o -a: Wysyła raport dla maszyny, nawet jeśli żaden użytkownik nie jest zalogowany

o -h: Sortuje alfabetycznie według nazwy hosta

o -I: Podaje dłuższą listę, podobną do komendy who

o -u: Sortuje według liczby użytkowników

o -i: Sortuje według czasu bezczynności

rkto

rwho wyświetla listę użytkowników zalogowanych do hostów w sieci lokalnej. Jego dane wyjściowe są podobne do wyników polecenia who i zawierają informacje o nazwie użytkownika, nazwie hosta oraz dacie i godzinie rozpoczęcia każdej sesji dla wszystkich komputerów w sieci lokalnej, na których działa demon rwho. Jego składnia jest następująca:

rkto [-a]

Ma następującą opcję.

o -a: obejmuje wszystkich użytkowników; bez tej flagi użytkownicy, których sesje są bezczynne przez co najmniej godzinę, nie są uwzględniani w raporcie

palec

finger wyświetla informacje o użytkownikach systemu, takie jak nazwa logowania użytkownika, prawdziwe imię i nazwisko, nazwa terminala, czas bezczynności, czas logowania, lokalizacja biura i numery telefonów biurowych. Jego składnia jest następująca:

palec [-1] [-m] [—p] [-s] [użytkownik ...] [host_użytkownika ...]

Opcje są następujące.

o -s: Wyświetla nazwę logowania użytkownika, prawdziwe imię i nazwisko, nazwę terminala, czas bezczynności, czas logowania, lokalizację biura i numer telefonu biura

o -I: Tworzy wielowierszowy format wyświetlający wszystkie informacje opisane dla opcji –s, jak również katalog domowy użytkownika, numer telefonu domowego, powłokę logowania, status poczty i zawartość plików „.plan", „.project", „.pgpkey" i „.forward" z katalogu domowego użytkownika

o -p: Uniemożliwia opcji -I polecenia finger wyświetlanie zawartości plików „.plan", „.project" i „.pgpkey".

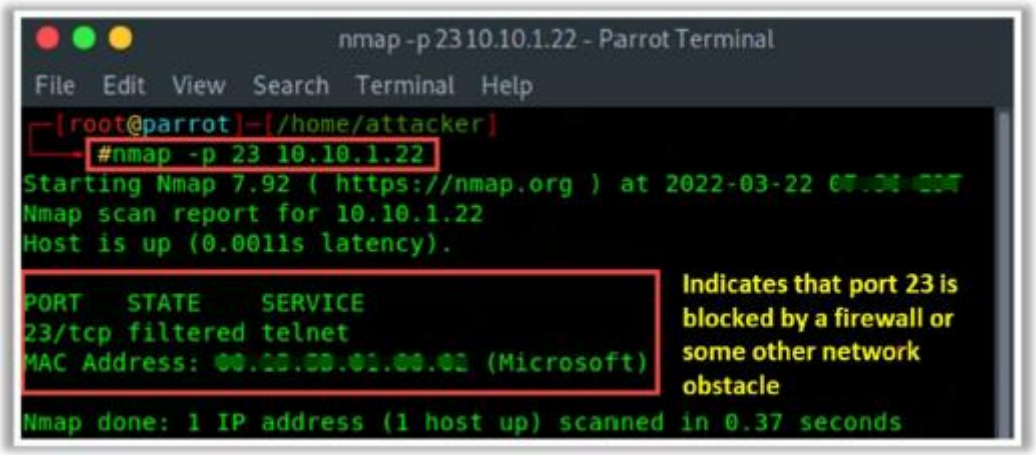
o -m: Zapobiega dopasowywaniu nazw użytkowników.

Wyliczanie Telnetu

Telnet to protokół terminala sieciowego, który umożliwia użytkownikom dostęp do zdalnych komputerów lub serwerów przez Internet. Protokół ten zapewnia dwukierunkową interaktywną komunikację dla komputerów w sieciach LAN iw Internecie. W zależności od uprawnień przypisanych użytkownikom, mogą oni używać usługi Telnet do logowania się do zdalnego systemu w celu uzyskania dostępu do określonych plików, usług, danych itp. Atakujący przeprowadzają skanowanie portów w celu zebrania informacji dotyczących otwartych portów i usług na docelowym serwerze. Jeśli okaże się, że port Telnet jest otwarty, osoby atakujące mogą uzyskać informacje o udostępnianych informacjach, w tym o sprzęcie i oprogramowaniu celu. Korzystając z tych informacji, osoby atakujące mogą wykorzystać swoje specyficzne luki i przeprowadzić atak siłowy w celu uzyskania nieautoryzowanego dostępu do systemu docelowego. Atakujący mogą użyć narzędzia Nmap do wykonania prostego bezpośredniego skanowania w poszukiwaniu portu Telnet 23.

Jak pokazano na zrzucie ekranu, atakujący używają następującego polecenia Nmap do wyliczenia usługi Telnet działającej w systemie docelowym:

