UNIVERSITY OF WISCONSIN
STOUT
WISCONSIN'S POLYTECHNIC UNIVERSITY

Cyber Security Curriculum Workshop

- November 1 - 2, 2018
- April 4 - 5, 2019
- University of Wisconsin-Stout
- PI : Holly Yuan
- Co-PI: Byron Anderson
- Office Assistant: Matt Wysocki
- Curriculum Consultant: Brandon Cross

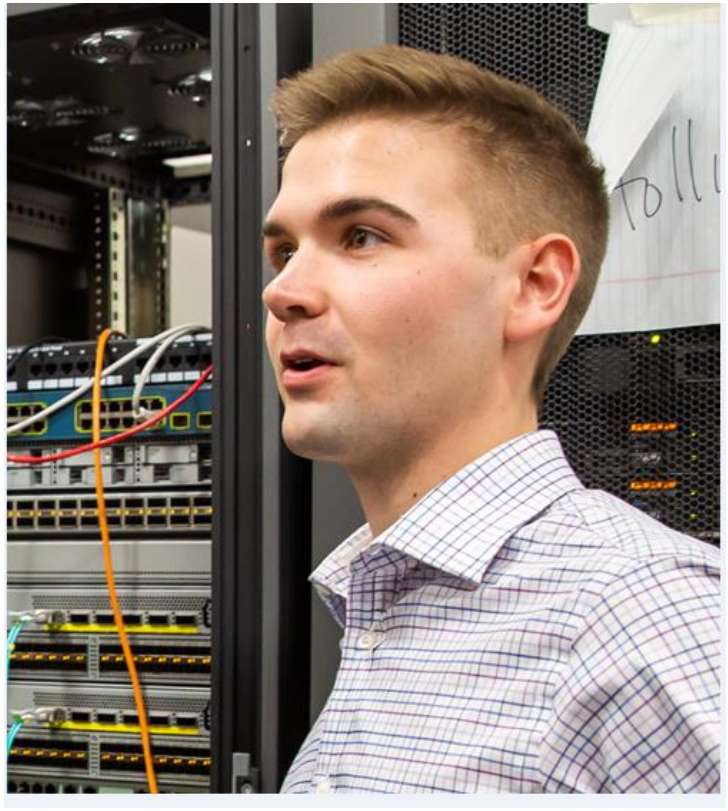

UNIVERSITY OF WISCONSIN
STOUT
WISCONSIN'S POLYTECHNIC UNIVERSITY
Menomonie, WI
MINNESOTA
WISCONSIN
MICHIGAN
IOWA
Lake Michigan
Chequamegon-Nicolet National Forest
Hiawatha National Forest
Huron-Manistee National Forests
Minneapolis
St Paul
Minnetonka
St Cloud
Willmar
Eau Claire
Wausau
Stevens Point
Green Bay
Appleton
Oshkosh
Rochester
Mankato
Winona
La Crosse
Austin
Wisconsin Dells
Madison
Milwaukee
Janesville
Kenosha
Rockford
Chicago
Naperville
Waterloo
Dubuque
Fort Dodge
Mason City
Marshalltown
Cedar Rapids
Iowa City
Des Moines
Iron Mountain
Escanaba
Mackinac Island
Petoskey
Traverse City
Muskegon
Grand Rapids
Holland
Lansing
Kalamazoo
Battle Creek
Elkhart
South Bend
Gary

