Testy Penetracyjne

Atakowanie zasobów sieciowych

Arkadiusz Chrobot

Katedra Systemów Informatycznych

5 maja 2024

Plan

1. Wstęp
2. Atakowanie infrastruktury
3. Atakowanie usług
4. Atakowanie sieci bezprzewodowych

Wstęp

W ramach testów penetracyjnych, w trakcie etapu eksploracji i ekspansji (ang. *exploitation and pivoting*), po uzyskaniu początkowego dostęp do systemu, konieczne jest użycie kilku technik ataku, aby ten dostęp poszerzyć. W ramach tego wykładu zostaną opisane możliwości atakowania sieci przewodowych i bezprzewodowych, a także usług sieciowych, takich jaki SMTP lub (SSH).

Atakowanie infrastruktury

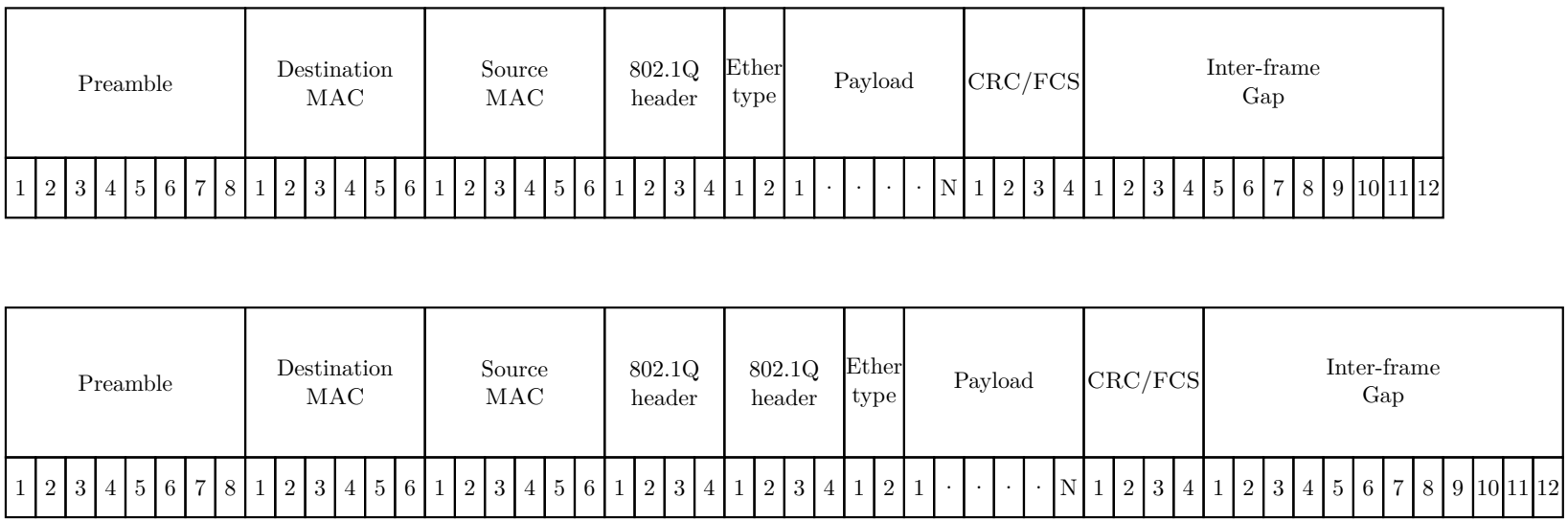
Przeskakiwanie VLAN

W wielu sieciach stosowane są rozwiązania typu VLAN (ang. *Virtual Local Area Network*), aby utworzyć wewnętrzne, bezpieczne granice między systemami o różnym poziomie krytyczności. Ich działanie opiera się na separacji domen rozgłoszeniowych, aby zwiększyć bezpieczeństwo lub wydajność sieci. Oznacza to, że w trakcie testów penetracyjnych testerzy będą musieli uzyskać dostęp do innej VLAN, niż ta, w której obecnie operują. Tego typu atak nazywa się *przeskakiwaniem* VLAN (ang. VLAN *hopping*) i może zostać przeprowadzony przy użyciu *podwójnego etykietowania* (ang. *double tagging*) lub *podszywania się pod przełącznik sieciowy* (ang. *switch spoofing*).

Podwójne etykietowanie jest używane we wspólnych interfejsach (*trunked interfaces*) w rozumieniu standardu 802.1Q. Rysunek 1 przedstawia schemat ramki Ethernet, do której można dodać drugą etykietę VLAN.

Atakowanie infrastruktury

Przeskakiwanie VLAN



Rysunek: Pakiet Ethernet z pojedynczą etykietą (góra) i podwójną (dół)

Atakowanie infrastruktury

Przeskakiwanie VLAN

Testerzy penetracyjni mogą użyć podwójnych etykiet do przeskakiwania do innych sieci VLAN. W takim przypadku jako pierwsza do pakietu jest dodawana etykieta natywnej VLAN, a jako druga docelowej wirtualnej sieci lokalnej. Ponieważ etykiety są przez przełączniki odczytywane dokładnie w tej kolejności, to pierwszy przełącznik zinterpretuje pakiet jako pochodzący z natywnej VLAN i przekaże go do kolejnego przełącznika, który odczyta drugą etykietę i wyśle pakiet do docelowej VLAN. Niestety, odpowiedź nie będzie podwójnie etykietowana, więc nie dotrze do urządzenia atakującego. Atak ten powiedzie się, jeśli przełączniki są skonfigurowane do obsługi natywnych VLAN, a administratorzy nie zastosowali żadnych mechanizmów zabezpieczających.

