UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI INFORMATICA

Corso di Laurea Magistrale in Informatica

Corso di Penetration Testing & Ethical Hacking

Penetration Testing Report: Architettura IoT Cloud-based

Docente:
Arcangelo CASTIGLIONE

Candidato:
Alberto MONTEFUSCO
Mat. 0522501498

ANNO ACCADEMICO 2023/2024

Indice

Capitolo 1

Penetration Testing Report

1.1 Executive Summary

Per l'attività progettuale relativa al corso di *Penetration Testing and Ethical Hacking* è stato svolto un processo di *Penetration Testing* su un asset riguardante un'architettura IoT Cloud-based che rappresenta la configurazione di una porta domotica la quale consente l'accesso in casa tramite un lettore di impronte digitali e, mediante un sensore di prossimità, rileva la presenza di estranei. In assenza di particolari e specifiche informazioni relative all'asset da analizzare, è stato utilizzato un approccio di tipo Black Box. Per svolgere l'analisi è stato configurato un opportuno ambiente simulato che consente un'interazione con l'asset, permettendo di esaminarlo e di rilevarne le vulnerabilità. In particolare, le vulnerabilità rilevate possono portare all'ottenimento del pieno controllo del sistema da parte di un attaccante che può assumere il ruolo di amministratore. Risulta anche possibile per un attaccante rubare dati sensibili e manipolarli con il fine di ottenere l'accesso alla porta domotica. Allo stato attuale, il livello di rischio complessivo associato all'asset risulta essere critico, tuttavia mediante alcuni accorgimenti, come meccanismi di autenticazione e l'implementazione di alcuni semplici controlli, è possibile abbassare sensibilmente il livello di rischio.

1.2 Engagement Highlights

Dal momento che il processo di *Penetration Testing* è stato svolto in un contesto puramente didattico, non è stato necessario definire particolari regole di ingaggio.

1.3 Vulnerability Report

Nel corso del processo di *Penetration Testing* sono state rilevate diverse vulnerabilità sfruttabili per compromettere vari aspetti del sistema. Di seguito è riportata una descrizione generale delle problematiche riscontrate.

1.3.1 HOST 192.168.14.240

- [**Severity: Alta**] **Versione del protocollo NTP obsoleta**: gli attaccanti possono sfruttare tale protocollo per ottenere informazioni sul sistema ed eseguire attacchi DDoS di tipo Amplification.
- [**Severity: Media**] **Il Broker MQTT non richiede una forma di autenticazione per i suoi client**: questo permette all'attaccante di connettersi al broker MQTT e sottoscriversi o pubblicare messaggi su qualsiasi topic. Infatti, è più facile inserirsi tra il client e il broker e intercettare o manipolare i messaggi (*MITM*). I dati intercettati da terzi possono essere modificati in transito e falsificati, alterando il comportamento dei sistemi che dipendono dai dati MQTT.
- [**Severity: Media**] **DNS Cache Snooping**: permette agli attaccanti di determinare se un determinato record DNS è presente nella cache del DNS resolver. Questo tipo di attacco può essere utilizzato per raccogliere informazioni sui comportamenti di navigazione degli utenti o per scoprire quali domini sono stati visitati di recente.
- [**Severity: Bassa**] **Trapelamento del timestamp del sistema**: ottenimento di informazioni sul timestamp del sistema con eventuale possibilità di prevedere dati generati in maniera arbitraria dal sistema.
- [**Severity: N/A**] **Password acces point debole**: l'access point del dispositivo target Raspberry Pi possiede una password molto semplice e comune che può essere scovata in pochi secondi mediante un attacco di *brute force*.
- [**Severity: N/A**] **Credenziali SSH deboli**: gli attaccanti possono effettuare facilmente un attacco di tipo *brute force* sul dispositivo target Raspberry Pi per recuperare le credenziali utilizzare dal protocollo *SSH*.

1.3.2 HOST 192.168.14.24

Non sono state rilevate vulnerabilità per questo dispositivo.

1.3.3 HOST 192.168.14.26

Non sono state rilevate vulnerabilità per questo dispositivo.

1.3.4 HOST 192.168.14.27

Non sono state rilevate vulnerabilità per questo dispositivo.

1.4 Remediation Report

Mediante vari accorgimenti risulta possibile rimuovere le vulnerabilità dal sistema evitando, in questo modo, tutti i rischi ad esse associate. Di seguito è riportata una descrizione generale delle operazioni consigliate:

1.4.1 HOST 192.168.14.240

- Aggiornare alle ultime versioni tutti i servizi installati;
- Inserire meccanismi di autenticazione per i dispositivi che si collegano all'asset;
- Utilizzare password forti e non prevedibili;
- Disabilitare il supporto ai timestamp ICMP o proteggere il device mediante un firewall per gestire il traffico in entrata e in uscita.

1.5 Findings Summary

Di seguito sono riportati i grafici relativi alle vulnerabilità identificate in rapporto alla severity.

