The Open Cyber Challenge Platform*

The University of Rhode Island

Jacob Fonseca, Kevin Bryan, Lisa DiPippo, Victor Fay-Wolfe

* Supported By The U.S. National Science Foundation grants:

- Federal Cyber Service Scholarship For Service Program: Award 1241515
- Research Experience For Undergraduates: Award 1004409

THE UNIVERSITY OF RHODE ISLAND

Problem

- Need for realistic, up-to-date, hands-on ways to teach cyber security.
- ***Cyber challenges*** –(team defends a real network data center from attacks) been proven effective in events and training.
- No low-cost option for establishing cyber challenge platform for high schools and colleges to use in their curriculum.

Current Cyber Challenges

- Some are restricted to government-only
  - Xnet
  - National Cyber Range
- Commercial packages are expensive
  - >$100K plus maintenance
  - E.g. SAIC solution used by CyberPatriot competitions
- Some are created from scratch each time
  - National Collegiate Competition
  - DEFCON Capture The Flag
- Challenges are typically "free for all" – not designed to be configurable to test specific concepts

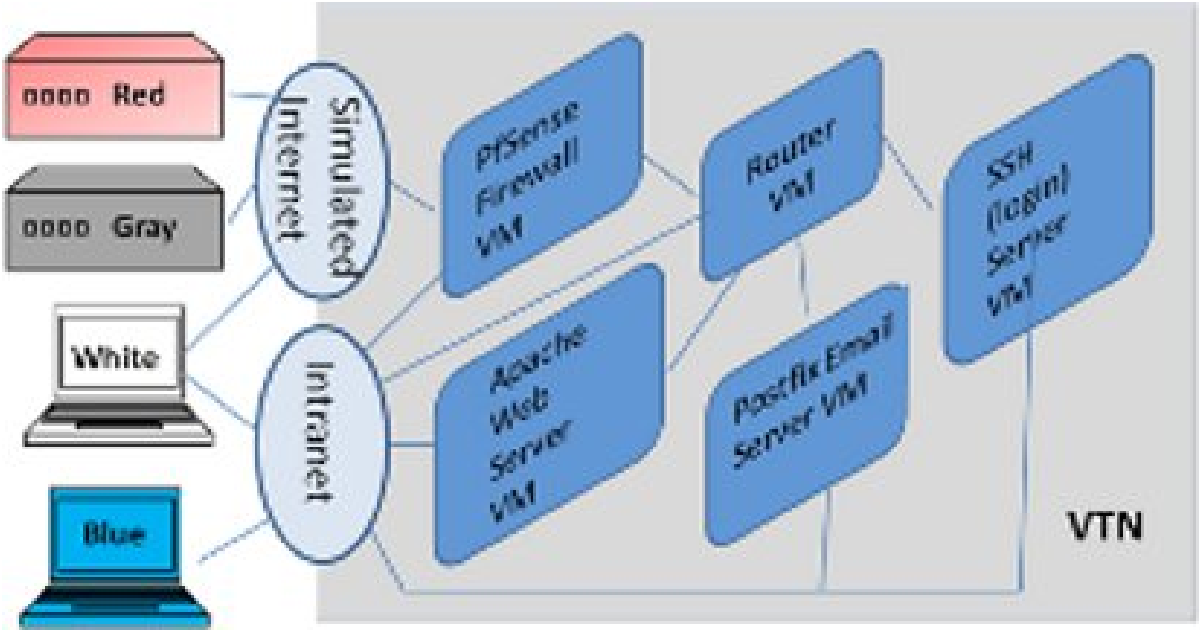
The University of Rhode Island

DFCSC

Digital Forensics & Cyber Security Center

OCCP Basic Concept

- ***Red Team*** – attacks network to steal data and deny services
- ***Gray Team*** - normal traffic and service requests that must be maintained
- ***Blue Team*** - defends network (patches vulnerabilities, etc)
- ***White Team*** – officiates and scores challenge



Uses In Teaching/Training/Challenges

Network Defense – Blue Team is students, Red Team is scripted attacks. Negative points assigned to Blue for data stolen and services denied

Penetration Testing – Red Team is students, Blue Team is scripted. Positive points assigned for data stolen and services denied