nmap -p 23 <domena docelowa/adres lP>

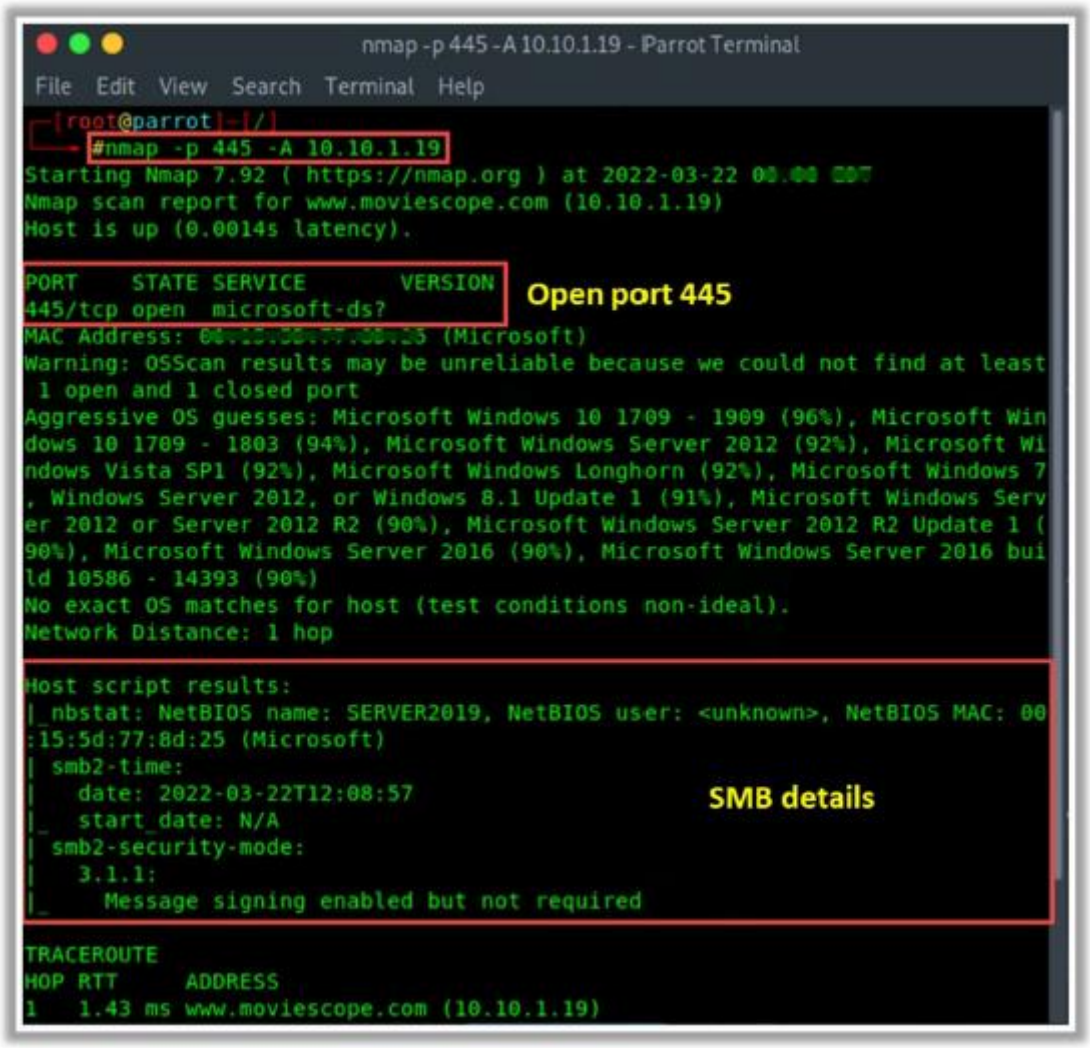


Wyliczanie SMB

Server Message Block (SMB) to protokół transportowy, który jest zwykle używany przez systemy Windows do zapewniania współdzielonego dostępu do plików, drukarek i portów szeregowych, a także zdalnego dostępu do usług Windows. Domyślnie SMB działa bezpośrednio na porcie TCP 445 lub poprzez NetBIOS API na portach UDP 137 i 138 oraz TCP 137 i 139. Korzystając z usługi SMB, użytkownicy mogą uzyskiwać dostęp do plików i innych danych przechowywanych na zdalnym serwerze. Usługa SMB umożliwia również użytkownikom aplikacji odczytywanie, zapisywanie i modyfikowanie plików na serwerze zdalnym. Sieć, w której działa ta usługa, jest bardzo podatna na wyliczanie SMB, które dostarcza sporej ilości informacji o celu. Podczas wyliczania SMB osoby atakujące zazwyczaj wykonują przechwytywanie banerów w celu uzyskania informacji, takich jak szczegóły systemu operacyjnego i wersje uruchomionych usług. Korzystając z tych informacji, osoby atakujące mogą przeprowadzać różne ataki, takie jak ataki przekaźnikowe SMB i ataki brute-force. Atakujący mogą również użyć narzędzi wyliczających SMB, takich jak Nmap, SMBMap, enum4linux, nullinux i NetScanTool Pro, aby przeprowadzić ukierunkowane skanowanie usługi SMB działającej na porcie 445.

Jak pokazano na zrzucie ekranu, osoby atakujące używają następującego polecenia Nmap do wyliczenia usługi SMB działającej na docelowym adresie IP:

nmap -p 445 -A <docelowy adres IP>



W powyższym poleceniu opcja -p określa port do skanowania (w tym przypadku 445), a opcja –A służy do wykrywania systemu operacyjnego, wykrywania wersji, skanowania skryptów i informacji o traceroute.

