CYBER SECURITY

Intelligence – Acquisizione di informazioni

COME SI SVOLGE UN ATTACCO? ➔ IT

1. Scoprire quali macchine/servizi ci sono "in giro" ➔ Scansione attiva;
   - per es., usando http://nmap.org/
2. Intercettazione del traffico;
   - per es., usando https://www.wireshark.org/
3. Ingegneria sociale: ottenere informazioni sfruttando meccanismi sociali
4. …
5. Trovare le vulnerabilità (già note);
   - per es., usando http://www.metasploit.com/ e http://www.exploit-db.com/
6. Sferrare l'attacco

- Esistono distribuzioni di Linux già belle e pronte con tutti gli strumenti a portata di mano. La più famosa è Kali https://www.kali.org/

Hacking etico - Ricognizione

- La ricognizione è un insieme di processi e tecniche (impronta digitale, scansione ed enumerazione) utilizzati per scoprire e raccogliere informazioni di nascosto su un sistema di destinazione.
- Durante la ricognizione, un hacker etico tenta di raccogliere quante più informazioni possibili su un sistema di destinazione, seguendo i sette passaggi elencati di seguito:
  - Raccogli le informazioni iniziali
  - Determina l'intervallo di rete
  - Identifica le macchine attive
  - Scopri porte aperte e punti di accesso
  - Impronta il sistema operativo
  - Scopri i servizi sui porti
  - Mappa la rete

COME SI TROVANO LE INFO ?

Acquisizione del maggior numero di info possibile per identificare possibili punti deboli.

Discipline di raccolta da Wikipedia

Le principali discipline (alcune in realtà consistono più che altro nell'elaborazione di dati grezzi acquisiti in precedenza) in questo campo sono:

1. Human Intelligence (HUMINT)
2. Intelligence delle immagini (IMINT)
3. Intelligence dei segnali (SIGINT = COMINT + ELINT)
4. Intelligence delle misurazioni e delle caratteristiche (MASINT)
5. Intelligence tecnica (TECHINT)
6. Intelligence delle fonti libere (Open Source) (OSINT)

QUALI INFORMAZIONI SONO DISPONIBILI PER GLI HACKER?

PII - Informazioni Personalmente Identificabili.

- Questo include il vostro nome, indirizzo e-mail, codice fiscale, data di nascita, cartelle cliniche, pagelle scolastiche, dati lavorativi.
- In questo tipo di dati c'è una miniera di informazioni che gli hacker potrebbero usare per rubare la vostra identità.
- Potrebbero includere i dettagli di un acquisto su Amazon, o un investimento fatto con un broker online. Tutte queste informazioni private potrebbero venire sfruttate per compromettere anche altri account che avete online.

QUALI INFORMAZIONI SONO DISPONIBILI PER GLI HACKER?

- E-mail, SMS e messaggi istantanei vengono tutti conservati in qualche server, da qualche parte.
- Nelle vostre e-mail potrebbero esserci un bel po' di informazioni che non volete rendere pubbliche, come documenti commerciali riservati, lettere d'amore, dettagli dei vostri conti bancari.
- Gli hacker saranno anche interessati ai vostri contatti, perché se riescono a impossessarsene possono mandar loro e-mail di phishing.

Quali informazioni sono disponibili per gli hacker?

- I vostri dati di navigazione includono cookie, registri del provider Internet e plugin del browser che potrebbero archiviare informazioni. Sono utili per gli inserzionisti e, con l'avvento di Big Data, potrebbero essere ancora più utili di quanto pensiate.
- Forse, spesso usate Skype per fare chiamate o videoconferenze. Siete sicuri che nessuno vi stia ascoltando di nascosto?

IL DATA BREACH

Nel dettaglio, le informazioni che possono essere ricercate, da esperti in sicurezza informatica o possibili criminal hacker, sono:

- e-mail personali ed aziendali;
- password usate in servizi terzi (Dropbox, Shein, social network o i provider mail stessi);
- nomi e cognomi e username;
- numeri di telefono;
- indirizzi IP e di abitazioni.
- …

Hacking etico - Ricognizione

- La ricognizione è un insieme di processi e tecniche (impronta digitale, scansione ed enumerazione) utilizzati per scoprire e raccogliere informazioni di nascosto su un sistema di destinazione.
- Durante la ricognizione, un hacker etico tenta di raccogliere quante più informazioni possibili su un sistema di destinazione, seguendo i sette passaggi elencati di seguito:
  - Raccogli le informazioni iniziali
  - Determina l'intervallo di rete
  - Identifica le macchine attive
  - Scopri porte aperte e punti di accesso
  - Impronta il sistema operativo
  - Scopri i servizi sulle porte
  - Mappa la rete