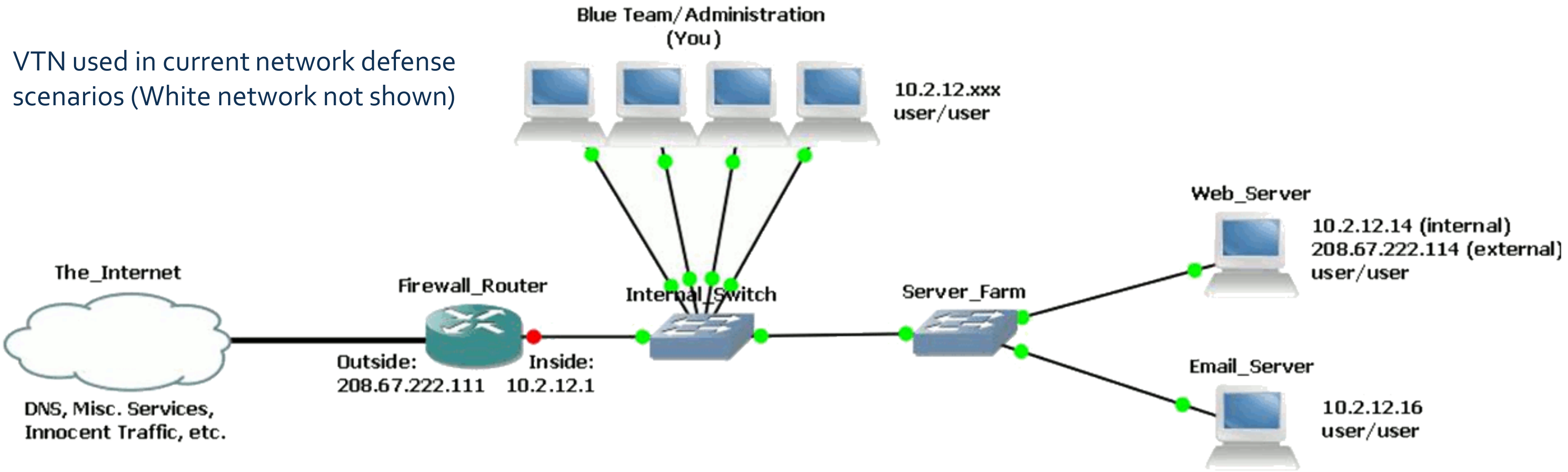
Secure Programming – Blue Team is student programmers, Red Team is scripted attacks (e.g. SQL injection). Negative points assigned for data stolen and services denied.

Digital Forensics – Read Team is scripted attack, Blue Team of students must find what data was stolen and who did it.

Virtual Scenario Network (VSN)

- Networked virtual machines
- Runs on one low-end/moderate physical computer/server
- Virtual internal network, external (Internet) network, private white team network
- Alpha network defense scenario uses “metasploitable”, which is a virtual web server with vulnerabilities as part of the metasploit project.

VTN used in current network defense scenarios (White network not shown)



Gray Team (normal service requests)