Atakowanie infrastruktury

Przeskakiwanie VLAN

Podszywanie się pod przełącznik sieciowy polega na skonfigurowaniu urządzenia atakującego, tak aby inne urządzenia w sieci rozpoznawały je jako przełącznik obsługujący ramki z nieznanych grup VLAN (ang. *trunking switch*). W ten sposób podszywające się pod przełącznik urządzenie może „widzieć” ruch przesyłany do innych sieci VLAN. Aby ten atak zadziałał pozostałe urządzenia w sieci lokalnej muszą być tak skonfigurowane, aby pozwalały na negocjację połączeń (ang. *trunk*). Ich interfejsy sieciowe muszą być ustawione w jednym z trzech trybów: *dynamic desirable*, *dynamic auto* lub *trunk*, co nie powinno mieć miejsca w dobrze skonfigurowanych i utrzymywanych sieciach.
Oba rodzaje ataków można przeprowadzić przy pomocy narzędzia *Yersinia*, które dodatkowo umożliwia atakowanie protokołów STP, DHCP i innych związanych z drugą warstwą modelu ISO/OSI.

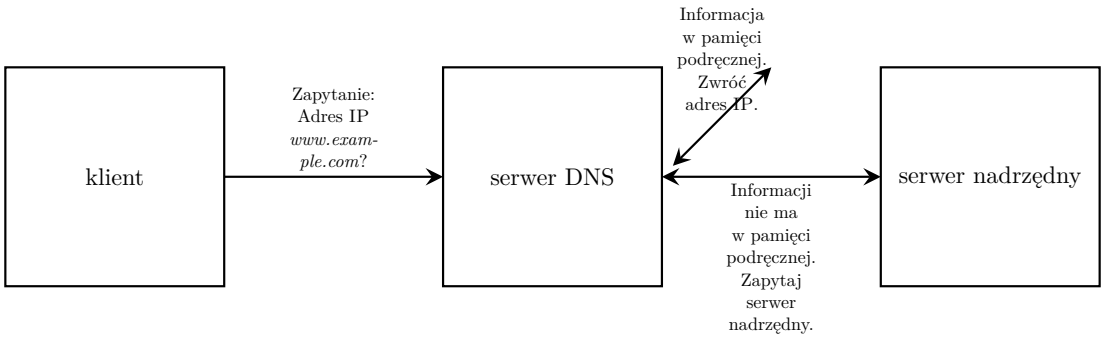
Atakowanie infrastruktury

Zatruwanie DNS

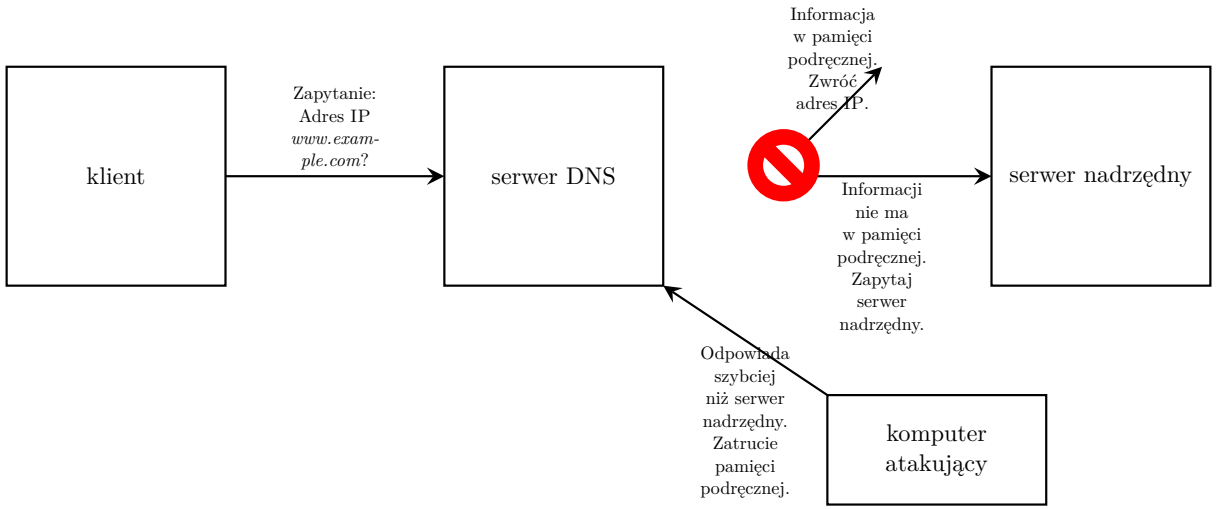
Zatruwanie pamięci podręcznej DNS (ang. DNS *Cache poisoning*) nazywane również *fałszowaniem* DNS (ang. DNS *spoofing*) jest atakiem na usługę DNS, który w 2008 roku odkrył i opisał Daniel (Dan) Kaminsky. Podatność pozwalająca na ten atak była obecna w większości popularnych implementacji serwerów DNS, ale została usunięta. Obecnie powodzenie tego ataku zależy od tego czy serwer jest poprawnie skonfigurowany i zabezpieczony.
Normalną obsługę zapytania DNS przedstawia Rysunek 2. Jeśli serwer ma zapisany w pamięci podręcznej adres IP powiązany z nazwą, o którą pyta klient, to od razu wysyła odpowiedź. Jeśli tej informacji nie ma, to przesyła zapytanie do serwera nadrzędnego (ang. *authoritative server*) i po uzyskaniu od niego odpowiedzi aktualizuje swoją pamięć podręczną, a następnie przesyła wynik do klienta.

