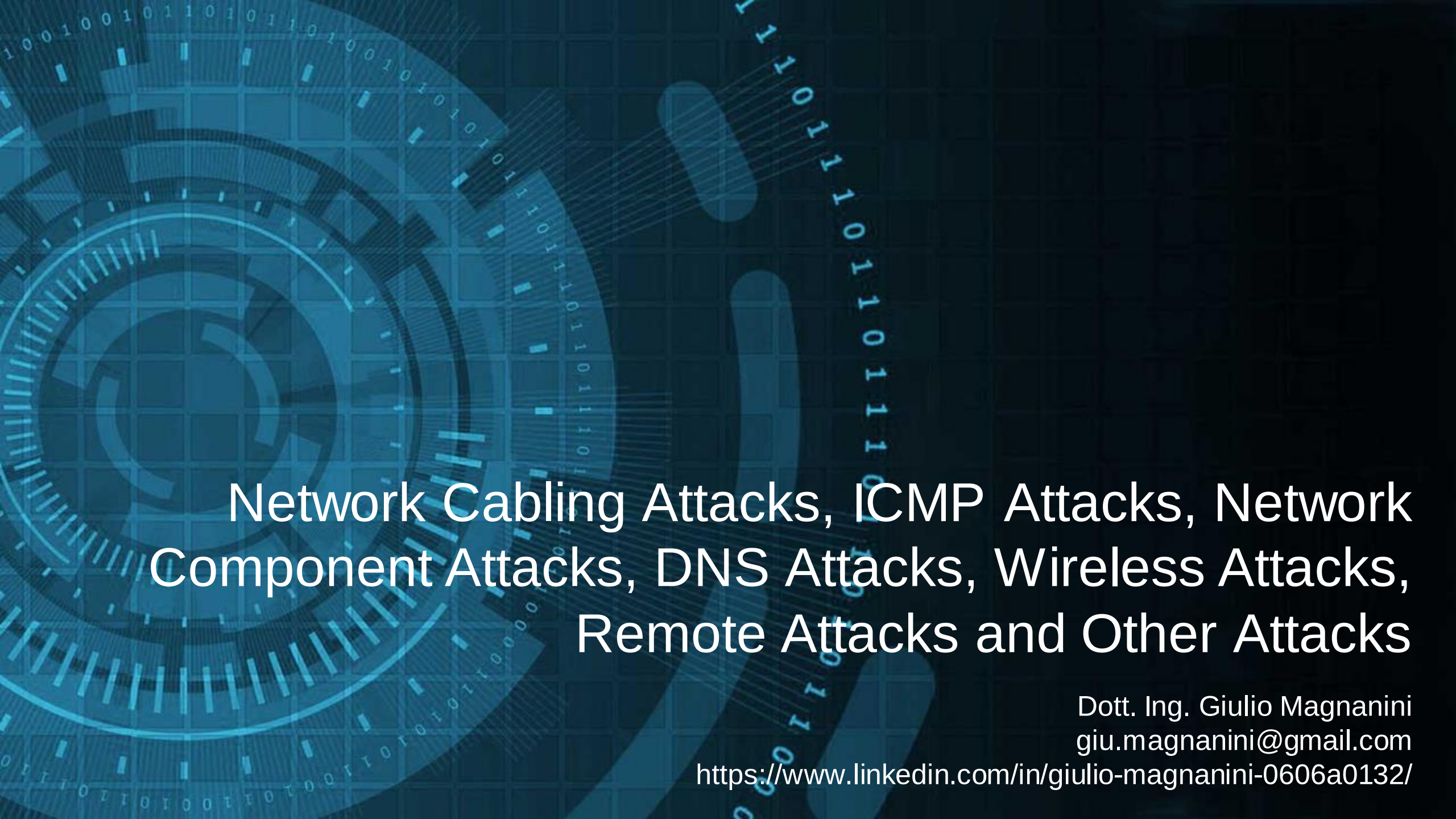


Network Cabling Attacks, ICMP Attacks, Network Component Attacks, DNS Attacks, Wireless Attacks, Remote Attacks and Other Attacks

Dott. Ing. Giulio Magnanini
giu.magnanini@gmail.com
https://www.linkedin.com/in/giulio-magnanini-0606a0132/

DISCLAIMER

1 – The following discussion is for informational and education purpose only.

2 – Hacking into private network without the written permission from the owner is Illegal and strictly forbidden.

3 – Misused could result in breaking the law so use it at your own risk.

Attacchi alle reti cablate

Gli attacchi alle reti cablate (Network Cabling Attacks - NCA) sono attività malevole che mirano all'infrastruttura fisica di una rete.

Tipologie di Network Cabling Attacks

1. **Intercettazione fisica:**
- Gli attaccanti ottengono accesso non autorizzato ai cavi di rete intercettandoli fisicamente.
- Possono collegarsi ai cavi per monitorare o manipolare il traffico di rete.

2. **Inserimento di dispositivi:**
- Gli attaccanti inseriscono dispositivi non autorizzati nella rete cablata.
- Questi dispositivi possono essere utilizzati per intercettare o manipolare il traffico di rete.

Conseguenze dei NCA

- **Interferenza nella comunicazione:** gli attaccanti possono intercettare, alterare o interrompere il flusso di dati tra i dispositivi di rete.

- **Furto di informazioni:** gli attaccanti possono ottenere accesso a dati sensibili o confidenziali che transitano attraverso la rete cablata.

