CYBER SECURITY

Modalita’ di attacco

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/

COME SI SVOLGE UN ATTACCO? ➔ IT

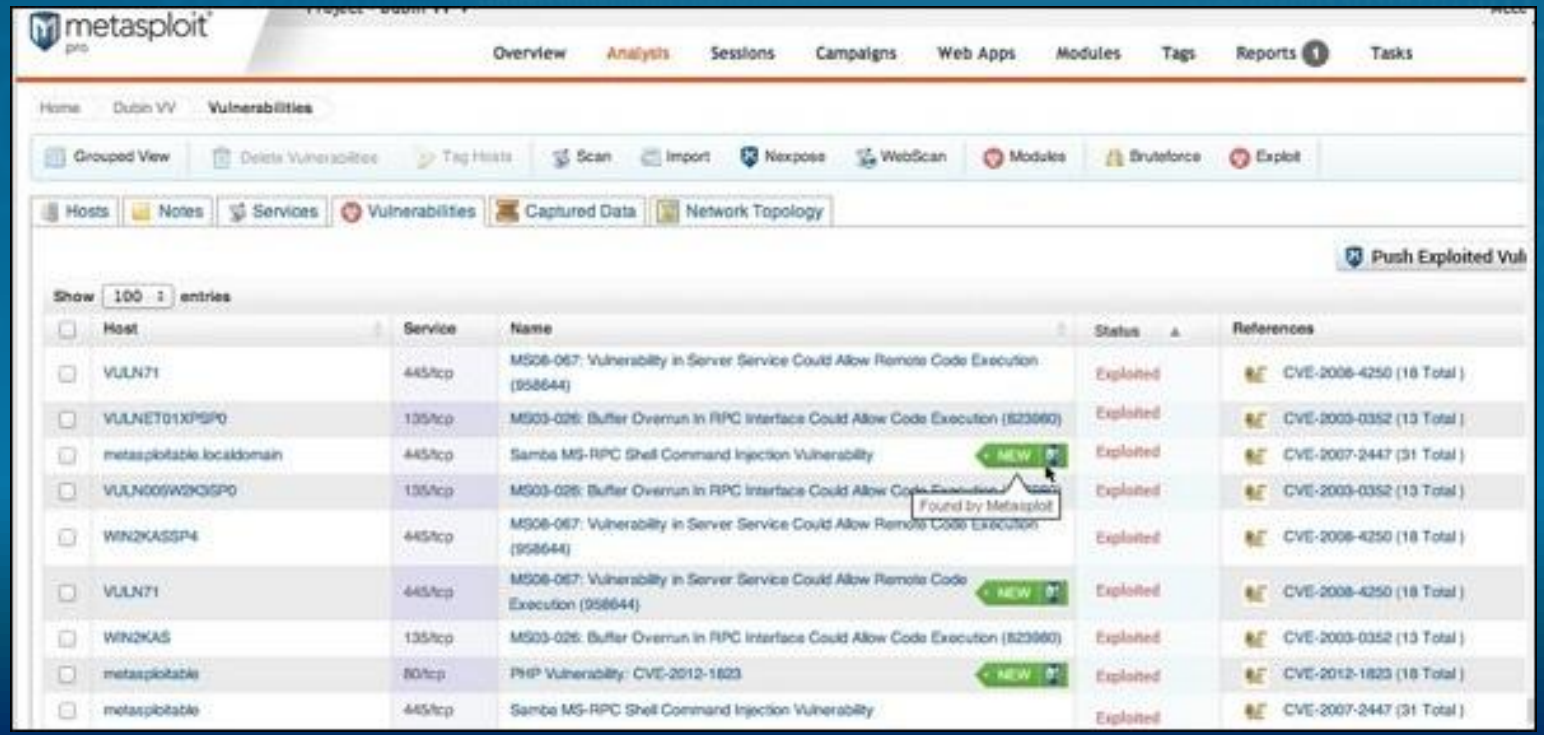
FASE 2: LA FORZATURA…

1. Cerchiamo dei bug
2. Fra questi, qualcuno potrebbe essere una vulnerabilità
3. Scriviamo un exploit che la sfrutti, per causare il comportamento voluto (dall'attaccante!)

https://it.wikipedia.org/wiki/Categoria:Tecniche_di_attacco_informatico

Ethical Hacking - Exploitation

- Ricerca di vulnerabilità
- Gli hacker normalmente utilizzano scanner di vulnerabilità come Nessus, Nexpose, OpenVAS, ecc. per trovare queste vulnerabilità



Ethical Hacking - Exploitation

- Ricerca di vulnerabilità
- Gli hacker normalmente utilizzano scanner di vulnerabilità come Nessus, Nexpose, OpenVAS, ecc. per trovare queste vulnerabilità
- https://www.exploit-db.com/
- https://cve.mitre.org/
- https://nvd.nist.gov/

