IDS - (Inttrusiion Dettecttiion Systtems) monitorowanie ruchu sieciowego, podejrzanej aktywności

Wireguard - is a communication protocol and free and open-source software that implements encrypted virtual private networks (**VPN**s). It aims for better performance and more power than **IPsec** and **OpenVPN**. The WireGuard protocol passes traffic over **UDP**.

TLS - (Transport Layer Security) certyfikat, ulepszony **SSL** (Secure Sockets Layer), TLS zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta. Opiera się na szyfrowaniu asymetrycznym oraz certyfikatach **X.509**. Według modelu OSI, TLS działa w warstwie prezentacji

SSL - wartswa sesji modeli ISO/OSI

SIEM - (Security Information & Event Management) zbieranie rozproszonych logów, selekcja katalogowanie, agregowanie

UAC - was introduced in Windows to limit the possibility of uncontrolled administrative operations. When this mechanism is active and a user with administrative rights logs into the system, 2 tokens are created for him: full—containing full administrative rights, and a restricted token—deprived of most security-critical rights (the so-called Filtered Admin Token).
Token pełny - zawiera wszystkie prawa administracyjne
Token ograniczony - jest pozbawiony większości praw dotyczących bezpieczeństwa

SSO - (Single Sign-On) uwierzytelnianie jednokrotne

klucz asymetryczny vs symetryczny - Główną różnicą pomiędzy tymi dwoma metodami jest fakt, iż w do szyfrowania symetrycznego wykorzystywany jest tylko jeden klucz, a dane zaszyfrowane asymetrycznie odkodowuje się innym kluczem niż zostały one pierwotnie zaszyfrowane

atak pasywny - Ataki pasywne polegają na podsłuchiwaniu lub monitorowaniu przesyłania. Celem osoby atakującej jest odkrycie treści komunikatu. Do ataków pasywnych należą dwa typy: odkrycie treści komunikatu lub analiza przesyłu.

atak aktywny - Polegają one na modyfikowaniu strumienia danych lub tworzeniu danych fałszywych i dzielą się na cztery typy: maskarada, powtórka, modyfikacja komunikatów, blokowanie działania.

Metoda Diffiego Hellmana - protokół uzgadniania kluczy szyfrujących, nie jest odporna na ataki aktywne typu **man in the middle**,

DNSsec - rozszerzenie systemu DNS mające na celu zwiększenie jego bezpieczeństwa. DNSSEC zapewnia uwierzytelnianie źródeł danych (serwerów DNS) za pomocą kryptografii asymetrycznej oraz podpisów cyfrowych.

HTTP 1.1 - typowo MD5 (chociaż teoretycznie jest to jedynie rekomendacja) klient konkatenuje identyfikator:realm:hasło i liczy skrót MD5 (=H1) dalej konkatenuje metodę HTTP (GET, POST,...) z URI i liczy skrót MD5 (=H2) ostatecznie konkatenuje H1:nonce:H2 i liczy wynikowy skrót MD5, wprowadził digest auth. (challenge-response)

HTTP 1.0 - klient w nagłówku Authorization: przekazuje token zawierający dane uwierzytelniające (credentials) token zawiera identyfikator podmiotu (np. username) skonkatenowany z hasłem np. Aladdin:OpenSesame token jest zakodowany Base64, wprowadził basic auth. czyli dane logowania (username&hasło) niezaszyfrowane

Defender Application Guard - Application Guard opens untrusted files in an isolated Hyper-V-enabled container.

Windows AppContainer - środowisko do wirtualizacji w windowsie

Randomizacji układ przestrzeni adresowej (ASLR) - jest techniką umieszczania losowo obszary danych w pamięci wirtualnej, ogranicza skutki ataków typu przepełnienie bufora

Stack cookie - kompilator alokuje dodatkowy obszar („kanarka”) pomiędzy wskaźnik poprzedniej ramki a adres powrotu przed powrotem z funkcji weryfikujemy wartość „kanarka”, ogranicza ataki przepełnienia bufora

Wykluczenie wykonywania kodu na stosie - zapewnienie by segment pamięci z prawem zapisu nie posiadał jednocześnie prawa wykonywania, chroni przed atakiem przepełnienia bufora

Kerberos - protokół uwierzytelniania i autoryzacji w sieci komputerowej z zastosowaniem centrum dystrybucji kluczy, zaprojektowany w Massachusetts Institute of Technology (MIT).