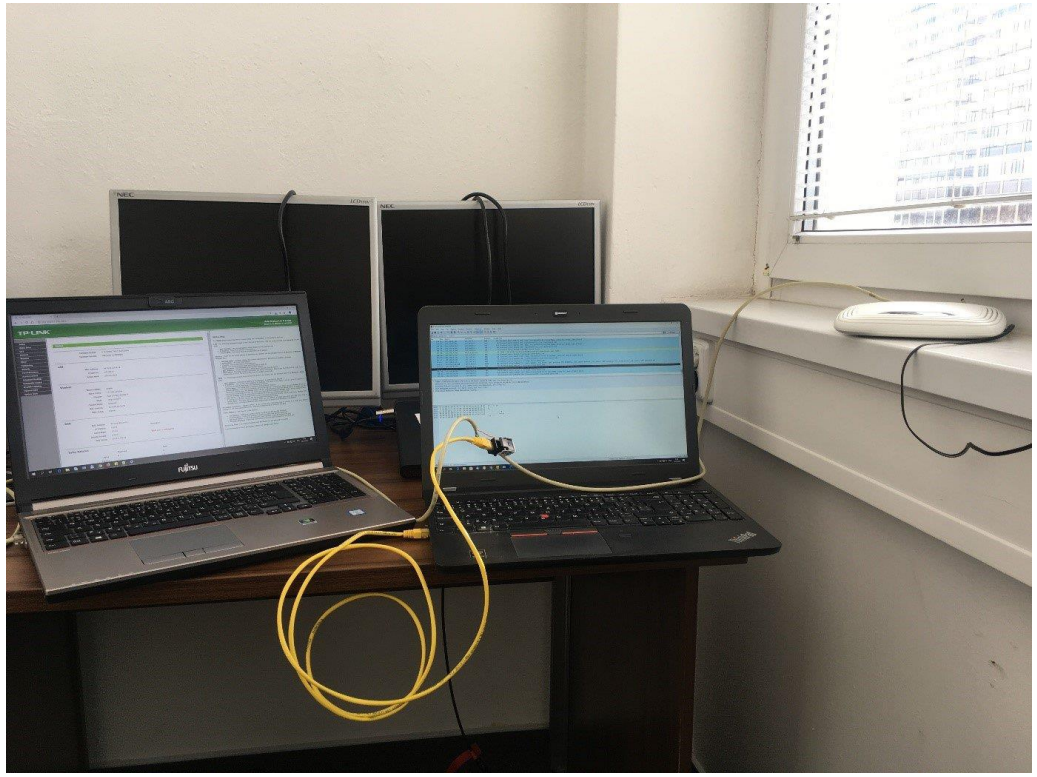
Contromisure per NCA

1. **Monitoraggio fisico:**
- Effettuare regolari ispezioni fisiche dell'infrastruttura di rete per rilevare eventuali cavi o dispositivi sospetti.
- Utilizzare telecamere di sorveglianza per monitorare le aree sensibili in cui sono presenti cavi di rete.
2. **Sicurezza fisica:**
- Limitare l'accesso fisico alle aree in cui sono presenti cavi di rete.
- Assicurarsi che i punti di accesso alla rete siano protetti da chiusure o sistemi di controllo degli accessi.
3. **Crittografia:**
- Utilizzare protocolli di crittografia per proteggere il traffico di rete.
- Ad esempio, utilizzare VPN (Virtual Private Network) per creare una connessione sicura attraverso reti non sicure.

WIRETAPPING

L’attacco consiste nell’inserire una socket a livello fisico su un cavo di comunicazione al fine di intercettare i pacchetti che transitano sul cavo di comunicazione.

https://hackinglab.cz/en/blog/wiretapping/

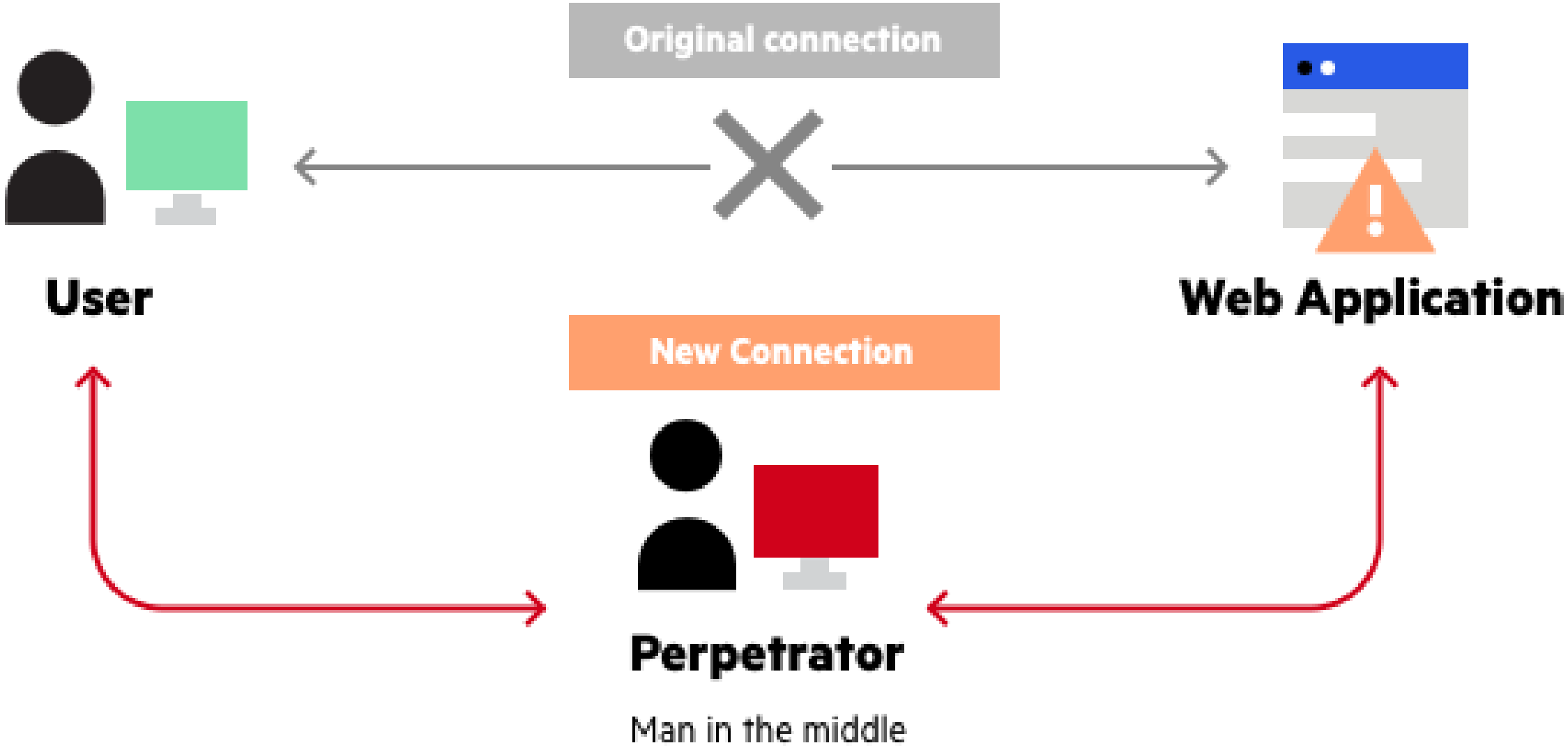


Man In the Middle

- **Il Man-in-the-Middle è un attacco informatico in cui un terzo malintenzionato si posiziona tra due parti che comunicano, intercettando e manipolando la comunicazione tra di loro.**

- *A MitM attack is a cybercrime method used to steal personal information or login credentials. Cyber criminals also use MitM attacks as a means to spy on, corrupt information, or disrupt communications between two parties.*

