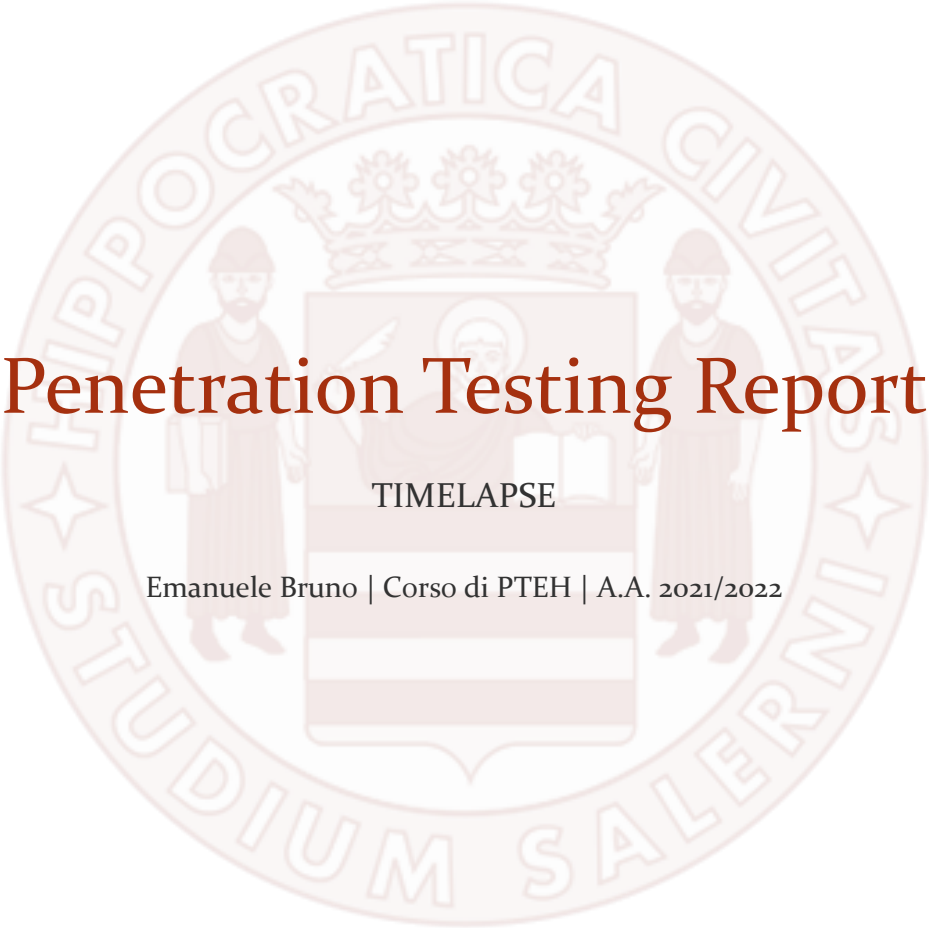
Università degli Studi di Salerno



Penetration Testing Report

TIMELAPSE

Emanuele Bruno | Corso di PTEH | A.A. 2021/2022

UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA

Sommario

Executive Summary

L'attività descritta in questo documento riguarda l'esecuzione di un penetration test verso il target identificato dalla macchina chiamata Timelapse presente sulla piattaforma Hack the Box https://app.hackthebox.com/machines/Timelapse

Data	Operatore	Asset testato
Luglio 2022	Emanuele Bruno	Timelapse

Durante l'attività l'operatore ha rilevato diverse vulnerabilità che nell'insieme delle stesse hanno permesso allo stesso di prendere il controllo dell'asset con privilegi elevati, registrando una precaria postura di sicurezza dell'asset.

Come descritto nelle sezioni a seguire, l'operatore ha svolto l'attività seguendo le fasi e le metodologie standard percorrendo tutte le fasi del penetration test.

L'operatore era a conoscenza solamente dell'indirizzo IP dell'asset.

Poiché' l'esito del test rivela un altissimo rischio di compromissione dell'asset e possibilmente dell'infrastruttura circostante, all'interno di questo documento oltre a descrivere dettagliatamente tutte le vulnerabilità e le misconfigurazioni rilevate, sono riportate e descritte le possibili mitigazioni da attuare.

Al termine dell'applicazione delle suddette mitigazioni è altamente consigliato se non obbligato testare di nuovo l'asset.