Tools per Hacking

- Google Hacking Database (GHDB)
- Nslookup
- Traceroute
- Ping
- Whois
- Harvester
- Social networking.

https://haveibeenpwned.com/

Ethical Hacking – Scanning

- **Scansione attiva**: Questo metodo implica l'invio di pacchetti alla rete di destinazione e l'analisi delle risposte per identificare i dispositivi attivi e i servizi in esecuzione. Un esempio di strumento utilizzato per la scansione attiva è **Nmap**.
- **Intercettazione del traffico**: Questo metodo prevede la cattura e l'analisi del traffico di rete per identificare i dispositivi e i servizi attivi. **Wireshark** è uno degli strumenti più comuni utilizzati per questa tecnica1.
- **Fingerprinting**: Determinare quale sistema operativo è in esecuzione su un computer remoto. Questo può essere fatto in modo attivo, inviando richieste al sistema remoto, o in modo passivo, sniffando il traffico proveniente dal sistema stesso.
- **Enumerazione**: Scoprire i servizi sui porti e mappare la rete per identificare i punti di accesso e le vulnerabilità.

Ethical Hacking - Footprinting

Durante questa fase, un hacker può raccogliere le seguenti informazioni –

- Nome del dominio
- Indirizzi IP
- Spazi dei nomi
- Informazioni sui dipendenti
- Numeri di telefono
- E-mail
- Informazioni sul lavoro

http://www.whois.com/whois
Ping www.google.com
https://www.ip2location.com/
https://www.arin.net/
https://archive.org/

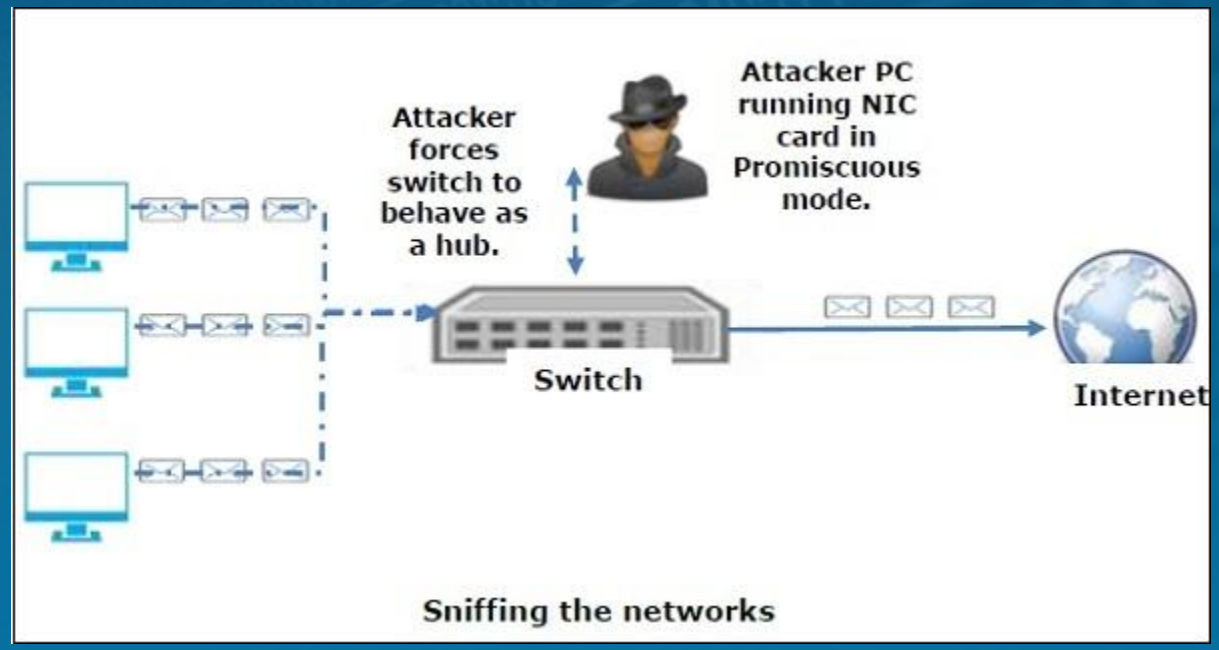
Ethical Hacking - Fingerprinting

- determinare quale sistema operativo è in esecuzione su un computer remoto
- ATTIVO ➔ invia richieste al sistema remoto
  - Scansione delle porte aperte
  - Scansione dei servizi attivi
  - Enumerazione dei DNS
- PASSIVO ➔ una volta in rete 'sniffa' il traffico proveniente dal sistema stessa

