

## **Project 3**

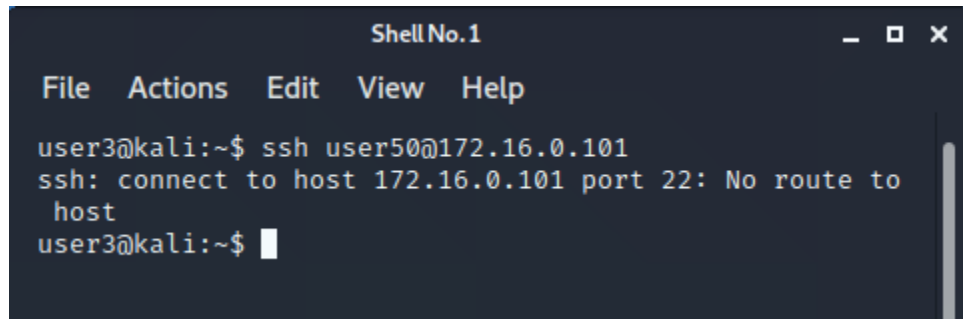
CS 4371

Benjamin Nye  
Brandon Shelton  
Bridgett Tijerina  
Jacob Lopez

## **Section I (Introduction) – Benjamin Nye:**

For Project 3, our group learned cryptographic algorithms and protocols using passwords and keys, how to crack passwords using different methods, and how to use and develop various security tools. The roles of the members in our group were for each of us to complete a task and section of the report. Task I was completed by Jacob, Task II was completed by Brandon, Task III was completed by Bridgett, and Task IV was completed by Benjamin. For the report, Benjamin worked on sections I and V, Jacob worked on section II, Brandon worked on section III, and Bridgett worked on section IV. As a group we met on Zoom and in the computer lab to discuss the project and work on the tasks. When not meeting, we used GroupMe to coordinate and ask each other questions when we needed assistance.

## Section II (Task I) – Jacob:



```
Shell No.1
File Actions Edit View Help
user3@kali:~$ ssh user50@172.16.0.101
ssh: connect to host 172.16.0.101 port 22: No route to
host
user3@kali:~$
```

I was unable to establish a connection to A.1 from A.2 using ssh. I was also unable to ssh to A.1 using user3 as well.

However I estimate that it would take about .00000006 seconds to test one password.

If the dictionary has 1 millions passwords I would estimate that it takes about .0587 seconds to test all of the passwords.

## Section III (Task II) – Brandon:

*Each attempt seems to start but gives messages that it could not connect to either 172.16.0.101 (A1) or 10.0.0.3 (B2), but then gives a message indicating “Scanned 1 of 1 hosts (100% complete)”. However, I don’t see the found username or password afterward though, even with the “info” command.*

*I’m wondering if there is something in task 1 that has to be done first or if our network settings aren’t quite right. But I don’t think we had a problem with the last task, bringing the file over from A1 to A2, so I’m confused.*