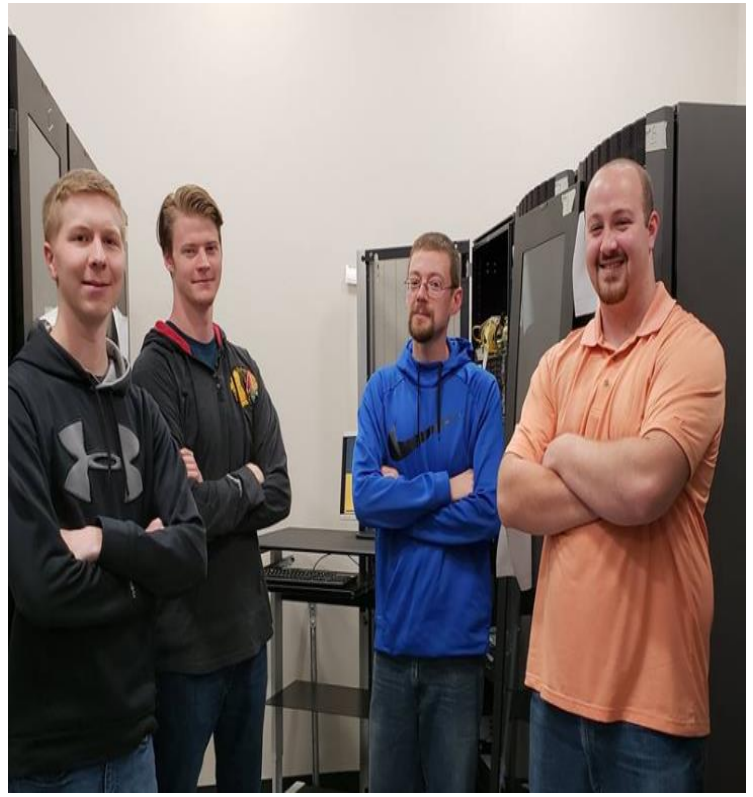
DoD Grant Workshop

Hacking Labs

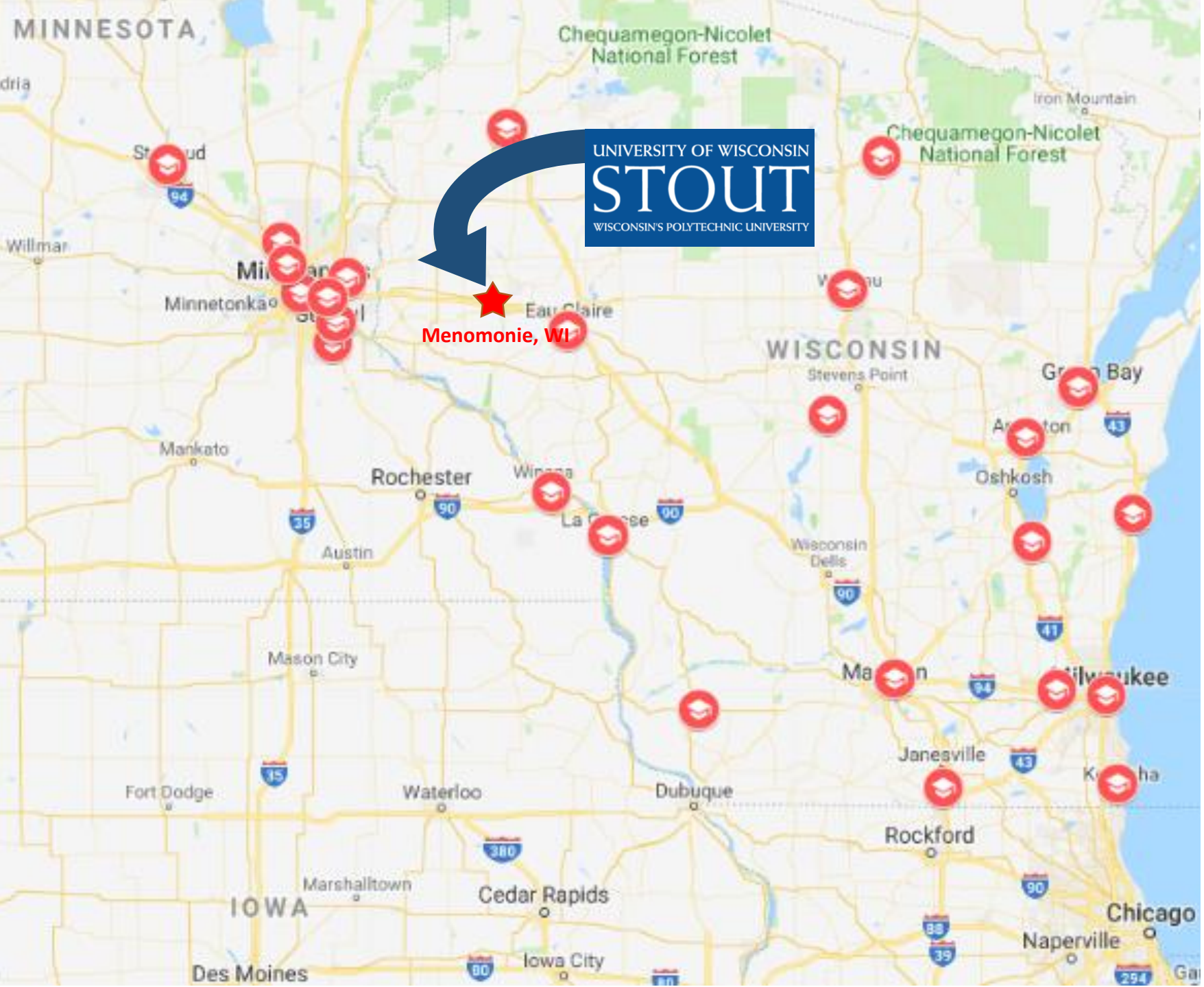
CAE Application

