Università degli Studi di Salerno

Penetration Testing Report

VULNERABLE LAB DC-2

Luca Izzo | Corso di PTEH | 07/04/2020

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

1. Executive Summary 3

2. Engagement Highlights 4

3. Vulnerability Report 6

4. Remediation Report 7

5. Findings Summary 8

6. Detailed Summary 10

6.1 DC:2-1 TCP Timestamps 10

6.2 DC:2-2 Improper Neutralization of Input During Web Page Generation 11

6.3 DC:2-3 Improper Authentication 11

7. References 12

8. Appendix 13

8.1 Table of Figures 13

1. Executive Summary

È stato eseguito un Penetration Test sulla macchina virtuale DC:2 reperita tramite il sito Vulhub. L'obiettivo del testing è stato quello di analizzare la posizione di sicurezza della macchina target e suggerire contromisure per tutte le vulnerabilità riscontrate. Questo progetto è stato realizzato nel Marzo 2020 da un Cyber Security Specialist Luca Izzo, Italia.

Si è trattato di un "Grey box" penetration test, infatti, si era a conoscenza di alcune informazioni base della macchina target e struttura della rete.

Come risultato d'ingaggio, siamo riusciti a trovare diverse vulnerabilità a basso e alto rischio, le quali hanno confermato che la postura di sicurezza dell'infrastruttura è molto bassa e che non sono state implementate adeguate contromisure di sicurezza all'interno dell'ambiente. Questo report contiene un'analisi dettagliata delle vulnerabilità rilevate durante la fase d'ingaggio, insieme ad un Remediation report che aiuterebbe a migliorare la posizione di sicurezza complessiva dell'infrastruttura. Il report contiene anche una spiegazione dettagliata di ogni vulnerabilità rilevata insieme alle contromisure dettagliate per correggere la vulnerabilità.

Il rischio di compromissione risulta essere alto e affrontare, quindi, i problemi di sicurezza presenti all'interno del report diminuirebbe in modo significativo questo rischio.

2. Engagement Highlights

In seguito all'accorto ottenuto con l'Università degli Studi di Salerno, nella figura del Rettore Vincenzo Loia, sono state definite le seguenti **Regole di ingaggio**.

A. Vendite e Marketing

1. È vietata l'offerta di servizi gratuiti per la mancata penetrazione dell'obiettivo.
2. È richiesto che gli utenti siano informati in modo veritiero e fattuale riguardo alla loro sicurezza e alle misure di sicurezza. L'ignoranza non è una scusa per una consulenza disonesta.

B. Valutazione / Consegna Stimata

1. È severamente vietato eseguire test di sicurezza contro qualsiasi ambito senza l'esplicita autorizzazione scritta del proprietario di destinazione o l'autorità competente.
2. È vietato il collaudo di sicurezza di sistemi, ubicazioni e processi ovviamente altamente insicuri e instabili fino a quando non sarà installata la corretta infrastruttura di sicurezza.

C. Contratti e negoziazioni

1. Con o senza un contratto di non divulgazione, l'analista della sicurezza è tenuto a fornire riservatezza e non divulgazione delle informazioni dei clienti e dei risultati dei test.
2. I contratti devono spiegare chiaramente i limiti e i pericoli di test di sicurezza come parte della dichiarazione di lavoro.
3. Nel caso di test remoti, il contratto deve includere l'origine degli analisti per indirizzo, numero di telefono o indirizzo IP.
4. I contratti devono contenere nomi di contatti di emergenza e numeri di telefono.
5. Il contratto deve includere autorizzazioni chiare e specifiche per o test di Social Engineering, Denial of Service, ove necessario.
6. I contratti devono contenere la procedura per future modifiche al contratto e alla dichiarazione di lavoro (Statement Of Work).

D. Definizione dell'ambito di applicazione

1. L'ambito di applicazione deve essere chiaramente definito contrattualmente prima di verificare i servizi vulnerabili.
2. La valutazione di sicurezza (audit) deve spiegare chiaramente i limiti di eventuali test di sicurezza in base al campo di applicazione.

E. Piano di ingaggio

1. Il piano di ingaggio non può contenere piani, processi, tecniche o procedure che esulano dall'area di competenza o livello di competenza dell'analista.

