ARMAGGEDON

CVAS

Vulnerability Assessment Report

Report of Findings

Certified Vulnerability Assessment Specialist (CVAS) Report

Candidate Name:

Umberto Favaro
Tommaso Barbolani
Leonardo Paglia
Rocco Zamarco
Marco Bagarolo
Luca Minello
Marco Simioni

WeakCorp

19 giugno 2024

Version: 1.0s

Table of Contents

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure.

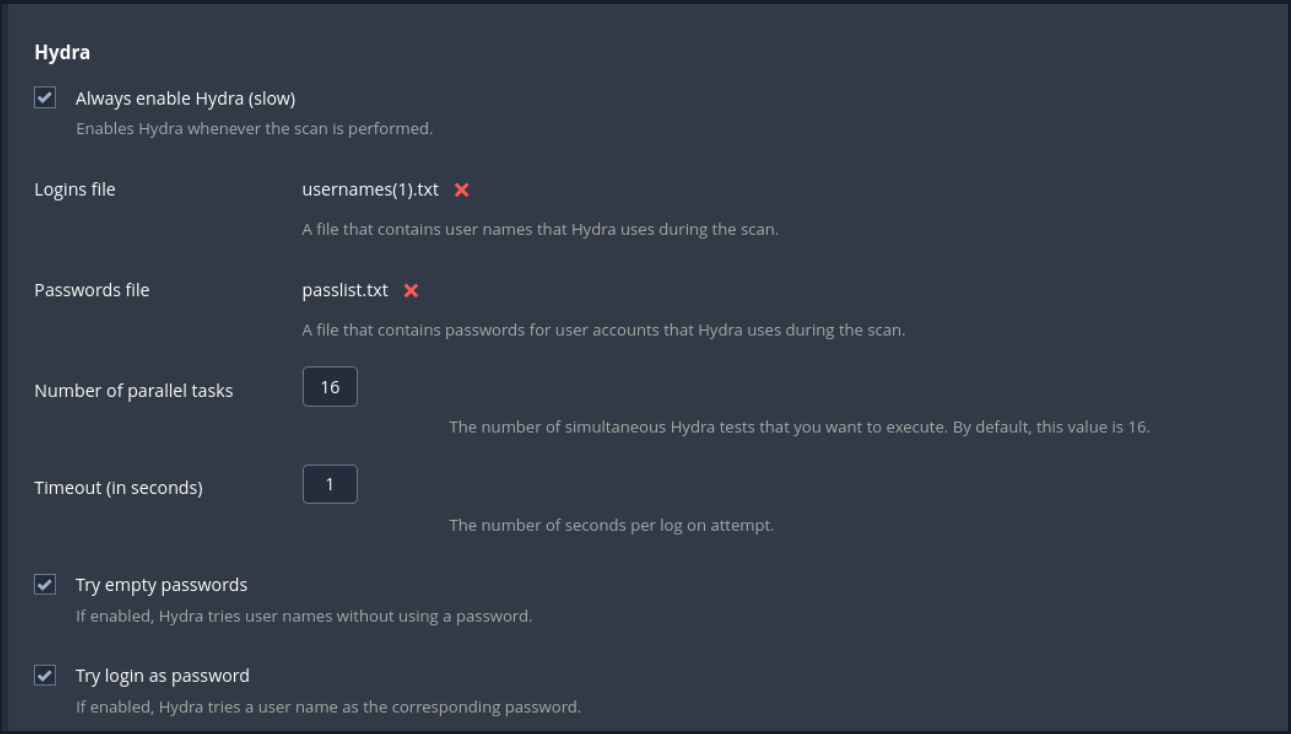
2 Engagement Contacts

WeakCorp Contacts		
Contact	**Title**	**Contact Email**
Marco Negro	CEO	marco.negro