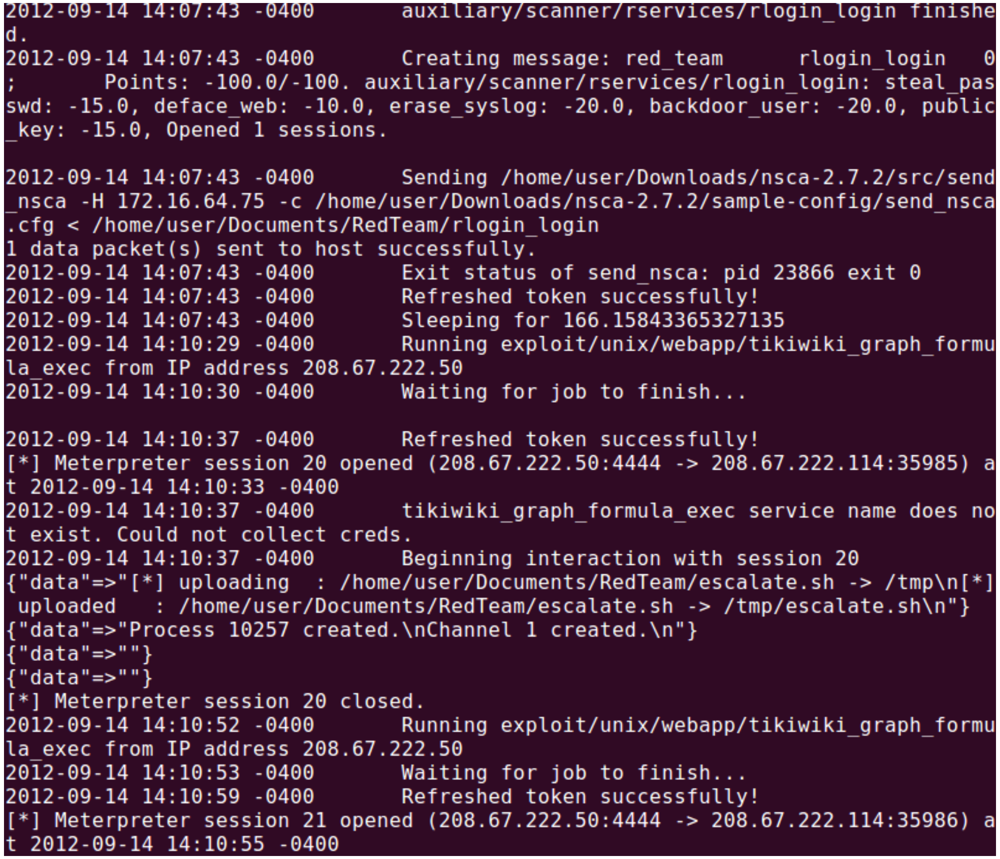
- Ruby scripts generate traffic
- What protocols, timing/density of requests, and specific VTN services are specified in configuration file
- Use of standard protocol libraries (e.g. http library) to generate traffic under Ruby scripting
- Gray scripts report to White Team successful receipt of services for scoring purposes

Red Team (attacks)

- Scripted for network defense, secure programming and forensics
- Human for penetration testing
- For Alpha network defense scenario:
  - Exploits come from Metasploit (open source) library
  - Configuration file specifies attacks and timing
  - Ruby (scripting language) scripts execute exploit attempts
  - Red scripts report success to White scripts for scoring

The University of Rhode Island
DFCSC
Digital Forensics & Cyber Security Center

Red Team Console in Alpha Network Defense Scenario



```
2012-09-14 14:07:43 -0400       auxiliary/scanner/rservices/rlogin_login finishe
d.
2012-09-14 14:07:43 -0400       Creating message: red_team      rlogin_login   0
;       Points: -100.0/-100. auxiliary/scanner/rservices/rlogin_login: steal_pas
swd: -15.0, deface_web: -10.0, erase_syslog: -20.0, backdoor_user: -20.0, public
_key: -15.0, Opened 1 sessions.

2012-09-14 14:07:43 -0400       Sending /home/user/Downloads/nsca-2.7.2/src/send
_nsca -H 172.16.64.75 -c /home/user/Downloads/nsca-2.7.2/sample-config/send_nsca
.cfg < /home/user/Documents/RedTeam/rlogin_login
1 data packet(s) sent to host successfully.
2012-09-14 14:07:43 -0400       Exit status of send_nsca: pid 23866 exit 0
2012-09-14 14:07:43 -0400       Refreshed token successfully!
2012-09-14 14:07:43 -0400       Sleeping for 166.15843365327135
2012-09-14 14:10:29 -0400       Running exploit/unix/webapp/tikiwiki_graph_formu
la_exec from IP address 208.67.222.50
2012-09-14 14:10:30 -0400       Waiting for job to finish...

2012-09-14 14:10:37 -0400       Refreshed token successfully!
[*] Meterpreter session 20 opened (208.67.222.50:4444 -> 208.67.222.114:35985) a
t 2012-09-14 14:10:33 -0400
2012-09-14 14:10:37 -0400       tikiwiki_graph_formula_exec service name does no
t exist. Could not collect creds.
2012-09-14 14:10:37 -0400       Beginning interaction with session 20
{"data"=>"[*] uploading  : /home/user/Documents/RedTeam/escalate.sh -> /tmp\n[*]
 uploaded   : /home/user/Documents/RedTeam/escalate.sh -> /tmp/escalate.sh\n"}
{"data"=>"Process 10257 created.\nChannel 1 created.\n"}
{"data"=>""}
{"data"=>""}
[*] Meterpreter session 20 closed.
2012-09-14 14:10:52 -0400       Running exploit/unix/webapp/tikiwiki_graph_formu
la_exec from IP address 208.67.222.50
2012-09-14 14:10:53 -0400       Waiting for job to finish...
2012-09-14 14:10:59 -0400       Refreshed token successfully!
[*] Meterpreter session 21 opened (208.67.222.50:4444 -> 208.67.222.114:35986) a
t 2012-09-14 14:10:55 -0400
```