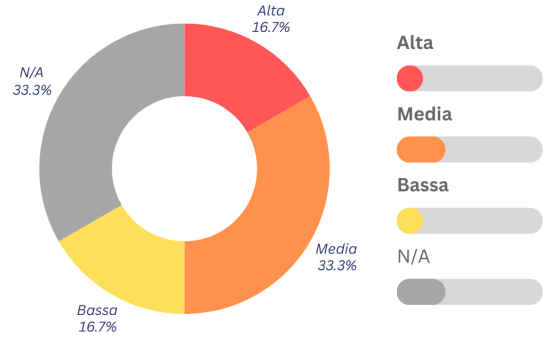

Figura 1.1: Areogramma vulnerabilità

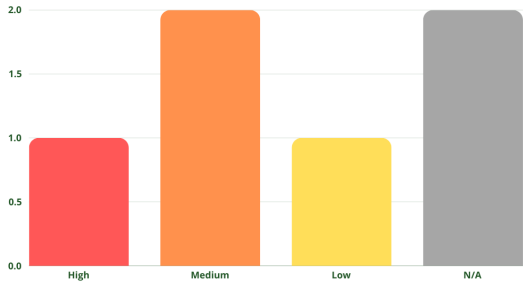

Figura 1.2: Ortogramma vulnerabilità

1.6 Detailed Summary

Di seguito saranno elencate le varie vulnerabilità riscontrate sia grazie ai tool di rilevazione automatica sia mediante tecniche manuali, correlate di eventuale ID e rischi associati. Durante la fase di *Penetration Testing* sono stati generati diversi report grazie ai tool di rilevazione automatica consultabili nella directory: `/outputs/3_Vulnerability Mapping`.

1.6.1 Host 192.168.14.240

Network Time Protocol (ntpd) read_mru_list Remote DoS	**CVE**	**CWE**
	CVE-2016-7434 [1]	CWE-20 [2]
ALTA		
Descrizione: Server remoto NTP che consente la sincronizzazione dell'orologio del dispositivo con la rete a cui è connesso.		
Impatto: Un attaccante può creare una query *mrulist NTP* per terminare il processo *ntpd* o esaurire le risorse del dispositivo.		
Soluzione: Aggiornare la versione NTP all'ultima release.		
Metodo di detection: Vulnerabilità individuata tramite il software Nessus.		

DNS Cache Snooping Vulnerability (UDP)	CVE	CWE
	N/A	N/A
MEDIA		
Descrizione: Il server DNS è soggetto ad una vulnerabilità di snooping della cache.		
Impatto: Gli attaccanti potrebbero ottenere informazioni sui record DNS memorizzati nella cache che potrebbero portare ad ulteriori attacchi.		
Soluzione: Sono possibili diverse mitigazioni a seconda della posizione e della funzionalità richiesta dal server DNS: 1. disabilitare la ricorsione; 2. non consentire l'accesso pubblico ai server DNS che eseguono la ricorsione; 3. lasciare la ricorsione abilitata se il server DNS si trova su una rete aziendale che non può essere raggiunta da client non affidabili.		
Metodo di detection: Vulnerabilità individuata tramite il software OpenVAS.		

MQTT Broker Does Not Require Authentication	CVE	CWE
	N/A	N/A
MEDIA		
Descrizione: Il broker MQTT remoto non richiede l'autenticazione dei dispositivi client.		
Impatto: Gli attaccanti potrebbero ottenere informazioni sui topic e sui messaggi scambiati falsificandoli e creandone alcuni ad hoc.		
Soluzione: Abilitare l'autenticazione.		
Metodo di detection: Vulnerabilità individuata tramite il software OpenVAS.		

ICMP Timestamp Reply Information Disclosure	CVE	CWE
	CVE-1999-0524 [3]	CWE-200 [4]
BASSA		
Descrizione: Il Timestamp Reply è un messaggio ICMP che risponde a un messaggio Timestamp. E' composto dal timestamp di origine inviato dal mittente del timestamp, da un timestamp di ricezione e da un timestamp di trasmissione.		
Impatto: Queste informazioni potrebbero teoricamente essere utilizzate per sfruttare i generatori di numeri casuali deboli time-based in altri servizi.		
Soluzione: Sono possibili diverse mitigazioni: 1. disabilitare il supporto per il timestamp ICMP sull'host remoto; 2. proteggere l'host remoto con un firewall bloccare i pacchetti ICMP che passano attraverso il firewall in entrambe le direzioni.		
Metodo di detection: Vulnerabilità individuata tramite il software OpenVAS.		

TCP Timestamps Information Disclosure	CVE	CWE
	N/A	N/A
BASSA		
Descrizione: L'host remoto implementa i timestamp TCP e consente quindi di calcolare l'uptime.		
Impatto: A volte è possibile calcolare il tempo di attività dell'host remoto.		
Soluzione: Disabilitare i timestamp TCP aggiungendo la riga 'net.ipv4.tcp_timestamps = 0' a /etc/sysctl.conf. Eseguire poi 'sysctl -p' per applicare le impostazioni in fase di esecuzione.		
Metodo di detection: Vulnerabilità individuata tramite il software OpenVAS.		

Impiego di password deboli	**CVE**	**CWE**
	N/A	CWE-1391 [5] CWE-521 [6]
N/A		
Descrizione: Per accedere al sistema e all'access point vengono utilizzate le stesse password o, in ogni caso, password facilmente compromissibili.		
Impatto: Un attaccante potrebbe riuscire a forzare con successo le password degli utenti tramite attacco a dizionario, compromettendo il sistema.		
Soluzione: Utilizzare password diverse per ogni servizio e impiegare dei requisiti di password più stringenti, come combinazioni di caratteri alfanumerici e caratteri speciali (anche combinazioni di maiuscole e minuscole) specificando anche una lunghezza minima e, soprattutto, non utilizzare password banali facilmente intuibili.		
Metodo di detection: Vulnerabilità individuata tramite tecniche manuali.		

Bibliografia

[1] CVE-2016-7434.

[2] CWE-20.

[3] CVE-1999-0524.

[4] CWE-200.

[5] CWE-1391.

[6] CWE-521.

Elenco delle figure