Ethical Hacking - Enumeration

L'enumerazione può essere utilizzata per ottenere informazioni su

- Condivisioni di rete
- dati SNMP, se non sono protetti correttamente
- tabelle IP
- Nomi utente di diversi sistemi
- Elenchi delle politiche delle password

Le enumerazioni dipendono dai servizi offerti dai sistemi. Possono essere –

- Enumerazione DNS
- Enumerazione NTP
- Enumerazione SNMP
- Enumerazione Linux/Windows
- Enumerazione SMB

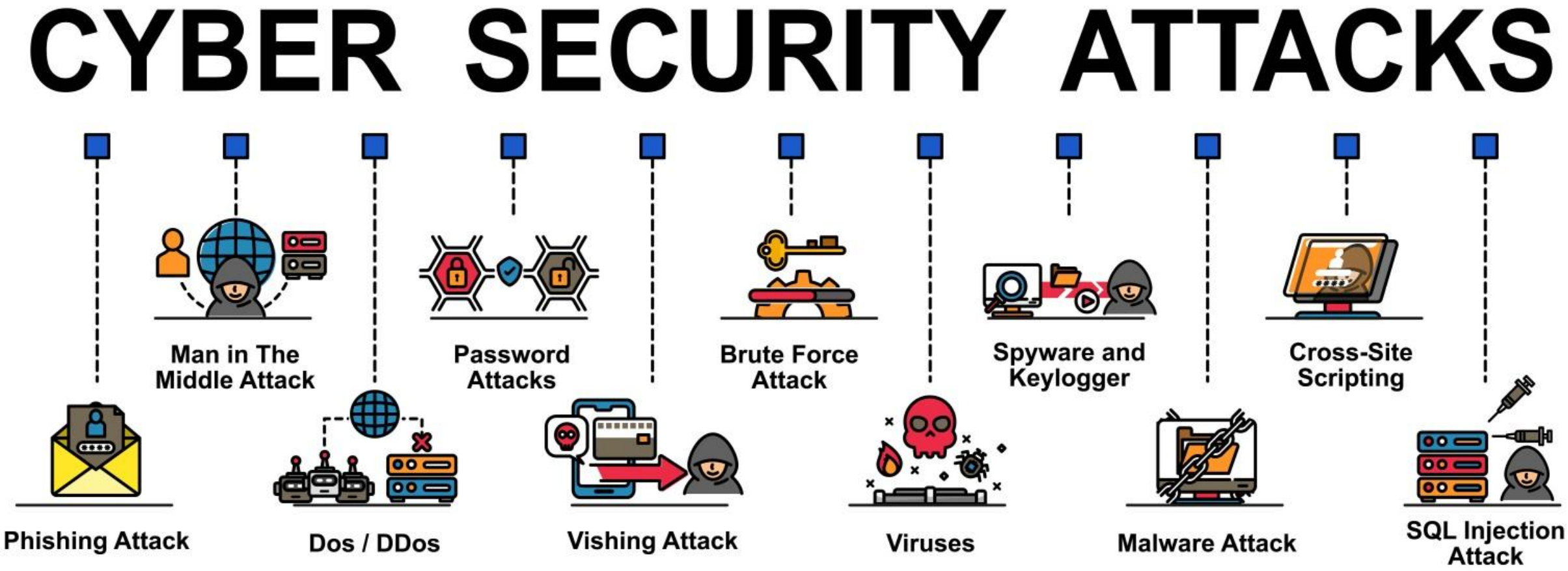
Ethical Hacking - Metasploit

Metasploit è uno degli strumenti di exploit più potenti.

La maggior parte delle sue risorse può essere trovata su:

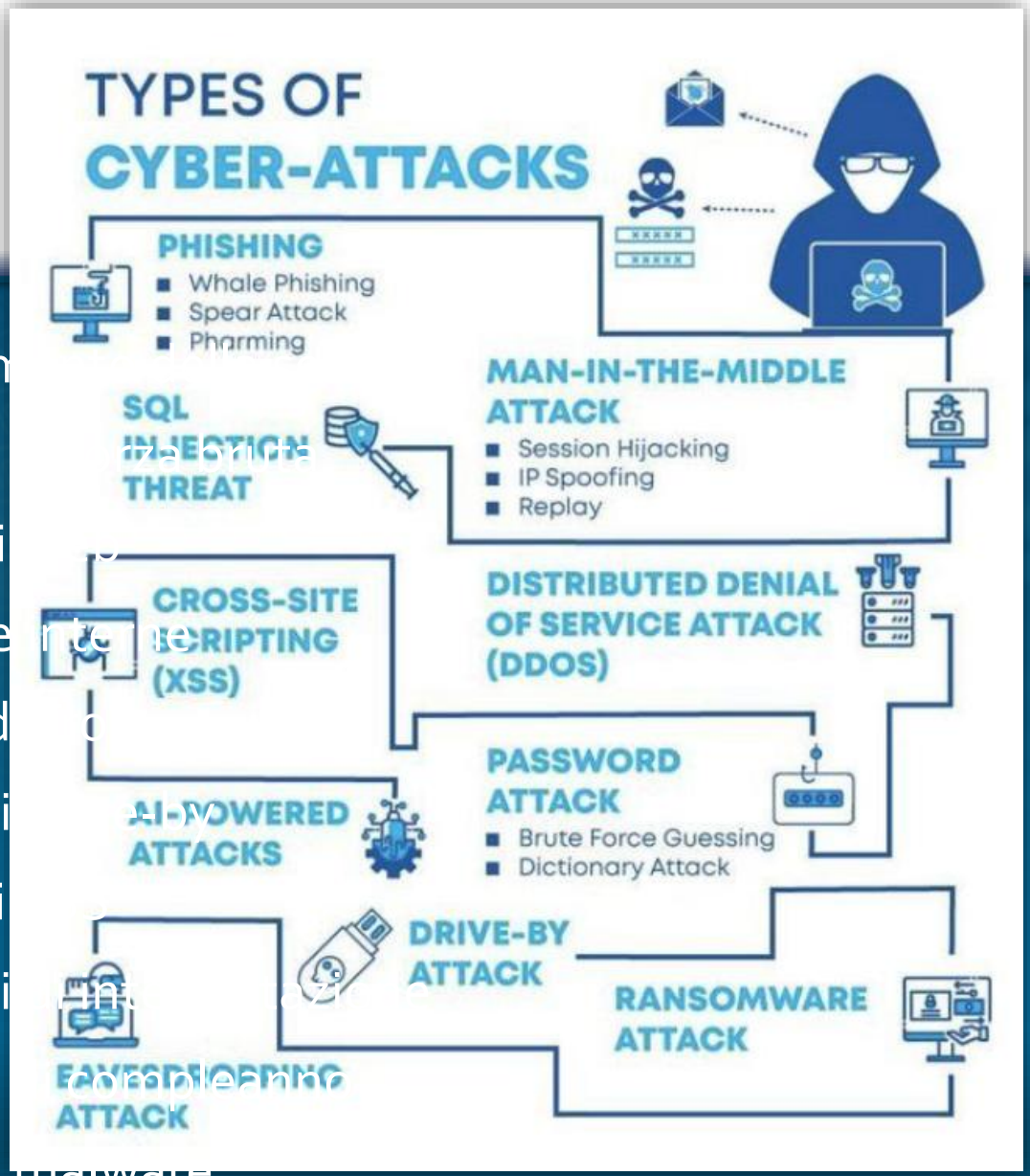
- https://www.metasploit.com/

TIPI DI ATTACCO



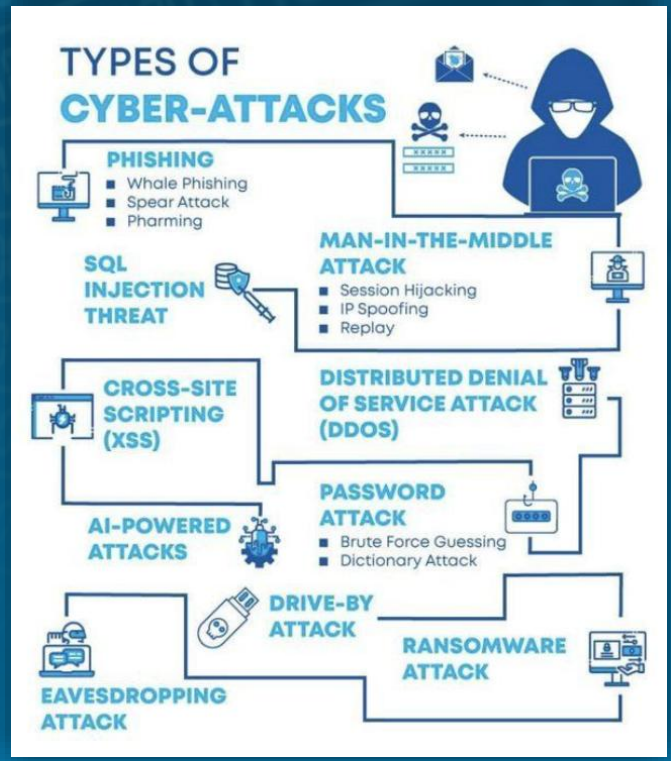
Tipi di attacco

- 1. Attacchi DoS e DDoS
- 2. Attacchi MITM
- 3. Attacchi di phishing
- 4. Attacchi di Whale-phishing
- 5. Attacchi di spear-phishing
- 6. Ransomware
- 7. Attacco alle password
- 8. Attacco SQL injection
- 9. Manipolazione dell'URL
- 10. Spoofing DNS
- 11. Dirottam
- 12. Attacco
- 13. Attacchi
- 14. Minacce
- 15. Cavalli d
- 16. Attacchi
- 17. Attacchi
- 18. Attacchi
- 19. Attacco
- 20. Attacco malware