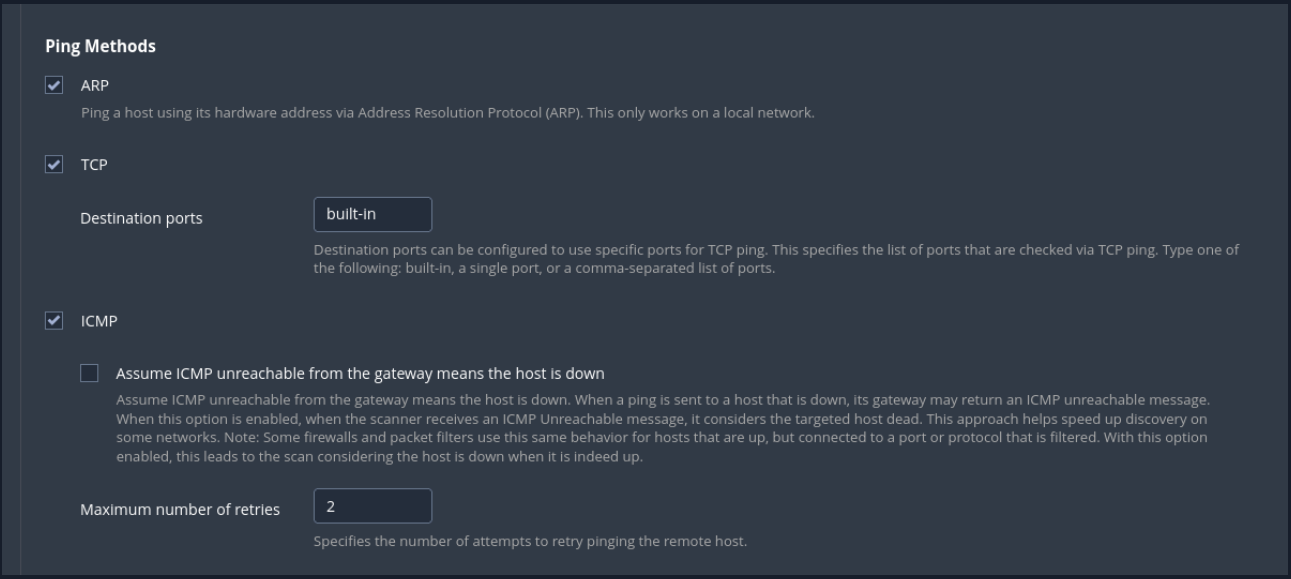
Assessor Contact		
Assessor Name	**Title**	**Assessor Contact Email**
	ARMAGEDDON	security@armageddon.pt

3 Executive Summary

Ci è stato assegnato dal nostro cliente il compito di eseguire un Vulnerability Assessment sulla rete del cliente. Il range di rete che ci è stato permesso di scansionare era 192.168.20.0/24, quindi abbiamo avviato Tenable Nessus per eseguire la nostra scansione. La nostra istanza di Nessus è stata configurata per effettuare anche un brute force sui servizi trovati sulle macchine utilizzando alcuni nomi utente e password comuni.



Abbiamo anche configurato Nessus per scoprire gli host utilizzando diversi protocolli.



La scansione è stata avviata e al suo completamento ha evidenziato la presenza di 8 host nell'intervallo di rete selezionato, con diverse vulnerabilità, che vanno da bassa a critica, che verranno spiegate in dettaglio qui sotto. Ecco un riepilogo delle vulnerabilità trovate in ciascun host: Ecco la traduzione in italiano del testo fornito:

Ci è stato assegnato dal nostro cliente il compito di eseguire una Valutazione delle Vulnerabilità sulla rete del cliente. L'intervallo di rete che ci è stato permesso di scansionare per le vulnerabilità era 192.168.20.0/24, quindi abbiamo avviato Tenable Nessus per eseguire la nostra scansione. Abbiamo configurato la nostra istanza di Nessus per effettuare anche un brute force sui servizi trovati sulle macchine utilizzando alcuni nomi utente e password comuni. {width="auto"} Abbiamo anche configurato Nessus per scoprire gli host utilizzando diversi protocolli. {width="auto"} Quando tutto era configurato, abbiamo avviato la scansione e aspettato il suo completamento. Nessus ha rivelato la presenza di 8 host nell'intervallo di rete selezionato, con diverse vulnerabilità, che vanno da bassa a critica, che verranno spiegate in dettaglio qui sotto. Ecco un riepilogo delle vulnerabilità trovate in ciascun host: Ecco la traduzione in italiano del testo fornito:

Ci è stato assegnato dal nostro cliente il compito di eseguire una Valutazione delle Vulnerabilità sulla rete del cliente. L'intervallo di rete che ci è stato permesso di scansionare per le vulnerabilità era 192.168.20.0/24, quindi abbiamo avviato Tenable Nessus per eseguire la nostra scansione. Abbiamo configurato la nostra istanza di Nessus per effettuare anche un brute force sui servizi trovati sulle macchine utilizzando alcuni nomi utente e password comuni. {width="auto"} Abbiamo anche configurato Nessus per scoprire gli host utilizzando diversi protocolli. {width="auto"} Quando tutto era configurato, abbiamo avviato la scansione e aspettato il suo completamento. Nessus ha rivelato la presenza di 8 host nell'intervallo di rete selezionato, con diverse vulnerabilità, che vanno da bassa a critica, che verranno spiegate in dettaglio qui sotto. Ecco un riepilogo delle vulnerabilità trovate in ciascun host:

IP	N° di vulnerabilità
192.168.20.101	11
192.168.20.102	9
192.168.20.103	9
192.168.20.104	10
192.168.20.105	9
192.168.20.106	16
192.168.20.132	12
192.168.20.142	3

Le vulnerabilità trovate sono in numero considerevole e alcune di esse sono di rilevante gravità:

Gravità	Numero di Vulnerabilità
Bassa	12
Media	57
Alta	9
Critica	1

3.1 Approach

ha eseguito i test sotto un approccio "Black Box" dal 17 giugno 2024 al 18 giugno 2024 senza credenziali o alcuna conoscenza preliminare dell'ambiente esterno di WeakCorp con l'obiettivo di identificare vulnerabilità sconosciute. I test sono stati eseguiti da un punto di vista non invasivo con l'obiettivo di scoprire il maggior numero possibile di configurazioni errate e vulnerabilità. I test sono stati eseguiti da remoto dai laboratori di valutazione di . Ogni vulnerabilità identificata è stata documentata e indagata manualmente per determinare le possibilità di sfruttamento e il potenziale di escalation. ha cercato di dimostrare il pieno impatto di ogni vulnerabilità, fino ad includere il compromesso del dominio interno. Se fosse riuscito a ottenere un punto d'appoggio nella rete interna, WeakCorp a seguito del test della rete esterna, WeakCorp ha consentito ulteriori test inclusi movimenti laterali e escalation di privilegi orizzontale/verticale per dimostrare l'impatto di un compromesso della rete interna.

3.2 Scope

L'ambito di questa valutazione includeva un indirizzo IP esterno, due range di rete interni, il dominio Active Directory TODO INSERT DOMAIN NAME e qualsiasi altro dominio Active Directory posseduto da WeakCorp scoperto in caso di accesso alla rete interna.

In Scope Assets

Host/URL/IP Address	Description
TODO 10.129.X.X	TODO
172.16.139.0/24	WeakCorp internal network
172.16.210.0/24	WeakCorp internal network
TODO	WeakCorp internal AD domain
TODO other discovered internal domain(s)	TODO

3.3 Assessment Overview and Recommendations

During the penetration test against WeakCorp, identified 13 findings that threaten the confidentiality, integrity, and availability of WeakCorp's information systems. The findings were categorized by severity level, with TODO SEVERITY RATINGS HERE 1 of the findings being assigned a critical-risk rating, high-risk, 8 medium-risk, and 0 low risk. There were also 0 informational finding related to enhancing security monitoring capabilities within the internal network.

TODO EXECUTIVE SUMMARY HERE

WeakCorp should create a remediation plan based on the Remediation Summary section of this report, addressing all high findings as soon as possible according to the needs of the business. WeakCorp should also consider performing periodic vulnerability assessments if they are not already being performed. Once the issues identified in this report have been addressed, a more collaborative, in-depth Active Directory security assessment may help identify additional opportunities to harden the Active Directory environment, making it more difficult for attackers to move around the network and increasing the likelihood that WeakCorp will be able to detect and respond to suspicious activity.