Atakowanie infrastruktury

Zatruwanie DNS



Rysunek: Normalny przebieg obsługi zapytania DNS



Rysunek: Zatrucie pamięci podręcznej DNS

Atakowanie infrastruktury

Zatruwanie DNS

▸ Zatrucie DNS przedstawia Rysunek 3. Jeśli atakujący prześle sfałszowaną odpowiedź do serwera DNS, zanim nadejdzie prawdziwa z serwera nadrzędnego, to ta pierwsza zostanie uznana za prawidłową i serwer DNS w swojej pamięci podręcznej zapisze, że podana nazwa jest powiązana z adresem IP wskazanym przez atakującego. Ten adres zostanie również wysłany do klienta, natomiast odpowiedź z prawdziwego serwera nadrzędnego zostanie zignorowana. Jest to zatem atak ograniczony czasowo, wymagający odpowiednio szybkiego działania, zatem trudny do przeprowadzenia.
W testach penetracyjnych praktyczniejsze może okazać się zmodyfikowanie lokalnych plików używanych do rozwiązywania nazw, np. `/etc/hosts` lub bezpośrednia modyfikacja konfiguracji serwera DNS, o ile umożliwiają to odkryte podatności.

Atakowanie infrastruktury

Ataki typu Man-In-The-Middle

Duża część ataków na sieci komputerowe polega na „umiejscowieniu” urządzenia atakującego tak, aby mogło ono przechwytywać przechodzący przez nie ruch sieciowy. Wymaga to wymuszenia na systemach zaangażowanych w ruch zmiany tras, po których się on odbywa, lub przejęcia kontroli nad urządzeniami sieciowymi, które już znajdują się na tych trasach. Ataki należące do tej kategorii nazywane są atakami *man-in-the-middle* lub *on-path*.