ETHICAL HACKING - SNIFFING

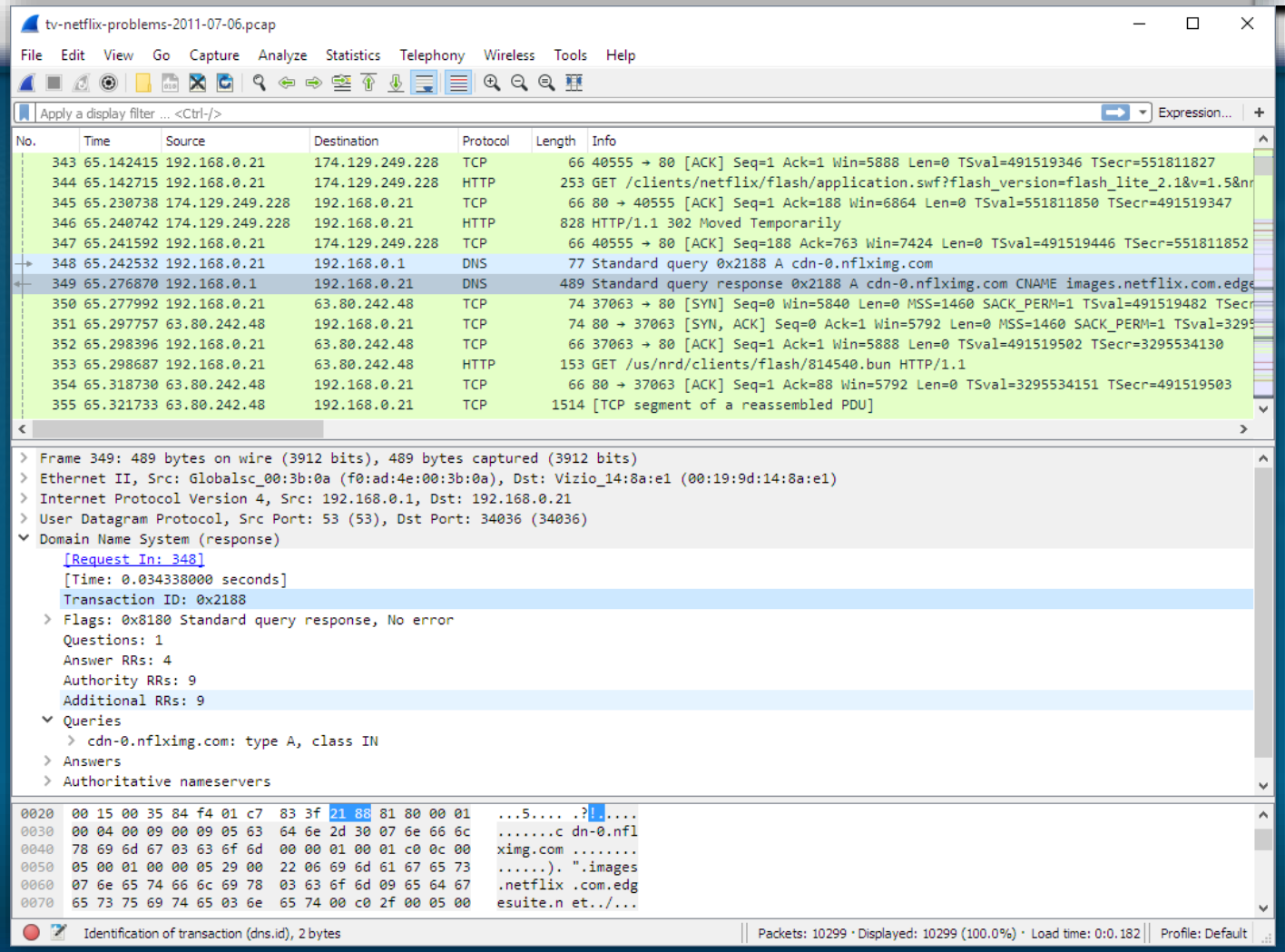
Si possono 'annusare' le seguenti informazioni sensibili da una rete