Engagement Highlights

Scope:

- Asset: Timelapse
- Informazioni: Macchina con sistema operativo windows
- Indirizzo IP: 10.10.11.152

Situazione iniziale:

- L'operatore raggiunge l'infrastruttura dell'asset tramite vpn fornita dal cliente

Regole di ingaggio:

- L'attività è autorizzata solo ed esclusivamente verso gli assets delineati nello scope.
- Durante l'attività è strettamente vietato l'uso di tecniche di phishing o di social engineering.
- Durante l'attività è strettamente vietato l'esfiltrazione e/o l'archiviazione di qualsiasi appunto, documento e/o dato che possa essere confidenziale nel contesto di business e/o privacy del cliente.
- Durante l'attività se si dovesse registrare la possibilità di movimento laterale è strettamente vietato procedere unilateralmente e la prosecuzione del test verso eventuali nuovi target deve essere discusso e contrattualizzato bilateralmente.
- È strettamente vietata la divulgazione a qualsiasi titolo di qualsiasi informazione relativa al cliente e/o agli assets testati da parte dell'operatore e/o qualsiasi dipendente del fornitore del servizio.
- Per qualsiasi chiarimento e/o informazione aggiuntiva sugli asset e/o la loro infrastruttura rivolgersi solo ed unicamente al seguente punto di contatto admin@hackthebox.htb

Fasi del test:

- Information gathering e target discovery
- Smb enumeration e discovery
- Sensitive File exfiltration e password protected file cracking
- Target exploitation
- Privilege escalation

Vulnerability Report

Durante l'attività sono state riscontrate molteplici vulnerabilità causate dalla scarsa comprensione di concetti relativi alla sicurezza (security awareness) del personale dell'organizzazione e di conseguenza dall'implementazione di errate configurazioni e dalla pericolosa gestione di file sensibili.

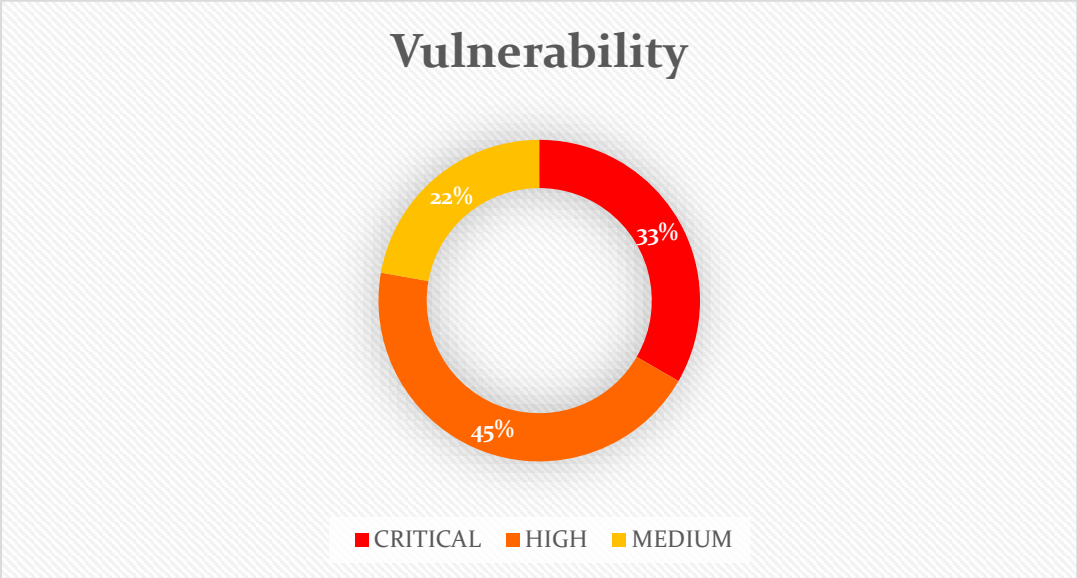
Remediation Report

Le attività di vulnerability assessment e penetration testing hanno messo in evidenza una precaria postura di sicurezza della macchina analizzata. Si raccomanda di adottare le seguenti remediations al fine di migliorare la sicurezza:

- Si raccomanda all'organizzazione delle campagne di sensibilizzazione sulla sicurezza e relativa gestione degli asset IT (*security awareness*).
- Implementazione e gestione di *policies* più stringenti relative alla gestione degli e alla confidenzialità degli *assets* e dei relativi dati.
- Risolvere le vulnerabilità presentate in questo documento in ordine decrescente in base alla gravita delle stesse, in generale si raccomanda di aggiornare sempre le versioni dei software ritenuti a rischio.
- Utilizzare password da più di 12 caratteri comprendendo alfanumerici e caratteri speciali. Per la gestione di password complesse si consiglia vivamente l'uso di un password manager.
- Rimuovere il permesso "all extended rights" dagli utenti e dai gruppi che non devono avere accesso alla password dell'amministratore locale (si tenga a mente che tale password è salvata in clear text in un attributo).
- Il "SELF" principal richiede la capacità di modificare gli attributi "ms-Mcs-AdmPwdExpirationTime" e "ms-Mcs-AdmPwd" in modo da poter aggiornare la password e l'expiration time quando una password scade, l'ACE per "SELF" è necessario su tutti gli oggetti governati da LAPS.
- Gli utenti e i gruppi a cui è permesso resettare la password sull'account degli amministratori locali devono avere accesso agli attributi su quegli oggetti
- Si raccomanda, oltre a proteggere i due attributi sopra citati, di monitorare il traffico LDAP su di essi in modo da poter identificare eventuali attaccanti che dovessero provare a richiederli. StealthDEFEND per active directory. può fornire degli alert in tempo reale.

