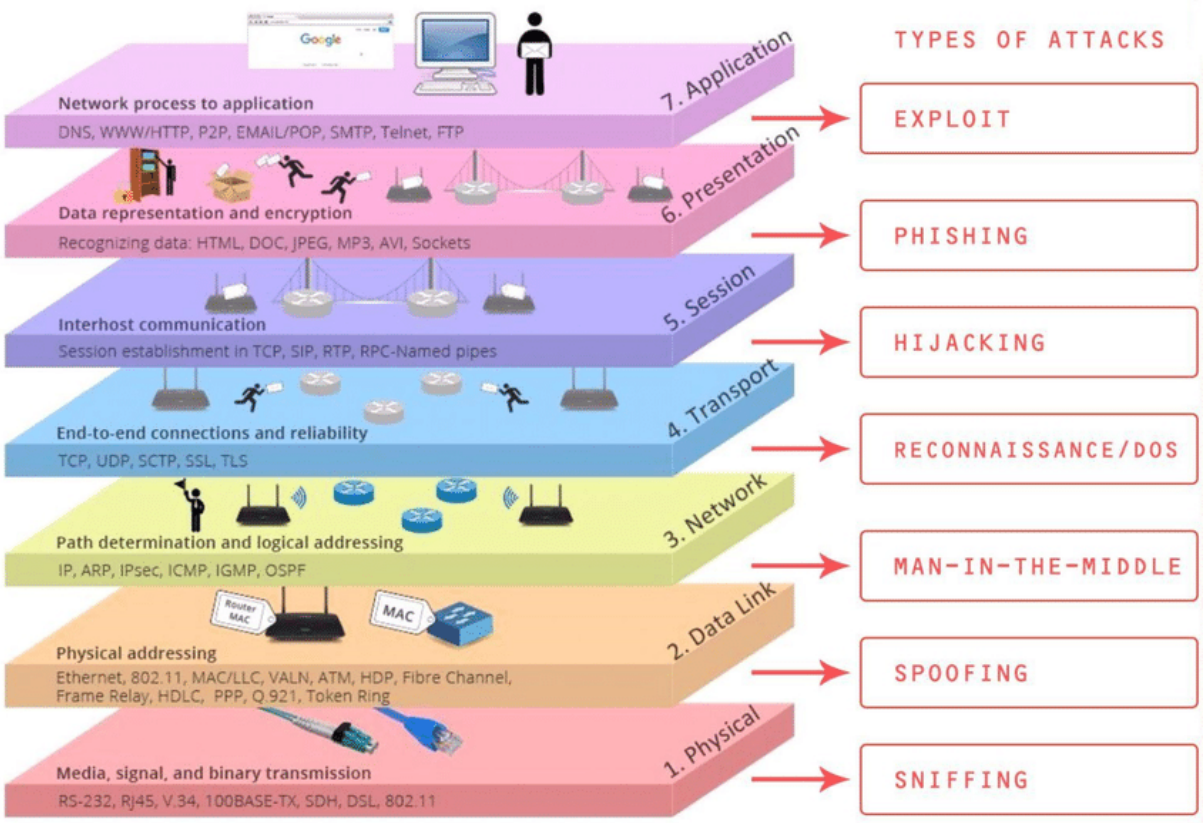
CCNA


TYPES OF ATTACKS
7. Application
Network process to application
DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP
EXPLOIT
6. Presentation
Data representation and encryption
Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets
PHISHING
5. Session
Interhost communication
Session establishment in TCP, SIP, RTP, RPC-Named pipes
HIJACKING
4. Transport
End-to-end connections and reliability
TCP, UDP, SCTP, SSL, TLS
RECONNAISSANCE/DOS
3. Network
Path determination and logical addressing
IP, ARP, IPsec, ICMP, IGMP, OSPF
MAN-IN-THE-MIDDLE
2. Data Link
Physical addressing
Ethernet, 802.11, MAC/LLC, VALN, ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring
SPOOFING
1. Physical
Media, signal, and binary transmission
RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11
SNIFFING

