colorlinks, citecolor=black, filecolor=black, linkcolor=black, urlcolor=black

pdfauthor=AuthorName, pdftitle=shortTitle, pdfsubject=subject, pdfkeywords=keyword1, keyword2

Università degli studi di Torino

SCUOLA DI SCIENZE DELLA NATURA

Corso di Laurea Triennale in Informatica

Tesi di Laurea Magistrale

THE FANCY TITLE OF MY FANCY THESIS

Relatore:
Chiar.mo Prof.
Paolino Paperino

Controrelatore:
Prof.
Zio Paperone

Candidato:
Alessio Minoi

Anno Accademico 2020/2021

Ringrazio me e me stesso
per il sostegno avuto Author, *Title*

Prova nella prova

Facciamo una prova testuale per vedere se funzionano tutte le modifiche che voglio apportare

Italian abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vestibulum nec augue tincidunt, sodales lorem fringilla, venenatis metus. Cras dictum nec urna vitae euismod. Nunc vulputate quam dolor, id convallis augue convallis sit amet. Aliquam nec felis sodales, condimentum massa ac, tincidunt nisi. Vestibulum posuere, lacus tempus facilisis cursus, velit libero mattis diam, vel aliquet magna turpis vitae ligula. Maecenas aliquet nulla at gravida mattis. Morbi vestibulum in ex sed ultricies. Morbi sodales mollis mauris, vitae tincidunt enim hendrerit et. Interdum et malesuada fames ac ante ipsum primis in faucibus. Suspendisse laoreet faucibus massa, quis elementum enim eleifend aliquet. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Etiam at tortor vestibulum, dictum augue ut, porta lorem. Sed venenatis feugiat diam. Integer eu diam nec dolor viverra hendrerit.

Vestibulum quis vehicula massa. Etiam dictum, enim vel luctus accumsan, dolor velit laoreet metus, nec pretium arcu dui nec nulla. Donec ac sollicitudin justo, ut ullamcorper nunc. Curabitur ornare, ipsum hendrerit dictum rutrum, nisl lectus cursus sapien, in condimentum ipsum magna vel lorem. Cras vulputate semper placerat. In nec quam condimentum, auctor nisl eu, viverra libero. Maecenas scelerisque, odio vel accumsan luctus, justo dui pharetra orci, sit amet feugiat lorem lacus ac enim. Donec ultrices nulla semper erat consectetur, vitae mattis nulla dictum. Fusce maximus tristique condimentum. Quisque et sodales lectus, vel posuere leo. In ac augue vel neque sagittis volutpat at nec justo. Proin bibendum lobortis neque, vitae vulputate lorem viverra in. Etiam neque risus, pretium sed tempor a, pharetra quis arcu. Morbi purus nibh, efficitur nec sollicitudin non, commodo vel massa.

Pellentesque eu neque lacus. Vivamus finibus consectetur tellus id imperdiet. In ut dolor ligula. Vivamus ac vehicula erat. Duis semper lacinia eros, sed ultrices orci tristique at. Proin in pellentesque massa. Nunc ultricies justo eget nibh condimentum sollicitudin. Mauris non ligula eget magna pulvinar pretium vel vitae ante. Aenean lacinia metus vel odio vehicula sollicitudin. Quisque nisi augue, faucibus a nulla faucibus, consequat vehicula elit. Donec dui mi, ornare quis sapien ac, finibus maximus mi. Etiam volutpat, arcu quis posuere sollicitudin, ligula elit tincidunt lectus, non dapibus augue nunc id est. Ut dictum et diam vel vulputate. Aliquam ut nibh eu nibh aliquet aliquam eget ut leo. Duis urna tellus, sodales non ornare ut, aliquet vitae mi. Nunc consequat est vitae elit consectetur, id iaculis libero congue.

Praesent sem neque, semper ac turpis eu, fringilla egestas erat. Fusce in leo velit. Sed faucibus viverra massa. Donec justo lorem, accumsan a nisi in, maximus placerat augue. Mauris posuere aliquet sapien sed viverra. In hac habitasse platea dictumst. Ut nec dictum purus, sit amet gravida risus.