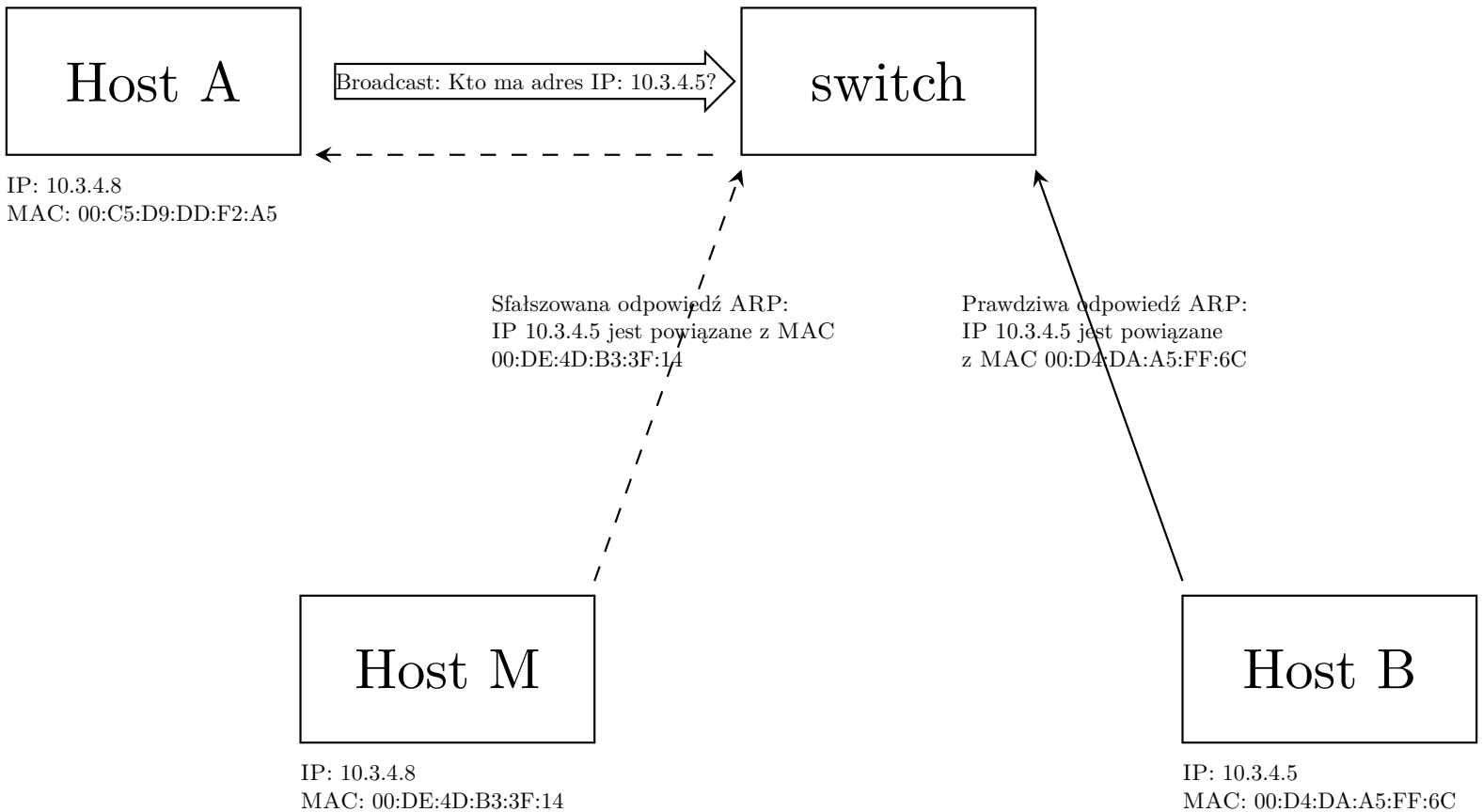
Atakowanie infrastruktury

Fałszowanie i zatruwanie ARP

ARP (ang. *Address Resolution Protocol*) jest protokołem używanym do translacji adresów IP na adresy MAC (ang. *Media Access Control*, nazywane także adresami fizycznymi. Podszywanie się lub fałszowanie ARP (ang. ARP *spoofing*) polega na wysyłaniu sfałszowanych odpowiedzi ARP, które informują, że podany adres IP prowadzi do urządzenia kontrolowanego przez atakującego. Ta technika może zostać wykorzystana do przeprowadzenia ataków typu *man-in-the-middle* lub do przejęcia sesji, albo wykonania ataku typu DoS. Rysunek 4 przedstawia przykład fałszowania ARP, nazywanego również *zatruwaniem* ARP. Jego zasięg jest ograniczony do domeny rozgłoszeniowej, w której znajduje się urządzenie atakującego. Do przeprowadzenia tego ataku można użyć polecenia `arpspoof`. Przydatnymi opcjami tego narzędzia są `-t` określająca adres IP celu i `-i` wskazująca interfejs sieciowy urządzenia atakującego.

Atakowanie infrastruktury

Fałszowanie i zatruwanie ARP



Rysunek: Fałszowanie ARP

Atakowanie infrastruktury

Fałszowanie adresu MAC (ang. MAC *Address Spoofing*)

Wiele usług sieciowych oraz mechanizmów zabezpieczających identyfikuje klienty w oparciu o ich adresy MAC (serwery DHCP, systemy NAC). Ten jednak można w przypadku określonych interfejsów sieciowych zmienić. Pozwalają na to nawet narzędzia systemowe. Dzięki temu atakujący nie tylko może uzyskać dostęp do lokalnej sieci obchodząc zabezpieczenia, ale także przechwycić ruch sieciowy skierowany do urządzenia faktycznie posiadającego sfałszowany adres MAC.

Atakowanie infrastruktury

Ataki powtórzeniowe (ang. *Replay Attacks*)

Ataki powtórzeniowe są skuteczne w przypadku uwierzytelniania opartego na protokołach typu *challenge-response*. Polegają one na przechwyceniu odpowiedzi (ang. *response*) i wysłaniu jej do serwera przeprowadzającego uwierzytelnienie. Taka technika jest stosowana w przypadku usług nie wymagających podpisywania SMB. Wystarczy, że atakujący przechwyci skróty NTLM (ang. NTLM *hashes*), funkcjonujące jako dane uwierzytelniając dla tych usług i prześle je do serwera ze źle skonfigurowaną usługą.

Ataki te wywodzą się z systemów IFF (ang. *Identification Friend or Foe*), stosowanych od czasów drugiej wojny światowej [1]. W swojej książce Ross Anderson podaje przykład takiego ataku, nazwany przez niego MIG-*In-The-Middle*, który przeprowadziło lotnictwo Angoli przeciwko najemnikom z RPA stacjonującym w Namibii. Choć autentyczność tej historii nie została potwierdzona, to podobne ataki przeprowadzano podczas wojny w Wietnamie oraz w wielu innych miejscach.

Atakowanie infrastruktury

Ataki typu *relay*

Ataki typu *relay* są podobne do ataków powtórzeniowych, ale w tym wypadku przechwycone komunikaty nie są modyfikowane, tylko przekazane (ang. *replay*) w niezmienionej postaci. Ta technika nie jest ograniczona wyłącznie do sieci bazujących na protokole IP.