F. Processo di Testing

1. L'analista deve sempre operare entro la legge della posizione fisica degli obiettivi oltre alle regole o alle leggi che regolano la posizione dell'analista stesso.
2. Quando il test include privilegi noti, l'analista deve prima eseguire il test senza privilegi (come in un ambiente black box) prima di ripetere il test con privilegi.
3. L'analista deve conoscere i suoi strumenti, da dove provengono gli strumenti, come funzionano gli strumenti e farli testare in un'area di test limitata prima di utilizzare gli strumenti nell'organizzazione client.
4. I test che coinvolgono persone possono essere eseguiti solo su quelli identificati nell'ambito di applicazione e non possono includere persone private, associati o altre entità esterne senza l'autorizzazione scritta di tali entità.

5. Limitazioni verificate, quali violazioni scoperte, vulnerabilità con severità nota o elevata, vulnerabilità sfruttabili per accesso completo, non monitorato o non rintracciabile o che possono mettere immediatamente in pericolo la vita, scoperte durante i test devono essere segnalate al cliente con una soluzione pratica non appena vengono trovati.

G. Report

1. L'analista deve rispettare la privacy di tutti gli individui e mantenere la loro privacy per tutti i risultati.
2. I rapporti devono rimanere obiettivi e senza falsità o malizia diretta.
3. Le notifiche del cliente sono richieste ogni volta che l'analista cambia il piano di test, cambia la sede del test di origine, ha risultati di scarsa fiducia o si sono verificati problemi di test. Le notifiche devono essere fornite prima di eseguire test nuovi, pericolosi o ad alto traffico e sono richiesti regolari aggiornamenti sui progressi.
4. Laddove le soluzioni e le raccomandazioni siano incluse nel report, devono essere valide e pratiche.
5. Il Report deve contrassegnare chiaramente tutte le anomalie.
6. Il cliente deve essere avvisato quando il rapporto viene inviato per aspettarsi il suo arrivo e per confermare la ricezione della consegna.
7. Tutti i canali di comunicazione per la consegna del rapporto devono essere end-to-end riservati.
8. Risultati e rapporti non possono mai essere utilizzati per guadagno commerciale oltre a quello dell'interazione con il cliente.

H. Obiettivi

Per effettuare il test di sicurezza si sono seguite le metodologie di un tipico processo di penetration testing, ossia: Information Gathering, Target Discovery, Enumerating Target e Vulnerability Mapping, Target Exploitation, Privilege Escalation, Maintaining Access. Dopo la prima fase di Information Gathering si è proceduto al completamento di nove obiettivi:

- Recupero indirizzo IP target;
- Scansione di rete (Nmap);
- Enumerazione Utente (WPscan);
- Creazione Wordlist (CeWl);
- Cracking WordPress passwords;
- Attacco tramite SSH;
- Evasione shell limitata;
- Aumento dei privilegi;
- Mantenimento accesso tramite Backdoor;

Per il processo di penetration testing sono stati utilizzati i seguenti strumenti: Nmap, WPScan, CeWL, Metasploit, Msfvenom.

N.B. Per maggiori informazioni sul dettaglio delle metodologie e strumenti utilizzati, è stato stilato un documento ad hoc in allegato al questo report.

3. Vulnerability Report

È stata effettuata una scansione delle vulnerabilità tramite Openvas, un software open-source che permette di effettuare scansioni di sicurezza.

Dai risultati abbiamo appreso che la macchina soffre di tre vulnerabilità:

- Due vulnerabilità a Bassa criticità, riguardo l'uso di Timestamps TCP e iniezione di codice tramite Wordpress.
- Una vulnerabilità a Alta criticità, riguardo l'evasione dell'autenticazione tramite server Apache.

Inoltre, la scansione ha riportato anche sedici Log, riguardati informazioni generali della macchina target.

Nel complesso queste vulnerabilità, soprattutto quella ad alta criticità, alzano il rischio di compromissione della macchina target fino al 80%.

4. Remediation Report

Dati i problemi di sicurezza della macchina target “DC-2” si suggeriscono alcune contromisure da adottare al fine di migliorare la sicurezza.

- **Correggere** le vulnerabilità rilevate.
- **Aggiornare** costantemente i servizi utilizzati.
- **Controlli** di sicurezza devono essere eseguiti regolarmente.
- Implementare un **Firewall** per la web application al fine di bloccare e filtrare i pacchetti maliziosi.