Attacks Run

- Brute force login
  - ssh
  - rlogin
- Web application exploit
  - tikiwiki php exec
- Exposed internal services

Post Exploit

- Privilege escalation
- Backdoor accounts
- Stolen passwords
- Website defacement
- Erase logs

The University of Rhode Island

DFCSC

Digital Forensics & Cyber Security Center

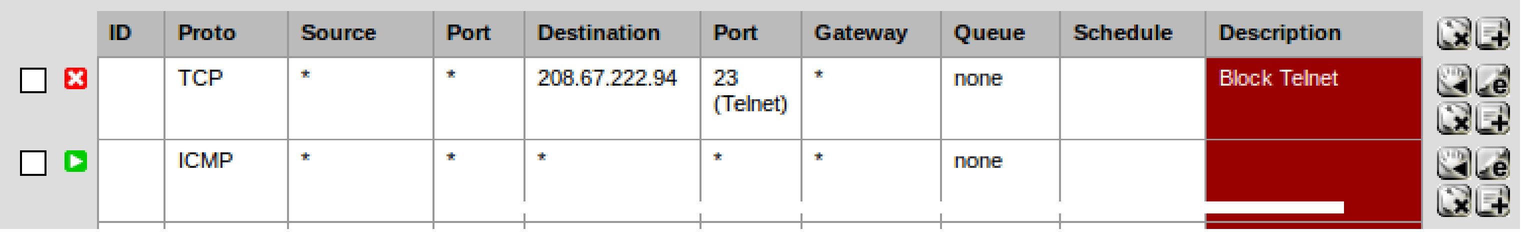
Blue Team (system administrators)

- Humans in Network Defense, Secure Programming, and Forensics.
- Scripts in Penetration Testing
- In Network Defense Alpha:
  - Blue Team gets short "network administrator" document showing network architecture, passwords, etc.
  - Blue Team is given pre-training on the specific tools and components used (e.g. psSense firewall)
  - Blue Team is provided a "network administrator" virtual desktop with all required tools (and possibly an Internet connection to get other tools and documentation). E.g.
    - WireShark
    - Interface to Snort Intrusion Detection
    - Putty and remote login tools
  - Blue Team has an email account on the network administrator desktop to which hints can be emailed

The University of Rhode Island
DFCSC
Digital Forensics & Cyber Security Center

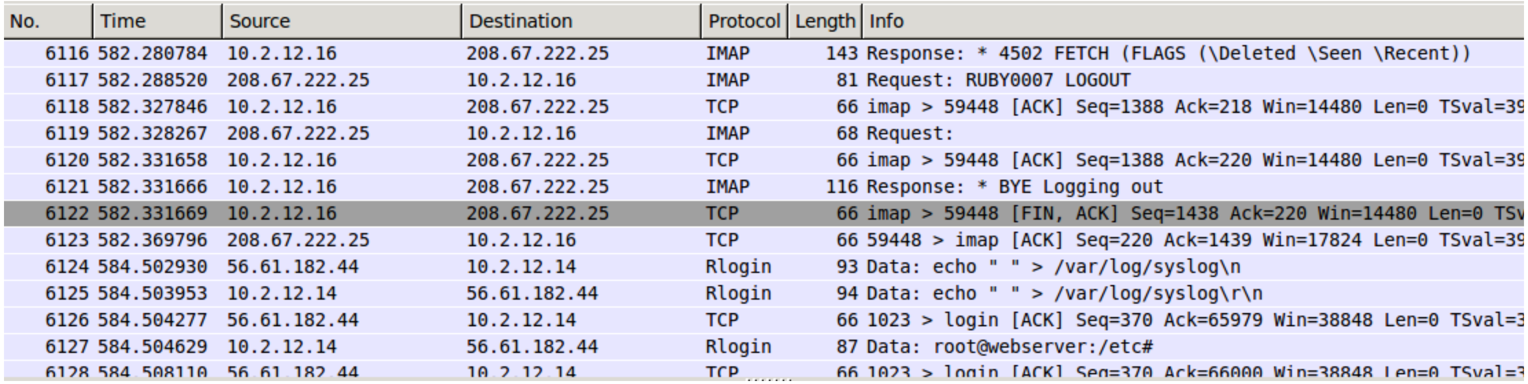
Blue Team Sys Admin VM in Alpha Network Defense Scenario

