

Deploying a Honeypot Server on the Network

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 05

Student:

Truc Huynh

Email:

huyntl02@pfw.edu

Time on Task:

1 hour, 46 minutes

Progress:

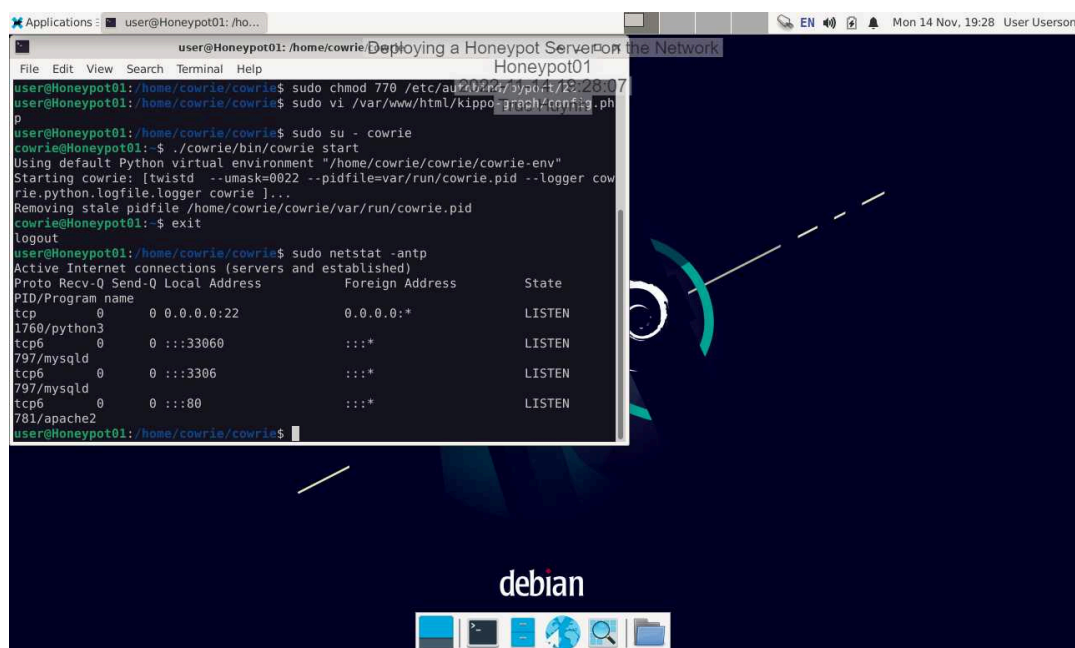
100%

Report Generated: Monday, November 14, 2022 at 8:46 PM

Hands-On Demonstration

Part 1: Configure an SSH Honeypot

37. **Make a screen capture** showing all three services listening on their default ports.

