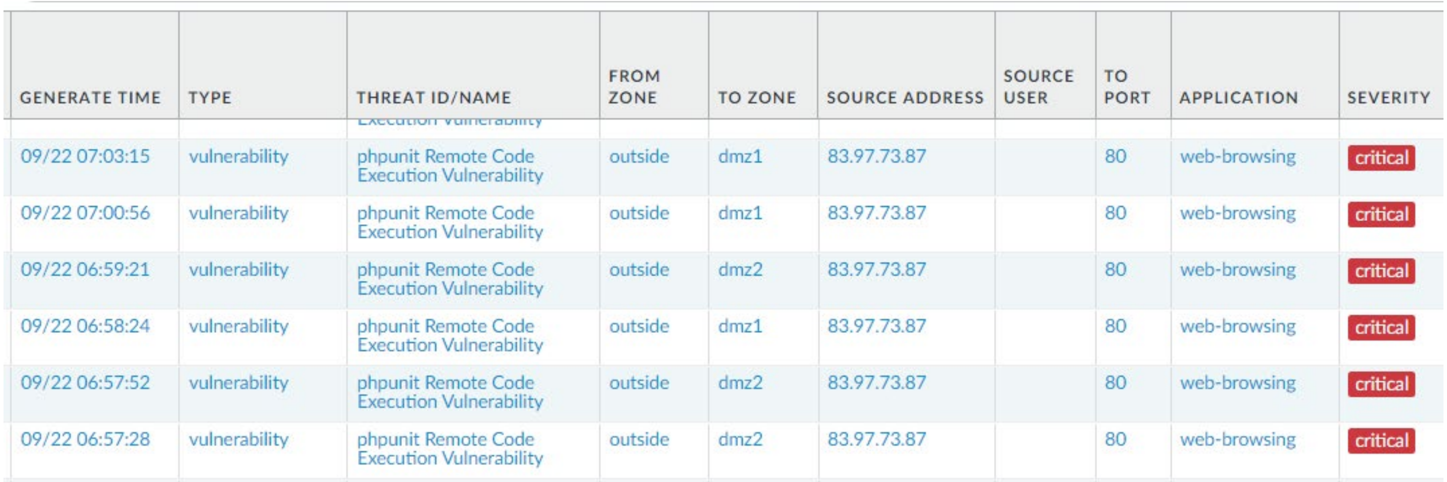
Security Challenge (ver 1.4)

1. (1.5pts) Analyze the meta data in the downloadable photo lake-picture.jpg at http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/ and answer the following questions. Include screenshots to support your answers.

   a. on which date what the picture taken?
   b. what was the make of the camera that took the picture?
   c. of which lake in the United States was the picture taken?

2. (1 pt) CSULA's threat log recently registered the following malicious activity originating from the source IP address shown below. Include screenshots of web pages where you found your answers.

   a. From which country did this malicious traffic originate?
   b. Which of the five Regional Internet Registries is responsible for the assignment of this IP address?



GENERATE TIME	TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	TO PORT	APPLICATION	SEVERITY
09/22 07:03:15	vulnerability	phpunit Remote Code Execution Vulnerability	outside	dmz1	83.97.73.87		80	web-browsing	critical
09/22 07:00:56	vulnerability	phpunit Remote Code Execution Vulnerability	outside	dmz1	83.97.73.87		80	web-browsing	critical
09/22 06:59:21	vulnerability	phpunit Remote Code Execution Vulnerability	outside	dmz2	83.97.73.87		80	web-browsing	critical
09/22 06:58:24	vulnerability	phpunit Remote Code Execution Vulnerability	outside	dmz1	83.97.73.87		80	web-browsing	critical
09/22 06:57:52	vulnerability	phpunit Remote Code Execution Vulnerability	outside	dmz2	83.97.73.87		80	web-browsing	critical
09/22 06:57:28	vulnerability	phpunit Remote Code Execution Vulnerability	outside	dmz2	83.97.73.87		80	web-browsing	critical

3. (1pt) Decrypt the following message using a shift cipher. Include screenshot of web page where you found your answer.

```
 Sbe zber frphevgl punyyratrf, ertvfgre sbe Angvbany Plore Yrnthr
pbzcrgvgvba
```

4. (2 pts) Use a password cracking tool (such as hashcat) and the rockyou.txt wordlist available in Kali (/usr/share/wordlists) or Internet to find the unencrypted passwords corresponding the following two MD5 hash values. Include screenshot from Kali showing how you found your answer.

```
f99dada87216cf9440ffef7f28ae720e

f30aa7a662c728b7407c54ae6bfd27d1
```

5. (1.5 pts) Analyze the downloadable log file access.log at http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/ and answer the following questions. Include screenshots showing how you obtained your answers.

a. How many unique IP addresses accessed the server?
b. How many requests yielded a 200 status?
c. What was the most commonly used HTTP method?

6. (1.5 pts) Analyze the downloadable packet capture file DNS.pcap at http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/ and answer the following questions. Include screenshots from Wireshark packet decode and circle the locations that shows where you found your answers.

a. What DNS record type was requested in DNS query?
b. What domain name was requested?
c. What is the IP address of host welcome.etas.com?

7. (1.5 pts) What is a valid input to the Python program python-authen.py in http://cs3.calstatela.edu/~egean/cs5781/lab-assignments/ that will result in a correct authentication? Provide screenshot showing how you were able to confirm the valid input for authentication.