Findings Summary

Durante le attività di vulnerability assessment con OenVAS e penetration testing sono state individuate diverse vulnerabilità nella macchina Timelapse, tali vulnerabilità sono state suddivise in quattro classi in base alla loro gravità.



	CRITICAL	HIGH	MEDIUM	LOW
# Vulnerabilità'	3	2	2	0

- CRITICAL: vulnerabilità che possono avere un impatto elevato e che possono consentire ad un utente malintenzionato di ottenere un controllo completo e/o parziale del sistema.

- HIGH: vulnerabilità che richiedono determinati requisiti per poter essere sfruttate e hanno un impatto relativamente alto sul sistema.

- MEDIUM: vulnerabilità non semplici da sfruttare e che, nella maggior parte dei casi, non hanno un impatto diretto molto significativo.

- LOW: vulnerabilità che hanno un impatto poco significativo e che hanno una bassa probabilità di essere sfruttate e, pertanto, non rappresentano, nell'immediato, una minaccia rilevante per il sistema.

Detailed Summary

File sensibili protetti con password deboli	CWE
	16
CRITICAL	
Descrizione: Proteggere file con informazioni sensibili per l'accesso ai sistemi con password deboli può agevolare l'attaccante nel processo di recupero di queste informazioni. In particolare, in questo caso il file "winrm_backup.zip" e il file "legacyy_dev_auth.pfx" contenuto in esso sono entrambi protetti da password deboli.	
Impatto: Il reperimento di informazioni sensibili riguardo i sistemi e/o l'infrastruttura da parte di un attaccante (eg credenziali, topologia della rete, versioni dei sistemi, report di precedenti audit, etc) in proporzione alla sensibilità possono avere impatti critici. In questo caso l'operatore ha facilmente ricavato tali password avendo accesso diretto alle credenziali di winrm	
Soluzione: Modificare tali password scegliendone di più forti.	
Metodo di detection: Vulnerabilità identificata manualmente durante il processo di penetration testing.	

Exposure of sensitive information to an unauthorized actor	CWE
	200
CRITICAL	
Descrizione: Il file "legacyy_dev_auth.pfx" si trova all'interno di un file zip in una share a cui è possibile accedere come guest	
Impatto: Un attaccante può ottenere il file accedendo alla cartella "Shares" come guest appropriandosi quindi di un file estremamente sensibile	
Soluzione: Modificare i permessi di accesso della cartella in modo da evitare che ci si possa accedere come guest	
Metodo di detection: Vulnerabilità identificata manualmente durante il processo di penetration testing.	

Exposure of sensitive information to an unauthorized actor	CWE
	200
CRITICAL	
Descrizione: Informazioni riguardo all'accesso, ovvero nome utente e password, lasciate su file di sistema in chiaro. In particolare, nella history di powershell sono rimaste tracce di comandi da parte di amministratore di sistema contenenti informazioni critiche relative all'accesso al sistema.	
Impatto: Un attaccante può utilizzare queste informazioni per accedere al sistema e garantirsi la persistenza essendo credenziali di account validi.	
Soluzione: Cancellare la history e in generale non tenere nessuna informazione di accesso in chiaro sui sistemi.	
Metodo di detection: Vulnerabilità identificata manualmente durante il processo di penetration testing.	

LAPS misconfiguration	CWE
	16
HIGH	
Descrizione: LAPS è un componente aggiuntivo per la sicurezza di sistemi a dominio windows, questa funzionalità, se implementata, deve sempre essere configurata con attenzione, altrimenti potrebbe aumentare la superficie di attacco ottenendo l'effetto contrario al suo scopo.	
Impatto: Un attaccante può sfruttare queste configurazioni non sicure per ottenere la password di amministratore locale. In particolare, sulla macchina è stato possibile ricavare la password dell'amministratore locale tramite un utente di servizio permettendo l'elevazione dei privilegi.	
Soluzione: Ricontrollare la configurazione usando le best practices citate nel capitolo remediations. In particolare, sull'asset testato eliminare l'utente "svc_deploy" dal gruppo "LAPS_readers"	
Metodo di detection: Vulnerabilità identificata manualmente durante il processo di penetration testing.	