Golden ticket - Atak Golden Ticket polega na pobraniu informacji na temat konta krbtgt z kontrolera domeny i utworzeniu biletu, który nie ulega przedawnieniu, dla dowolnego konta. Może to być nawet konto nieistniejące w domenie, tzw. ghost, wtedy najtrudniej jest wykryć taki przypadek.

Silver ticket - A hacker can create a Silver Ticket by cracking a computer account password and using that to create a fake authentication ticket. Kerberos allows services (low-level Operating System programs) to log in without double-checking that their token is actually valid, which hackers have exploited to create Silver Tickets.

Komputer-Twierdza -

- fizyczna i logiczna separacja prywatnej sieci lokalnej od zewnętrznej sieci publicznej
- tylko Komputer Twierdza jest widoczny z sieci publicznej
- aby wtargnąć do sieci prywatnej trzeba uprzednio zawładnąć Komputerem Twierdzą
- brama aplikacyjna – proxy rozwiązuje problem usług trudnych do filtracji

IEEE 1609.2 - This standard defines secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.

IEEE 802.1X - standard IEEE kontroli dostępu do sieci przewodowych i bezprzewodowych. Umożliwia uwierzytelnianie urządzeń dołączonych do portów sieci lokalnej, ustanowienie połączenia punkt-punkt i nie zezwala na dostęp z określonego portu, jeśli uwierzytelnienie się nie powiedzie.

X.509 - standard definiujący schemat dla certyfikatów kluczy publicznych, unieważnień certyfikatów oraz certyfikatów atrybutu służących do budowania hierarchicznej struktury PKI. Kluczowym elementem X.509 jest urząd certyfikacji, który pełni rolę zaufanej trzeciej strony w stosunku do podmiotów oraz użytkowników certyfikatów.

EFS - system szyfrowania plików, wprowadzony dla systemu plików NTFS w wersji 3.0 przez firmę Microsoft dla systemów Windows. EFS umożliwia szyfrowanie plików z poziomu systemu, aby zapewnić ochronę poufnych danych przed atakami osób, które mają fizyczny dostęp do komputera. Stosuje symetryczna kryptografie oraz public key.

Trusted Platform Module - standard układu scalonego (nazywany jest tak również sam układ), Układy zgodne z TPM potrafią wykonać najbardziej typowe operacje obliczeniowe związane z kryptografią. Wśród operacji takich wymienić należy:

- generowanie liczb pseudolosowych
- generowanie podpisu cyfrowego dla ciągu bajtów
- generowanie skrótów dla ciągu bajtów
- szyfrowanie ciągu bajtów

- generowanie skrótów dla sekwencji operacji wykonywanych przez procesor

Układy TPM mają zaimplementowane następujące algorytmy:

- RSA
- SHA-1
- HMAC
- AES – niewymagany – jednak powszechnie stosowany

Ponadto każdy układ TPM ma unikatowy numer seryjny oraz prywatny klucz RSA.

NAC (Network Access Control) - Network Access Control, zwane także kontrolą dostępu do sieci, to narzędzie zwiększające bezpieczeństwo, widoczność, ogólnie pomaga w zarządzaniu firmową siecią. Ogranicza dostępność zasobów sieciowych do urządzeń końcowych i użytkowników, którzy przestrzegają zdefiniowanych zasad bezpieczeństwa.

- **Wstępna kontrola dostępu:** Pierwszy typ kontroli dostępu do sieci jest nazywany wstępnym dostępem. Ma miejsce przed przyznaniem dostępu do sieci gdy użytkownik lub urządzenie końcowe inicjuje żądanie dostępu do sieci. Kontrola sieci przed uzyskaniem dostępu ocenia próbę dostępu i zezwala na wejście do sieci tylko wtedy, gdy urządzenie lub użytkownik zgłaszający żądanie może udowodnić, że jest zgodny z korporacyjnymi zasadami bezpieczeństwa i jest upoważniony do dostępu do sieci.
- **Post-admission:** Kontrola dostępu do sieci po dopuszczeniu ma miejsce wewnątrz sieci. Gdy użytkownik lub urządzenie próbuje wejść do innej części sieci. Jeśli kontrola dostępu do sieci przed uzyskaniem dostępu nie powiedzie się, kontrola dostępu do sieci po uzyskaniu dostępu może ograniczyć ruch boczny w sieci i zmniejszyć szkody spowodowane cyberatakiem. Użytkownik lub urządzenie musi ponownie uwierzytelnić się przy każdym żądaniu przejścia do innej części sieci.