	Model ISO/OSI	Protokoły	Model TCP/IP
Data	**Aplikacji**	DNS, HTTP, POP, SMTP, Telnet, FTP	**Aplikacji**
	Prezentacji	Rozpoznawanie danych: HTML, DOC, JPEG, MP3, Sockets	
	Sesji	TCP, SIP, RTP, RPC-Named pipes	
Segments	**Transportowa**	TCP, UDP, SCTP, SSL, TLS	**Transportowa**
Packets	**Sieci**	IP, ARP, IPsec, ICMP, IGMP, OSPF	**Sieci**
Ramka(Frames)	**Łącza danych**	Etherent 802.11, MAC	**Łącza danych**
Bits	**Fizyczna**	RJ45	**Fizyczna**

Model ISO/OSI i TCP/IP

Warstwa (Layer) 1.

Warstwa Łącza danych (Layer) 2.

ARP (Address Resolution Protocol) - służy do mapowania adresów warstwy sieciowej (IP) na adresy warstwy łącza danych (MAC)

Kiedy urządzenie w sieci potrzebuje wysłać pakiet do innego urządzenia, musi znać jego adres MAC. Aby uzyskać adres MAC docelowego urządzenia, urządzenie wysyła żądanie ARP typu "Who has" (czyli "Kto ma") na wszystkie urządzenia w sieci. W żądaniu ARP zawarty jest adres IP docelowego urządzenia, a każde urządzenie w sieci odbiera to żądanie. Docelowe urządzenie odsyła odpowiedź ARP typu "Reply" (czyli "Odpowiedź"), w której przesyła swój adres MAC

Informacje o odwzorowaniu adresu IP na adres MAC zapisywane są w tablicy ARP każdego urządzenia, tak aby można je było wykorzystać w późniejszym czasie. Domyślnie, w systemach Windows wpis taki utrzymuje się maksymalnie do 10 minut, po tym czasie zostaje usunięty. Aby wyświetlić tablicę ARP, należy w konsoli wykonać polecenie

arp -a – wyświetlenie tablicy ARP

Warstwa Sieci (Layer) 3.

ICMP (Internet Control Message Protocol) – protokół warstwy sieciowej wykorzystywany w diagnostyce sieci oraz routingu.

Polecenie **ping** korzysta z pakietów ICMP

Warstwa Transportowa (Layer) 4.

DHCP (Dynamic Host Configuration Protocol) – DHCP umożliwia podłączonym do sieci komputerom pobieranie **adresu IP, maski podsieci, adresu bramy** i **serwera DNS** oraz innych ustawień ze skonfigurowanej wcześniej puli adresów. Serwer DHCP może być skonfigurowany na osobnym komputerze i stanowił będzie osobne urządzenie w sieci przydzielające komputerom klienckim adresy IP, może również działać na już istniejącym serwerze jako osobna usługa, osobny proces.

Serwery aplikacji, baz danych, uwierzytelniania użytkowników, drukarki sieciowe czy **rutery** powinny, a wręcz muszą posiadać adresy przydzielone statycznie

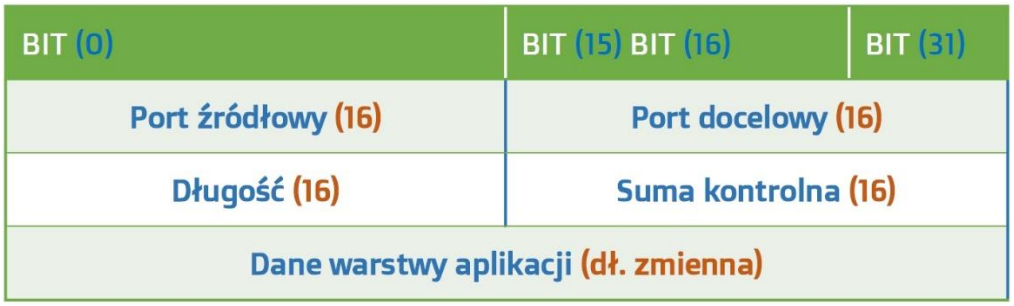
DHCP używa protokołu UDP. Wszystkie pakiety wysyłane przez klienta mają port źródłowy 68 i port docelowy 67. Pakiety wysyłane przez serwer mają port źródłowy 67 i port docelowy 68.

