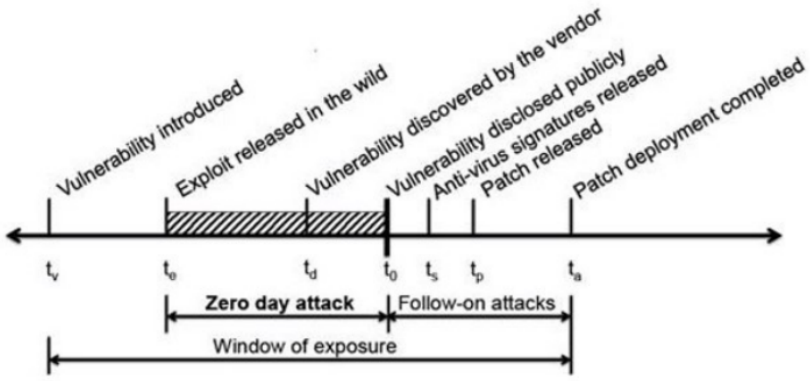
SICUREZZA INFORMATICA

Pierluca Pevere

OFFENSIVE SECURITY

Il ciclo di vita della vulnerabilità



I periodi più critici per la sicurezza sono la finestra degli zero day attack, perchè il produttore del software non sa che esiste questa vulnerabilità, e la finestra dei follow-on attacks perchè dopo la pubblicazione della vulnerabilità molti più attaccanti ne sono a conoscenza.

Qualche definizione:

- Vulnerabilità zero day: una vulnerabilità sconosciuta a coloro che dovrebbero essere interessati a mitigarla.
- Finestra di opportunità: tempo trascorso da quando il primo exploit del software diventa attivo al momento in cui il fornitore interessato rilascia una patch e viene applicata
- Attacco zero-day: un attacco che si verifica durante la finestra di opportunità, questa finestra nel 2005 durava in media 54 giorni, dal 2014 è cresciuta ad un anno
- Gli attacchi si intensificano dopo la finestra, perché tutti vengono a conoscenza della vulnerabilità, tipicamente scansioni massicce iniziano dopo 15 minuti dalla pubblicazione della CVE

La comunità pubblica le vulnerabilità scoperte secondo un principio di responsible disclosure su diversi siti:

- Common Vulnerabilities and Exposures http://cve.mitre.org/
- National Vulnerability Database http://nvd.nist.gov/
- Open Sourced Vulnerability Database http://osvdb.org/
- SecurityFocus http://www.securityfocus.com/vulnerabilities
- US-CERT http://www.kb.cert.org/vuls/

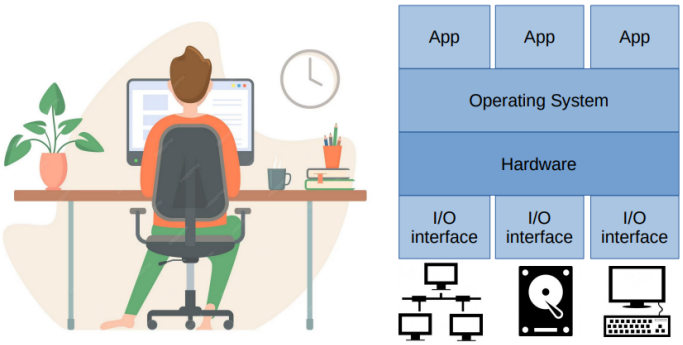
Esistono anche iniziative per cercare le vulnerabilità attivamente:

- Google project zero
- Programmi di bug bounty che le pagano profumatamente (es. Zerodium)

Ed esistono database pronti per sfruttarle:

- https://www.cvedetails.com/
- https://www.exploit-db.com/
- https://packetstormsecurity.com/

La maggior parte dell vulnerabilità stanno “fra la tastiera e la sedia” (il programmatore) ma ce ne possono essere anche nelle periferiche, sistema operativo, applicativi vari o interfacce I/O.



OFFENSIVE SECURITY

Consiste nel porsi nel ruolo degli attaccanti e verificare l’esistenza di vulnerabilità, stimare con precisione l’impatto degli attacchi e testare l’efficacia delle contromisure.

Reconnaissance = primo anello della killchain (https://attack.mitre.org/tactics/TA0043/)

Si usano le stesse tecniche degli attaccanti, il problema è che attaccare sistemi informatici è reato!
Bisogna farlo solo sotto uno preciso contratto e avere il permesso di farlo.
Il problema è che ci possono essere conseguenze legali e soprattutto effetti imprevisti, che potrebbero essere anche fatti in buona fede, per di più si possono verificare su reti attraversate per raggiungere l’obiettivo lecito.
Si potrebbe, inoltre, inciampare in un tipo di difesa che contrattacca e quindi si rischia di subire danni ai propri dati o alla propria rete.

