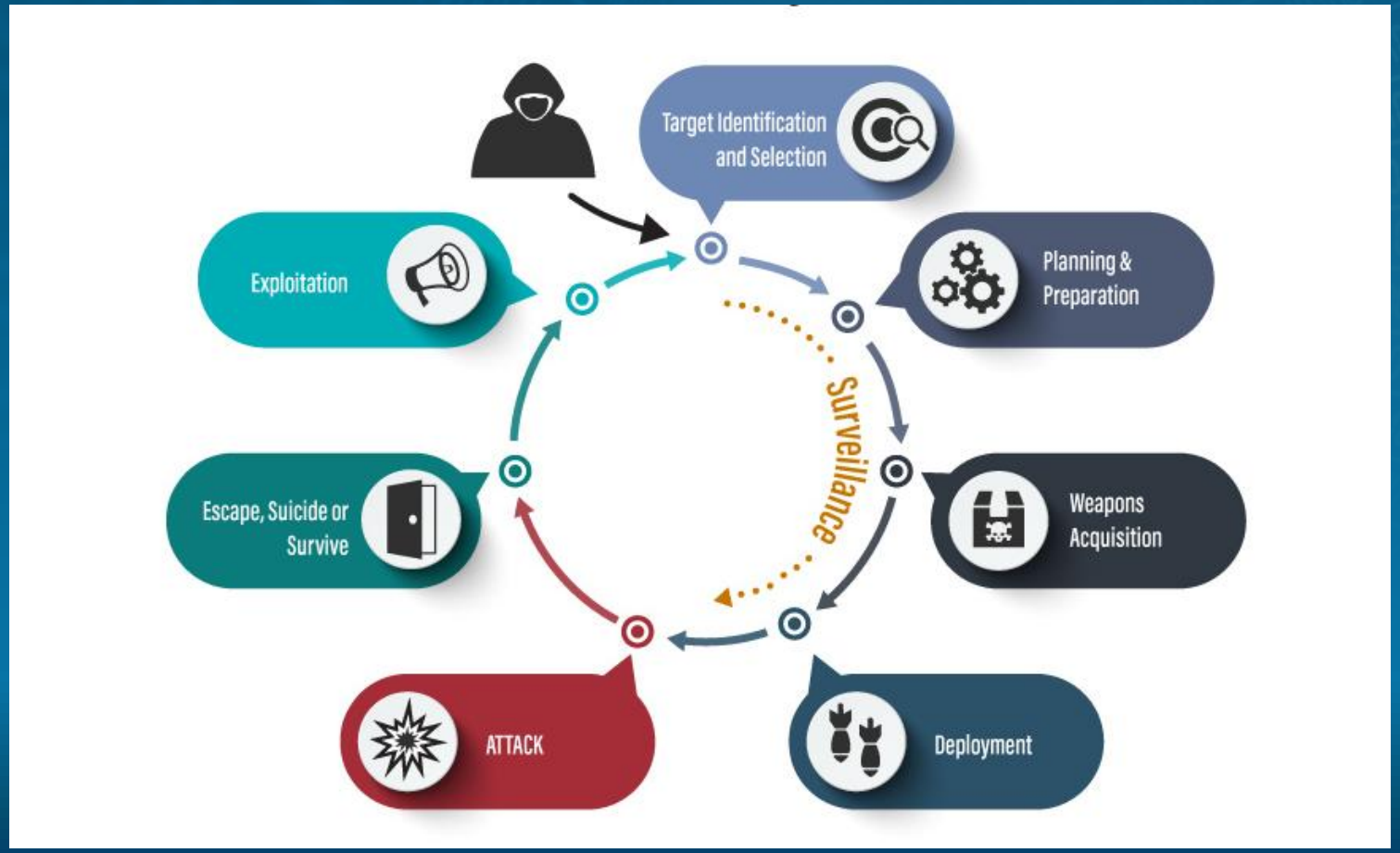
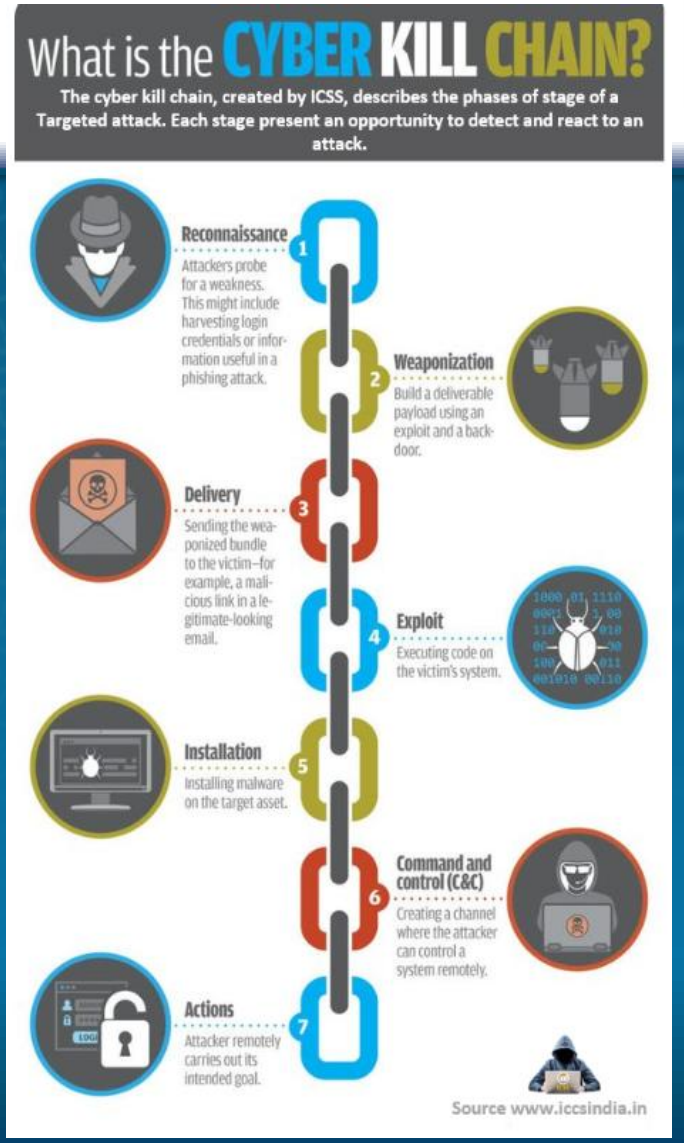
CYBER SECURITY