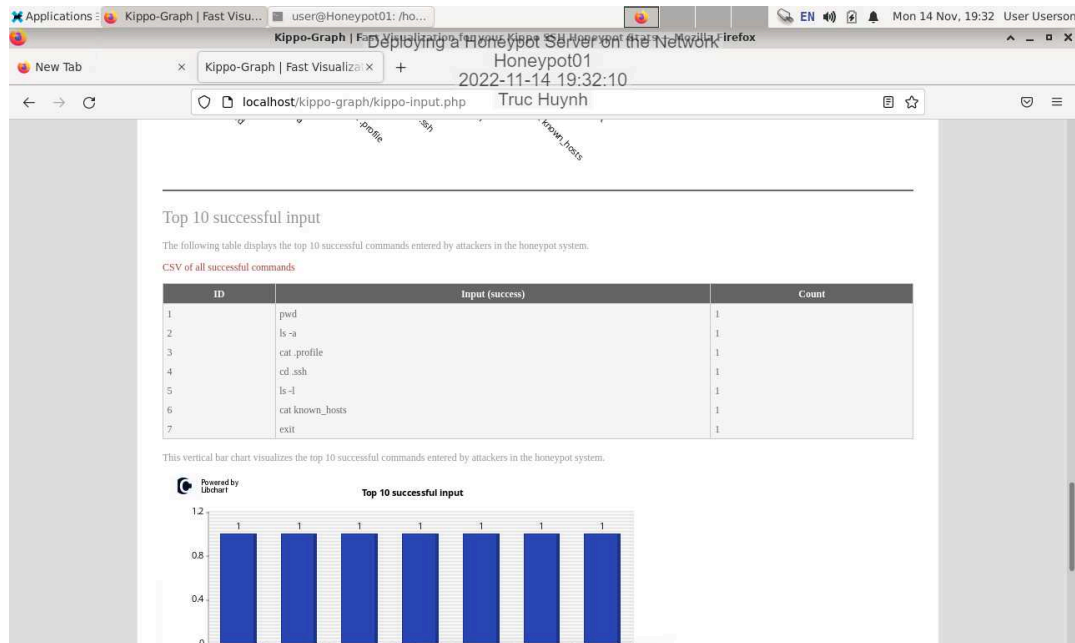


```
user@HoneyPot01: /home/cowrie$ sudo chmod 770 /etc/audit/audit.rules
user@HoneyPot01: /home/cowrie/cowrie$ sudo vi /var/www/html/Kippo-graph/config.php
user@HoneyPot01: /home/cowrie/cowrie$ sudo su - cowrie
cowrie@HoneyPot01: ~$ ./cowrie/bin/cowrie start
Using default Python virtual environment "/home/cowrie/cowrie-env"
Starting cowrie: [twisted --umask=0022 --pidfile=/var/run/cowrie.pid --logger cowrie.python.logfile.logger cowrie ]...
Removing stale pidfile /home/cowrie/cowrie/var/run/cowrie.pid
cowrie@HoneyPot01: ~$ exit
logout
user@HoneyPot01: /home/cowrie/cowrie$ sudo netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
1760/python3
tcp6       0      0 :::33060                :::*                    LISTEN
797/mysqld
tcp6       0      0 :::3306                 :::*                    LISTEN
797/mysqld
tcp6       0      0 :::80                   :::*                    LISTEN
781/apache2
user@HoneyPot01: /home/cowrie/cowrie$
```

Deploying a Honeypot Server on the Network

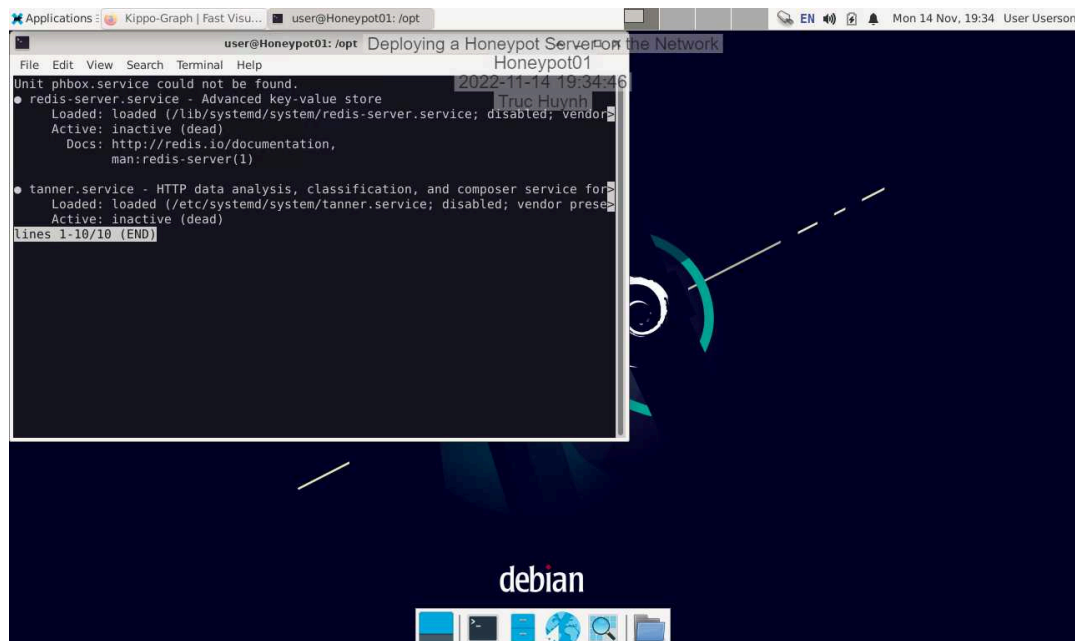
Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 05

51. **Make a screen capture** showing the commands used per the accompanying table.