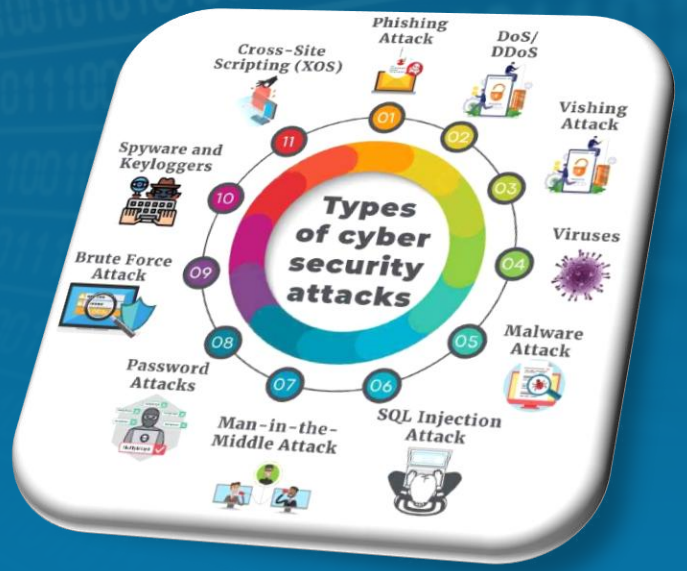
Tipi di attacco

- 1. Attacchi DoS e DDoS
- 2. Attacchi MITM
- 3. Attacchi di phishing
- 4. Attacchi di Whale-phishing
- 5. Attacchi di spear-phishing
- 6. Ransomware
- 7. Attacco alle password
- 8. Attacco SQL injection
- 9. Manipolazione dell'URL
- 10. Spoofing DNS
- 11. Dirottamento della sessione
- 12. Attacco di forza bruta
- 13. Attacchi Web
- 14. Minacce interne
- 15. Cavalli di Troia
- 16. Attacchi drive-by download
- 17. Attacchi XSS
- 18. Attacchi di intercettazione
- 19. Attacco "Birthday" (su hash di stringhe)
- 20. Attacco malware



ALCUNE TIPOLOGIE DI ATTACCO

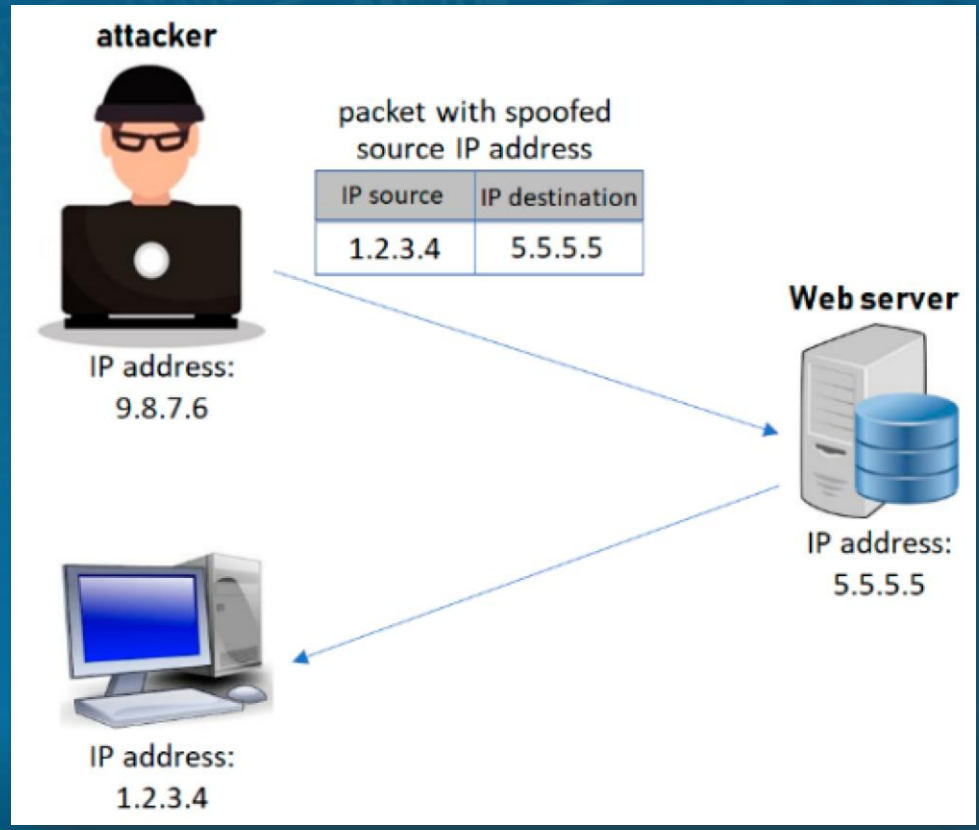
- **IP spoofing / shadow server** (qualcuno si sostituisce ad un host)
- **packet sniffing** (si leggono password di accesso e/o dati riservati)
- **connection hijacking / data spoofing** (si inseriscono / modificano dati durante il loro transito in rete)
- **denial-of-service** (distributed D-o-S) (si impedisce il funzionamento di un servizio (es. la guerra dei ping))