*\*Just a note, you can use the command “unset” to clear any flags [such as “unset USERNAME”], after the first run so that it does not try running with both USERNAME and USER\_FILE both set to something. That may cause problems.*

```
msf5 > use auxiliary/scanner/ssh_login
msf5 auxiliary(scanner/ssh_login) > set RHOSTS 172.16.0.101
RHOSTS => 172.16.0.101
msf5 auxiliary(scanner/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/ssh_login) > set USERNAME users0
USERNAME => users0
msf5 auxiliary(scanner/ssh_login) > set PASS_FILE dictionary.txt
PASS_FILE => dictionary.txt
msf5 auxiliary(scanner/ssh_login) > set VERBOSE true
VERBOSE => true
msf5 auxiliary(scanner/ssh_login) > info

Name: SSH Login Check Scanner
Module: auxiliary/scanner/ssh_login
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
todb <toadb@metasploit.com>

Check supported:
No

Basic options:


| Name             | Current Setting | Required | Description                                                  |
|------------------|-----------------|----------|--------------------------------------------------------------|
| BLANK_PASSWORDS  | false           | no       | Try blank passwords for all users                            |
| BRUTEFORCE_SPEED | 5               | yes      | How fast to bruteforce, from 0 to 5                          |
| DB_ALL_CREDS     | false           | no       | Try each user/password couple stored in the current database |
| DB_ALL_PASS      | false           | no       | Add all passwords in the current database                    |



msf5 auxiliary(scanner/ssh_login) > run

[-] Could not connect: The host (172.16.0.101:22) was unreachable.
[-] No active DB -- Credential data will not be saved!
[-] Could not connect: The host (172.16.0.101:22) was unreachable.
[-] Could not connect: The host (172.16.0.101:22) was unreachable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh_login) > set RHOSTS 10.0.0.2
RHOSTS => 10.0.0.2
msf5 auxiliary(scanner/ssh_login) > set RHOSTS 10.0.0.3
RHOSTS => 10.0.0.3
msf5 auxiliary(scanner/ssh_login) > set USER_FILE /usr/share/metasploit-framework/data/wordlists/http_default_users.txt
USER_FILE => /usr/share/metasploit-framework/data/wordlists/http_default_users.txt
msf5 auxiliary(scanner/ssh_login) > set PASS_FILE /usr/share/metasploit-framework/data/wordlists/http_default_pass.txt
PASS_FILE => /usr/share/metasploit-framework/data/wordlists/http_default_pass.txt
msf5 auxiliary(scanner/ssh_login) > info

Name: SSH Login Check Scanner
Module: auxiliary/scanner/ssh_login
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
todb <toadb@metasploit.com>

Check supported:
No
```

```
msf5 auxiliary(scanner/ssh_login) >
msf5 auxiliary(scanner/ssh_login) >
msf5 auxiliary(scanner/ssh_login) > unset USERNAME
msf5 auxiliary(scanner/ssh_login) > run

[-] Could not connect: The host (10.0.0.3:22) was unreachable.
[-] No active DB -- Credential data will not be saved!
[-] Could not connect: The host (10.0.0.3:22) was unreachable.
[-] Could not connect: The host (10.0.0.3:22) was unreachable.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh_login) > info

Name: SSH Login Check Scanner
Module: auxiliary/scanner/ssh_login
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
todb <toadb@metasploit.com>

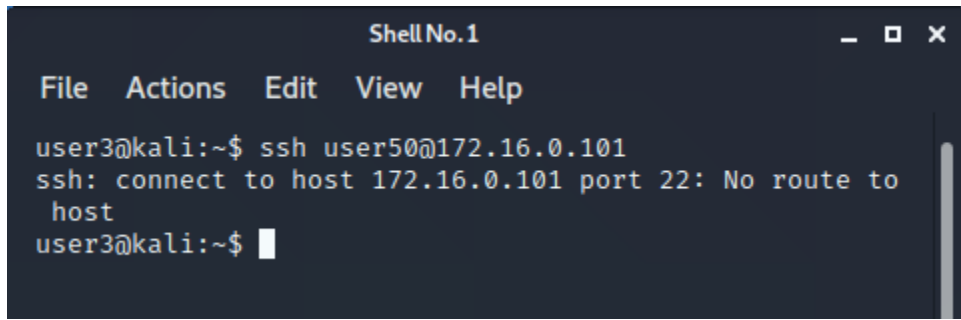
Check supported:
No

Basic options:


| Name            | Current Setting | Required | Description                       |
|-----------------|-----------------|----------|-----------------------------------|
| BLANK_PASSWORDS | false           | no       | Try blank passwords for all users |


```

## Section IV (Task III) – Bridgett:

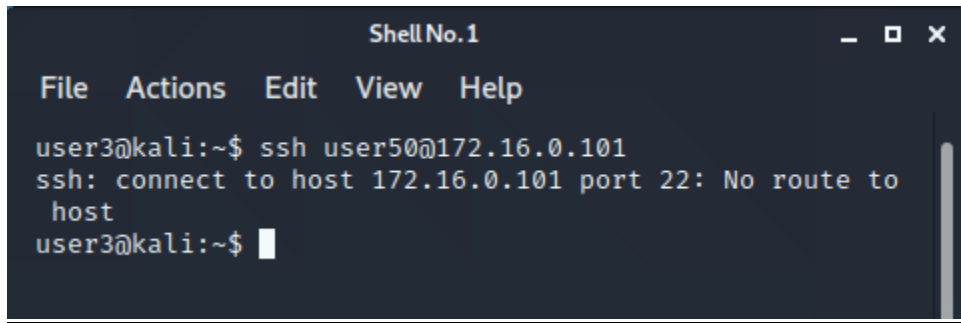


```
Shell No.1
File Actions Edit View Help
user3@kali:~$ ssh user50@172.16.0.101
ssh: connect to host 172.16.0.101 port 22: No route to
host
user3@kali:~$
```

We were unable to ssh to A.1 from A.2 therefore, I was unable to retrieve the “secret.pdf.enc1” and “secret.pdf.enc2” in order to attempt the cryptanalysis cracking.

I believe that it would not take very long to brute force these encryptions since the first 8 bytes of “secret.pdf.enc1” are always going to be the same. This would make it easy to guess the key since we already know what those first 8 bytes will correspond to.

## Section V (Task IV) – Benjamin:



```
Shell No.1
File Actions Edit View Help
user3@kali:~$ ssh user50@172.16.0.101
ssh: connect to host 172.16.0.101 port 22: No route to
host
user3@kali:~$
```

Due to our issues with being able to ssh to A.1, I was unable to retrieve the file to apply the cryptanalysis program to.

If I was able to retrieve the file then I would have had the program come up with a possible key, and a second possible key to try if the first one fails. If the first one fails then create another possible key to try after testing the second key and continue that until one of the keys works. If it works then stop generating possible keys and apply the one that worked.