Indice

Capitolo 1

Vulnerabilità e attacchi

1.1 Vulnerabilità

Una **vulnerabilità informatica** può essere intesa come una componente (esplicita o implicita) di un sistema informatico, in corrispondenza alla quale le misure di sicurezza sono assenti, ridotte o compromesse, il che rappresenta un punto debole del sistema e consente ad un eventuale aggressore di compromettere il livello di sicurezza dell'intero sistema.
Essa può indicare una debolezza che può consentire un possibile **attacco informatico** di compromettere un sistema, cioè di ridurre il livello di protezione fornito da tale sistema, fino al caso limite di inficiare il funzionamento.

1.1.1 Ciclo di vita

Le vulnerabilità attraversano un ciclo di vita che passa attraverso la scoperta e finisce con l'installazione del fix su sistemi affetti, passando per quattro fasi principali:

1. **Creazione**: la vulnerabilità nasce nel momento in cui viene scritto del codice contenente un errore e e tale codice viene rilasciato. In questa fase la vulnerabilità non rappresenta un problema, poiché nonostante esista non è nota, quindi non sfruttabile.

2. **Scoperta**: può avvenire in vari modi, anche per caso, e anche ad opera di soggetti malevoli. Da questo momento si parla di vulnerabilità e non più di errore nel codice.

3. **Diffusione**: viene condivisa la conoscenza delle vulnerabilità e il problema assume carattere globale. in questa fase vengono spesso creati automatismi e tool per sfruttare la vulnerabilità, permettendo ad utenti anche meno esperti di lanciare con successo un attacco. Proprio in questo momento gli attacchi aumentano esponenzialmente.

4. **Patch deploy**: il produttore del sistema elabora e pubblica un aggiornamento che risolve il bug nel codice.