TESTING

A questo punto il testing dei sistemi diventa fondamentale per verificare se sono sfuggite delle vulnerabilità e se il sistema è esposto a rischi nuovi rispetto al momento della progettazione. Tuttavia non si può dimostrare la totale assenza di problemi, si può solo tentare di sollecitare il sistema nel modo più completo possibile per trovare eventuali problemi esistenti.
Esistono 3 livelli di approfondimento dei test:

1. Vulnerability Assessment (VA)
2. Penetration Testing (PT)
3. Red Team Operations (RTO)

VA $\longrightarrow$ PT

I test di **Vulnerability Assessment** trovano solo le vulnerabilità note, non procede oltre: sfruttando una vulnerabilità si potrebbe accedere a una vista più interna e approfondita del sistema, svelandone altre.
In più i VA test sono considerano la specificità del sistema. A volte, infatti, si verificano dei falsi positivi ad esempio i servizi che dichiarano una versione vulnerabile ma sono stati corretti.
Mentre il **Penetration Testing** è un tipo di test dove il tester (umano) avanza fin dove può, sfruttando le vulnerabilità per mezzo di exploit. Il PT è più realistico, porta ad un report più dettagliato ma molto più RISCHIOSO.

PENETRATION TESTING

I punti di partenza per il Penetration Testing sono:

- **Valutazione del target**: vengono stabilite le regole di ingaggio e c'è la mappatura, prioritizzazione e tracciamento dei confini
- **Postura e visibilità**: gli attacchi ciechi possono sembrare più realistici, ma fanno solo perdere tempo al tester esperto che è meglio spendere sui dettagli veramente nascosti. Ad esempio se è semplice accedere a determinate informazioni magari si danno queste informazioni al tester e gli si chiede di andare a scovare le vulnerabilità davvero nascoste.
- **Protezione del bersaglio**: dove possibile viene creata una replica per evitare di danneggiare il bersaglio ma alcuni sistemi sono semplicemente troppo complessi oppure altri sono troppo critici per rischiare di perdere qualche dettaglio nella replica che potrebbe alterare il test

Metodolodie

Seguire una metodologia consente di assicurarsi che il test sia coerente e ripetibile, in più consente di eseguire una misurazione accurata della sicurezza.
Esistono alcune metodologie generalmente accettate:

- **Open Source Testing Methodology Manual** (OSSTMM): consente a qualsiasi tester di sicurezza di fornire idee per eseguire i test di sicurezza più accurati ed efficienti. Consente la libera diffusione delle informazione e delle proprietà intellettuale.
- **Open Web Application Security Project** (OWASP): specifico per web app
- **Payment Card Industry Data Security Standard** (PCI DSS): per il settore finanziario (la sezione 11.3 riguarda il pentesting)
- **Technical Guide to Information Security Testing and Assessment** (NIST800-115): uno standard ufficiale del governo USA
- **Information Systems Security Assessment Framework** (ISSAF): completo ma non sviluppato attivamente

Preparazione

La preparazione avviene in 2 fasi:

1. Reconnaissance: raccolta di informazioni utili, estensione del perimetro dei test e preparazione degli strumenti.

2. Enumeration: delimitazione del perimetro di test e verifica puntuale delle risorse e delle loro proprietà

OSINT

OSINT sta per Open Source INTelligence e consiste nell'uso di qualsiasi fonte pubblicamente disponibile oer ricavare informazioni su di uno specifico obiettivo. È importante specificare che si tratta di un campo di applicazione più ampio rispetto alla cybersecurity.
OSINT su altri è una componente della threat intelligence e dell'incident response. Mentre OSINT su se stessi si può scoprire che cosa possono a loro volta scoprire gli avversari e come possono essere usate quelle informazioni.
È legale ma attenzione alle aree grigie.
Ci sono strumenti online per fare OSINT: https://osintframework.com/

Ad esempio per misurare l'esposizione dell'infrastruttura:

- collocazione fisica
  - geolocation
  - rilevazione di indirizzi da documenti e pagine web
- collocazione in rete:
  - domini DNS associati all'obiettivo
  - range di IP
  - provider di connettività e autonomous systems
  - certificati X.509
- accesso ai servizi
  - porte raggiungibili
  - fingerprint dei sistemi → anche notoriamente vulnerabili
  - username validi → anche relative password