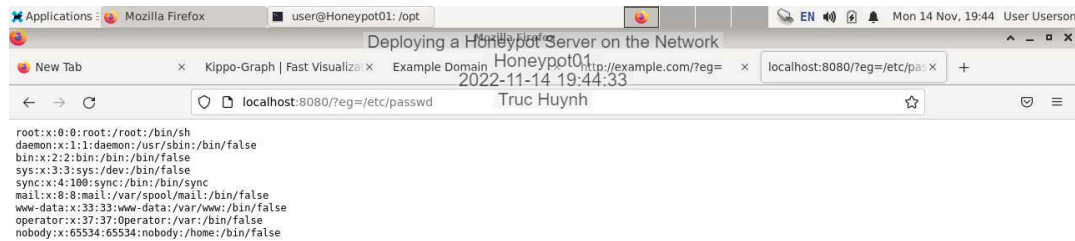
Part 2: Configure an HTTP Honeypot

6. **Make a screen capture** showing the current status of the Tanner, PHP sandbox, and Redis services.

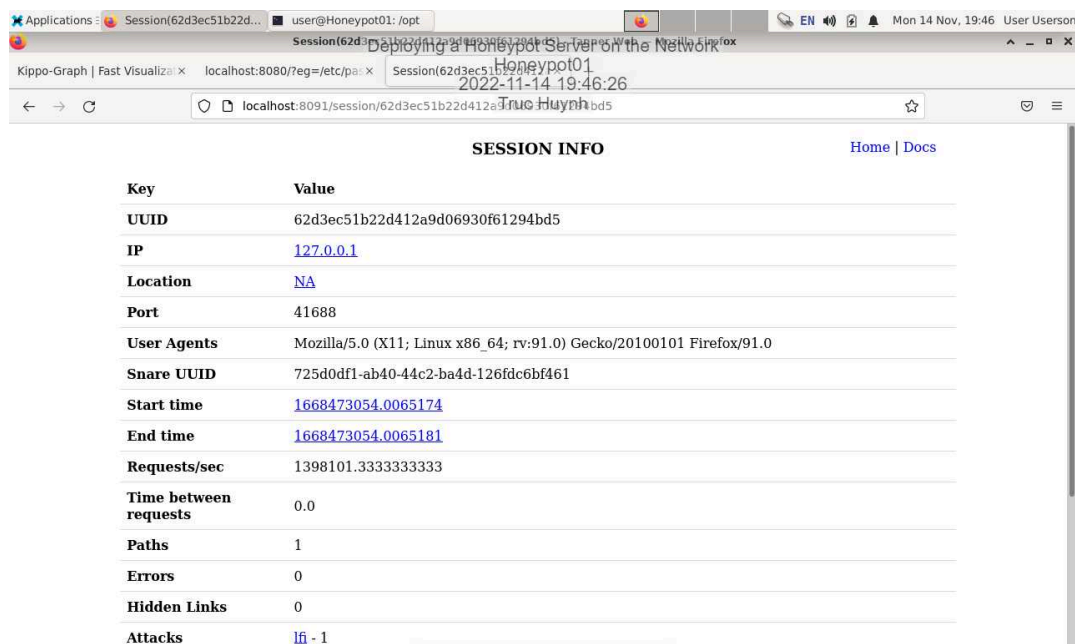


Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 05

34. **Make a screen capture** showing output from the successful LFI attack.



42. **Make a screen capture** showing your LFI payload threat actor session in Tannerweb.