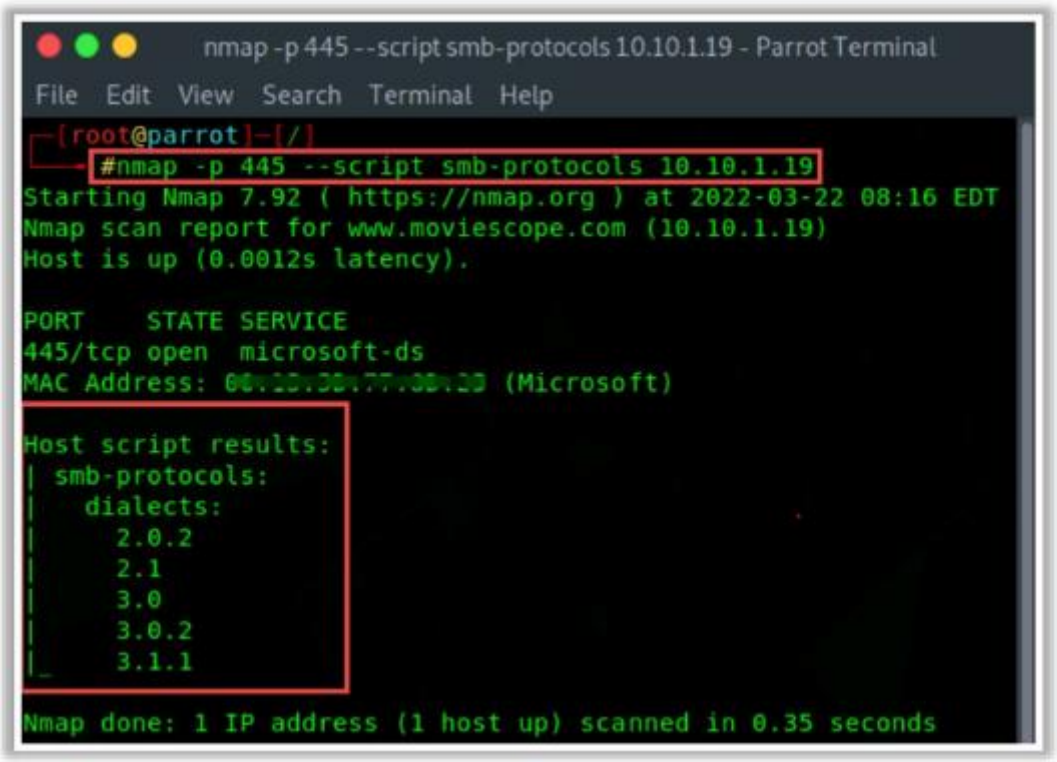
Stan PORT 445/tcp to OTWARTY, co oznacza, że port 445 jest otwarty i że usługa SMB jest uruchomiona. Korzystając z tego polecenia, osoby atakujące mogą również uzyskać szczegółowe informacje na temat systemu operacyjnego i trasy śledzenia określonego celu.

Jak pokazano na zrzucie ekranu, osoby atakujące używają następujących poleceń Nmap do wyliczenia

obsługiwane protokoły i wersje docelowego serwera SMB:

nmap -p 445 —script smb-protocols <Docelowy adres IP>

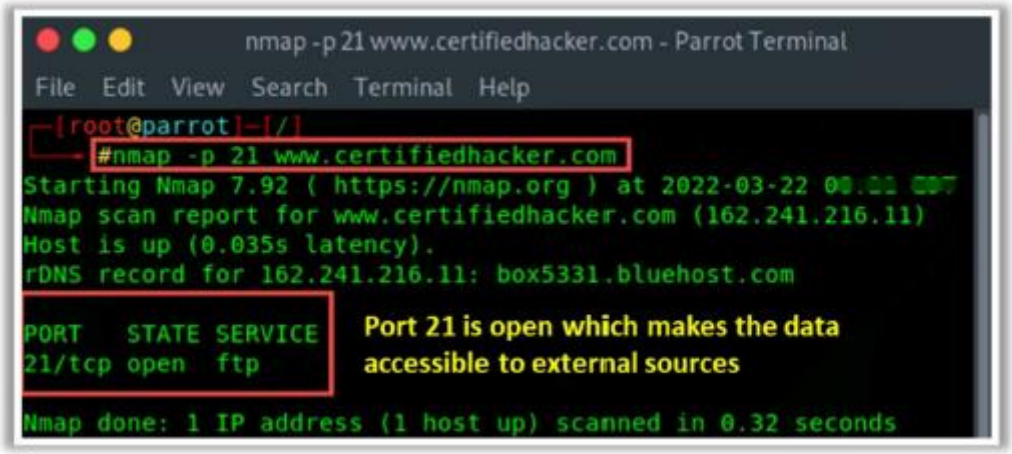
nmap -p 139 —script smb-protocols <Docelowy adres IP>



Wyliczanie FTP

Protokół przesyłania plików (FTP) służy do przesyłania plików przez protokół TCP, a jego domyślnym portem jest 21. W FTP dane są przesyłane między nadawcą a odbiorcą w postaci zwykłego tekstu, co naraża atakujących na krytyczne informacje, takie jak nazwy użytkowników i hasła. FTP nie oferuje ani bezpiecznego środowiska sieciowego, ani bezpiecznego uwierzytelniania użytkowników. Osoby fizyczne nie potrzebują uwierzytelniania, aby uzyskać dostęp do serwera FTP w sieci. Zapewnia to atakującym łatwą metodę uzyskiwania dostępu do zasobów sieciowych. Wdrożenie FTP w sieci organizacji umożliwia dostęp do danych ze źródeł zewnętrznych. Atakujący mogą skanować i wyliczać otwarty port 21, na którym działają usługi FTP, a następnie wykorzystywać te informacje do przeprowadzania różnych ataków, takich jak odrzucanie FTP, brutalna siła FTP i wąchanie pakietów. Jak pokazano na zrzucie ekranu, atakujący używają następującego polecenia Nmap do wyliczenia usługi FTP działającej w domenie docelowej:

nmap -p 21 <domena docelowa>



Atakujący używają również Metasploit do wyliczania usług FTP działających na zdalnych hostach. Do wykrycia wersji FTP serwera docelowego można użyć następujących poleceń:

