Who am I?

- Davide Berardi [davide.berardi6@unibo.it].
- Laurea Magistrale in Computer Science nel 2016.
- Dottorando presso l'universita' di Bologna da 1/11/2018.
- Ex firmware engineer @ T3Lab.
- Interessi: Malware analysis, Network Security, Embedded Security, Virtualizzazione, Sistemi Operativi.

Red vs Blue

Hats...

- La comunita' hacker crea alcune distinzioni tra vari tipi di comportamento:
  - Black Hat
  - White Hat
  - Gray Hat

Il vero significato di hacker.

"A computer hacker is any skilled computer expert that uses their technical knowledge to overcome a problem."

- Pensieri personali sulla filosofia hacker:
  - Non azzardatevi a pensare che "S0n0 1 h4x0r!!!1!1!!" sia filosofia hacker (piuttosto "foodp? T")
  - Hacker != Script kiddie.
  - Non abbattetevi se qualcosa non viene al primo colpo (ma dovrete passare l'esame...).

Disclamer

Tools

- Kali Linux (Parrot Os, Black Arch, ...);
- DVWA;
- Lot of opensource/freeware tools (`http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html`).
- VulnHub / HackTheBox

Sequenze di un attacco informatico

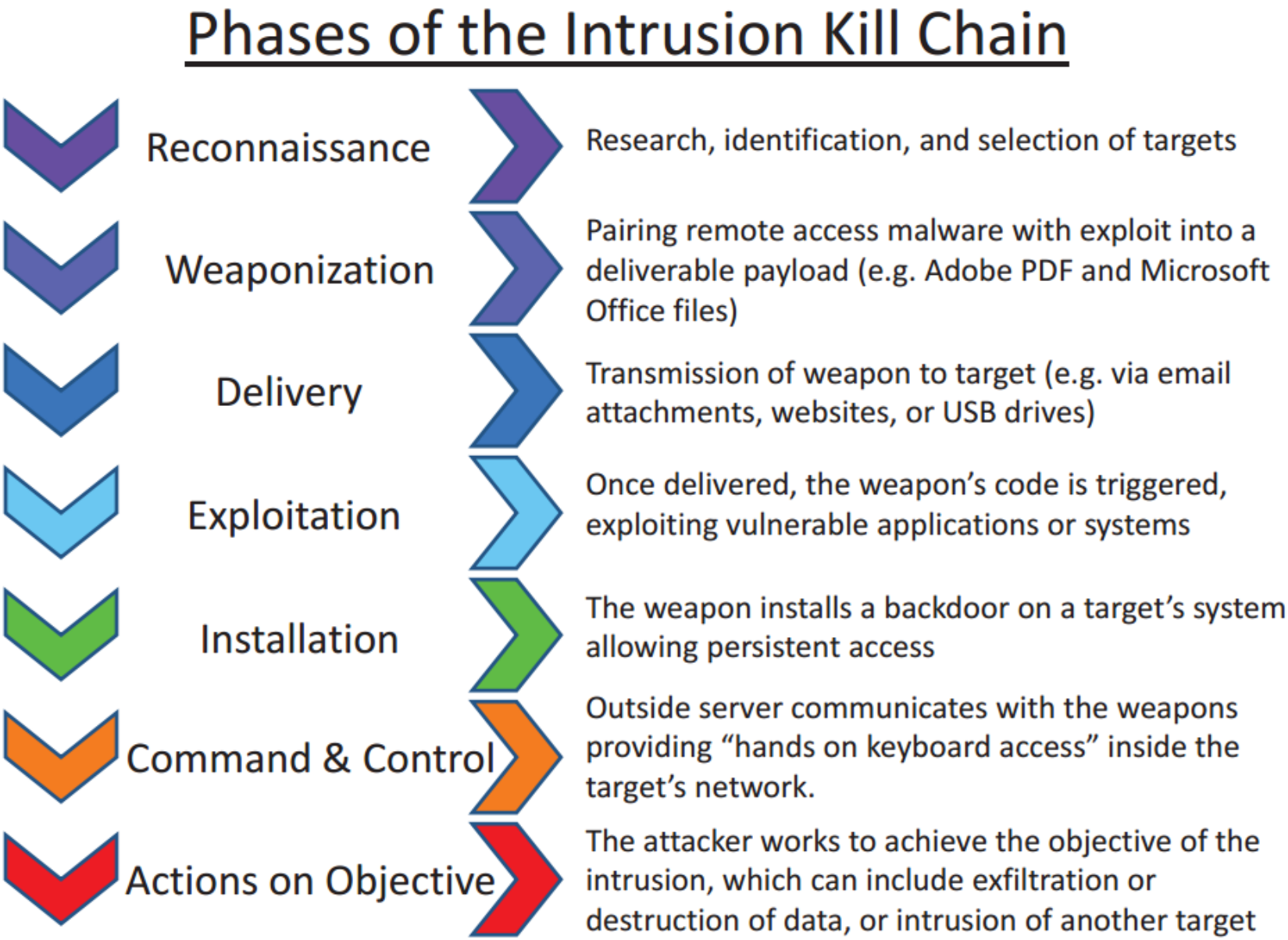


Figure: Kill chain di un attacco informatico (wikipedia en).

recap di reti / techweb

- ARP - Address resolution protocol (da indirizzi lv 3 - IPv4 a indirizzi lv 2 - MAC).
- TCP handshake - SYN, SYN/ACK, ACK
- HTTP cookies - token con informazioni personali.
- Client side: HTML, CSS, JavaScript.
- Server side: CGI.