Atakowanie infrastruktury

Omijanie zabezpieczeń NAC

Zabezpieczenia NAC (ang. *Network Access Control*) mają na celu zapobieganie podłączaniu do sieci nieautoryzowanych urządzeń. Wykrywają one nowe urządzenia i przeprowadzają ich uwierzytelnienie oraz autoryzację, które mogą być oparte na:

- oprogramowaniu klienckim łączącym się z serwerem NAC;
- pośredniku DHCP (ang. DHCP *proxy*), który nasłuchuje żądań DHCP;
- oprogramowaniu typu *listener* lub *sniffer*, które nasłuchuje zapytań ARP lub analizuje ruch IP;
- rozwiązaniach opartych na protokole SNMP, które odpytuje przełączniki, czy pojawiły się nowe adresy MAC w lokalnej sieci.

Tester penetracyjny musi ustalić, która z tych metod jest stosowana. Obejście niektórych z nich może być proste i polegać na zmianie adresu MAC lub użyciu statycznego IP używanego w danej sieci.

Atakowanie infrastruktury

Ataki typu DoS

Ataki typu DoS (ang. *Denial of Service*) zazwyczaj nie są częścią testów penetracyjnych lub w niektórych przypadkach mogą być wprost zakazane. Zazwyczaj pojawiają się przypadkowo i reakcja zespołu testującego na takie sytuacje powinna być klarownie określona w dokumentach regulujących zasady zatrudnienia. Niekiedy jednak zleceniodawcy wprost mogą nalegać na przeprowadzenie symulacji takich ataków. Można je sklasyfikować następująco:

- Ataki DoS w warstwie aplikacyjnej, mające na celu zablokowanie usługi lub całego serwera.
- Ataki wykorzystujące podatności w protokołach komunikacyjnych.
- Ataki polegające na generowaniu dużego ruch sieciowego, celem przeciążenia atakowanego urządzenia.

Atakowanie infrastruktury

Ataki typu DoS

Do przeprowadzenia ataków należących do drugiej kategorii można użyć narzędzi takich jak Metasploit lub Hping3. Popularnym przykładem ataku należących do tej kategorii jest SYN *flood*, który polega na wygenerowaniu dużej liczby pakietów TCP z ustawioną flagą SYN.

Atakowanie usług

W przypadku systemów Windows popularne ataki wykorzystują luki w protokole NetBIOS, który służy do wielu zdań, takich jak współdzielenie plików i rozwiązywanie nazw. W tym ostatnim przypadku NetBIOS używany jest przez usługę NBNS (ang. *The Net*BIOS *Name Service*). Przesyłane są nim zapytania LLMNR (ang. *Link Local Multicast Name Resolution*) oraz NBT-NS (ang. *Net*BIOS Name Service). Ta usługa jest wykorzystywana, gdy brakuje informacji o adresie IP powiązanym z daną nazwą w pliku `hosts`, lokalnej pamięci podręcznej oraz nie zwraca jej serwer DNS. Dzięki podszywaniu się pod tę usługę atakujący może przekierować ruch do kontrolowanego przez siebie urządzenia. Tego typu atak może być przeprowadzony z użyciem narzędzi *Metasploit* i ▸ Responder.
Innym popularnym celem ataku w przypadku systemów Windows są implementacje SMB (ang. *Server Message Block*), zawierające np. luki pozwalające na zdalne wykonanie kodu. Odpowiednie eksploity zawiera Metasploit.

Atakowanie usług

Routery i przełączniki sieciowe korzystają z protokołu SNMP (ang. *Simple Network Management Protocol*), ale jest on również używany do monitorowania drukarek, serwerów i innych urządzeń sieciowych. Protokół ten organizuje informację w hierarchiczne struktury MIB (ang. *Message Information Base*). Każda zmienna w tej strukturze jest identyfikatorem obiektu OIT. Istnieją trzy wersje tego protokołu:

SNMP v1 słabo zabezpieczona i nie powinna być współcześnie stosowana;

SNMP v2 dodano w niej możliwości administracyjne i mechanizmy zabezpieczające, które jednak nie są najlepszej jakości i wymagają konfiguracji, dlatego często są niestosowane;

SNMP v3 posiada lepsze zabezpieczenia niż wersja druga i takie same możliwości jako ona.

Atakowanie usług

Bezpieczeństwo protokołu SNMP w wersji pierwszej i drugiej bazuje na łańcuchach społecznościowych (ang. *community strings*), które określają, czy dane urządzenie może wykonywać operacje odczyty, zapisu lub wysyłać informacje o zdarzeniach. Informacje o konfiguracji urządzeń obsługujących protokół SNMP można uzyskać z użyciem narzędzi `snmpenum` i `snmpwalk`. Poza uzyskaniem łańcuchów społecznościowych można przy użyciu tego protokołu zmienić konfigurację urządzeń, jeśli są one nieodpowiednio zabezpieczone.