use pomocniczego/skanera/ftp/ftp_version

msf pomocniczy(skaner/ftp/wersja_ftp) > ustaw RHOSTS <docelowy adres IP>

msf pomocniczy(skaner/ftp/wersja_ftp) > exploit

Wyliczanie TFTP

Trivial File Transfer Protocol (TFTP) jest uproszczoną wersją FTP i służy do przesyłania plików między urządzeniami sieciowymi. Domyślnie serwery TFTP nasłuchują na porcie UDP 69. Ten protokół jest używany, gdy nie jest wymagana widoczność katalogu ani uwierzytelnianie użytkownika; w związku z tym nie zapewnia żadnych funkcji bezpieczeństwa. Aby przeprowadzić wyliczanie TFTP, osoby atakujące mogą użyć narzędzi, takich jak PortQry i Nmap, w celu wyodrębnienia informacji, takich jak uruchomione usługi TFTP i pliki przechowywane na serwerze zdalnym. Korzystając z wyliczonych informacji, osoby atakujące mogą dodatkowo uzyskać nieautoryzowany dostęp do systemu docelowego, ukraść ważne pliki i przesłać złośliwe skrypty w celu przeprowadzenia dalszych ataków. Ponadto informacje te umożliwiają atakującym przeprowadzanie różnych ataków, takich jak ataki z amplifikacją DNS, ataki odbicia TFTP i ataki DDoS.

PortQry

Narzędzie PortQry zgłasza stan portów TCP i UDP w wybranym miejscu docelowym. Atakujący mogą użyć narzędzia PortQry do wykonania wyliczenia TFTP. To narzędzie raportuje stan docelowych portów TCP i UDP na komputerze lokalnym lub zdalnym. W narzędziu PortQry osoby atakujące mogą określić cel skanowania w poszukiwaniu uruchomionej usługi TFTP na otwartym porcie 69. Jak pokazano na zrzucie ekranu, osoby atakujące wykonują wyliczanie TFTP w domenie docelowej, ustawiając Porty do zapytania: wartość na 69 i Protokół na UDP.

Atakujący mogą również użyć narzędzia wiersza polecenia PortQry do wykonania wyliczenia TFTP za pomocą następującego polecenia:

portqry -n <domena docelowa/adres IP> -e 69 -p udp

Nmap

Atakujący mogą użyć narzędzia Nmap do przeprowadzenia prostego bezpośredniego skanowania w poszukiwaniu portu TFTP 69. Jak pokazano na zrzucie ekranu, atakujący używają następującego polecenia Nmap do wyliczenia usługi TFTP działającej w domenie docelowej:

nmap -p 69 <domena docelowa/IP>

Wyliczanie IPv6

Protokół internetowy w wersji 6 (IPv6) to protokół adresowania, który identyfikuje systemy komputerowe, w tym informacje o lokalizacji, i pomaga w kierowaniu ruchu między systemami w sieci. Jest to zaawansowana wersja IPv4 i dlatego obsługuje większą liczbę hostów w porównaniu z IPv4. Został zaprojektowany w celu przezwyciężenia problemu wyczerpania adresów IPv4. Atakujący przeprowadzają wyliczanie adresów IPv6 na hostach docelowych w celu uzyskania ich adresów IPv6, a następnie skanują wyliczone adresy IP w celu wykrycia różnych problemów związanych z bezpieczeństwem, takich jak dostęp do struktury routingu, ujawnienie poufnych treści i list kontroli

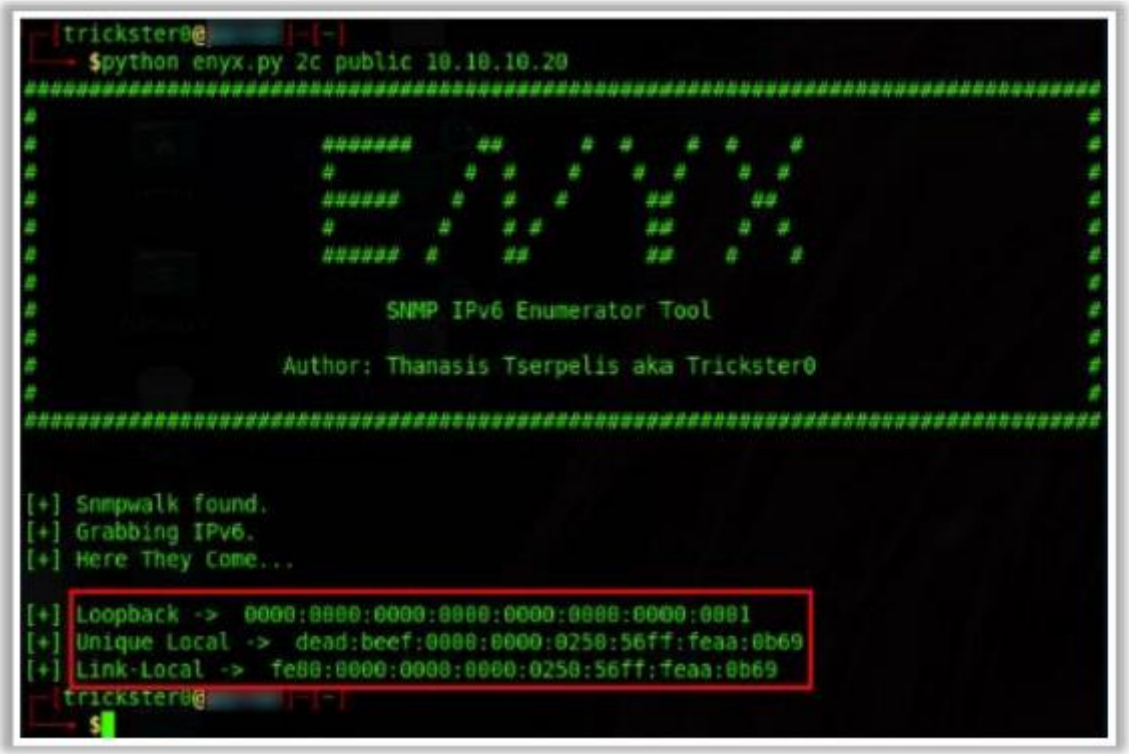
dostępu użytkowników. Korzystając z tych informacji, atakujący mogą przeprowadzać różne ataki, takie jak ataki SYN flood, ataki DNS amplifikacji i ataki DDoS. Atakujący mogą skanować i wyliczać adres IPv6 docelowej maszyny w sieci za pomocą różnych narzędzi, takich jak Enyx i IPv6 Hackit.