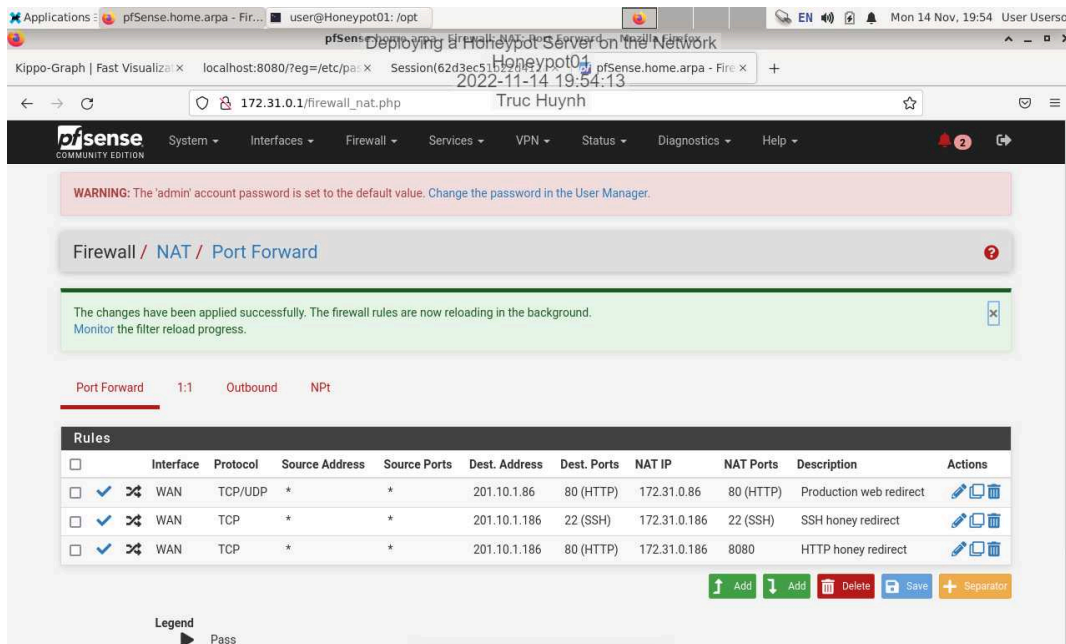


Part 3: Simulate Attacks and Evaluate Threat Intelligence

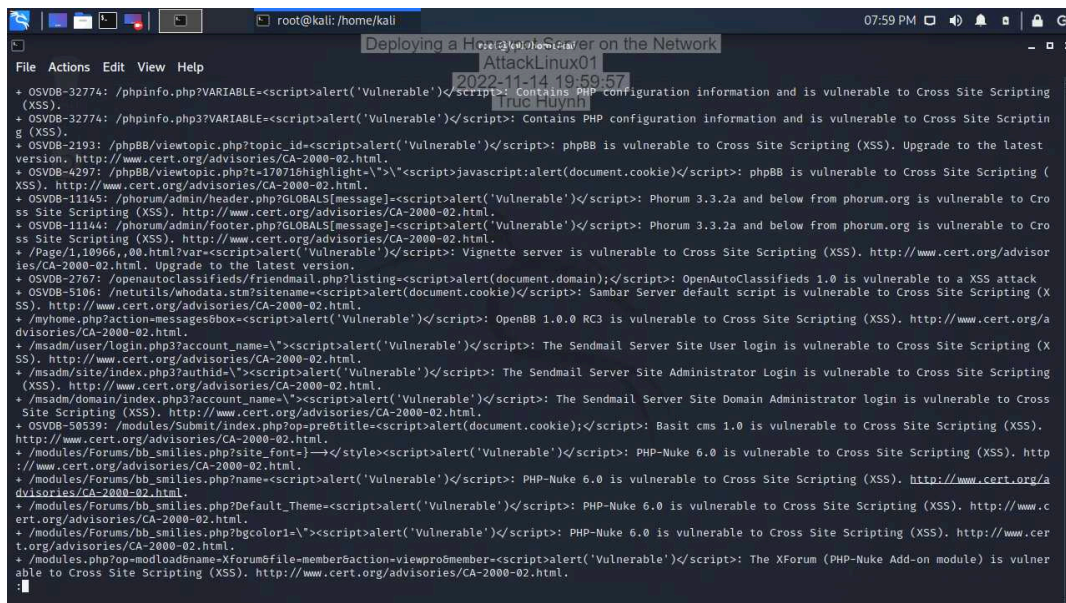
Deploying a Honeypot Server on the Network