- Traffico di posta elettronica
- Password FTP
- Traffico web
- Password Telnet
- Configurazione del router
- Sessioni di chat
- Traffico DNS



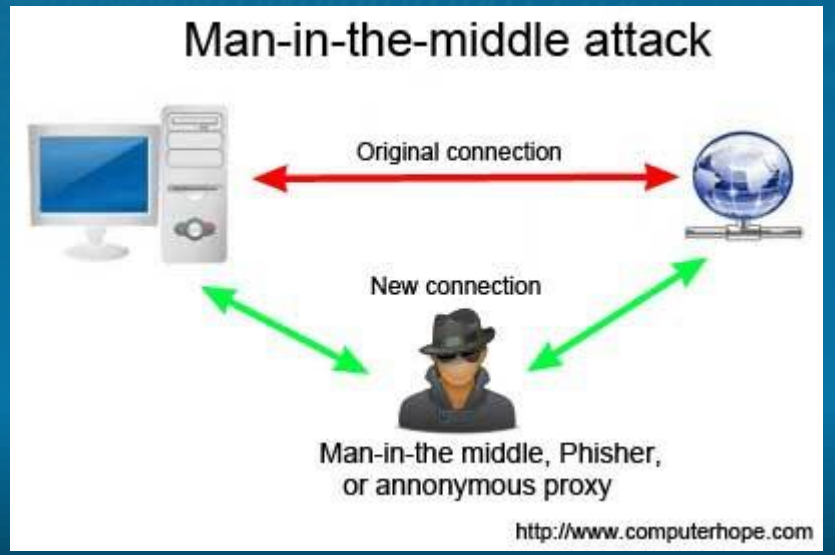
Ethical Hacking – Sniffing Tools

- BetterCAP
- Ettercap
- Wireshark
- Tcpdump
- WinDump
- OmniPeek
- Dsniff
- EtherApe
- MSN Sniffer
- NetWitness NextGen



Ethical Hacking - ARP Poisoning

- **ARP Spoofing**
  - I pacchetti ARP (Address Resolution Protocol) possono essere falsificati per inviare dati alla macchina dell'attaccante.
- **MITM**
  - L'attacco Man-in-the-Middle (abbreviato MITM, MitM, MIM, MiM, MITMA) implica un attacco attivo in cui l'avversario impersona l'utente creando una connessione tra le vittime e invia messaggi tra di loro



COME SI SVOLGE UN ATTACCO? ➔ IT

3. **Ingegneria sociale: ottenere informazioni sfruttando meccanismi sociali**
   Ricognizione Passiva

- Spesso basta chiedere: in un sondaggio il 70% delle persone ha rivelato la (propria?) password in cambio di una barretta di cioccolato! http://news.bbc.co.uk/2/hi/technology/3639679.stm
- Pennette USB "dimenticate" nel parcheggio https://www.schneier.com/crypto-gram/archives/2006/0615.html#6
- SPAM (posta indesiderata)/phishing con cose del tipo:
  - Attività sospetta sul suo account Pinco-Pallo, cambia subito la password cliccando QUI…
  - Il tuo computer ha un virus! Scarica il NOSTRO antivirus
  - E' morto . . . , clicca QUI per vedere le foto/video/. . .
    - Per esempio, nel 2013 Totti TOTTI
  - collegamenti a siti che richiedono di installare software o "codec" per vedere un video, una cartolina, ricevere una suoneria, . . . nel 99.9% dei casi, si tratta di trojan

COME SI SVOLGE UN ATTACCO? ➔ IT

3. Ingegneria sociale: ottenere informazioni sfruttando meccanismi sociali

- telefonate dalla "reception" che chiedono informazioni (per es.: carta di credito, di identità, informazioni personali)
- wifi (di "hotel", "aeroporti", . . .) aperte
- ordinare una pizza (pagando con carta di credito), grazie al volantino che qualcuno vi ha fatto passare sotto la porta
- postazioni di ricarica (spesso la porta `e una USB)
  - http://krebsonsecurity.com/2011/08/beware-of-juice-jacking/

. . .

http://www.10news.com/money/consumer/thieves-develop-new-way-to-get-credit-card-numbers-at-hotels