Network recoinassance

- Tramite ARP possiamo ottenere la lista delle macchine visibili (in rete locale). `arp-scan`.
- Ottenuto un target o una rete di target possiamo analizzare i servizi disponibili su di ess* tramite pacchetti SYN (ma anche altri attacchi come Xmas, FIN, ...). `nmap`.
- Per internet esistono servizi come Shodan / Zmap.

Exploiting

- Sicuramente la fase piu' difficile e dispendiosa
- e' necessario scegliere con cura le vulnerabilita' da testare.
- Alcune volte il test e' one shot.
- Per software diffusi e' possibile usare Metasploit / searchsploit.

OWASP top 10

- OWASP e' una metodologia di penetration test orientata al mondo web.
- E' famosa anche per rilasciare una top 10 dei tipi di vulnerabilita' piu' pericolose.

Broken authentication / Password non sicure

- Parametri di autenticazione con richieste GET, autenticazione bypassabile tramite cookie, etc...
- Tools: `THC Hydra, Medusa`

Injection

- SQL injection: `"SELECT * FROM USERS WHERE user='$USER' AND password='$PASSWORD';"`
  - Cosa succede se in password inserisco `x' OR true; --` ?
  - `"SELECT * FROM USERS WHERE user='$USER' AND password='x' OR 1=1; --';"`
- Command injection.
- Tools: `sqlmap`

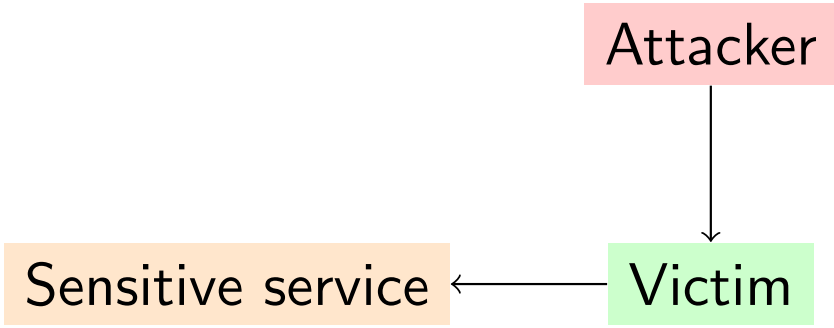
File Disclosure

- L'attaccante puo' visualizzare file (piu' o meno arbitrari) sul sistema.
- `http://192.168.0.1/index.php?language=en.php`
- `http://192.168.0.1/index.php?language=../../etc/passwd`
- Tools: `dotdotpwn`

Sensitive data exposure

- Cosa succede se i dati sensibili non sono cifrati?
- Cosa succede se i dati sensibili (p.e. password) sono cifrati con meccanismi poco sicuri (p.e. md5 senza sale?)
- Tools: `haveibeenpwnd.org`, `john the ripper`

CSRF - cross site request forgery



- In questo caso l'attaccante puo' inviare alla vittima un link a un html composto nel seguente modo:
- `<img src="<ip of sensitive service>/?.../>`
- `<img src="http://192.168.0.1/?action=changeDNS=1&dns=8.8.4.4/>`

XSS - Cross site scripting

- Il codice javascript e' vincolato a fare richieste solo sul sito di provenienza (SOP).
- Se l'attaccante pero' riesce ad iniettare del javascript all'interno del dominio (o a passare un link che scatena codice javascript) puo' controllare il codice eseguito dall'utente.

Local File Inclusion

- `include($_GET['ln']);`
- Tramite questa vulnerabilita' possiamo ottenere l'accesso al sistema (posto che possiamo fare upload di file arbitrari).

Remote File Inclusion

- L'attaccante puo' includere file remoti, non necessita quindi di una fase di upload.
- E' possibile rendere LFI una RFI tramite i log di sistema.

Risorse per migliorare

- Ulisse lab - ogni mercoledi' dalle 17/18 in lab2.
- CTF - overthewire.org (natas)
- Macchine - HackTheBox

Prossimamente...

- Sicurezza Web parte 2.
- Sicurezza degli applicativi (p.e. buffer overflow / spectre).
- Sicurezza delle reti (p.e. Wireless, bluetooth).
- Reverse di algoritmi (p.e. crack di videogame).
- Crittografia.
- Privilege escalation.