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 05

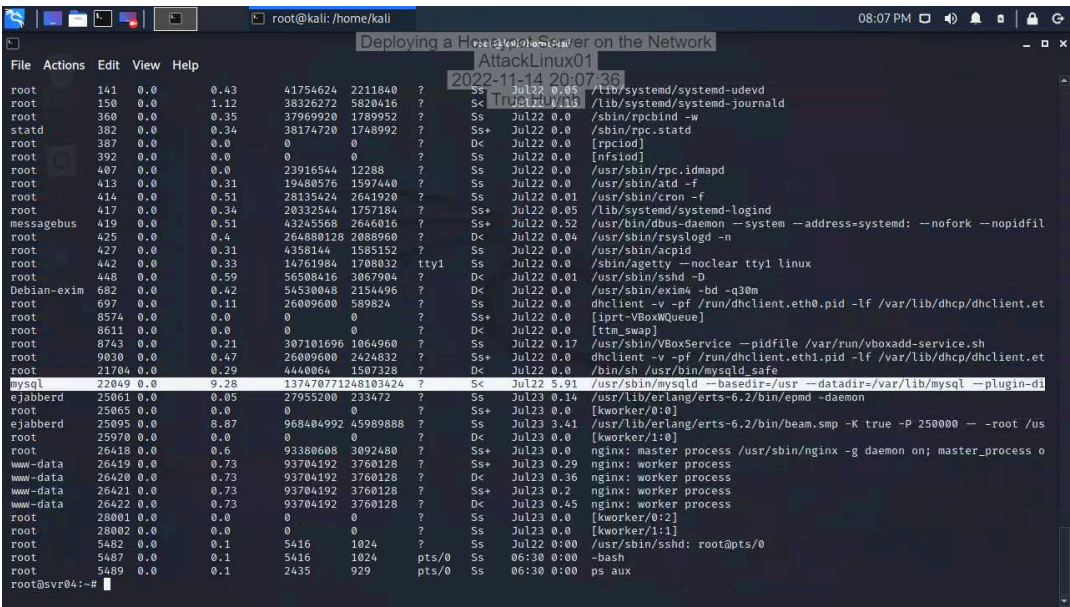
15. **Make a screen capture** showing the updated Firewall / NAT / Port Forward rules table and the feedback indicating their successful application.



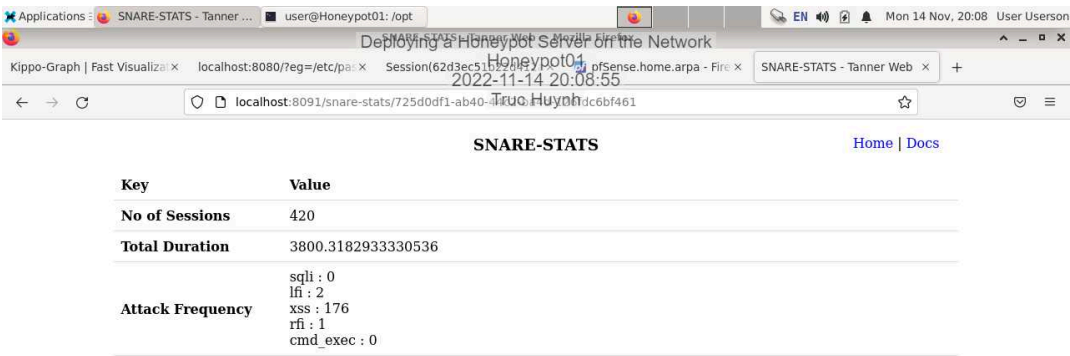
22. **Make a screen capture** showing the Server banner changed message in your Nikto output.