ALCUNE TIPOLOGIE DI ATTACCO

IP spoofing

- **falsificazione dell'indirizzo di rete del mittente**
- **solitamente si falsifica l'indirizzo di livello 3 (IP) ma nulla vieta di falsificare anche quello di livello 2 (ETH, TR, …)**
- **meglio chiamarlo *source address spoofing***
- **attacchi:**
  - falsificazione di dati
  - accesso a sistemi
- **contromisure:**
  - autenticazione non basata sugli indirizzi



ALCUNE TIPOLOGIE DI ATTACCO

Packet sniffing

- **lettura dei pacchetti destinati ad un altro nodo della rete**
- **facile da fare in reti broadcast (es. LAN) o nei nodi di smistamento**
- **attacchi:**
  - permette di intercettare qualunque cosa (password, dati, …)
- **contromisure:**
  - reti non broadcast
  - crittografia dei pacchetti

ALCUNE TIPOLOGIE DI ATTACCO

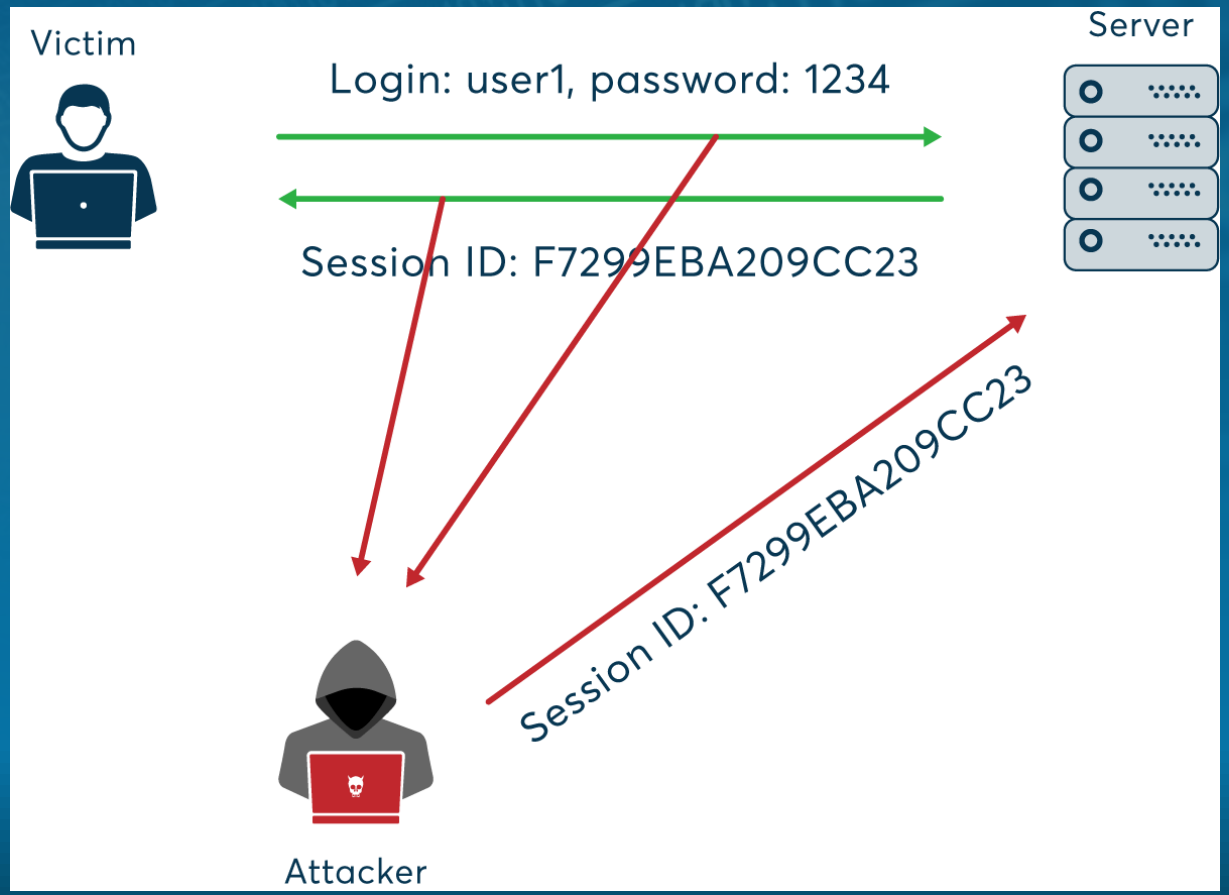
Shadow server

- **elaboratore che si pone come fornitore di un servizio senza averne il diritto**
- **richiede address spoofing e packet sniffing**
- **il server ombra deve essere più veloce di quello reale, oppure questo non deve essere in grado di rispondere (guasto o sotto attacco, ad esempio tramite DoS)**
- **attacchi:**
  - fornitura di un servizio sbagliato
  - cattura di dati forniti al servizio sbagliato
- **contromisure:**
  - autenticazione del server