4 Network Penetration Test Assessment Summary

4.1 Summary of Findings

In the course of this penetration test **1 Critical**, **4 High** and **8 Medium** vulnerabilities were identified:

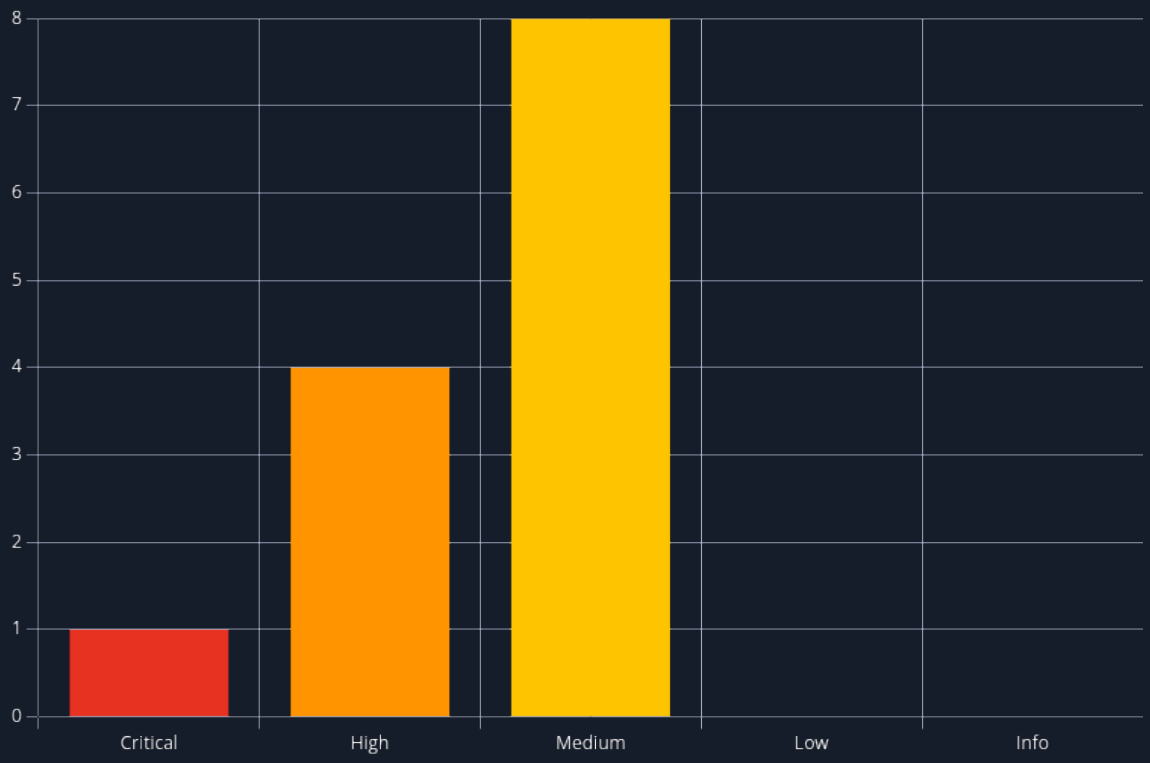


Figure 1 - Distribution of identified vulnerabilities

Below is a high-level overview of each finding identified during testing. These findings are covered in depth in the Technical Findings Details section of this report.

#	Severity Level	Finding Name	Page
1	9.8 (Critical)	Windows Administrator Default Password	13
2	7.5 (High)	Apache Tomcat 9.0.71 < 9.0.74 DoS	14
3	7.5 (High)	SSL Certificate Signed Using Weak Hashing Algorithm	15
4	7.5 (High)	SSL Medium Strength Cipher	16
5	7.5 (High)	SSL Weak Hashing Algorithm	17
6	6.8 (Medium)	OpenSSH multiple vulnerabilities	18
7	6.5 (Medium)	OpenSSH < 9.6 Multiple Vulnerabilities	19
8	6.5 (Medium)	SSL Certificate Cannot Be Trusted	20

End of Report

This report was rendered
by SysReptor with
♥