Enyx

Enyx to narzędzie wyliczające, które pobiera adres IPv6 maszyny przez SNMP.

Jak pokazano na zrzucie ekranu, osoby atakujące używają następującego polecenia, aby wyliczyć adres IPv6 maszyny docelowej (10.10.10.20), ustawiając wersję SNMP na 2c i ciąg społeczności na wartość publiczną:

Python enyx.py 2c public <docelowy adres IP>



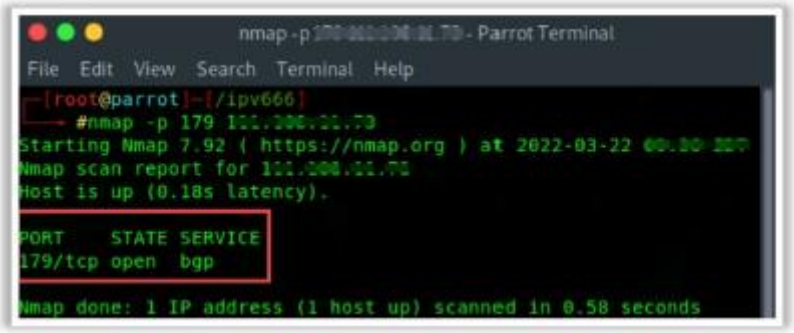
Włamanie do IPv6

Hackit to narzędzie skanujące, które udostępnia listę aktywnych hostów IPv6. Może przeprowadzać skanowanie portów TCP i identyfikować rekordy hostów AAAA IPv6. Jak pokazano na zrzucie ekranu, atakujący mogą określić maszynę docelową i uruchomić skanowanie w celu wyliczenia informacji IPv6.

Wyliczanie BGP

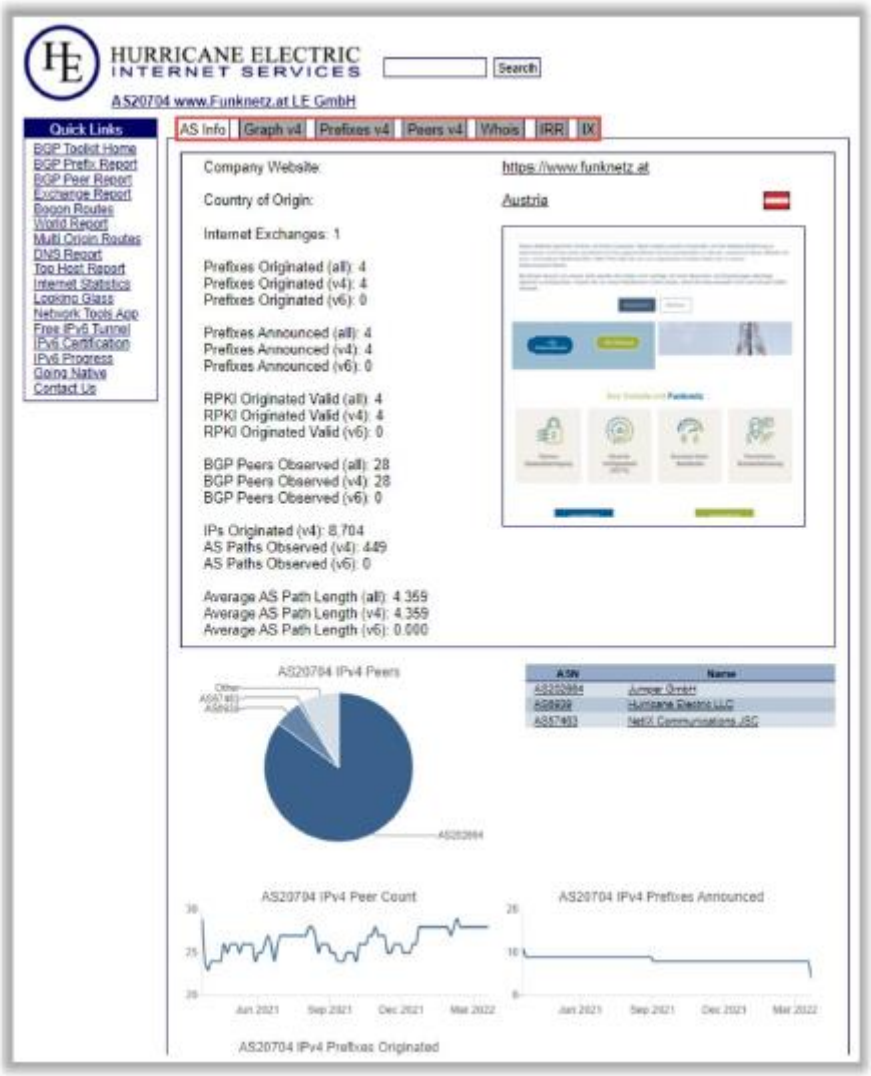
Border Gateway Protocol (BGP) to protokół routingu używany do wymiany informacji o routingu i osiągalności między różnymi systemami autonomicznymi (AS) w Internecie. Ponieważ ten protokół jest używany do łączenia jednego AS z innymi AS, jest również nazywany zewnętrznym BGP (eBGP). BGP znajduje najkrótszą ścieżkę do wydajnego kierowania ruchu z jednego adresu IP do drugiego. BGP tworzy swoją sesję TCP na porcie 179. Atakujący przeprowadzają wyliczanie BGP na celu za pomocą narzędzi, takich jak Nmap i BGP Toolkit, w celu wykrycia prefiksów IPv4 wskazywanych przez numer AS i ścieżki routingu, po której podąża cel. Atakujący wykorzystują te informacje do przeprowadzania różnych ataków na cel, takich jak ataki manin-the-middle, ataki polegające na porwaniu BGP i ataki DoS. Jak pokazano na zrzucie ekranu, osoby atakujące używają następującego polecenia Nmap do wyliczenia protokołu BGP działającego w systemie docelowym:

nmap -p 179 <docelowy adres IP>



Jak pokazano na zrzucie ekranu, osoby atakujące używają narzędzia BGP Toolkit do wyliczenia BGP w domenie docelowej. To narzędzie online może służyć do wyszukiwania domeny docelowej i

uzyskiwania szczegółowych informacji, takich jak informacje DNS, informacje o witrynie internetowej, informacje o adresie IP, informacje AS i informacje Whois. Na podstawie zidentyfikowanych AS atakujący mogą dalej wyliczać szczegóły, takie jak prefiksy IPv4, wykresy routingu BGP i peery IPv4.



Środki zaradcze wyliczania

Do tej pory opisaliśmy techniki wyliczania i narzędzia wykorzystywane do wydobywania wartościowych informacji z celów. Następnie omówimy środki zaradcze, które mogą uniemożliwić atakującym wyliczanie poufnych informacji z sieci lub hosta. Ta sekcja koncentruje się na metodach unikania wycieku informacji przez wyliczanie SNMP, DNS, SMTP, LDAP, SMB, NFS i FTP.

Środki zaradcze wyliczania SNMP

• Usuń agenta SNMP lub wyłącz usługę SNMP.

• Jeśli wyłączenie SNMP nie wchodzi w grę, zmień domyślne nazwy ciągów społeczności.

• Uaktualnij do SNMP3, który szyfruje hasła i wiadomości.

• Zaimplementuj opcję bezpieczeństwa zasad grupy o nazwie „Dodatkowe ograniczenia dla połączeń anonimowych”.

• Upewnij się, że masz dostęp do potoków sesji zerowej, udziałów sesji zerowej i filtrowania IPsec ograniczony.

• Zablokuj dostęp do portu TCP/UDP 161.

• Nie instaluj składnika Windows do zarządzania i monitorowania, jeśli nie jest to wymagane.

• Szyfruj lub uwierzytelniaj za pomocą protokołu IPsec.

• Nie należy błędnie konfigurować usługi SNMP z autoryzacją odczytu i zapisu.

• Skonfiguruj listy kontroli dostępu (ACL) dla wszystkich połączeń SNMP, aby zezwalać tylko na legalne połączenia użytkownikom dostęp do urządzeń SNMP.

•Regularnie kontroluj ruch sieciowy.

• Szyfruj poświadczenia przy użyciu trybu „AuthNoPriv", który wykorzystuje MD5 i SHA dla dodatkowej ochrony.

• Zmodyfikuj rejestr, aby zezwolić na ograniczony lub dozwolony dostęp do społeczności SNMP

• Zmień domyślne hasło i okresowo zmieniaj bieżące hasło.

• Zidentyfikuj wszystkie urządzenia SNMP z uprawnieniami do odczytu/zapisu i nadaj uprawnienia tylko do odczytu określonym urządzeniom, które nie wymagają uprawnień do odczytu/zapisu.

• Unikaj używania trybu „NoAuthNoPriv", ponieważ nie szyfruje on komunikacji.

Środki zaradcze wyliczania LDAP

• Domyślnie ruch LDAP jest przesyłany niezabezpieczony; dlatego używaj technologii Secure Sockets Layer (SSL) lub STARTTLS do szyfrowania ruchu.

• Wybierz nazwę użytkownika inną niż adres e-mail i włącz blokadę konta.

• Ogranicz dostęp do usługi Active Directory (AD) za pomocą oprogramowania takiego jak Citrix.

• Użyj NT LAN Manager (NTLM), Kerberos lub dowolnego podstawowego mechanizmu uwierzytelniania, aby ograniczyć dostęp do legalnych użytkowników.

• Loguj dostęp do usług Active Directory (AD).

• Zablokuj użytkownikom dostęp do niektórych jednostek AD, zmieniając uprawnienia do tych obiektów/atrybutów.

• Wdrażaj konta kanaryjskie, które przypominają prawdziwe konta, aby wprowadzać w błąd atakujących.

• Twórz grupy wabików ze słowem „Administrator" w nazwie, aby wprowadzić atakujących w błąd. Osoby atakujące zwykle wyszukują konta administratora LDAP.

Środki zaradcze wyliczania NFS

• Implementuj odpowiednie uprawnienia (odczyt/zapis musi być ograniczony do określonych użytkowników) w eksportowanych systemach plików.

• Zaimplementuj reguły zapory, aby zablokować port NFS 2049.

• Zapewnij odpowiednią konfigurację plików, takich jak /etc/smb.conf, /etc/exports i etc/hosts.allow w celu ochrony danych przechowywanych na serwerze.

• Rejestruj żądania dostępu do plików systemowych na serwerze NFS.

• Pozostaw opcję root_squash w pliku /etc/exports włączoną, aby żadne żądania użytkownika root nie były traktowane jako zaufane.

• Zaimplementuj tunelowanie NFS przez SSFH w celu szyfrowania ruchu NFS w sieci.