Man In the Middle



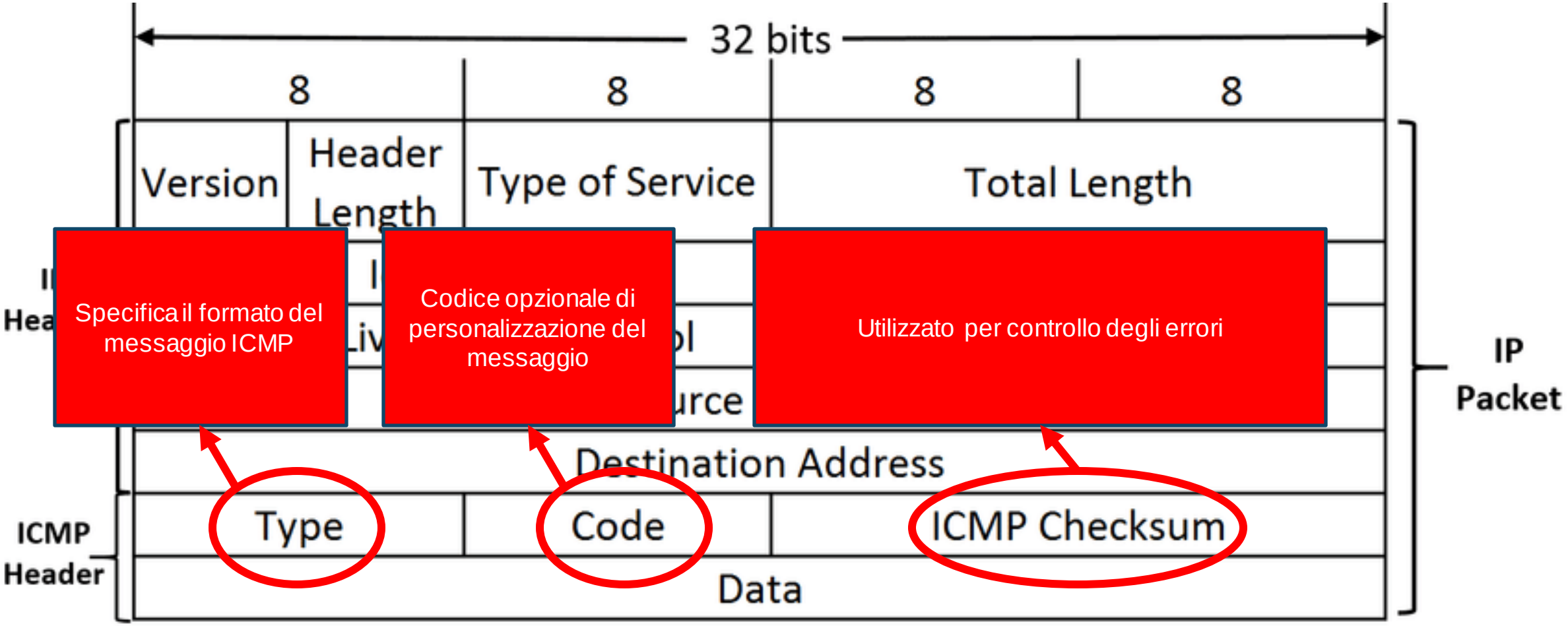
Man In the Middle con Wireshark & Ettercap

https://www.youtube.com/watch?v=DElzWHWDG9Q

ICMP

- **ICMP (Internet Control Message Protocol) è un protocollo a livello di rete («Internet» nel modello TCP/IP) che ha l'obiettivo di controllare la salute di una rete**
- **Lavora spesso unito al protocollo IP**
- **ICMP è famoso per essere usato per *ping, traceroute* ed altri tool di scansione di una rete**
- **ICMP è anche usato per causare diversi exploit quali DoS sulla banda, *ping of death, smurf attack, e ping flood***

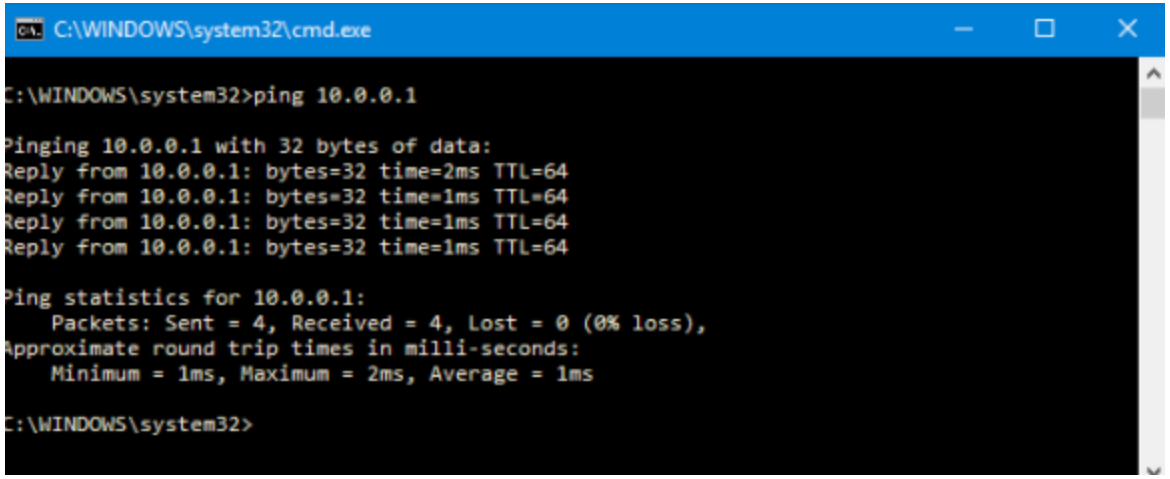
ICMP

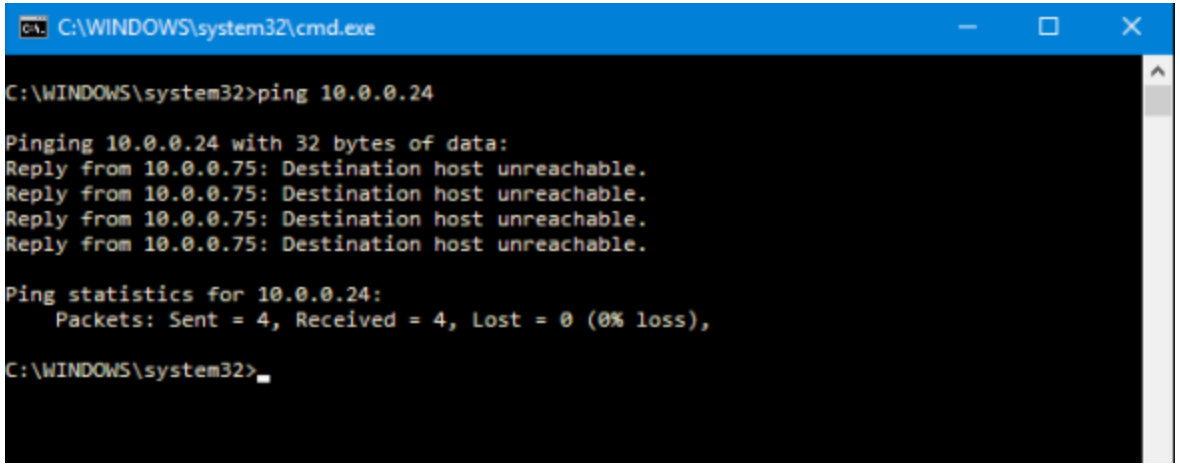

32 bits
8
8
8
8
Version
Header Length
Type of Service
Total Length
Specifica il formato del messaggio ICMP
Codice opzionale di personalizzazione del messaggio
Utilizzato per controllo degli errori
Destination Address
Type
Code
ICMP Checksum
Data
ICMP Header
IP Packet