Blue Team member using web interface from the Blue network administrator desktop to fix a weak firewall rule



		ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
□	☒		TCP	*	*	208.67.222.94	23 (Telnet)	*	none		Block Telnet
□	▶		ICMP	*	*	*	*	*	none		

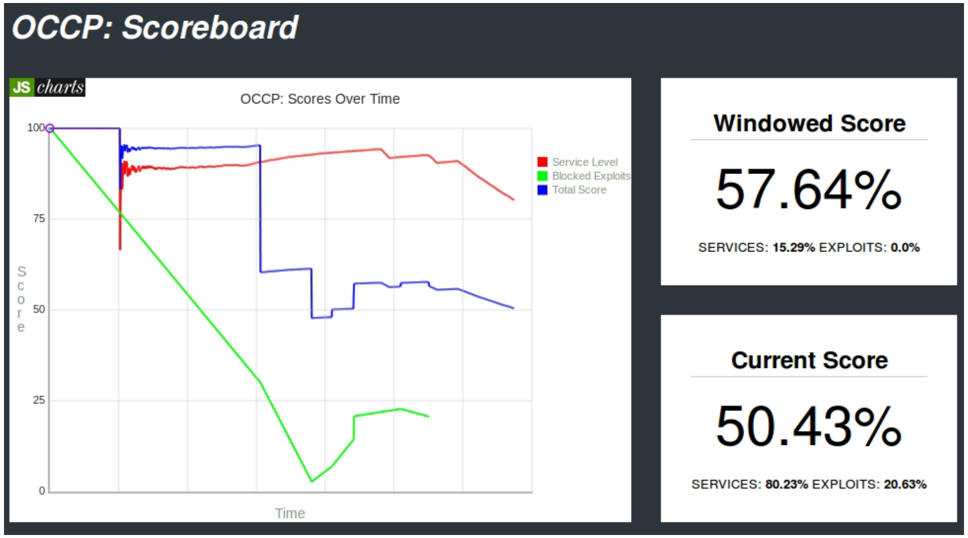
Blue Team member using web interface from the Blue network administrator desktop to examine the mail server system log



```
No.     Time        Source          Destination     Protocol Length Info
   6116 582.280784  10.2.12.16      208.67.222.25   IMAP       143 Response: * 4502 FETCH (FLAGS (\Deleted \Seen \Recent))
   6117 582.288520  208.67.222.25   10.2.12.16      IMAP        81 Request: RUBY0007 LOGOUT
   6118 582.327846  10.2.12.16      208.67.222.25   TCP         66 imap > 59448 [ACK] Seq=1388 Ack=218 Win=14480 Len=0 TSval=39
   6119 582.328267  208.67.222.25   10.2.12.16      IMAP        68 Request:
   6120 582.331658  10.2.12.16      208.67.222.25   TCP         66 imap > 59448 [ACK] Seq=1388 Ack=220 Win=14480 Len=0 TSval=39
   6121 582.331666  10.2.12.16      208.67.222.25   IMAP       116 Response: * BYE Logging out
   6122 582.331669  10.2.12.16      208.67.222.25   TCP         66 imap > 59448 [FIN, ACK] Seq=1438 Ack=220 Win=14480 Len=0 TSv
   6123 582.369796  208.67.222.25   10.2.12.16      TCP         66 59448 > imap [ACK] Seq=220 Ack=1439 Win=17824 Len=0 TSval=39
   6124 584.502930  56.61.182.44    10.2.12.14      Rlogin      93 Data: echo " " > /var/log/syslog\n
   6125 584.503953  10.2.12.14      56.61.182.44    Rlogin      94 Data: echo " " > /var/log/syslog\r\n
   6126 584.504277  56.61.182.44    10.2.12.14      TCP         66 1023 > login [ACK] Seq=370 Ack=65979 Win=38848 Len=0 TSval=3
   6127 584.504629  10.2.12.14      56.61.182.44    Rlogin      87 Data: root@webserver:/etc#
   6128 584.508110  56.61.182.44    10.2.12.14      TCP         66 1023 > login [ACK] Seq=370 Ack=66000 Win=38848 Len=0 TSval=3
```