32. Make a screen capture showing MySQL, erlang, and NGINX processes in the output.



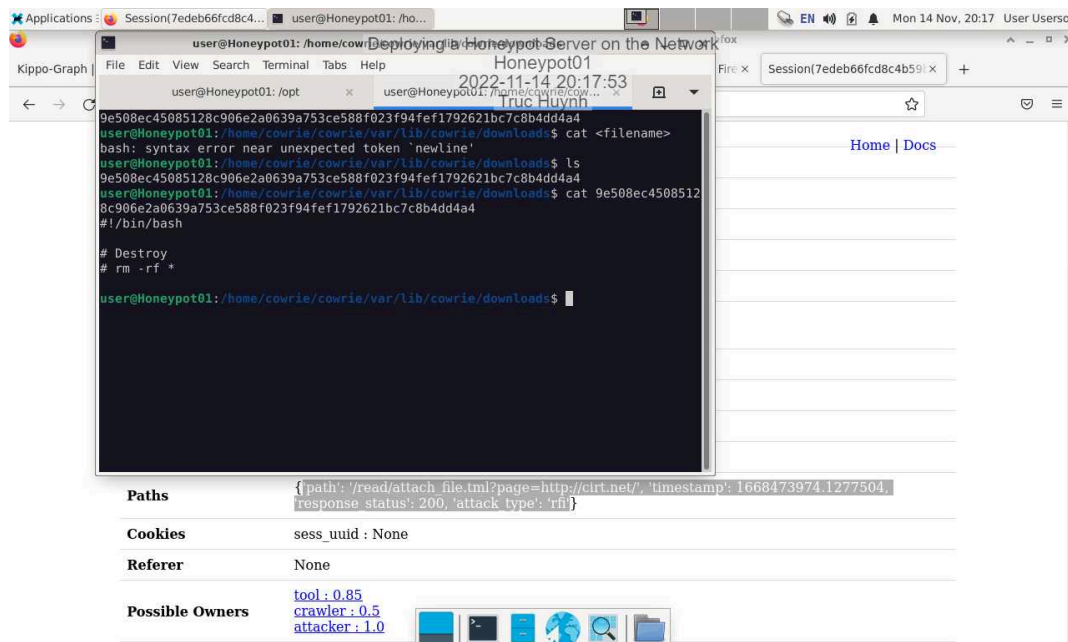
40. Make a screen capture showing the overall Snare-Stats.



46. Record the website the Red Team threat actor attempted to include in the path.

/read/attach_file.tml?page=http://cirt.net/

53. **Make a screen capture** showing the contents of the file that the Red Team member uploaded to the SSH honeypot.



Deploying a Honeypot Server on the Network

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 05

58. **Record** the most popular username/password combination.