ALCUNE TIPOLOGIE DI ATTACCO

Connection hijacking

- anche detto *data spoofing*
- si prende il controllo di un canale di comunicazione e si inseriscono, cancellano o manipolano dei pacchetti
- contromisure:
  - autenticazione, integrità e serializzazione di ogni singolo pacchetto di rete



ALCUNE TIPOLOGIE DI ATTACCO

Denial-of-service (DoS)

- **si tiene impegnato un host in modo che non possa fornire i suoi servizi**
- **esempi:**
  - saturazione della posta / log
  - ping flooding ("guerra dei ping")
  - SYN attack
- **attacchi:**
  - impedisce l'uso di un sistema / servizio
- **contromisure:**
  - nessuna definitiva

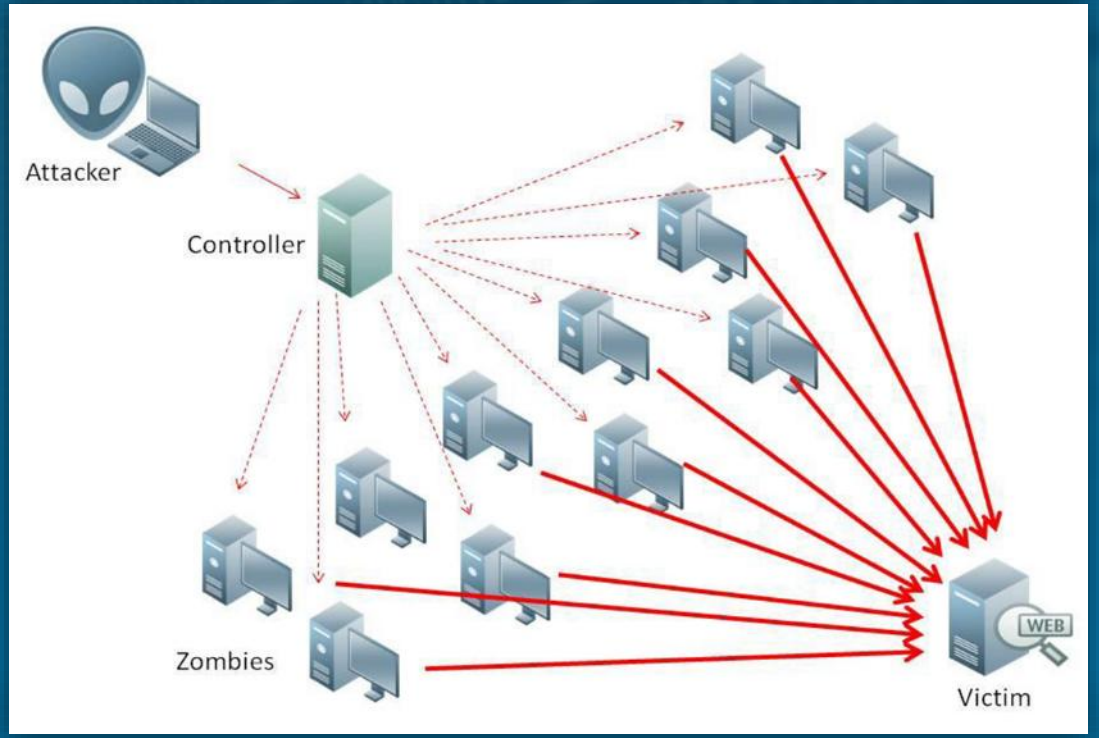
http://www.welivesecurity.com/2014/12/31/xbox-psn-lizard-squad-ddos/

http://www.cnet.com/news/buggy-mcafee-update-whacks-windows-xp-pcs/

ALCUNE TIPOLOGIE DI ATTACCO

Distributed denial-of-service (DDOS)