Microsoft Windows SMB Guest Account Local User Access	CVE
	1999-0519
HIGH	
Descrizione: Microsoft Windows è soggetto a una vulnerabilità di bypass dell'autenticazione tramite SMB/NETBIOS.	
Impatto: Un attaccante può accedere come utente guest.	
Soluzione: aggiornamento a una release più recente, la disattivazione delle rispettive funzionalità, rimuovere il prodotto o sostituirlo con un altro. - Disattivare il login a sessione non autenticata ("guest" account). - Rimuovere la condivisione. - Abilitare le password sulla condivisione.	
Metodo di detection: Vulnerabilità identificata manualmente durante il processo di penetration testing.	

NVT: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	CWE
	1999-0519
HIGH	
Descrizione: Microsoft Windows is prone to an authentication bypass vulnerability via SMB/NETBIOS.	
Impatto: Successful exploitation could allow attackers to use shares to cause the system to crash	
Soluzione: Solution type: WillNotFix No known solution was made available for at least one year since the disclosure of this vulnerability. Likely none will be provided anymore. General solution options are to upgrade to a newer release, disable respective features, remove the product or replace the product by another one. A workaround is to, - Disable null session login. - Remove the share. - Enable passwords on the share.	
Metodo di detection: Details: Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability OID:1.3.6.1.4.1.25623.1.0.801991 Version used: 2022-03-03T10:23:45Z	

NVT: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	CWE
	2016-2183 2016-6329 2020-12872
HIGH	
Descrizione: This routine reports all SSL/TLS cipher suites accepted by a service where attack vectors exists only on HTTPS services.	
Soluzione: Solution type: Mitigation The configuration of this services should be changed so that it does not accept the listed cipher suites anymore. Please see the references for more resources supporting you with this task.	
Metodo di detection: Details: SSL/TLS: Report Vulnerable Cipher Suites for HTTPS OID:1.3.6.1.4.1.25623.1.0.108031 Version used: 2021-09-20T09:01:50Z	

NVT: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	CWE
	2011-3389 2015-0204
MEDIUM	
Descrizione: It was possible to detect the usage of the deprecated TLSv1.0 and/or TLSv1.1 protocol on this system.	
Impatto: An attacker might be able to use the known cryptographic flaws to eavesdrop the connection between clients and the service to get access to sensitive data transferred within the secured connection. Furthermore newly uncovered vulnerabilities in this protocols won't receive security updates anymore.	
Soluzione: Solution type: Mitigation It is recommended to disable the deprecated TLSv1.0 and/or TLSv1.1 protocols in favor of the TLSv1.2+ protocols. Please see the references for more information.	
Metodo di detection: Check the used TLS protocols of the services provided by this system. Details: SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection OID:1.3.6.1.4.1.25623.1.0.117274 Version used: 2021-07-19T08:11:48Z	

NVT: DCE/RPC and MSRPC Services Enumeration Reporting	CWE
	-
MEDIUM	
Descrizione: Distributed Computing Environment / Remote Procedure Calls (DCE/RPC) or MSRPC services running on the remote host can be enumerated by connecting on port 135 and doing the appropriate queries.	
Impatto: An attacker may use this fact to gain more knowledge about the remote host.	
Soluzione: Solution type: Mitigation Filter incoming tra-c to this ports.	
Metodo di detection: Details: DCE/RPC and MSRPC Services Enumeration Reporting OID:1.3.6.1.4.1.25623.1.0.10736 Version used: 2022-06-03T10:17:07Z	

References

- https://github.com/crackpkcs12/crackpkcs12
- https://sleeplessbeastie.eu/2015/05/25/how-to-crack-archive-password-faster/
- https://en.wikipedia.org/wiki/PKCS_12
- https://tecadmin.net/extract-private-key-and-certificate-files-from-pfx-file/#:~:text=Command%20to%20Extract%20Private%20Key%20from%20PFX%20Open,the%20SSL%20certificate%20file%20from%20the%20pfx%20file
- https://github.com/crackpkcs12/crackpkcs12
- https://www.openssl.org/docs/man1.1.1/man1/openssl-pkcs12.html
- https://www.kali.org/tools/evil-winrm/
- https://github.com/carlospolop/PEASS-ng/blob/master/winPEAS/winPEASexe/README.md
- http://woshub.com/powershell-commands-history/
- https://adsecurity.org/?p=3164
- https://smarthomepursuits.com/export-laps-passwords-powershell/
- https://attack.mitre.org/