White Team (officiating and scoring)

- Uses Nagios (open source network monitoring) to get status of services
- Uses Nagios messages to receive updates from the other teams
- In Alpha Network Defense scenario:
  - Red team reports successful exploits (negative points)
  - Gray team report successful services (positive points) and denied/incorrect service (negative points)
  - Provides “hint” communication for White Team humans to help Blue Team humans



OCCP: Scoreboard

Windowed Score

57.64%

SERVICES: **15.29%** EXPLOITS: **0.0%**

Current Score

50.43%

SERVICES: **80.23%** EXPLOITS: **20.63%**

The University of Rhode Island
DFCSC
Digital Forensics & Cyber Security Center

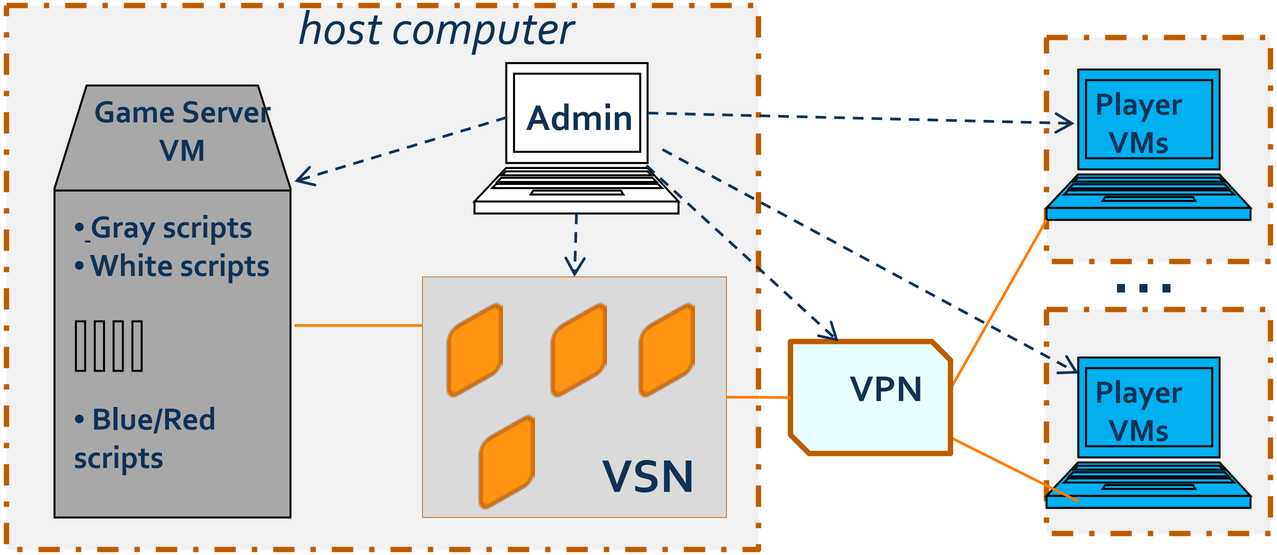
OCCP Architecture

- ***Configuration file*** - XML file that specifies Gray traffic protocols and timing, Red attacks, White scoring algorithms, etc

- ***Admin VM*** – Vm that reads config file and deploys Game server and Player VMs.

- ***Game Server*** – VM reads config file and runs all automated scripts (Gray, White, Red/Blue)

- All VMs written in ***Open Virtual Format*** (OVF) text files (can be read by VMWare, VirtualBox, etc)