La Geolocalizzazione

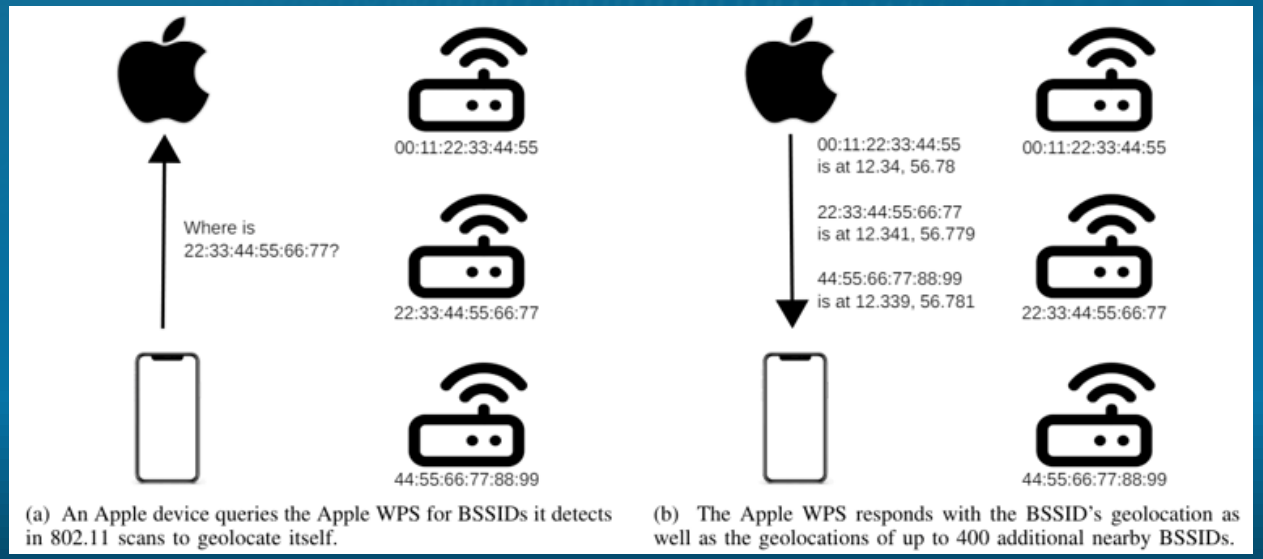
- **Servizi Geo dei dispositivi**: Questi servizi utilizzano vari sensori e tecnologie integrate nei dispositivi mobili per determinare la posizione geografica. Ad esempio, i dispositivi possono utilizzare il GPS, il Wi-Fi e le reti cellulari per ottenere una posizione precisa1.
- **Localizzazione tramite gli hotspot WiFi**: Questo metodo sfrutta la presenza di hotspot WiFi per determinare la posizione di un dispositivo. I dispositivi possono rilevare gli hotspot nelle vicinanze e utilizzare queste informazioni per calcolare la propria posizione1.
- **WPS (Wi-Fi-Based Positioning Systems)**: Questi sistemi utilizzano i segnali WiFi per determinare la posizione di un dispositivo. I dispositivi inviano i segnali ricevuti da vari punti di accesso a un server di posizionamento, che utilizza un database di impronte digitali per calcolare la posizione2.

La Geolocalizzazione

- **GPS (Global Positioning System)**: Il sistema GPS è uno dei metodi più comuni e precisi per la geolocalizzazione. Utilizza una rete di satelliti in orbita attorno alla Terra per determinare la posizione di un dispositivo con un'accuratezza di pochi metri3.
- **GLONASS**: Simile al GPS, GLONASS è un sistema di navigazione satellitare sviluppato dalla Russia. Funziona in modo simile al GPS e può essere utilizzato in combinazione con esso per migliorare la precisione4.
- **Localizzazione tramite le celle della rete telefonica cellulare**: Questo metodo analizza la potenza del segnale radio di ogni cella telefonica in relazione alla rispettiva stazione radio base per determinare la distanza del dispositivo da questa4.
- **Localizzazione tramite la rete WiFi o WLAN**: Questo metodo utilizza il segnale delle diverse fonti WiFi per determinare la posizione di un dispositivo4.
- **Localizzazione tramite l'indirizzo IP**: Questo metodo utilizza l'indirizzo IP della rete Internet del dispositivo per determinare la posizione geografica

SE UTILIZZATE UN HOTSPOT WIFI POTRESTE ESSERE TRACCIATI … OVUNQUE !

WPS, Wi-Fi-Based Positioning Systems



(a) An Apple device queries the Apple WPS for BSSIDs it detects in 802.11 scans to geolocate itself.

(b) The Apple WPS responds with the BSSID's geolocation as well as the geolocations of up to 400 additional nearby BSSIDs.