Fasi di Un Attacco

Fasi di un 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/

Fasi di un attacco

Ricognizione

- La ricognizione è la fase in cui l'attaccante raccoglie informazioni su un bersaglio utilizzando mezzi attivi o passivi. Gli strumenti ampiamente utilizzati in questo processo sono NMAP, Hping, Maltego e Google Dorks.

Scansione

- In questo processo, l'attaccante inizia a sondare attivamente una macchina o una rete di destinazione alla ricerca di vulnerabilità che possono essere sfruttate. Gli strumenti utilizzati in questo processo sono Nessus, Nexpose e NMAP.

Fasi di un attacco

Ottenere accesso

- In questo processo, la vulnerabilità viene individuata e si tenta di sfruttarla per entrare nel sistema. Lo strumento principale utilizzato in questo processo è Metasploit.

Mantenimento dell'accesso

- È il processo in cui l'hacker ha già ottenuto l'accesso a un sistema. Dopo aver ottenuto l'accesso, l'hacker installa alcune backdoor per entrare nel sistema quando in futuro avrà bisogno di accedere a questo sistema di proprietà. Metasploit è lo strumento preferito in questo processo.
- in base alle tue tecniche con cui ti senti a tuo agio. Il processo è di minore importanza finché sei in grado di ottenere i risultati desiderati.

Fasi di un attacco

Cancellare le tracce

- Questo processo è in realtà un'attività non etica. Ha a che fare con la cancellazione dei log di tutte le attività che hanno luogo durante il processo di hacking.

Segnalazione

- La segnalazione è l'ultimo passaggio per completare il processo di **hacking etico**. Qui l'hacker etico compila un rapporto con le sue scoperte e il lavoro svolto, come gli strumenti utilizzati, la percentuale di successo, le vulnerabilità rilevate e i processi di exploit.