MAC (Mandatory Access Control) - precyzyjne reguły dostępu automatycznie wymuszają uprawnienia, nawet właściciel zasobu nie może dysponować prawami dostępu, MAC pozwala łatwiej zrealizować (narzucić) silną politykę bezpieczeństwa i konsekwentnie stosować ją do całości zasobów.

MAC poufność
No read-up - Podmiot nie może czytać danych o wyższej etykiecie niż jego aktualna
No write-down - Podmiot nie może zapisywać danych o niższej etykiecie niż jego akutualna.

MIC (Mandatory Integrity Control) - integralność
część standardu szyfrowania stosowanego w sieciach bezprzewodowych zdefiniowanego w protokole 802.11i służący do gwarantowania integralności przesyłanych danych.
Podmiot nie może zapisywać danych o wyższej etykiecie niż swoja aktualna
Podmiot nie może czytac danych o nizszej etykiecie niż swoja aktualna

POSIX Capabilities (CAP) - rozdzielenie uprawnień administracyjnych superużytkownika root na zbiór szczegółowych uprawnień (polega na dziedziczeniu)

RADIUS (Remote Authentication Dial In User Service) - usługa zdalnego uwierzytelniania użytkowników, którzy wdzwaniają się do systemu (poprzez usługę „połączenie wdzwaniane").Obecnie jest najpopularniejszym protokołem uwierzytelniania i autoryzowania użytkowników sieci telefonicznych i tunelowych. Używany jest także w sieciach bezprzewodowych.

TACACS (ang. Terminal Access Controller Access-Control System) – protokół uwierzytelniania, używany do komunikacji ze zdalnym serwerem uwierzytelniania, stosowany w sieciach Unix. Umożliwia on komunikację zdalnego serwera z serwerem uwierzytelniania w celu określenia czy użytkownik posiada prawo dostępu do sieci.

ISAKMP (Internet Security Association and Key Management Protocol) - is a protocol defined by RFC 2408 for establishing Security association (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent; protocols such as Internet Key Exchange (IKE) and Kerberized Internet Negotiation of Keys (KINK) provide authenticated keying material for use with ISAKMP.

Application Layer Gateway (ALG) - działa jako pośrednik pomiędzy Internetem oraz serwerem aplikacji, który rozpoznaje protokół aplikacji. ALG funkcjonuje jako serwer końcowy i decyduje o tym, czy zezwolić na ruch do serwera aplikacji, czy odmówić go. Dzieje się to przez przechwytywanie oraz analizowanie określonego ruchu, przydzielanie zasobów oraz definiowanie dynamicznych procedur w celu zezwalania na ruch przez bramkę.

NAT (Network Address Translation) - funkcje: rozszerzenie dostępu do sieci publicznej na stanowiska nieposiadające adresów publicznych (adresy prywatne – RFC 1918), ukrycie wewnętrznej struktury sieci przed światem zewnętrznym, przekierowanie portów (NAPT = Network Address & Port Translation), RFC1631 (translacja na pojedynczy adres, tj. N:1), RFC1597,1918 (translacja na pulę adresową, tj. N:M)

Translacja adresów źródłowych (SNAT) - pakiety wychodzące z sieci wewnętrznej otrzymują nowy adres źródłowy w nagłówku

Translacja adresów docelowych (DNAT) - pakiety przychodzące ze strony inicjującej (na ogół – sieci zewnętrznej) otrzymują nowy adres docelowy (w tym w szczególności – port)

Łańcuch funkcji:

funkcje podstawowe:

funkcje dodatkowe:

- wykrywanie i rejestrowanie prób ataków na chronione systemy

Kolizja funkcji skrótu H to taka para różnych wiadomości m1, m2, że mają one taką samą wartość skrótu

Algorytm lamporta - nie wymaga kryptografii, wymaga funkcji jednokierunkowej, ustala tajne hasło funkcją *h* sekwencji i *t* haseł jednorazowych, wykorzystuje hasła od końca

Metoda ARP -

Fragmentacja IP - problem fragmenty mogą powodować błędy i pozwalać na ataki np teardrop attack

xinted (superserwer) - Firewall oparty na iptables odfiltrowuje niepożądane pakiety sieciowe w stosie sieciowym jądra.