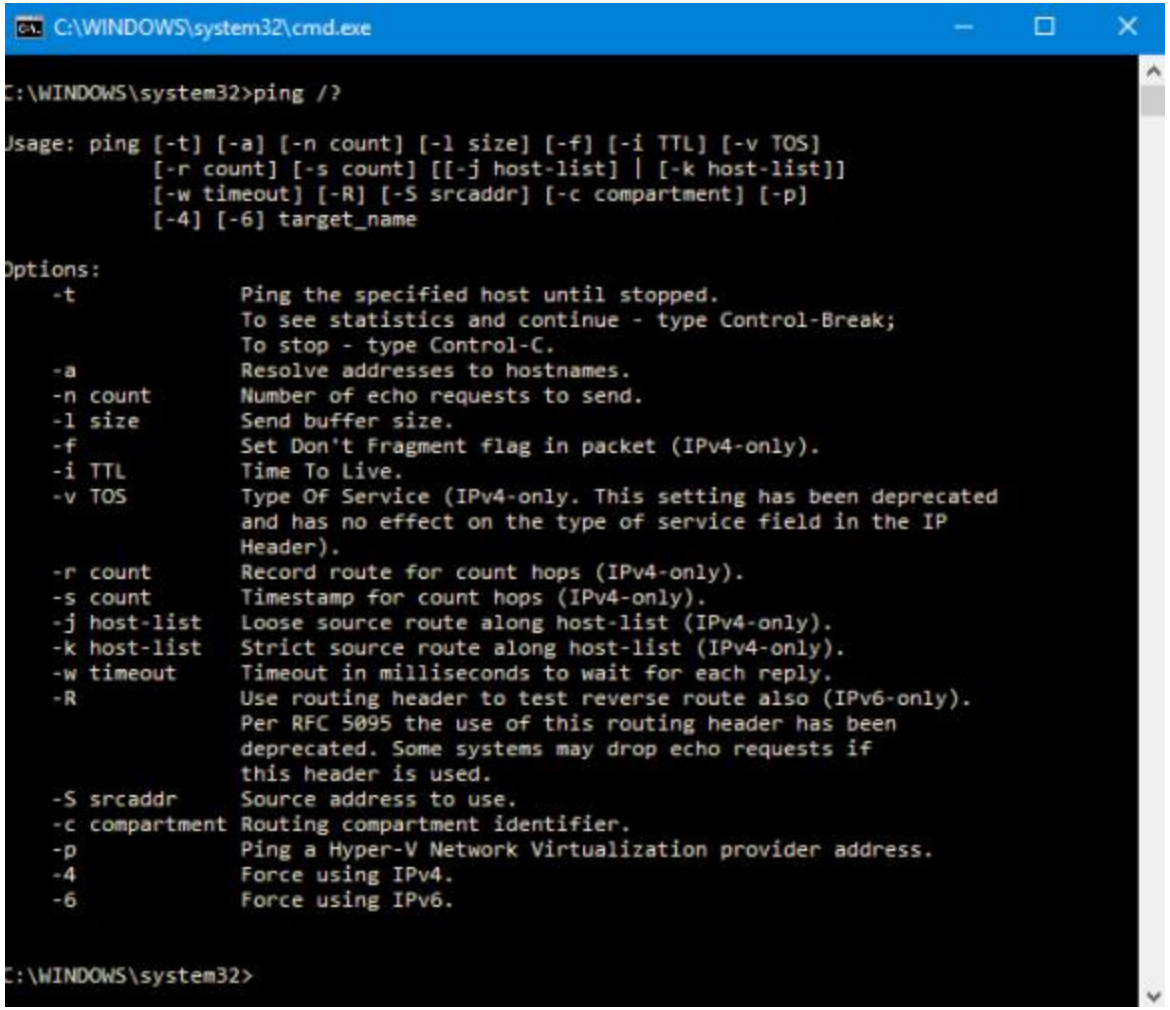
ICMP

ICMP Type	Code	Description
0	0	eco reply (to ping)
3	0	destination network unreachable
3	1	destination host unreachable
3	2	destination protocol unreachable
3	7	destination host unknown
8	0	eco request
10	0	router discovery
11	0	TTL expired

Ping


C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>ping 10.0.0.1
Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=2ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Reply from 10.0.0.1: bytes=32 time=1ms TTL=64
Ping statistics for 10.0.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\WINDOWS\system32>


C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>ping 10.0.0.24
Pinging 10.0.0.24 with 32 bytes of data:
Reply from 10.0.0.75: Destination host unreachable.
Reply from 10.0.0.75: Destination host unreachable.
Reply from 10.0.0.75: Destination host unreachable.
Reply from 10.0.0.75: Destination host unreachable.
Ping statistics for 10.0.0.24:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
C:\WINDOWS\system32>

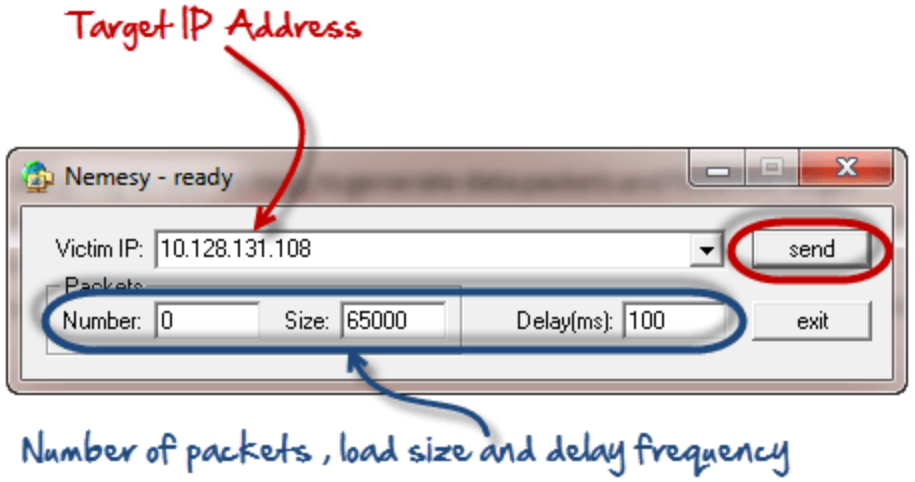

C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\system32>ping /?
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
[-r count] [-s count] [[-j host-list] | [-k host-list]]
[-w timeout] [-R] [-S srcaddr] [-c compartment] [-p]
[-4] [-6] target_name
Options:
-t Ping the specified host until stopped.
To see statistics and continue - type Control-Break;
To stop - type Control-C.
-a Resolve addresses to hostnames.
-n count Number of echo requests to send.
-l size Send buffer size.
-f Set Don't Fragment flag in packet (IPv4-only).
-i TTL Time To Live.
-v TOS Type Of Service (IPv4-only. This setting has been deprecated
and has no effect on the type of service field in the IP
Header).
-r count Record route for count hops (IPv4-only).
-s count Timestamp for count hops (IPv4-only).
-j host-list Loose source route along host-list (IPv4-only).
-k host-list Strict source route along host-list (IPv4-only).
-w timeout Timeout in milliseconds to wait for each reply.
-R Use routing header to test reverse route also (IPv6-only).
Per RFC 5095 the use of this routing header has been
deprecated. Some systems may drop echo requests if
this header is used.
-S srcaddr Source address to use.
-c compartment Routing compartment identifier.
-p Ping a Hyper-V Network Virtualization provider address.
-4 Force using IPv4.
-6 Force using IPv6.
C:\WINDOWS\system32>