root/passwordroot/hackthegibson

root/secret

root/angel

root/love

root/secretsecretsecret

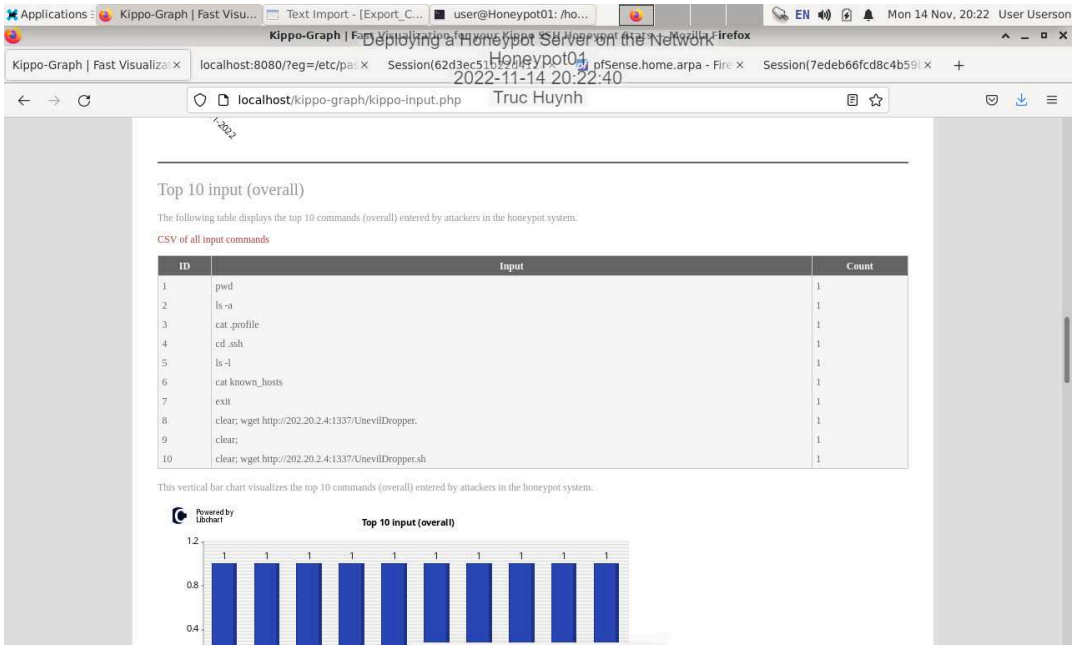
root/tigger

root/sunshine

root/chocolate

root/jennifer

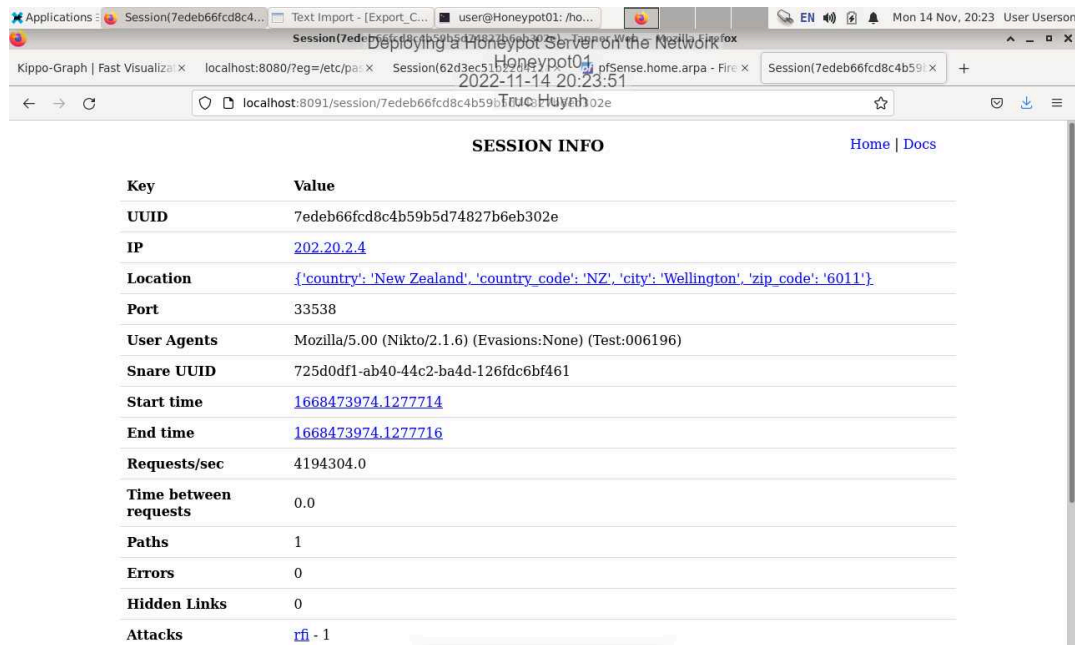
61. Make a screen capture showing the Top 10 successful input commands.



Challenge and Analysis

Part 1: Identify XSS Attacks in Tannerweb

Make a screen capture showing the details of one cross-site scripting event.



