



# Grey Hats

University of Hawaii at Manoa

# NCL

## National Cyber League



- How many of you signed up?
- Meet up?
- **Late Registration is still available until Oct. 4 - 35\$**

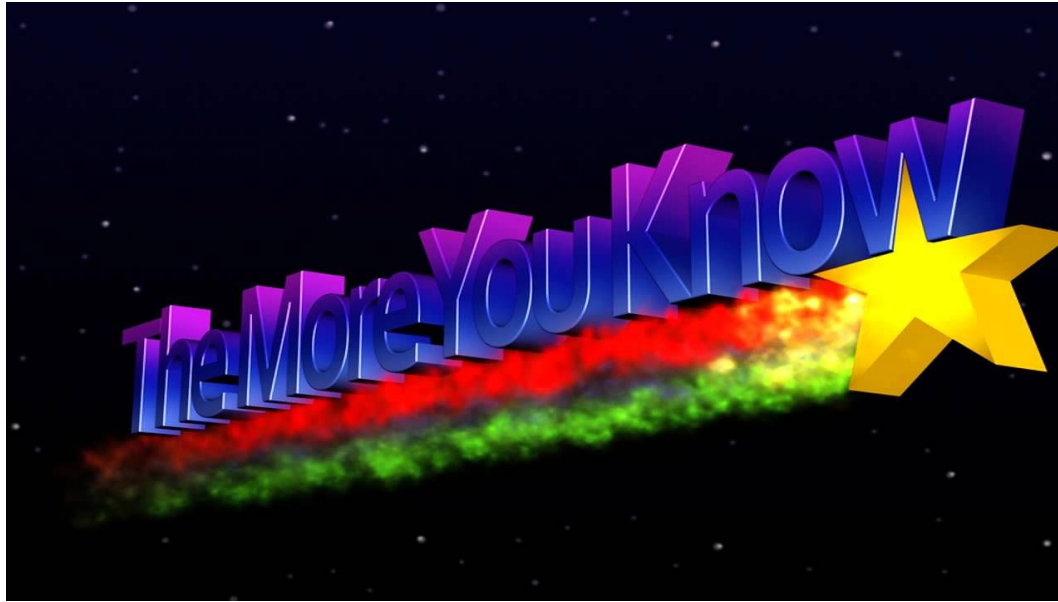
## Times of the Competition

Pre-season: 10/20-10/28

Regular Game: 11/03-11/05

Post-season: 11/17-11/19

# Preparation for Preseason



# The Categories

- Open Source Intelligence
- Network Traffic Analysis
- Log Analysis
- Cryptography

# Open Source Intelligence



## Threat Intel Report

Question	Points	Answer
What is the CVE of the original POODLE attack?	15	✓
What version of VSFTPD contained the smiley face backdoor?	15	✓
What was the first 1.0.1 version of OpenSSL that was NOT vulnerable to heartbleed?	15	✓
What was the original RFC number that described Telnet?	15	✓
How large (in bytes) was the SQL Slammer worm?	15	✓

# Network Traffic Analysis



## Network Traffic Analysis Report

Use the provided packet capture to answer the following questions.

Question	Points	Answer
What was the first username/password combination attempt made to log in to the server? e.g. 'user/password'	20	✓
What software is the FTP server running? (Include name and version)?	20	✓
What is the first username/password combination that allows for successful authentication?	20	✓
What is the first command the user executes on the ftp server?	20	✓
What file is deleted from the ftp server?	20	✓
What file is uploaded to the ftp server?	20	✓
What is the MD5 sum of the uploaded file?	20	✓
What file does the anonymous user download?	20	✓

# Log Analysis

## Browser History Analysis

Download the Firefox sqlite history database to answer the following questions.

Question	Points	Answer
What did the user search for on craigslist?	10	✓
What was the current price of bitcoin when the user was browsing?	30	✓
What Bitcoin exchange did the user log in to?	30	✓
What is the email that was used to log into the exchange?	30	✓
What was the ID of the Bitcoin transaction that the user looked at?	40	✓
What was the total value of all the inputs of the Bitcoin transaction?	40	✓
To which IP address did the majority of the Bitcoin in the transaction go?	50	✓






# Cryptography



## Passwords

Host @ 130.132.1.25

Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that they are all encoded using different number bases.

User	Value	Encrypted Password	Plaintext
 Ade	15	0x616761696e74687265653538	✓
 Christian	15	cGVvcGxIY3Jvd2Q1MQ==	✓
 Elyse	15	01101101 01100001 01110100 01110100 01100101 01110010 01110011 01100001 01101001 01101100 00110110 00110010	✓

# More Crypto



## Passwords

Host @ 130.132.1.25

Our officers have obtained password dumps storing hacker passwords. After obtaining a few plaintext passwords, it appears that some sort of shift cipher was used.


User	Value	Encrypted Password	Plaintext
 Ade	25	znggrefnvy	✓



## Passwords

Host @ 130.132.1.25

Our officers have found a custom encryption algorithm the hackers were using. See if you can use it to decrypt this message.

User	Value	Encrypted Password	Plaintext
 Ade	35	qbkl dro owksvc ypp dro wksvcobfob	✓