Ping of death e Smurf Attack

- **Ping of death: Attacco nel quale vengono inviati pacchetti ICMP di tipo ping malformati che mandano in tilt il sistema attaccato**
- **Smurf Attack: Attacco nel quale vengono mandati innumerevoli pacchetti ping di tipo Echo Request ad un indirizzo di broadcast di una rete in modo da ottenere in risposta gli ip degli host facenti parte della rete attaccata**

Ping Flood

- **Ping flood: Attacco nel quale vengono mandati innumerevoli pacchetti ping di tipo Echo Request che sommergono di richieste il sistema attaccato. Per fare questo tipo di attacco (Qui solo per motivi di ricerca e studio!) si può usare Nemesy**

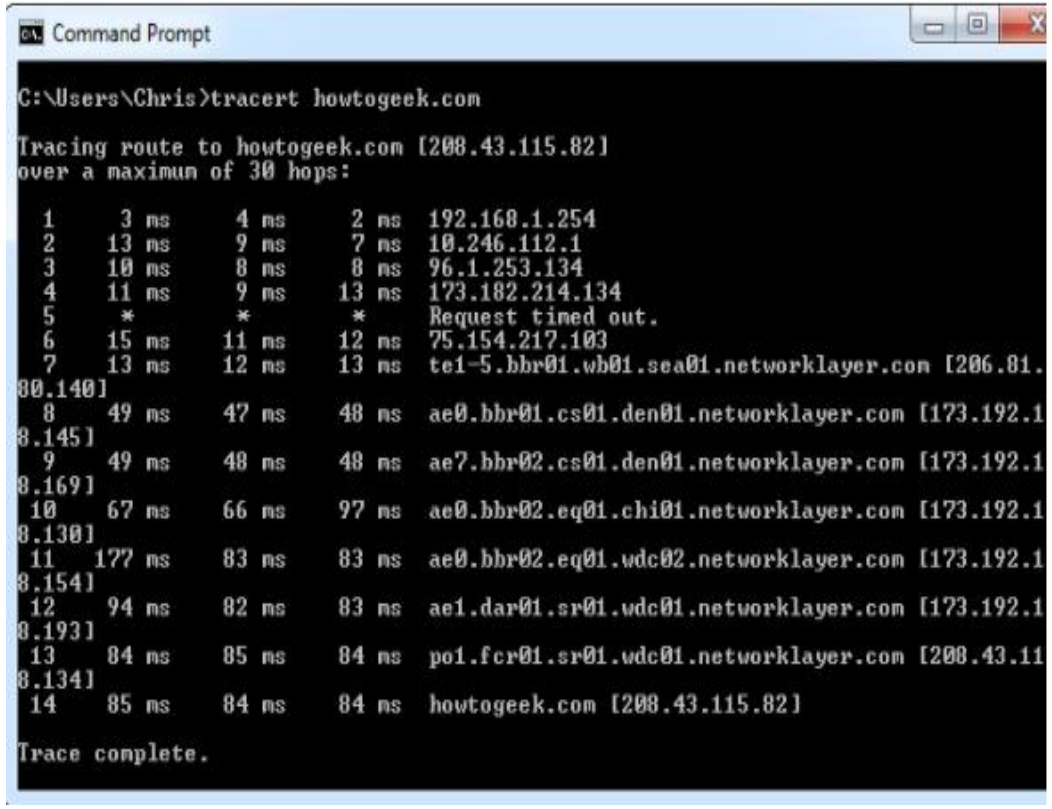


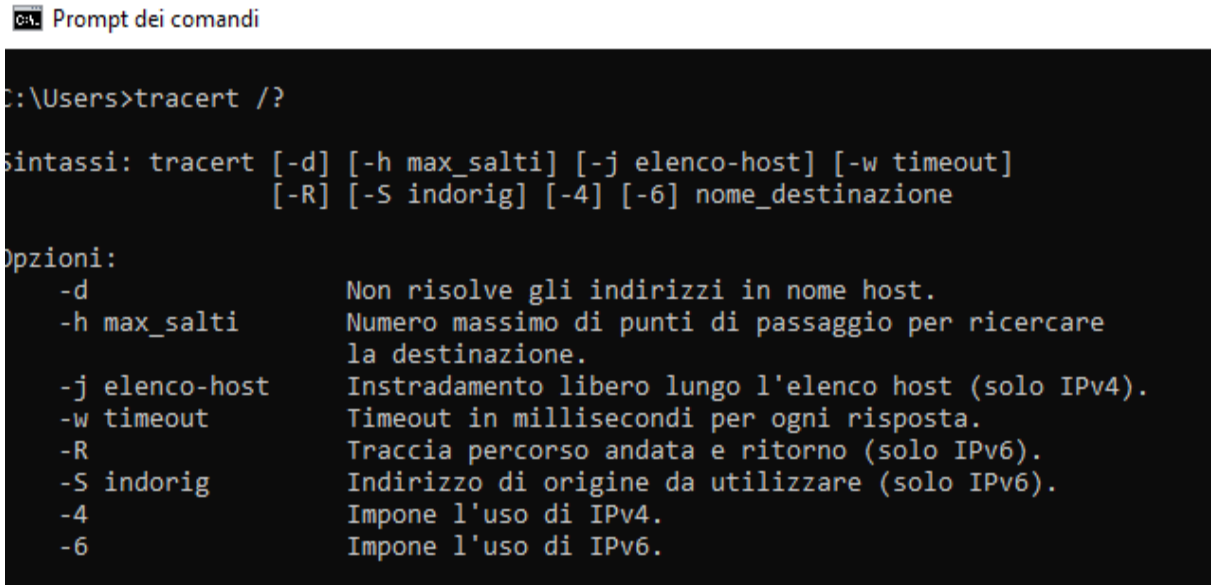
- **0 = identifica un numero di pacchetti infinito (si mandano infiniti ping) da inviare alla vittima**
- **Size = identifica quanto grandi saranno i pacchetti da inviare alla vittima**
- **Delay = identifica l'intervallo di tempo in millisecondi per ogni invio**

Contromisure a questi attacchi

- **Utilizzare firewall che filtrano il numero di pacchetti ICMP**
- **Utilizzare sonde per il controllo del traffico interno ed esterno (inbound ed outbound) delle varie reti**
- **Utilizzare SIEM che inviano alert in caso di pattern ripetuti di pacchetti uguali nella rete**

Traceroute


Command Prompt
C:\Users\Chris>tracert howtogeek.com
Tracing route to howtogeek.com [208.43.115.82]
over a maximun of 30 hops:
1 3 ms 4 ms 2 ms 192.168.1.254
2 13 ms 9 ms 7 ms 10.246.112.1
3 10 ms 8 ms 8 ms 96.1.253.134
4 11 ms 9 ms 13 ms 173.182.214.134
5 * * * Request timed out.
6 15 ms 11 ms 12 ms 75.154.217.103
7 13 ms 12 ms 13 ms te1-5.bbr01.wb01.sea01.networklayer.con [206.81.
80.140]
8 49 ms 47 ms 48 ms ae0.bbr01.cs01.den01.networklayer.com [173.192.1
8.145]
9 49 ms 48 ms 48 ms ae7.bbr02.cs01.den01.networklayer.com [173.192.1
8.169]
10 67 ms 66 ms 97 ms ae0.bbr02.eq01.chi01.networklayer.com [173.192.1
8.130]
11 177 ms 83 ms 83 ms ae0.bbr02.eq01.wdc02.networklayer.com [173.192.1
8.154]
12 94 ms 82 ms 83 ms ae1.dar01.sr01.wdc01.networklayer.com [173.192.1
8.193]
13 84 ms 85 ms 84 ms po1.fcr01.sr01.wdc01.networklayer.com [208.43.11
8.134]
14 85 ms 84 ms 84 ms howtogeek.com [208.43.115.82]
Trace complete.