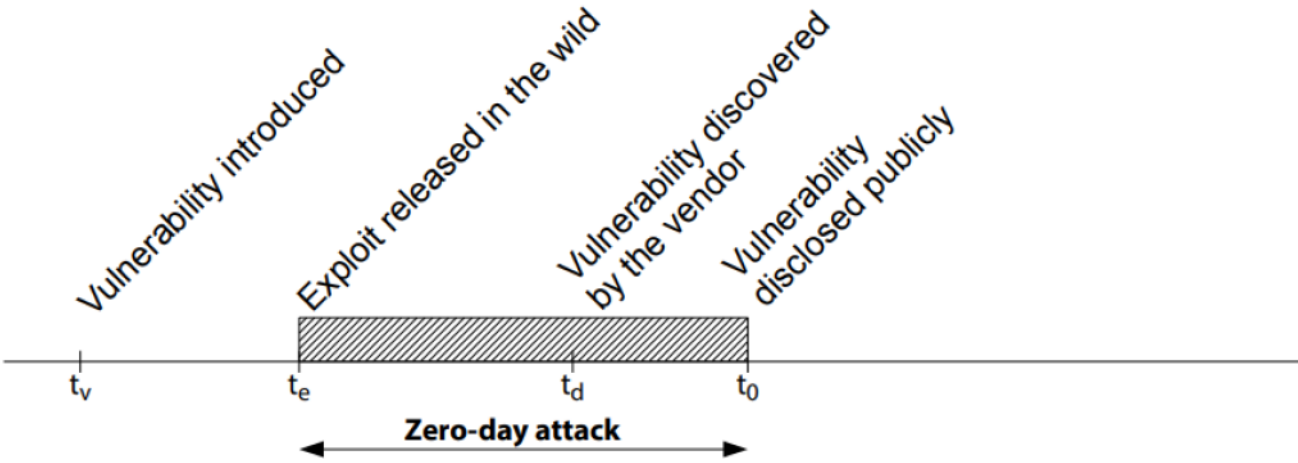

Figura 1.1

La scoperta di nuove vulnerabilità viene chiamata **vulnerabilità zero-day**, questo implica che tutti i sistemi sono soggetti ad una finestra di esposizione alla vulnerabilità. Il numero di **attacchi zero-day**, nel periodo $[t_e, t_0]$(figura1.1), aumenta rapidamente e ciò è dovuto alla rapida diffusione di conoscenza e alla creazione di **Exploit zero-day** [1] che permettono ad utenti meno esperti di sfruttare con successo tale vulnerabilità. Quando una vulnerabilità diventa nota, gli sviluppatori creano una patch per cercare di fermare l'attacco, ma spesso potrebbe passare del tempo prima che la patch venga rilasciata. Infatti capita spesso che le patch interferiscano con il corretto funzionamento dei sistemi o dei software installati, creando non pochi disagi; ciò comporta una preventiva fase di test su un numero limitato di macchine, e solo dopo accurati test un rilascio massivo a tutti i sistemi della società.

[1] è un qualunque programma che sfrutti una vulnerabilità zero-day per causare effetti indesiderati.

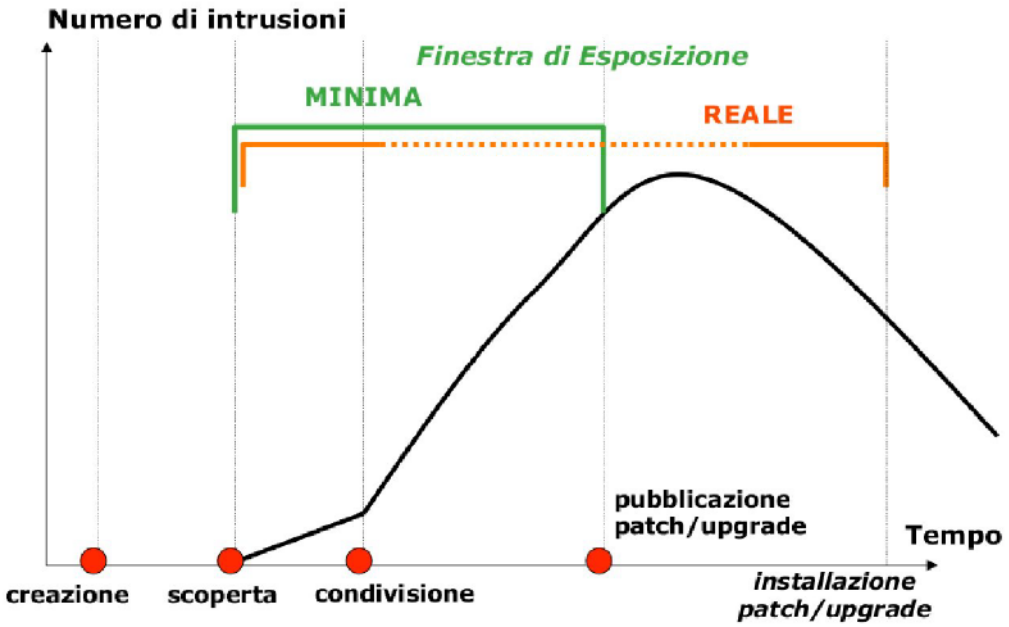

Figura 1.2: Ciclo di vita di una vulnerabilità

1.1.2 Obiettivi degli exploit zero-day (non so se tenerla o no)

Un attacco zero-day può sfruttare le vulnerabilità di svariati sistemi, tra cui:

- Sistemi Operativi
- Browser Web
- Applicazioni Office
- Componenti open-source
- Hardware e firmware
- Internet of Things

Esiste per tanto un'ampia gamma di potenziali vittime:

- Singoli utenti che utilizzano un sistema vulnerabile
- Singoli utenti che accedono a dati aziendali importanti
- Dispositivi hardware, firmware e Internet of Things
- Aziende e organizzazioni di grandi dimensioni
- Agenzie governative
- Obiettivi politici

È utile comprendere due tipologie di attacchi zero-day:

- Gli attacchi zero-day **mirati** hanno obiettivi potenzialmente di valore, ad esempio grandi organizzazioni, agenzie governative o persone di alto profilo.
- Gli attacchi zero-day **non mirati** sono invece rivolti contro utenti di sistemi vulnerabili, ad esempio un sistema operativo o un browser.

Anche quando gli autori degli attacchi non prendono di mira utenti specifici, moltissime persone possono tuttavia rimanere vittime di **attacchi zero-day**, solitamente come danno collaterale.