Atakowanie usług

Serwery poczty, czyli obsługujące protokół SMTP (ang. *Simple Mail Transfer Protocol*) pracują zwykle na porcie nr 25. Jeśli są one źle skonfigurowane (niezabezpieczone). To można je wykorzystać do uzyskania informacji o użytkownikach używając tak prostych technik jak połączenie się z usługą przy pomocy polecenia `telnet` i odpytania serwera poleceniami `VRFY nazwa_użytkownika` lub `EXPN alias_użytkownika`. W bardziej zaawansowane narzędzie, jakim jest enumerator SMTP wyposażony jest Metasploit. Uzyskanie dostępu do wszystkich funkcji serwera poczty może być przydatne w atakach socjotechnicznych, gdyż umożliwia wysyłanie wiadomości *e-mail* z zaufanej domeny.

Atakowanie usług

Protokół FTP (ang. *File Transfer Protocol*) został w dużej mierze zastąpiony przez swoje szyfrowane wersje, takie jak SFTP — przesyła pliki korzystając z protokołu SSH oraz FTPS — używa TLS, albo został zastąpiony protokołem HTTP(S). Są jednak implementacje serwerów FTP, których zastąpienie wersją bezpieczną lub wyłączenie jest niemożliwe. Zwykle są one zainstalowane na urządzeniach wbudowanych. Cechą takiego oprogramowania jest to, że przesyła nieszyfrowane dane na porcie nr 21 (TCP). Używany jest także dodatkowy port, ustalany w trakcie połączenia, do transferów pasywnych. Pozyskanie zatem danych uwierzytelniających sprowadza się do podsłuchiwania transmisji. Niektóre wersje serwerów FTP mają także podatności, dla których opracowano eksploity. Jeśli serwer jest źle skonfigurowany lub działa z uprawnieniami niewłaściwego użytkownika, to możliwe jest wykorzystanie podatności typu *path traversal*.

Atakowanie usług

Konta stworzone na potrzeby usług zazwyczaj mają hasła, które długo nie wygasają, a dodatkowo nie są monitorowane przez użytkowników. Stanowią zatem dobry cel w trakcie testów penetracyjnych, bo zapewniają dostęp do systemu przez długi czas. Aby przejąć takie konta można wykorzystać technikę o nazwie *Kereroasting*. Polega ona na skanowaniu usługi Active Directory, aby znaleźć konta użytkowników z ustawionymi głównymi nazwami usług (ang. *Service Principal Names* —SPNs), na następnie uzyskaniu biletu usługi (ang. *service ticket*) przy użyciu SPN. Ten bilet należy zapisać w pliku i za pomocą narzędzia takiego, jak *Mimikatz* ustalić hasło, jakim został on zaszyfrowany. Do szyfrowania biletów usług używane jest hasło do konta usługi. Istnieje gotowy ▸ zestaw narzędzi do przeprowadzenia tego ataku.

Atakowanie usług

Implementacją usługi SMB dla Linuksa jest serwer *Samba*. Podobnie jak odpowiednik Microsoftu może on zawierać luki, umożliwiające różne rodzaje ataków. Przykładowo, w 2017 roku pojawił się eksploit *The SambaCry*, który pozwalał na zdalne wykonanie kodu w systemie, gdzie zainstalowany był podatny serwer. Ponieważ zarówno SMB, jak i Samba operują na tych samych portach, to konieczne jest rozpoznanie systemu operacyjnego i serwera usługi przez przypuszczeniem ataku.

Atakowanie usług

Również usługa SSH może zawierać podatności. Zwykle są one szybko usuwane, ale w przypadku systemów wbudowanych może pojawić się trudność z aktualizacją tego oprogramowania. Zatem rozpoznanie zarówno jego wersji, jak i wersji systemu operacyjnego może pomóc wybrać odpowiedni eksploit.
Inną możliwością jest atak siłowy (ang. *brute-force*) mający na celu ustalenie hasła. Można w tym celu użyć narzędzia THC *Hydra* lub jego odpowiednika zintegrowanego z Metasploit. Działa ono wielowątkowo próbując haseł ze wskazanego słownika. Dodatkowo Metasploit posiada moduły umożliwiające wypróbowanie uzyskanych haseł na innych urządzeniach podłączonych do tej samej sieci.

Atakowanie usług

Ataki na hasła, nazywane też czasem niezbyt precyzyjnie „łamaniem haseł”, można przeprowadzić na kilka sposobów:

Metoda siłowa (ang. *brute-force*) Polega na próbach zalogowania przy użyciu wygenerowanych haseł. Hasła mogą być tworzone z przypadkowych znaków lub według prostych reguł. Ten sposób jest skuteczny tylko jeśli użytkownicy stosują proste hasła. Dodatkowo jest on czasochłonny i łatwy do wykrycia.

Atak słownikowy (ang. *dictionary attack*) Polega na próbach zalogowania przy użyciu haseł z wcześniej zdefiniowanego słownika (pliku). Czasem stosowane są reguły, według których te hasła mogą być modyfikowane. Tworząc słownik można uwzględnić, że użytkownicy mogą stosować jako hasła pojęcia związane z ich zawodem lub miejscem pracy. Tego typu ataki mogą być skuteczniejsze niż siłowe.