Status

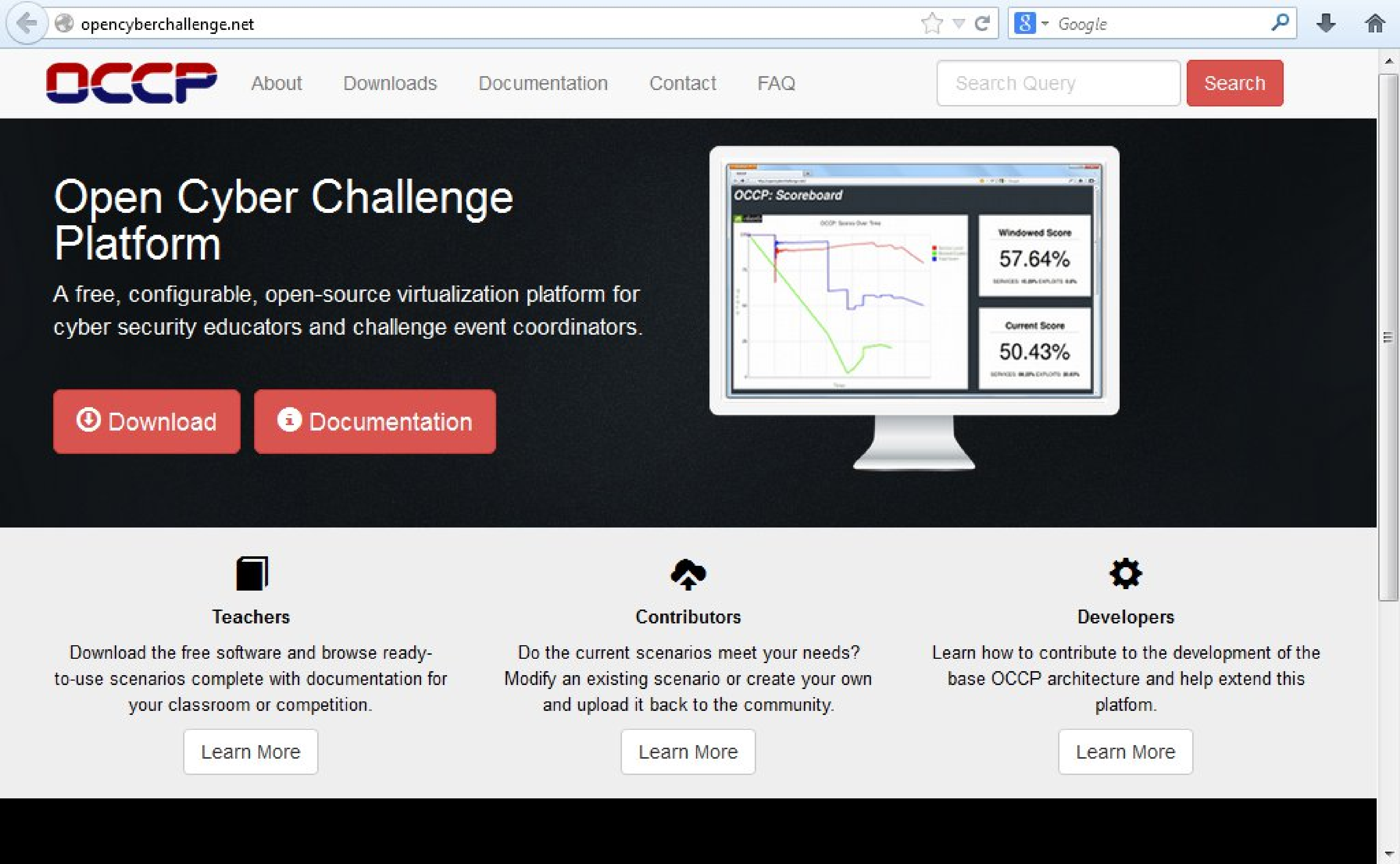
OCCP
OPEN CYBER CHALLENGE PLATFORM

- University of Rhode Island is building Open Cyber Challenge Platform (OCCP) under funding from the U.S. National Science Foundation
- Free virtual environment with low cost hardware requirements
- OCCP to be release open source on web portal
- Community expected to add educational modules and features to keep OCCP current and expand its breadth
- First Network Defense scenario developed and Alpha tested
- First Beta (public) OCCP scenario expected by the end of 2013.

The University of Rhode Island
DFCSC
Digital Forensics & Cyber Security Center

Dr. Victor Fay-Wolfe
The University of Rhode Island
wolfe@cs.uri.edu

OpenCyberChallenge.net



Open Cyber Challenge Platform

A free, configurable, open-source virtualization platform for cyber security educators and challenge event coordinators.

Teachers

Download the free software and browse ready-to-use scenarios complete with documentation for your classroom or competition.

Contributors

Do the current scenarios meet your needs? Modify an existing scenario or create your own and upload it back to the community.

Developers

Learn how to contribute to the development of the base OCCP architecture and help extend this platform.