Transfer Agreement





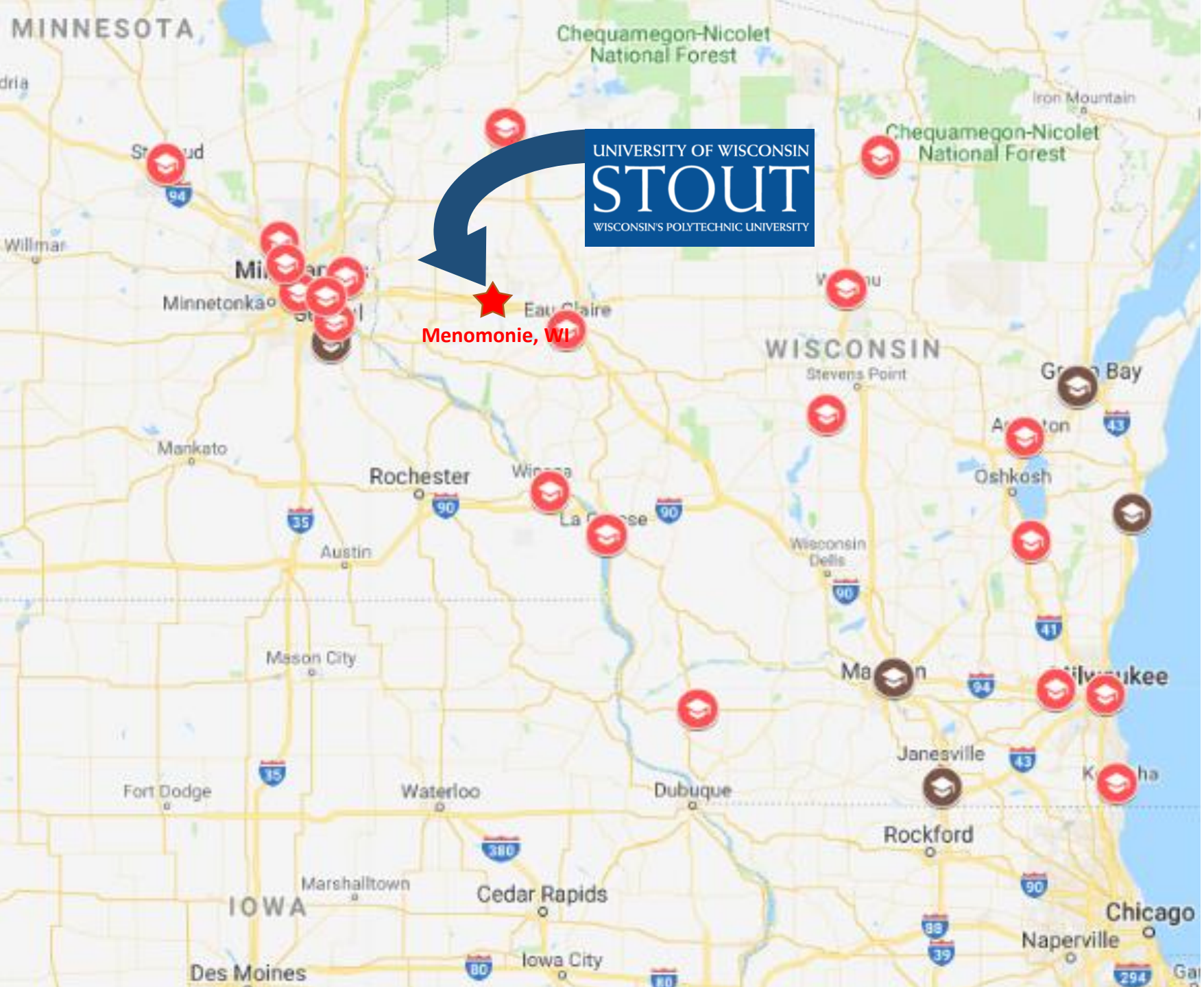
We Deployed about 1000 Virtual Machines for the Workshop