• Wdrożyć zasadę najmniejszych uprawnień w celu ograniczenia zagrożeń, takich jak modyfikacja danych, dodawanie danych i modyfikacja plików konfiguracyjnych przez zwykłych użytkowników.

• Upewnij się, że użytkownicy nie korzystają z suid i sgid w wyeksportowanym systemie plików.

• Upewnij się, że grupa sieci NIS ma w pełni zdefiniowaną nazwę hosta, aby uniemożliwić przyznanie wyższego dostępu innym hostom.

Środki zaradcze wyliczania SMTP

Serwery SMTP należy skonfigurować w następujący sposób:

• Ignoruj wiadomości e-mail do nieznanych odbiorców.

• Wyklucz poufne informacje na serwerach pocztowych i hostach lokalnych w odpowiedziach pocztowych.

• Wyłącz funkcję otwartego przekaźnika.

• Ogranicz liczbę akceptowanych połączeń ze źródła, aby zapobiec atakom typu brute-force.

• Wyłącz polecenia EXPN, VRFY i RCPT TO lub ogranicz je do autentycznych użytkowników.

• Ignoruj wiadomości e-mail do nieznanych odbiorców, konfigurując serwery SMTP.

• Identyfikuj spamerów za pomocą rozwiązań uczenia maszynowego (ML).

• Nie udostępniaj wewnętrznych informacji o adresie IP/hoście ani informacji o systemie przekazywania poczty.

Środki zaradcze dotyczące wyliczania SMB

Wspólne usługi udostępniania lub inne nieużywane usługi mogą stanowić punkty wejścia dla atakujących w celu obejścia zabezpieczeń sieci. Sieć z uruchomionym SMB jest narażona na wysokie ryzyko wyliczenia. Ponieważ serwery WWW i DNS nie wymagają tego protokołu, zaleca się wyłączenie go na nich. Protokół SMB można wyłączyć, wyłączając właściwości Klient sieci Microsoft Networks oraz Udostępnianie plików i drukarek w sieciach Microsoft Networks w Połączeniach sieciowych i telefonicznych. Na serwerach dostępnych z Internetu, zwanych także hostami bastionowymi, protokół SMB można wyłączyć, wyłączając te same dwie właściwości w oknie dialogowym Właściwości protokołu TCP/IP. Inną metodą wyłączania protokołu SMB na hostach bastionowych bez jawnego wyłączania go jest blokowanie portów używanych przez usługę SMB. Są to porty TCP 139 i 445. Ponieważ wyłączenie usług SMB nie zawsze jest wykonalną opcją, mogą być wymagane inne środki zaradcze przeciwko wyliczaniu SMB. Rejestr systemu Windows można skonfigurować tak, aby ograniczał anonimowy dostęp z Internetu do określonego zestawu plików. Te pliki i foldery są określone w ustawieniach Dostęp do sieci: nazwane potoki, do których można uzyskać dostęp anonimowy, oraz Dostęp do sieci: udziały, do których można uzyskać dostęp anonimowy. Ta

konfiguracja obejmuje dodanie parametru RestrictNullSessAccess do klucza rejestru w następujący sposób:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Parametr RestrictNullSessAccess przyjmuje wartości binarne, gdzie 1 oznacza włączenie, a 0 oznacza wyłączenie. Ustawienie tego parametru na 1 lub włączony ogranicza dostęp anonimowych użytkowników do plików określonych w ustawieniach dostępu do sieci.

Poniżej przedstawiono dodatkowe środki zaradcze do obrony przed wyliczeniem SMB.

• Upewnij się, że w komputerze jest włączona Zapora systemu Windows lub podobne systemy ochrony punktów końcowych systemu.

• Zainstaluj najnowsze poprawki zabezpieczeń dla systemu Windows i oprogramowania innych firm.

• Wdrożyć odpowiedni mechanizm uwierzytelniania z silną polityką haseł.

• Zaimplementuj silne uprawnienia, aby zapewnić bezpieczeństwo przechowywanych informacji.

• Przeprowadzaj regularne audyty dzienników systemowych.

• Wykonuj aktywne monitorowanie systemu, aby monitorować systemy pod kątem wszelkich złośliwych incydentów.

• Zaimplementuj bezpieczne sieci VPN, aby zabezpieczyć dane organizacji podczas zdalnego dostępu.

• Korzystaj z systemów analizy zachowań plików, takich jak zapory nowej generacji (NGFW), aby obserwować wzorce ruchu i uzyskiwać terminowe raporty analityczne dotyczące zasobów SMB.

• Korzystaj z wysoce niezawodnych i bezpiecznych systemów monitorowania, takich jak czujniki globalnych zagrożeń dla bardzo wrażliwych i ściśle tajnych danych.

• Implementacja podpisanej cyfrowo transmisji danych i komunikacji w celu uzyskania dostępu do zasobów SMB.

• Zablokuj/wyłącz porty TCP 88, 139 i 445 oraz porty UDP 88,137 i 138, aby zapobiec atakom SMB.

• Włącz ustawienia profilu publicznego w systemie zapory.

Środki zaradcze dotyczące wyliczania FTP

• Zaimplementuj bezpieczny FTP (SFTP, który używa SSH) lub bezpieczny FTP (FTPS, który używa SSL).

szyfrować ruch FTP w sieci.

• Implementuj silne hasła lub zasady uwierzytelniania oparte na certyfikacjach.

• Upewnij się, że nieograniczone przesyłanie plików na serwer FTP jest zabronione

• Wyłącz anonimowe konta FTP. Jeśli nie jest to możliwe, monitoruj anonimowe konta FTP

regularnie.

• Ogranicz dostęp do serwera FTP za pomocą adresu IP lub nazwy domeny.

• Konfigurowanie kontroli dostępu na uwierzytelnionych kontach FTP przy użyciu list kontroli dostępu (ACL).

