



NUCIA

Nebraska University Center for Information Assurance

2009 NebraskaCERT

Capture The Flag

Information Assurance Exercise

Presented by
Nebraska University Center for Information Assurance (NUCIA)
University of Nebraska at Omaha

NebraskaCERT August 18-19, 2009



Purpose

- Combine all the knowledge and skills learned
- Simulate a real-world environment
 - Applications with a purpose
 - See the effects of a real attack
- Work together



Goals

- Protect your server
 - Prevent flags from being stolen
 - Prevent malicious usage of your server
- Compromise opposing servers
 - Capture flags from opposing servers
 - Plant backdoors, malicious code, etc...
- Have fun!!



Applications

- Each team server has 4 applications/services:
 - Aircraft Reservation
 - Vehicle Reservation
 - Lodging Reservation
 - Forums



Flags

- Example flags:
 - d457846324932fd74d8ffb35a4667591
 - 0f65147976d1002ef3a01ec2e1c2682a
 - 86b5e6ce7f1322306919e4afa115060c
- Where are the flags?
 - Flags are planted inside of the services on your server by the score bot.
 - Used as a token by that service



Scoring

- Each flag defended is awarded 1 point
 - The score bot chains up to 3 previous flags
 - If you have long up-times you will gain more points
 - Each service has it's own flag chain
- Each flag captured is awarded 1 point
 - You cannot report your own flags
 - Flags can only be submitted once
- NOTE: You may notice a slight synchronization difference between teams on the score board.



Rules

- NO IP blocking
- NO Network Floods/Denial of Service
- DO NOT target the score bot/flag server
- DO NOT target the IRC server
- Be careful with your image
 - If you break your server, you are responsible for restoring it.
 - You will not receive a replacement server



Noteworthy Addresses

- Flag Server: 100.100.X.X
 - Use this server to view the current scores
 - Flags reported here
- IRC Server: 100.100.X.X
 - DO NOT target these machines! (Violations will result in point deductions)