Prompt dei comandi
:\Users>tracert /?
intassi: tracert [-d] [-h max_salti] [-j elenco-host] [-w timeout]
[-R] [-S indorig] [-4] [-6] nome_destinazione
pzioni:
-d Non risolve gli indirizzi in nome host.
-h max_salti Numero massimo di punti di passaggio per ricercare
la destinazione.
-j elenco-host Instradamento libero lungo l'elenco host (solo IPv4).
-w timeout Timeout in millisecondi per ogni risposta.
-R Traccia percorso andata e ritorno (solo IPv6).
-S indorig Indirizzo di origine da utilizzare (solo IPv6).
-4 Impone l'uso di IPv4.
-6 Impone l'uso di IPv6.

Attacchi ai componenti di rete

Gli attacchi ai componenti di rete (Network components attacks - NCoA) mirano a sfruttare le vulnerabilità presenti negli elementi che compongono una rete.

Tipologie di Network Components Attacks

1. **Router compromesso:**
- Gli attaccanti sfruttano le vulnerabilità o le debolezze dei router per ottenere accesso non autorizzato alla rete.
- Possono manipolare le impostazioni di routing, intercettare il traffico o eseguire altri attacchi all'interno della rete.

2. **Switch compromesso:**
- Gli attaccanti prendono il controllo di uno o più switch di rete per intercettare il traffico o eseguire attacchi di tipo "man-in-the-middle".
- Possono anche effettuare attacchi di spoofing o manipolare la configurazione di rete.

3. **Access Point (AP) compromesso:**
- Gli attaccanti sfruttano le vulnerabilità degli access point wireless per ottenere accesso non autorizzato alla rete.
- Possono intercettare il traffico wireless, eseguire attacchi di spoofing o rubare informazioni sensibili.

Tipologie di Network Components Attacks

4. **Attacco al server DNS:**
- Un attaccante sfrutta una vulnerabilità nel server DNS per manipolare le risposte DNS inviate ai client.
- Questo può indirizzare i client verso siti web malevoli o consentire all'attaccante di intercettare il traffico di rete.

5. **Attacco al firewall:**
- Un attaccante sfrutta una vulnerabilità nel firmware o nelle configurazioni del firewall per bypassare le regole di sicurezza o ottenere accesso non autorizzato alla rete interna.
- Una volta compromesso il firewall, l'attaccante può eseguire attacchi diretti alla rete interna o intercettare il traffico di rete.

Conseguenze dei NCoA

- **Interruzione del servizio:** gli attaccanti possono causare interruzioni nella connettività di rete o nel funzionamento dei servizi.
- **Furto di dati:** gli attaccanti possono ottenere accesso a informazioni sensibili o riservate presenti nella rete.
- **Manipolazione del traffico:** possono alterare o iniettare dati maligni nel flusso di traffico di rete.

Contromisure per NCoA

1. **Aggiornamenti del firmware:**
- Mantenere costantemente aggiornati i router, gli switch e gli access point con le ultime patch di sicurezza.

2. **Autenticazione e autorizzazione:**
- Utilizzare password forti e complesse per accedere ai dispositivi di rete.
- Impostare correttamente i permessi di accesso per evitare accessi non autorizzati.

3. **Monitoraggio del traffico di rete:**
- Implementare strumenti di monitoraggio del traffico per identificare attività sospette o anomalie.
- Rilevare tempestivamente gli attacchi e intraprendere azioni correttive.

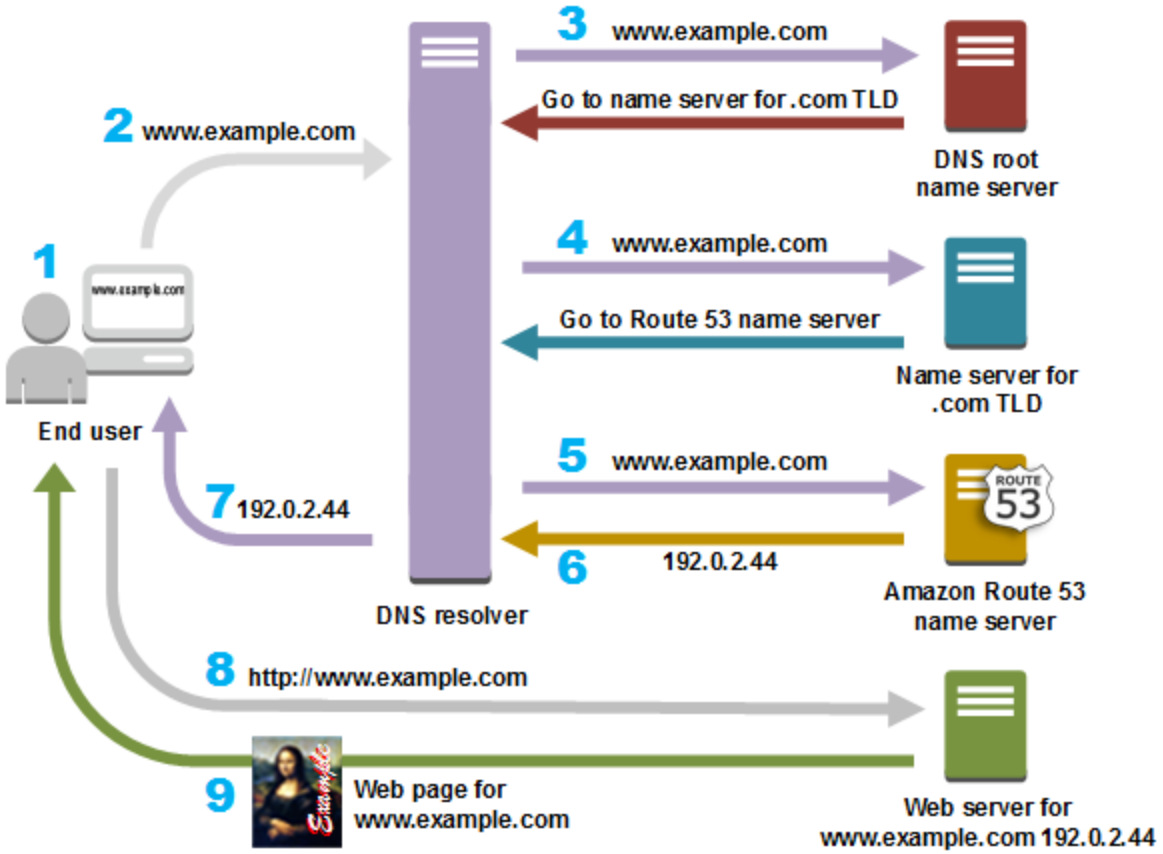
DNS – Domain Name System

- **Il livello applicazione ha l'obiettivo di interfacciarsi con gli utenti, dunque bisogna cercare di rendere le cose facili**
- **E' molto più semplice ricordare www.google.com piuttosto che 64.233.187.99**
- **Questo è il motivo per cui è stata sviluppata la traduzione degli indirizzi. Il Domain Name System (DNS)**