• Ogranicz próby i czas logowania.

• Skonfiguruj reguły filtrowania ruchu przychodzącego i wychodzącego dla usług FTP.

• Użyj SSL/FTPS dla uwierzytelnionych kont FTP.

• Nie uruchamiaj zwykłych usług publicznych, takich jak poczta lub sieć, na pojedynczym serwerze FTP.

• Zaimplementuj model analizy oparty na grach Markowa do oceny podatności i testów penetracyjnych (VAPT) na serwerach FTP w chmurze.

Środki zaradcze wyliczania DNS

Poniżej omówiono różne środki zapobiegające wyliczaniu DNS.

Ogranicz dostęp do programu tłumaczącego: upewnij się, że dostęp do programu tłumaczącego mają tylko hosty w sieci, aby zapobiec zatruwaniu zewnętrznej pamięci podręcznej.

Losuj porty źródłowe: upewnij się, że pakiety żądań wychodzące z sieci używają portów losowych, a nie portu UDP 53. Ponadto losuj identyfikatory zapytań i zmieniaj wielkość liter w nazwach domen, aby chronić się przed zatruciem pamięci podręcznej.

Audyt stref DNS: Audyt stref DNS w celu zidentyfikowania luk w domenach i subdomenach oraz rozwiązania problemów związanych z DNS.

Łatanie znanych luk w zabezpieczeniach: aktualizowanie i łatanie serwerów nazw za pomocą najnowszych wersji oprogramowania, takiego jak BIND i Microsoft DNS.

Monitoruj serwery nazw: Monitoruj zachowanie serwerów nazw, aby jak najszybciej zidentyfikować złośliwe działania lub nieoczekiwane zachowania.

• Ogranicz transfery stref DNS: Ogranicz transfery stref DNS do określonego adresu IP podrzędnego serwera nazw

adresy, ponieważ transfer strefy może obejmować kopię główną bazy danych serwera głównego. Wyłącz transfery stref DNS do niezaufanych hostów.

• Używaj różnych serwerów dla funkcji autorytatywnych i rozstrzygających: Oddzielanie funkcji resolwera i autorytatywnego serwera nazw może zmniejszyć przeciążenie i zapobiec atakom typu „odmowa usługi” (DoS) na domeny.

Używaj izolowanych serwerów DNS: Unikaj hostowania serwera aplikacji wraz z serwerem DNS. Użyj izolowanego i dedykowanego serwera dla usług DNS, aby zminimalizować ryzyko ataków na aplikacje internetowe.

Wyłącz rekursję DNS: Wyłącz rekursję DNS w konfiguracji serwera DNS, aby rekursywnie ograniczyć zapytania z domen innych lub stron trzecich i złagodzić ataki amplifikacji i zatruwania DNS.

• Wzmocnij system operacyjny: wzmocnij system operacyjny, zamykając nieużywane porty i blokując niepotrzebne usługi.

• Użyj VPN: użyj VPN do bezpiecznej komunikacji. Ponadto zmień domyślne hasła.

• Zaimplementuj uwierzytelnianie dwuskładnikowe: Wymuś uwierzytelnianie dwuskładnikowe w celu zapewnienia bezpiecznego dostępu, gdy serwer DNS jest zarządzany przez stronę trzecią.

Użyj blokady zmiany DNS: Użyj blokady zmiany DNS lub blokady klienta, aby ograniczyć zmianę ustawień DNS bez odpowiedniej autoryzacji.

Użyj DNSSEC: Zaimplementuj DNSSEC jako dodatkową warstwę zabezpieczeń dla serwera DNS, aby zezwalać tylko na żądania DNS podpisane cyfrowo i ograniczać przejmowanie DNS.

Użyj rejestracji DNS premium: Użyj usług rejestracji DNS premium, które ukrywają przed opinią publiczną poufne informacje, takie jak informacje o hoście (HINFO).

Inne środki zaradcze do obrony przed wyliczaniem DNS są następujące:

• Upewnij się, że prywatne hosty i ich adresy IP nie są publikowane w plikach stref DNS publicznego serwera DNS.

• Używaj standardowych kontaktów administratora sieci do rejestracji DNS, aby uniknąć ataków socjotechnicznych.

• Przytnij pliki stref DNS, aby uniknąć ujawnienia niepotrzebnych informacji.

• Utrzymuj niezależne wewnętrzne i zewnętrzne serwery DNS.

• Upewnij się, że stare lub nieużywane rekordy DNS są okresowo usuwane.

• Ogranicz kwerendy żądań wersji.bind za pomocą list ACL. Usuń lub uruchom BIND z najmniejszymi uprawnieniami.

• Używaj pliku /etc/hosts do tworzenia lub przemieszczania subdomen zamiast używania rekordów DNS

Podsumowanie modułu

W tym module omówiliśmy koncepcje wyliczania wraz z technikami, usługami i portami używanymi do wyliczania. Omówiliśmy również, w jaki sposób osoby atakujące działają inaczej z technikami wyliczania (NetBIOS, SNMP, LDAP, NTP, NFS, SMTP, DNS, IPsec, VoIP, RPC, Linux/Unix, Telnet, FTP, TFTP, SMB, IPv6 i wyliczanie BGP) w celu zebrania informacji o celu. Ten moduł zakończył się szczegółową dyskusją na temat środków zaradczych, które organizacje mogą zastosować w celu obrony przed działaniami wyliczającymi. W następnym module szczegółowo omówimy, w jaki sposób osoby atakujące, a także etyczni hakerzy i testerzy piór przeprowadzają analizę podatności w celu zidentyfikowania luk w zabezpieczeniach sieci, infrastruktury komunikacyjnej i systemów końcowych atakowanej organizacji.