Atakowanie usług

Łamanie skrótów (ang. *hash cracking*) Stosuje się je po przechwyceniu skrótów haseł w sieci lub pobraniu ich z pliku. Najefektywniejszą metodą jest zastosowanie *tablic tęczowych* (ang. *rainbow tables*), czyli wcześniej wygenerowanych baz zawierających skróty i odpowiadające im ciągi znaków. Stosując je trzeba pamiętać o oczekiwanej długości hasła i zbiorze dopuszczalnych znaków jakie może ono zawierać.

Rozsiewanie haseł (ang. *passwor spraying*) Polega na sporządzeniu listy haseł i wypróbowywaniu ich po kolei na wielu usługach, systemach, aplikacjach internetowych, itp. Najczęściej używane są hasła, które wyciekły w wyniku innych ataków. Użytkownicy mają tendencję do używania tych samych haseł w wielu systemach.

Atakowanie sieci bezprzewodowych

Metody ataku na sieci przewodowe mogą być zastosowane również wobec sieci bezprzewodowych. Jednakże w przypadku tych ostatnich opracowano także kilka specjalizowanych podejść. W trakcie testów penetracyjnych można zastosować:

Podsłuch (ang. *eavesdropping*) przy użyciu snifferów przeznaczonych dla sieci bezprzewodowych, które rejestrują dane w ruchu.

Modyfikację danych (ang. *data modification*) atak, przeprowadzany równolegle do innych (np. man-in-the-middle), mający na celu zmianę przesyłanych danych.

Uszkodzenie danych (ang. *data corruption*) metoda ataku mająca na celu uszkodzenie przesyłanych danych lub zaburzenie ruchu sieciowego. Przykładem mogą być ataki, których celem jest dezaktualizacja uwierzytelnienia (ang. *de-authentication*) i ponowne uwierzytelnienie (ang. *reauthentication*).

Atakowanie sieci bezprzewodowych

Przekazanie (ang. *relay*) technika ataku powiązana z man-in-the-middle, polegająca na przechwyceniu danych, ich analizie przez atakującego, potencjalnej modyfikacji i przesłaniu do oryginalnego miejsca docelowego.

Podszycie (ang. *spoofing*) polega na wysyłaniu sfałszowanych informacji, które pozwalają atakującemu udawać inny system lub użytkownika, na różne sposoby.

Dezaktualizację uwierzytelnienia (ang. *deauthentication*) atak polegający na wysyłaniu sfałszowanych pakietów, aby doprowadzić do zerwania przez system połączenia i nawiązania go ze złośliwym punktem dostępowym (ang. *access point*), który może być *złym bliźniakiem* (ang. *evil twin*), lub do ponownego uwierzytelnienia, co pozwala atakującemu przechwycić dane uwierzytelniające.

Atakowanie sieci bezprzewodowych

Zagłuszanie (ang. *jamming*) polega na przerwaniu ruchu sieciowego poprzez przeciążenie urządzeń sieciowych lub zakłócanie (ang. *interfering*) ich działania.

Przechwytywanie potwierdzeń (ang. *handshake capturing*) pozwala na pozyskanie hasła (ang. *passphrase*) i odtworzenie z niego kluczy szyfrujących. Często stosowane wraz z atakiem dezaktualizacji uwierzytelnienia.

Ataki typu main-in-middle polegają na zmuszeniu systemu, by przesłał ruch sieciowy przez atakujące urządzenie. Pozwalają na monitorowanie ruch, jego zmianę oraz ataki polegające na przekazaniu (ang. *relay*).

Atakowanie sieci bezprzewodowych

Dostęp początkowy

Aby uzyskać początkowy dostęp do sieci bezprzewodowych należy ustalić gdzie znajdują się jej punkty dostępowe (ang. *access points*). Można informację o nich uzyskać prowadząc nasłuch w okolicy gdzie prowadzone są testy penetracyjne, w poszukiwaniu SSID i badając moc sygnału. Pomocne mogą okazać się także strony takie, jak ▸ WiGLE (ang. *Wireless Geographic Logging Engine*), które zawierają informację o sieciach Wi-Fi i zbierają je praktycznie z całego świata. Stosunkowo dobrym celem ataku są portale dostępowe (ang. *captive portals*), które stosowane są np. w hotelach. Pozwalają one urządzeniu na dostęp do sieci po podaniu ogólnodostępnej informacji uwierzytelniającej i/lub na podstawie jakiejś dodatkowej informacji, np. adresu MAC.

Atakowanie sieci bezprzewodowych

Złe bliźnięta

Technika złych bliźniąt (ang. *evil twins*) polega na zastąpieniu legalnego punktu dostępowego, jego sfałszowanym odpowiednikiem. Należy odróżnić złe bliźnięta od *fałszywych punktów dostępowych* (ang. *rogue access points*), które mogą być dowolnym urządzeniem podłączonym do sieci, którego tam nie powinno być, a które tworzy dodatkowy, znany intruzowi punkt dostępowy. W najprostszym przypadku technika złego bliźniaka polega na utworzeniu punktu o podobnym SSID, ale mocniejszym sygnale. Jednakże uważni użytkownicy szybko zauważą różnice w nazwie, haśle lub certyfikacie. Inną forma tej metody polega na wymuszeniu na klientach użycia mniej bezpiecznego niż domyślne szyfrowania, aby umożliwić atakującemu podsłuchiwanie i monitorowanie ruch sieciowego. Istnieje także wersja, o nazwie ▸ KARMA, w której atakujący nasłuchuje komunikatów klientów wyszukujących sieć Wi-Fi i przedstawia się jako punkt dostępowy do tej sieci.