TCP (Transmission Control Protocol) – zapewnia niezawodną i uporządkowaną transmisję danych między aplikacjami działającymi na różnych komputerach w sieci. Protokół ten korzysta z mechanizmów kontrolowania przepływu i zapewniania integralności danych, co oznacza, że dane są przesyłane w kolejności, w jakiej zostały wysłane i że odbiorca otrzyma wszystkie dane bez utraty lub duplikacji.

Rysunek 1 nagłówek tcp

- **Port źródłowy** – port aplikacji, z której wysłano dane.
- **Port docelowy** – port aplikacji, do której wysłano dane.
- **Numer sekwencyjny** – numer ostatniego bajtu w segmencie.
- **Numer potwierdzenia** – numer następnego bajtu oczekiwanego przez odbiorcę.
- **Długość** – długość całego segmentu TCP.
- **Bity kodu (flagi)** – informacje kontrolne dotyczące segmentu.
- **Okno** – ilość danych jaka może zostać przesłana bez potwierdzenia.
- **Suma kontrolna** – używana do sprawdzania poprawności przesłanych danych.
- **Wskaźnik pilności** – używany tylko kiedy ustawiona jest flaga URG.

UDP (User Datagram Protocol) – jest szybki, ale nie zapewnia gwarancji dostarczenia i kolejności danych. Jest wykorzystywany do przesyłania dużych plików oraz do transmisji strumieniowej. Np. Rozmowy(Teams), Live



Rysunek 2 nagłówek UDP

- **Port źródłowy** – określa port aplikacji, z której wysłano dane.
- **Port docelowy** – określa port aplikacji, do której wysłano dane.
- **Długość** – 16 – bitowe pole określające długość całego datagramu UDP
- **Suma kontrolna** – 16 – bitowe pole służące do sprawdzania poprawności przesłanych danych.

Warstwa (Layer) 5.

Warstwa (Layer) 6.

Warstwa (Layer) Aplikacji 7.

HTTP (Hypertext Transfer Protocol) – protokouł do przesyłania dokumentów hipertekstowych. HTTP jest protokołem sieciowym używanym do komunikacji między serwerami internetowymi a przeglądarkami internetowymi.

Nazwa usługi	*TCP lub UDP*	*Port*
http	TCP	80
https	TCP	443

FTP (File Transfer Protocol) - Protokół transferu plików. Jest to standardowy protokół internetowy wykorzystywany do przesyłania plików między komputerami w sieci, na przykład między serwerem a klientem

Nazwa usługi	*TCP lub UDP*	*Port*
FTP	TCP	20, 21

DNS (Domain Name System) – Dzięki DNS nazwa mnemoniczna, np. pl.wikipedia.org jest tłumaczona na odpowiadający jej adres IP, czyli 91.198.174.192.

DNS działa na zasadzie hierarchicznej struktury serwerów, które są odpowiedzialne za przekształcanie nazw domenowych na adresy IP. Gdy użytkownik wprowadza adres URL do przeglądarki internetowej, komputer wysyła zapytanie do serwera DNS, aby uzyskać odpowiadający mu adres IP. Jeśli serwer DNS nie ma odpowiedzi, to kieruje pytanie do kolejnego serwera na wyższym poziomie hierarchii, aż do momentu znalezienia odpowiedzi.