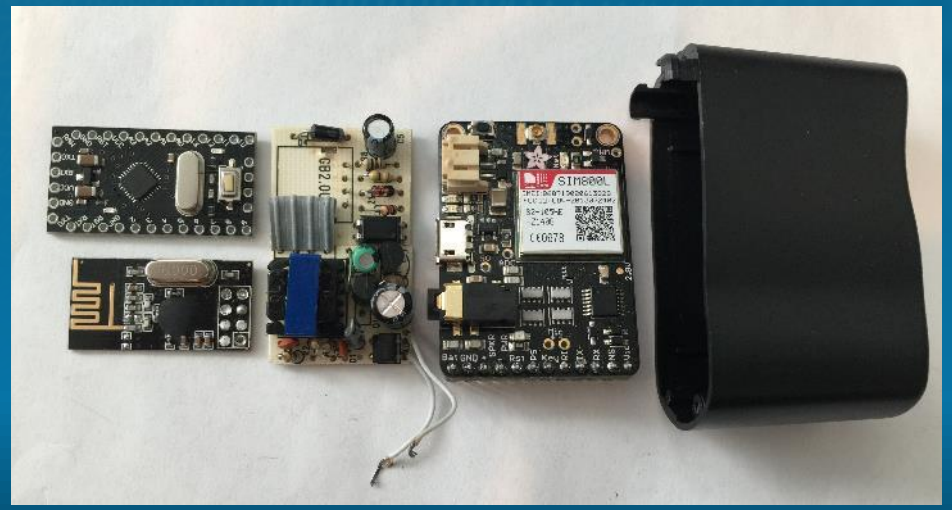
- software di attacco DOS installato su molte macchine (chiamate daemon)
- daemon controllati remotamente da un master (spesso tramite canali cifrati) e con capacità di auto-aggiornamento
- effetto dell'attacco base moltiplicato per il numero di daemon
- esempi:
  - TrinOO
  - TFN (Tribe Flood Network)
  - Stacheldraht



ALCUNE TIPOLOGIE DI ATTACCO

Hardware keylogger

strumento hardware o software in grado di effettuare lo sniffing della tastiera di un computer, cioè è in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente si accorga di essere monitorato



USB: Clicca qui

PS2: venduti perfino su Amazon! Clicca qui

Thunderbolt (Mac): Clicca qui

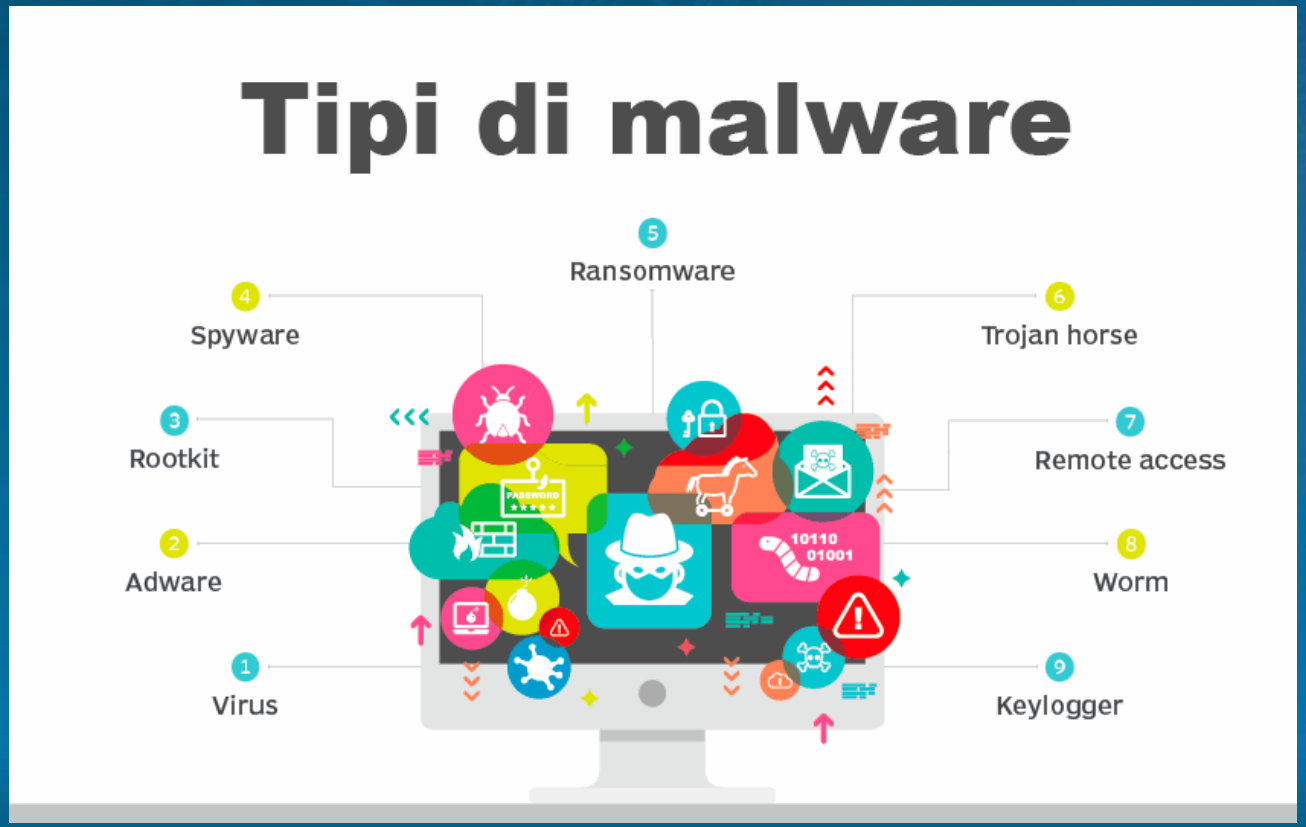
PHISHING O FISHING ?