Atakowanie sieci bezprzewodowych

Złe bliźnięta

Techniką złych bliźniąt można zastosować przy pomocy pakietu `Aircrack-ng` wykonując następujące czynności:

1. Ustalić SSID i MAC legalnego punktu dostępowego.
2. Sklonować ten punkt dostępowy przy pomocy narzędzia `airbase--ng`.
3. Przeprowadzić atak dezaktualizacji uwierzytelnienia.
4. Upewnić się, że sygnał ze sfałszowanego punktu jest silniejszy od legalnego i tym samym bardziej prawdopodobne jest, że zostanie wybrany przez klienty, podczas próby ponownego połączenia (ang. *reconnect*).
5. Przeprowadzić inne typy ataków.

Innym narzędziem umożliwiającym wykorzystanie tej techniki jest EAPHammer, które jest skuteczne przeciwko sieciom z szyfrowaniem WPA2 Enterprise.

Atakowanie sieci bezprzewodowych

Atak na WPS

Metoda WPS (ang. Wi-Fi Protected Setup) została zaprojektowana, aby ułatwić bezpieczne podłączanie nowych urządzeń do sieci bezprzewodowej. Niestety, zawiera ona szereg luk, które mogą być wykorzystane w testach penetracyjnych. Jedną z nich jest ośmiocyfrowy PIN, który może być złamany przy pomocy ataku siłowego o nazwie ▸ *pyłek wróżki* (ang. *pixie dust*). Narzędzie umożliwiające ten atak, ▸ Reaver, może go przeprowadzić nawet wtedy, gdy WPS nie został w punkcie dostępowym aktywowany oraz w trybie off-line, na podstawie przechwyconego ruchu sieciowego.

Atakowanie sieci bezprzewodowych

Sieci Bluetooth

Sieci bezprzewodowe to nie tylko Wi-Fi. W testach penetracyjnych można ▸ wykorzystać również łączność bazującą na protokole Bluetooth. Najpowszechniej stosowane metody ataku przeciwko takiemu rozwiązaniu to:

Bluesnarfing umożliwia kradzież informacji z urządzeń, które mają włączoną obsługę protokołu Bluetooth.

Bluejacking pozwala na wysyłanie niechcianych wiadomości przez łącza Bluetooth.

Urządzenia IoT obsługują zazwyczaj energooszczędną formę protokołu Bluetooth, nazwaną BLE (ang. *Bluetooth Low Energy*), która także jest podatna na ataki. Jednym z nich jest BLESA (*Bluetooth Low Energy Spoofing Attack*), który wykorzystuje fakt, że podczas ponownego nawiązywania połączenia BLE nie wymaga ponownego uwierzytelnienia.

Atakowanie sieci bezprzewodowych

Narzędzia

Zarówno do przełamywania, jak i weryfikowania zabezpieczeń sieci bezprzewodowych przydatne są narzędzia w formie oprogramowania, jak również sprzętu. Do tej pierwszej kategorii można zaliczyć następujące programy:

Aircrack-ng zbiór narzędzi do przeprowadzania ataków na sieci Wi-Fi.

mdk4 narzędzie umożliwiające eksplorację podatności protokołu 802.11.

Kismet umożliwia przechwytywanie i podsłuch (ang. *sniffing*) pakietów, ale także może pracować jako IDS (ang. *Intrusion Detection System*)

WiFite2 zostało stworzone do audytu zabezpieczeń sieci Wi-Fi.

Fen umożliwia przeprowadzenie wielu różnych ataków na sieci Wi-Fi, np. ataku słownikowego na szyfrowanie WPA2.

Atakowanie sieci bezprzewodowych

Narzędzia

Do narzędzi sprzętowych zaliczane są *radia definiowane oprogramowaniem* (ang. *Software Defined Radio* — SDR). Zgodnie z nazwą, nie są to rozwiązania ściśle sprzętowe. Aby działały wymagają podłączenia do komputera z odpowiednim oprogramowaniem. Posługiwanie się nimi może wymagać uzyskania odpowiednich pozwoleń, w zależności od zakresu częstotliwości i mocy z jaką te urządzenia, a dokładniej ich nadajniki, pracują. Mogą one umożliwiać testowanie dowolnych sieci bezprzewodowych, nie tylko Wi-Fi. Rysunek 5 przedstawia przykładową implementację sprzętową radia definiowanego oprogramowaniem.

Atakowanie sieci bezprzewodowych

Narzędzia

Rysunek: Urządzenie HackRF One (źródło: https://greatscottgadgets.com/hackrf/one/)

Bibliografia

 Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2020. URL: https://www.cl.cam.ac.uk/~rja14/book.html.

Pytania

?

Koniec

Dziękuję Państwu za uwagę!