DNS używa portu 53 do komunikacji między klientami a serwerami DNS. Ten port jest stosowany zarówno w protokole UDP (User Datagram Protocol) jak i TCP (Transmission Control Protocol) w celu przesyłania zapytań i odpowiedzi.

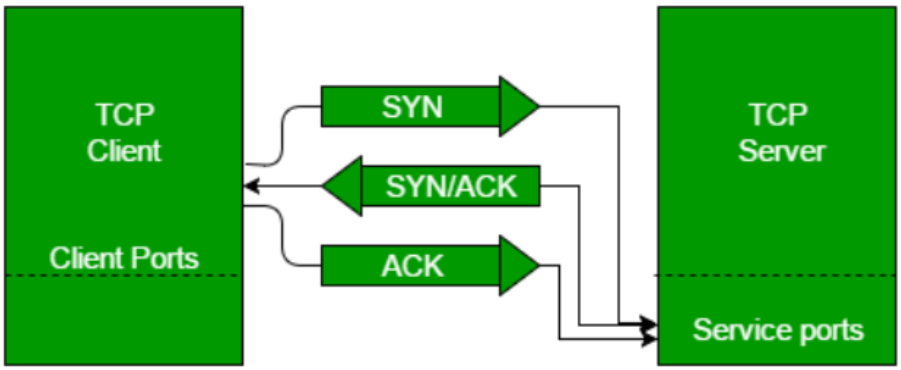
Nazwa usługi	*TCP lub UDP*	*Port*
DNS	TCP / UDP	53

TCP

TCP Handoff - to technika polegająca na przełączeniu połączenia TCP między różnymi interfejsami sieciowymi na tym samym urządzeniu lub między różnymi urządzeniami w sieci. Technika ta jest szczególnie przydatna w przypadku, gdy jedno z urządzeń lub interfejsów sieciowych ulega awarii lub osiągnęło swoją maksymalną wydajność, a połączenie musi zostać przeniesione na inny interfejs lub urządzenie.

TCP Handoff jest szczególnie ważny w przypadku sieci bezprzewodowych, gdzie urządzenia mogą przechodzić między różnymi punktami dostępowymi lub między różnymi sieciami, co może prowadzić do utraty połączenia. Dzięki technice TCP Handoff urządzenia mogą automatycznie przenosić połączenia między różnymi sieciami i punktami dostępowymi, zapewniając ciągłość połączenia i unikając utraty danych.

TCP 3-way handshake (trójstopniowe ustanowienie połączenia) to procedura używana przez protokół TCP w celu nawiązania połączenia między dwoma hostami w sieci.



Rysunek 3 TCP 3-Way Handshake Process

Jak działa Traceroute?

Komenda **traceroute** próbuje śledzić trasę pakietu IP do hosta internetowego, wysyłając pakiety sondujące UDP

Działanie traceroute opiera się na protokołach komunikacyjnych UDP oraz ICMP

Sieci, protokoły #1

- Czy w sieciach jest broadcast, multicast, unicast oraz anycast?
- Jaka jest różnica między segmentami, pakietami i ramkami?
- Czy potrafisz opisać co zawiera nagłówek TCP?
- Czym się różnią protokoły routingu od protokołów routowalnych?
- W jaki sposób odpytać konkretny serwer DNS o konkretny rekord?
- Co oznacza wartość TTL w rekordzie DNS?
- Wymień znane Ci metody HTTP (przynajmniej te najpopularniejsze)?
- Jaka jest różnica między metodami POST i GET w HTTP?
- Jakie są różnice pomiędzy HTTP 1.* a HTTP 2?
- Wymień znane Ci numery błędów (niekoniecznie konkretne), które może zwracać HTTP?
- W jaki sposób możesz dowiedzieć się, która usługa standardowo na jakim porcie nasłuchuje?
- Co to jest IPv6 i czym się różni od “standardowego”?
- Do jakiej klasy IP należy adres IP X.X.X.X?

Sieci, protokoły #2