- Il **phishing** è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale.
- Il termine phishing è una variante di fishing (letteralmente "pescare" in lingua inglese)

Varianti

- Whale-phishing
- Spear-phishing
- Smishing
- Vishing

I Malware



- Malware (abbreviazione dell'inglese **mal**icious software, lett. "soft**ware** malevolo"), nella sicurezza informatica, indica un qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer.

- Approfondimenti…

ALCUNE TIPOLOGIE DI ATTACCO

Ramsonware

Un ransomware è un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (ransom in Inglese) da pagare per rimuovere la limitazione

TIPI DI ATTACCO? ➔ IT

FASE 2: LA FORZATURA… ESEMPIO SQL INJECTION

```
"SELECT * FROM users WHERE name = '" + userName + "';"
```

```
' OR '1'='1' --
' OR '1'='1' ({
' OR '1'='1' /*
```

```
SELECT * FROM users WHERE name = '' OR '1'='1';
```

https://it.wikipedia.org/wiki/SQL_injection

TIPI DI ATTACCO? ➔ IT

FASE 2: LA FORZATURA… ESEMPIO SQL INJECTION

```
String comandoSQL="INSERT INTO Studenti(nome, cognome) VALUES (’"+
nomeDaInserire +"’, ’"+ cognomeDaInserire +"’);";
// per es.: INSERT INTO Studenti(nome, cognome)  VALUES(’mario’, ’rossi’);
executeSQL(comandoSQL); // esegue il comando sul DB server
```

```
nomeDaInserire = "mario’, ’rossi’); DROP Studenti; -- ";
cognomeDaInserire = "esempio di SQL Injection";
```

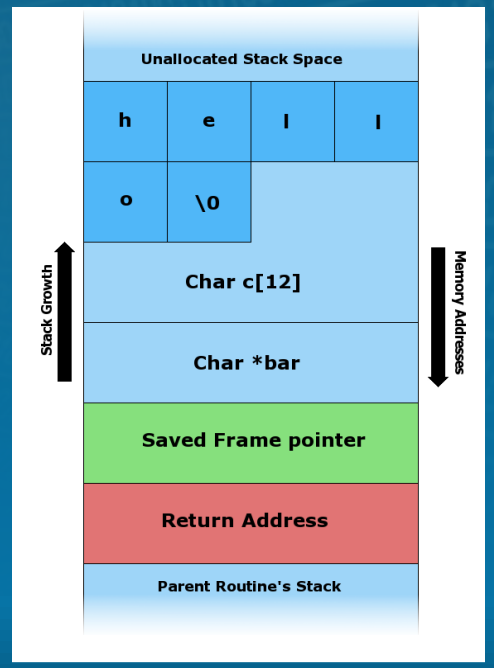
```
"INSERT INTO Studenti(nome, cognome) VALUES(’mario’, ’rossi’);
DROP Studenti; -- ’, ’esempio di SQL Injection’);"
```

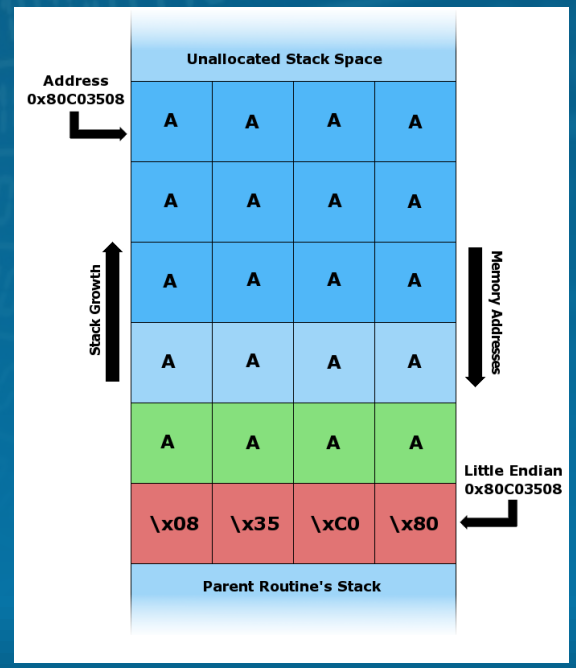
TIPI DI ATTACCO? ➔ IT

FASE 2: LA FORZATURA… Buffer overflow

```
#include <string.h>
void foo (char *bar)
{
  char  c[12];
  strcpy(c, bar);  // no bounds checking
}

int main (int argc, char **argv)
{
  foo(argv[1]);
  return 0;
}
```





https://en.wikipedia.org/wiki/Stack_buffer_overflow