5. Findings Summary

In questa sezione verranno presentate maggiori informazioni nel dettaglio riguardo la macchina target e le sue vulnerabilità. Nel seguente grafico, le vulnerabilità sono state raggruppate per criticità:

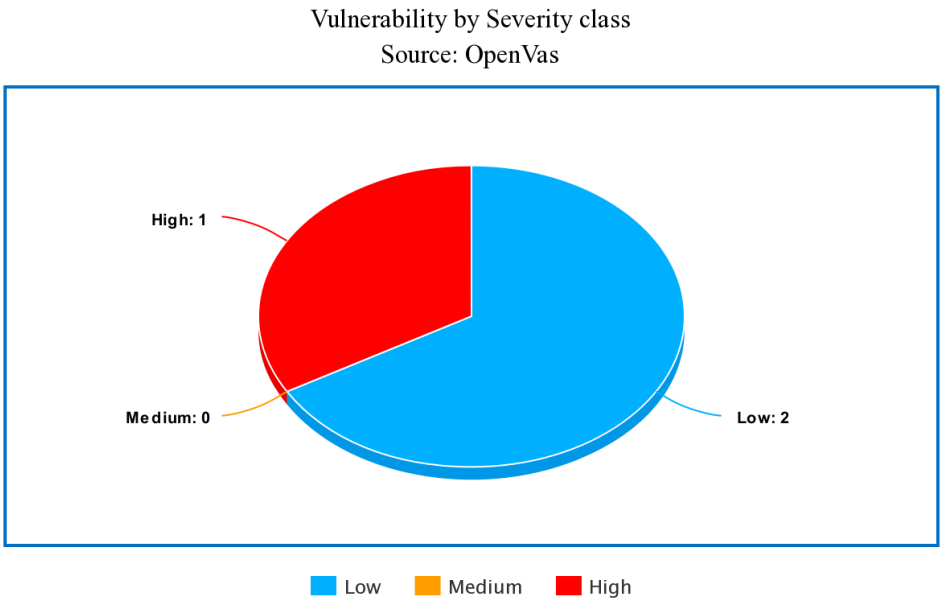

Figura 1. Grafico a torta delle vulnerabilità

Come già specificato in precedenza, il processo di Penetration Testing ha coinvolto un solo host:

ID	Indirizzo IP	Hostname	Alta	Media	Bassa	Log
1	10.0.2.7	DC-2	1	1	1	16

Nella tabella seguente verrà schematizzata la vulnerabilità a bassa criticità identificata:

ID	Vulnerabilità	Criticità	Host	Location
DC:2-1	TCP Timestamps	2.6(Bassa)	10.0.2.7	general/tcp
DC:2-2	Improper Neutralization of Input During Web Page Generation	3.5(Media)	10.0.2.7	80/tcp
DC:2-3	Improper Authentication	7.5(Alta)	10.0.2.7	7744/tcp