Domain Name	www.google.com
IP address	64.233.187.99
MAC address	Aa:bb:cc:ff:11

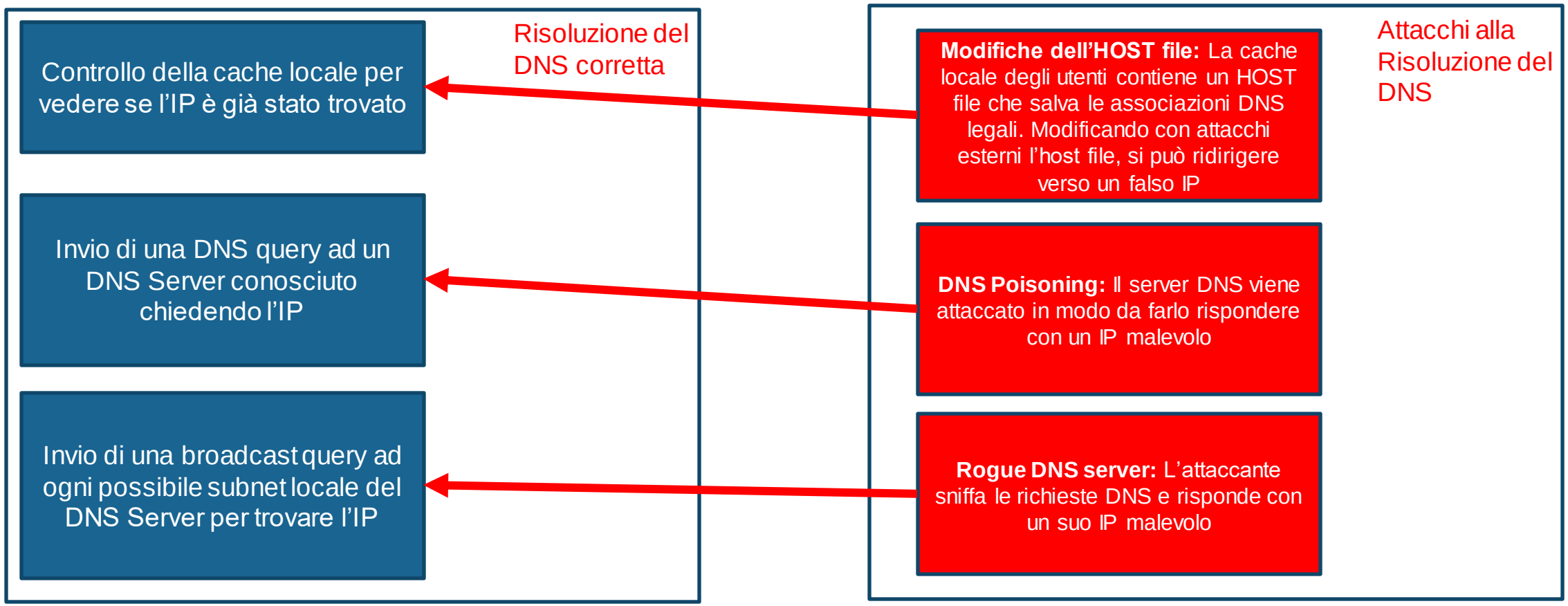
Il funzionamento del DNS

Il DNS (Domain Name System): traduce nomi comprensibili come **www.amazon.com** in indirizzi IP utilizzati dai computer **(ad esempio 192.0.2.44).**



Attacchi al DNS

- **Attacco che crea una falsificazione del DNS in modo da ridirigere un client verso un IP non desiderato.**



Wireless Network

- **La rete wireless attualmente costituisce il tipo di collegamento più usato in quanto facile da installare ed a basso costo.**

- **Un rete wireless è una rete con collegamento «Wire» = Filo, «Less» = Senza**

- **Il collegamento wireless è possibile grazie a quella che viene detta *Data Emanation* ovvero la trasmissione di dati attraverso dei segnali elettromagnetici. Questi segnali elettromagnetici si hanno attraverso il movimento degli elettroni il quale crea dei campi magnetici. Leggendo questi campi magnetici è possibile riprodurre il flusso di elettroni originale. Se il flusso di elettroni originale è stato usato per comunicare dei dati, allora il flusso ri-creato di elettroni è una ri-creazione dei dati originali e quindi fa si che possa essere usato per la comunicazione**

Le reti wireless soffrono delle stesse vulnerabilità, threat e rischi delle reti cablate con, in aggiunta, l’eavesdropping, nuove forme di packet sniffing e di intrusioni

Rete wireless - Terminologia

- **Wireless device:** Periferica che si connette ad un wireless access point
- **Wireless access point:** Punto di accesso per la connessione degli wireless devices
- **Wireless Cell:** Area entro la quale è possibile connettere un wireless device ad un wireless access point

- **SSID (Service Set Identifier):** indica il nome della rete wireless. Due tipi di SSID: ESSID e BSSID. **ESSID**: è il nome della rete wireless quando viene usato il WAP (Wireless access point). **BSSID**: MAC address della base station che utilizza l'ESSID, utilizzato per connettere più access point allo stesso ESSID.

802.11x

- **802.11:** IEEE standard per le comunicazioni wireless di rete. Cambia il numero in base alla versione ed alla velocità e frequenza di comunicazione ammessa

Amendment	Speed	Frequency
802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	200+ Mbps	2.4 GHz or 5 GHz
802.11ac	1 Gbps	5 GHz

Securizzare l'SSID

- **Se un client wireless conosce l'SSID, questo può configurare la sua scheda di rete per comunicare con il WAP (Wireless Access point)**
- **Molti SSID sono spesso definiti dai vendor e standardizzati (quindi spesso facilmente ricavabili)**
- **È altamente consigliato cambiare l'SSID fornito dal Vendor (nome della rete) perché potrebbe dare notevoli informazioni ad un attaccante (Vendor della rete, password di default ecc…)**
- **L'SSID inoltre viene comunicato ai vari device attraverso una transazione chiamata beacon frame, questo broadcast può essere disabilitato per rendere la rete wi-fi nascosta**

Protocolli di cifratura del wireless

- **L'IEEE 802.11** definisce due metodi che possono usare i client wireless per autenticarsi ad un WAP: **l'open system authentication (OSA) e la shared key authentication (SKA).**

- **OSA indica protocolli senza autenticazione e quindi reti wireless aperte a tutti**

- **SKA prevede l'implementazione di protocolli di cifratura ed autenticazione (WEP, WPA, WPA2) sulle reti wireless**

WEP

- **WEP (Wired equivalent privacy) è introdotto nello standard IEEE 802.11 come primo protocollo SKA.**

- **Il protocollo WEP ha l'obiettivo di garantire lo stesso livello di protezione di una rete cablata ed ha meccanismi anti- packet sniffing ed eavesdropping.**