Key	Value
UUID	7edeb66fcd8c4b59b5d74827b6eb302e
IP	202.20.2.4
Location	{'country': 'New Zealand', 'country_code': 'NZ', 'city': 'Wellington', 'zip_code': '6011'}
Port	33538
User Agents	Mozilla/5.0.0 (Nikto/2.1.6) (Evasions:None) (Test:006196)
Snare UUID	725d0df1-ab40-44c2-ba4d-126fdc6bf461
Start time	1668473974.1277714
End time	1668473974.1277716
Requests/sec	4194304.0
Time between requests	0.0
Paths	1
Errors	0
Hidden Links	0
Attacks	rfi - 1

Part 2: Change SNARE's Web Server Header

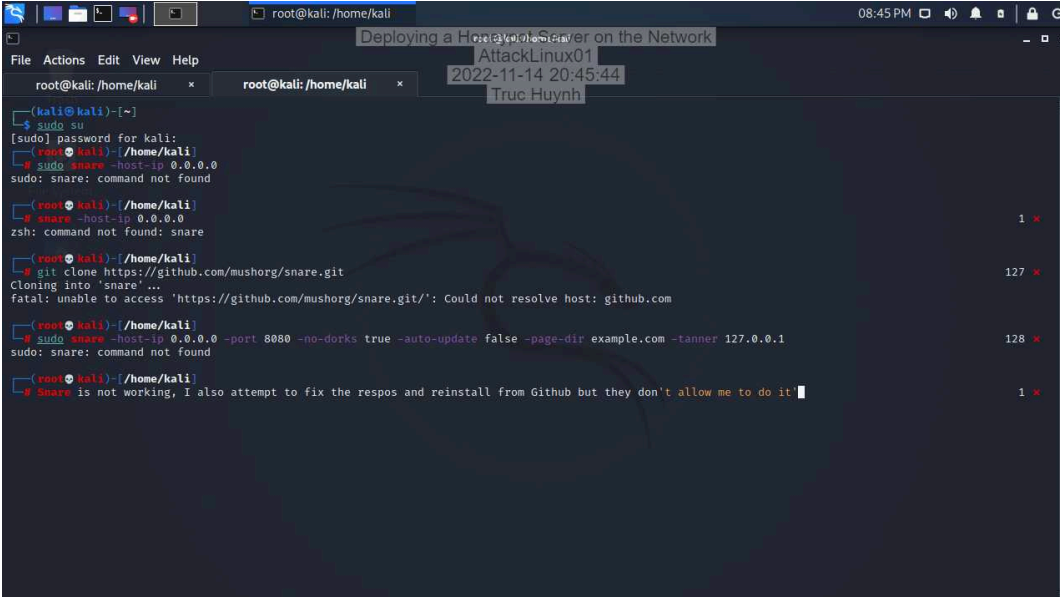
Document the additional option(s) and argument(s) used to change the SNARE Web Server Header to Apache.

```
sudo snare -host-ip 0.0.0.0 -port 8080 -no-dorks true -auto-update false -page-dir example.com  
-tanner 127.0.0.1 -server-header apache
```

Deploying a Honeypot Server on the Network

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 05

Make a screen capture showing that the **SNARE Web Server Header** is set to Apache (using output from Nikto).



```
(kali@kali)~$ sudo su
[sudo] password for kali:
root@kali: /home/kali
root@kali: /home/kali# sudo snare -host-ip 0.0.0.0
sudo: snare: command not found

root@kali: /home/kali# snare -host-ip 0.0.0.0
zsh: command not found: snare

root@kali: /home/kali# git clone https://github.com/mushorg/snare.git
Cloning into 'snare' ...
fatal: unable to access 'https://github.com/mushorg/snare.git/': Could not resolve host: github.com

root@kali: /home/kali# sudo snare -host-ip 0.0.0.0 -port 8080 -no-dorks true -auto-update false -page-dir example.com -tanner 127.0.0.1
sudo: snare: command not found

root@kali: /home/kali# # snare is not working, I also attempt to fix the respos and reinstall from Github but they don't allow me to do it
```