Tali valori sono stati ottenuti tramite una scansione dettagliata su Openvas

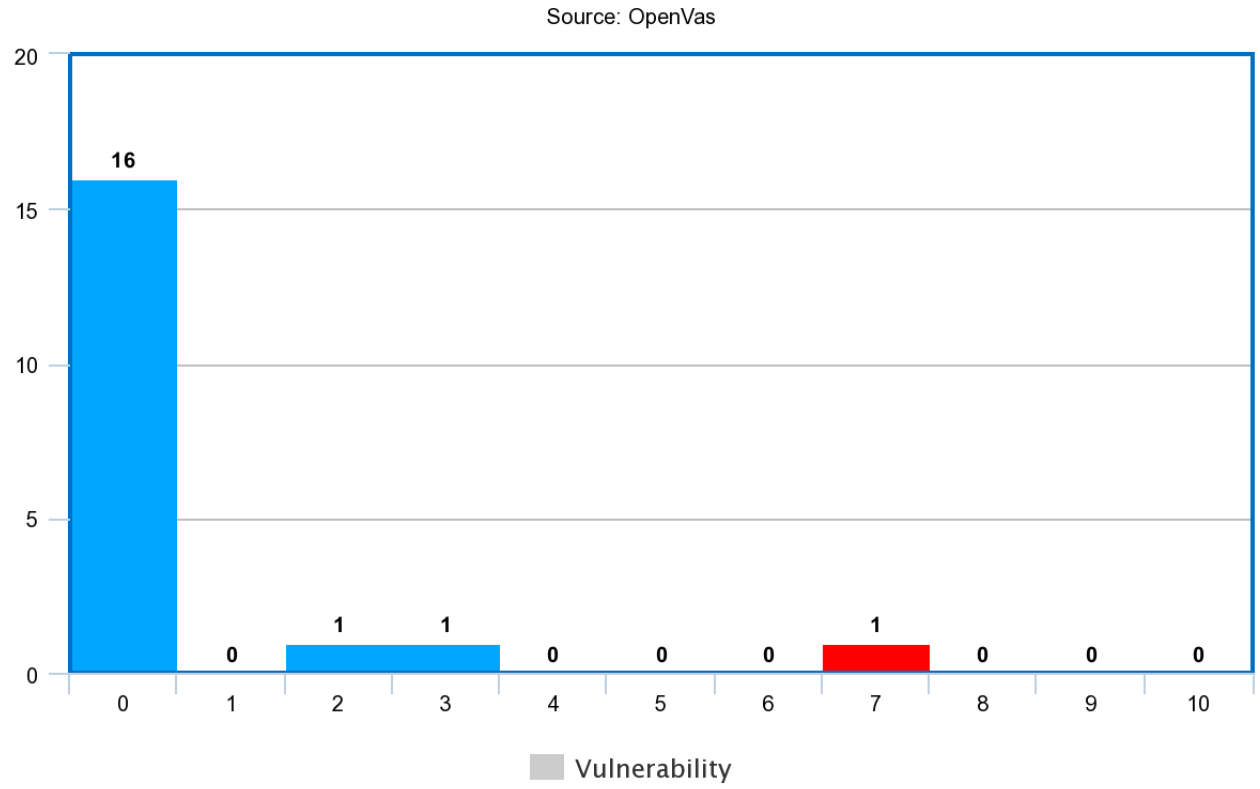

Figura 2. Istogramma numero delle vulnerabilità

Non si è ritenuto necessario schematizzare i dati riguardanti la sezione "Log" poiché trattano semplicemente di informazioni generali e non riguardano in maniera diretta le vulnerabilità.

6. Detailed Summary

In questa sezione si analizzerà ogni vulnerabilità nel dettaglio.

a. DC:2-1 Timestamps TCP

TIMESTAMPS TCP
Criticità
Bassa
Descrizione
Questo host remoto implementa i timestamps TCP tramite l'estensione RFC1323 di TCP.
Impatto
Un effetto collaterale di questa funzionalità è che il tempo di attività dell'host remoto può talvolta essere calcolato. Raccomandazioni.
Raccomandazioni
Disabilitare i timestamps TCP.
Sistemi Coinvolti
Tutte le implementazioni TCP/IPv4 che sfruttano RFC1323.
Riferimenti
http://www.ietf.org/rfc/rfc1323.txt

b. DC:2-2 Improper Neutralization of Input During Web Page Generation

Improper Neutralization of Input During Web Page Generation
Criticità
Bassa
Descrizione
Gli utenti di WordPress con privilegi inferiori possono inserire codice JavaScript nell'editor dei blocchi utilizzando uno specifico payload, che viene eseguito nella dashboard.
Impatto
Questo può portare ad un Cross Site Scripting (XSS) se un amministratore apre il post nell'editor.
Raccomandazioni
Aggiornare il servizio alla versione più recente
Sistemi Coinvolti
WordPress version from 3.7 to 5.3
Riferimenti
Https://www.debian.org/security/2020/dsa-4599

c. DC:2-3 Improper Authentication

Improper Authentication
Criticità
Alta
Descrizione
In Apache l'uso di ap_get_basic_auth_pw () da parte di moduli di terze parti al di fuori della fase di autenticazione può comportare l'aggiramento dei requisiti di autenticazione.
Impatto
Un utente malintenzionato remoto potrebbe utilizzare questo difetto per bypassare l'autenticazione richiesta se l'API è utilizzata in modo errato da uno dei moduli di httpd.
Raccomandazioni
Aggiornare il servizio alla versione più recente
Sistemi Coinvolti
Apache http server 2.4.10
Riferimenti
https://access.redhat.com/security/cve/cve-2017-3167

7. References

- E-Learning platform: PTEH
- ISECOM:OSSTMM report
- National Vulnerability DB
- Juliocesarfort Public-Pentesting-Reports
- RedHat CVE Database

8. Appendix

8.1 Table of Figures

Figura 1. Grafico a torta delle vulnerabilità 8
Figura 2. Istogramma numero delle vulnerabilità 9