- **WEP utilizza una chiave predefinita e condivisa. La chiave generata è statica e viene scambiata tra tutti gli access point ed i devices che si connettono a questi. Questa chiave è utilizzata per cifrare i pacchetti prima dell'uscita dall'access point e per decifrarli sui devices. Viene usato un valore di hash nei pacchetti per verificarne l'integrità.**

- **WEP è basato su RC4 (Rivest Cypher) e si decifra in meno di 1 minuto con un attacco a forza bruta, intercettando il pacchetto contenente la chiave che si scambiano WAP e devices.**

WPA

- **WPA (Wi-Fi protected access) nasce per sostituire il WEP. Ad oggi, è ancora usato!**

- **WPA è basato su LEAP (authentication framework che implementa MD-5 per la cifratura, sviluppato da Cisco) e TKIP (Temporal Key Integrity Protocol: La chiave di cifratura viene mischiata con un vettore di inizializzazione prima di usare RC4 per la cifratura) ed offre una passphrase segreta per l'autenticazione**

- **Leap è attaccabile attraverso un tool denominato «ASLEAP» e TKIP è attaccabile con un tool chiamato «coWPAtty» in pochi secondi**

- **Poiché sia Leap che TKIP sono attaccabili allora anche WPA è facilmente attaccabile!**

WPA2

- **WPA2 nasce per risolvere i problemi di attaccabilità di WPA**
- **Sfrutta un nuove schema di autenticazione detto Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) basato su AES (Cifrario a blocchi)**
- **Nel 2017 è stata trovata una falla in WPA2 poiché questo permetteva il riuso di password (attacco KRACK (Key reinstallation Attack)) che è stato prontamente «fixed» nelle nuove versioni**
- **Attualmente è l'unico protocollo di autenticazione sicuro su WI-FI!**

Attacchi noti alle reti WI-FI

- **War Driving:** **Si utilizzano tool di scanning dei wi-fi per individuare reti nascoste. È utilizzato perché spesso le reti nascoste sono aperte e si pensa di proteggerle proprio nascondendole……ERRATO!!!!**

- **War Chalking:** **Evoluzione del War Driving usato nei primi anni di sviluppo del wireless (1997-2002). Veniva effettuato un war driving per identificare le reti nascoste ed aperte, poi veniva usato un dispositivo collegato alla rete nascosta aperta per fare da WAP sulla rete nascosta ad altri dispositivi**

- **Rogue Wireless Access point:** **Un attaccante crea un Access Point accessibile a tutti con un nome simile a quello di un WAP autentico (Es. se l'autentico è «ABCcafe», un rogue wap potrebbe avere nome «ABCcafe-LTE») che agisce ad una frequenza diversa da quello autentico, in modo da indurre le persone a connettersi ed effettuare eavesdropping degli utenti connessi**

Securizzare una rete WI-FI (Consigli)

- **Securizzare l'SSID: Disabilitare il broadcast nel bacon frame; Cambiare l'SSID di default del vendor e la sua password di autenticazione**
- **Nascondere l'SSID**
- **Utilizzare WPA2/PSK per la cifratura delle chiavi e l'autenticazione della password immettendo una password composta di lettere, simboli, caratteri speciali e di minimo 14 caratteri**
- **Cambiare la password ogni 2-3 mesi per evitare attacchi a forza bruta**
- **Disabilitare il WPS (Alcuni router hanno il WPS, un codice di 4 cifre o un pulsantino fisico sul retro che permette l'autenticazione diretta senza PWD, bypassando il WPA2/PSK)**

Un attacco wireless in pratica

L’attacco ci mostra come attraverso un adattatore si è in grado di intercettare il traffico di una rete, disconnettere i dispositivi connesse, colpire l’handshake ed ottenere la password con un forza bruta

https://youtu.be/WfYxrLaqlN8?si=TWKgTo251PjE7Buo

Bluetooth

- **Il Bluetooth (IEEE 802.15, PAN) rappresenta un altro standard di rete molto importante ed utilizzato nella società attuale**
- **Molti oggetti quali cuffie, mouse, tastiere, dispositivi GPS sono connessi attraverso questa tecnologia**
- **La tecnologia in realtà è una rete wireless che lavora ad una frequenza radio di 2.4GHZ ed utilizza, una volta individuato il dispositivo da accoppiare, un PIN per autorizzare il «pairing»**
- **Anche questa tecnologia è suscettibile a parecchi attacchi**

Attacchi al Bluetooth

- **Blue Snarfing:**
  Tecnica in grado di dare accesso in terminale Bluetooth permettendo la copia di dati dal dispositivo.
  L'attacco è praticabile sia nel caso di un bluetooth visibile sia nel caso di un bluetooth "nascosto".
  Il protocollo colpito è denominato Object Exchange Protocol (OBEX), e serve per inviare e ricevere file tra dispositivi. Un tool molto utilizzato in questi casi è btscanner (Kali) creato per prelevare le maggiori informazioni da un dispositivo bluetooth.

- **BlueBug:**
  Un Attacco BlueBug si effettua sfruttando un noto bug del servizio in questione.
  Grazie a questa tecnica è possibile ottenere il controllo di un cellulare sfruttandolo per inviare e leggere SMS, per effettuare chiamate,vedere video,foto,e tanto altro… L'attaccante deve trovarsi in un raggio di 10 m dalla vittima.

- **BlueSmack:**
  Identico al famigerato "Ping of Death" il Bluesmack è in grado di mettere fuori combattimento un dispositivo Bluetooth.

- **Blue Snarf++:**
  Tipologia di attacco BlueSnarf a cui sono vulnerabili però solo alcuni device Bluetooth. La particolarità di questo bug consiste nella possibilità, da parte dell'attaccante, di avere a disposizione il filesystem con permessi di scrittura e lettura.

- **https://hackrz.wordpress.com/2010/02/06/tools-for-hacking-bluetooth-enabled-devices/**

VoIP

- **Il VoIP è una tecnologia che incapsula l'audio all'interno di pacchetti IP per inserire le comunicazioni all'interno della pila TCP/IP basato su RTP (Real-Time Protocol)**

- **Fare molta attenzione alle soluzioni VoIP scelte: alcuni sistemi VoIP sono essenzialmente comunicazioni di pacchetti plain-form (SENZA ALCUNA CIFRATURA) che possono essere facili da intercettare**

- **I principali attacchi al VoIP sono:**
  - **Caller ID: Esistono tool che falsificano il Caller ID sul VoIP e quindi permettono ad un attaccante di fare attacchi vishing (VoIP phishing)**
  - **Attacchi al firmware del sistema VoIP: spesso il sistema VoIP ha falle nel firmware e viene attaccato all'origine**
  - **Man in The Middle: Se la comunicazione non è cifrata si verificano attacchi di man in the middle**
  - **https://hakin9.org/voip-hacking-techniques/**

- **Il nuovo protocollo SRTP (secure RTP) è attualmente l'unico protocollo ritenuto sicuro per VoIP**

John The Ripper per Brute Force

- **Obiettivo dell’attacco è quello di provare tutte le combinazioni per ricavare una Pwd. In questo video si mostrano le funzionalità di John The Ripper per un Brute Force su pwd ZIP e di sistema di test.**

https://www.youtube.com/watch?v=nV2HEU7HldY


Grazie per l’attenzione