1.1.3 Identificare gli attacchi zero-day

Può essere difficile individuare le vulnerabilità zero-day, dal momento che possono assumere diverse forme. Data la natura di questi tipi di vulnerabilità, le informazioni dettagliate sugli exploit zero-day sono disponibili solo dopo che sono stati identificati. Le organizzazioni vittime di un exploit zero-day potrebbero notare traffico imprevisto o un'attività sospetta di scansione originata da un client o un servizio. Alcune delle tecniche di rilevamento zero-day includono:

1. Si utilizza come riferimento di database esistenti di malware che ne descrivono anche il comportamento. Anche se questi database vengono aggiornati molto velocemente e possono essere utili come riferimento, per definizione gli exploit zero-day sono nuovi e sconosciuti. Le informazioni reperibile in un database esistente sono quindi limitate.
2. In alternativa, alcune tecniche cercano le caratteristiche dei malware zero-day in base a come interagiscono con il sistema preso di mira. Invece di esaminare il codice dei file in ingresso, questa tecnica analizza le loro interazioni con il software esistente e cerca di determinare se sono il risultato di azioni dannose.
3. Il machine learning viene sempre utilizzato per rilevare i dati dagli exploit registrati in precedenza e poter stabilire un riferimento per il comportamento di un sistema sicuro in base ai dati delle interazioni passate e attuali con il sistema. Maggiore è la quantità di dati disponibili, più affidabile sarà il rilevamento.

Spesso si utilizza una combinazione di sistemi di rilevamento diversi.

1.1.4 Come proteggersi da attacchi zero-day

Per la protezione zero-day e la sicurezza del computer e dei dati, è essenziale sia per i singoli utenti che per le organizzazioni seguire delle **best-practice**, tra cui:

1. **Mantenere aggiornati tutti i software e i sistemi operativi.** I fornitori includono infatti nelle nuove versioni patch di sicurezza che coprono le vulnerabilità appena identificate. Mantenere i sistemi informatici aggiornati garantisce una sicurezza ancora maggiore.

2. **Usare solo le applicazioni essenziali.** Più software si utilizzano, maggiori saranno le potenziali vulnerabilità. Per ridurre i rischi nella propria rete, utilizzare solo applicazioni necessarie.

3. **Usare un firewall.** Un firewall [2] svolge un ruolo essenziale nella protezione del sistema dalle minacce zero-day.

4. **Educare gli utenti nelle organizzazioni.** Molti attacchi zero-day sfruttano l'errore umano. Insegnare ai dipendenti e utenti buone abitudini di sicurezza li proteggerà dalle minacce digitali.

[2] specificare il firewall cos'è

1.2 Attacchi informatici

L'**attacco informatico** viene definito come il tentativo di ottenere un accesso non autorizzato a servizi, risorse o informazioni di sistema e/o di compromettere l'integrità e, in generale, consiste nell'atto intenzionale di tentare di eludere uno o più servizi di sicurezza o i controlli di un sistema informativo digitale per alterare la riservatezza, l'integrità e la disponibilità dei dati.

1.2.1

Capitolo 2

Lorem Ipsum

Bullet list example

- first point
- second point
- third point

Enumeration example

1. first point
2. second point
3. third point

Description example

first descr first point

second descr second point

third descr third point

. . . but you can also build nested lists

- first point
  - first point
  - second point
- second point
- third point

Capitolo 3

Lorem Ipsum

A figure example, with text in line (NO CAPTION)

A figure example, with floating object and caption

Figura 3.1: the logo of UniTo

Elenco delle figure

Elenco delle tabelle

Bibliografia

[1] A. Einstein, "Zur Elektrodynamik bewegter Körper. (German) [On the electrodynamics of moving bodies]," *Annalen der Physik*, vol. 322, no. 10, pp. 891–921, 1905.

[2] M. Goossens, F. Mittelbach, and A. Samarin, *The LaTeX Companion*. Reading, Massachusetts: Addison-Wesley, 1993.

[3] D. Knuth, "Knuth: Computers and typesetting."