TCP wrapper - to taka usługa, która została skompilowana z biblioteką libwrap.so. Ten proces — tcpd lub TCP wrapper — zajmuje się kontrolą dostępu do usług obsługiwanych przez xinetd. Operuje na dwóch listach opisujących politykę kontroli dostępu — lista jawnych uprawnień dostępu do usług (plik /etc/hosts.allow) i jawnych zakazy dostępu (plik /etc/hosts.deny). Każde nowe żądanie połączenia jest następnie konfrontowane z regułami polityki w pierwszej liście, a jeśli to nie przyniesie rozstrzygnięcia – na drugiej liście.
Wrapper TCP może zostać wywołany przez xinetd, dzięki czemu zostanie wpleciony między nim a ostatecznie realizowany proces usługi sieciowej, który wymaga dość oczywistej modyfikacji odpowiedniego plik konfiguracyjny tej usługi, np. /etc/xinetd.d/rlogin.
W nowszych wersjach demona opakowania TCP zasady kontroli dostępu można skonfigurować za pomocą jednego plik konfiguracyjny, czyli **/etc/hosts.allow.**

Opcjonalna pozycja dodatkowej definicji (kolejny dwukropek) może zawierać słowo kluczowe ALLOW lub DENY.

ADS (Alternate Data Streams) - Mechanizm alternatywnych strumieni danych ADS (ang. Alternate Data Streams) w NTFS został zaadaptowany z systemu plików HFS (MacOS), gdzie służy do przechowywania metadanych. System Windows aktualnie wykorzystuje strumienie alternatywne w zasadzie tylko do przechowywania informacji o tzw. strefie internetowej, z której pobrany został plik zapisany następnie w lokalnym systemie plików. Na podstawie owej strefy, Eksplorator Windows określa poziom ostrzeżeń przy rozpoczęciu przetwarzania pobranego pliku (np. przy uruchomieniu programu wykonywalnego). Informacja ta umieszczana jest w strumieniu :Zone.Identifier pobranego pliku. Jest to strumień tekstowy zawierający w sekcji [ZoneTransfer]deklarację parametru ZoneId. Strumienie ujawnia polecenie dir /r. Strumienie ADS identyfikuje przyrostek :$DATA podawany na listingu z tego polecenia. Jednym z nielicznych narzędzi systemu Windows, które pozwalają odczytać strumienie ADS jest Notatnik (notepad). Brak zarządzania strumieniami alternatywnymi przez system operacyjny wprowadza ogromne ryzyko potencjalnego wykorzystania strumieni jako doskonałej kryjówki złośliwego lub niechcianego oprogramowania.

AH (ang. Authentication Header) - protokół do zapewnienia uwierzytelniania i integralności pakietów IP w IPsec, gdzie używany jest także protokół ESP. AH (jak i ESP) wykorzystywane są w trybach pracy: transportowym lub tunelowym. AH został opisany w RFC 2402, a ESP w RFC 2406

ESP (ang. Encapsulating Security Payload) – protokół bezpieczeństwa zapewniający: uwierzytelnianie źródła danych, integralność danych (przy pomocy obliczenia skrótu z zaszyfrowanych już danych), niezaprzeczalność danych (przy pomocy obliczenia skrótu z zaszyfrowanych już danych), obsługuje unikanie duplikacji pakietów jak również ataku przez powtórzenie (zastosowanie numerów sekwencji), zapewnia poufność danych. Obok protokołu AH wykorzystywany w IPsec.

Internet Key Exchange (IKE lub IKE2) – protokół służący do zestawienia bezpiecznego skojarzenia SA (ang. Security Association) pomiędzy dwoma hostami, zwłaszcza w protokole **IPsec**. Nawiązanie bezpiecznej sesji IKE przebiega w dwóch fazach:

- **Faza 1** – ustanowienia bezpiecznego, uwierzytelnionego kanału komunikacji. Strony przy użyciu protokołu Diffiego-Hellmana ustanawiają wspólny sekretny klucz/hasło wykorzystywany dalej do szyfrowana komunikacji IKE w fazie 2.
- **Faza 2** – korzystając z bezpiecznego kanału ustanowionego w fazie 1, strony połączenia występują w imieniu innych usług, takich jak np. IPsec.