COLLEGES INVITED

- Anoka Technical College
- Blackhawk Technical College
- Century College
- Chippewa Valley Technical College
- Dakota County Technical College
- Fox Valley Technical College
- Gateway Technical College
- Inver Hills Community College
- Lakeshore Technical College
- Madison Area Technical College
- Mid-State Technical College
- Milwaukee Area Technical College
- Minneapolis Community and Technical College
- Minnesota State College Southeast
- Moraine Park Technical College
- Nicolet Area Technical College
- North Hennepin Community College
- Northcentral Technical College
- Northeast Wisconsin Technical College
- Saint Paul College
- Southwest Wisconsin Technical College
- St. Cloud Technical and Community College
- Waukesha County Technical College
- Western Technical College
- Wisconsin Indianhead Technical College

40 Community & Technical College instructors attended the workshop and tested the labs



COLLEGES ATTENDING

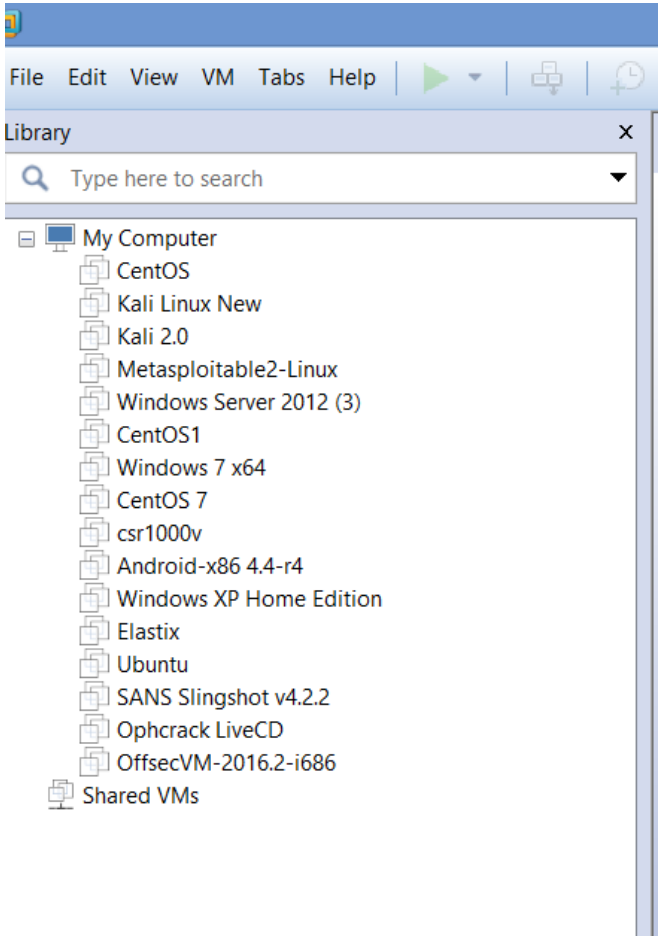
- Anoka Technical College
- Blackhawk Technical College
- Century College
- Chippewa Valley Technical College
- Dakota County Technical College
- Fox Valley Technical College
- Gateway Technical College
- Inver Hills Community College
- Lakeshore Technical College
- Madison Area Technical College
- Mid-State Technical College
- Milwaukee Area Technical College
- Minneapolis Community and Technical College
- Minnesota State College Southeast
- Moraine Park Technical College
- Nicolet Area Technical College
- North Hennepin Community College
- Northcentral Technical College
- Northeast Wisconsin Technical College
- Saint Paul College
- Southwest Wisconsin Technical College
- St. Cloud Technical and Community College
- Waukesha County Technical College
- Western Technical College
- Wisconsin Indianhead Technical College

Topic	Ethical Hacking Hands-on Lab
Lab Setup	• Lab 1: Setup lab environment and discover IP addresses of virtual machines
Footprinting, Enumeration, Reconn	• Lab 2: Reconn attack email harvesting, whois, netcraft • Lab 3: Recon-Personal information gathering • Lab 4: Website copy with HTTrack • Lab 5: Nslookup, dnsreconn, dnsenum • Lab 6: UDP and TCP packet crafting using HPING3 • Lab 7: Collecting information with Google search operators • Lab 8: TCPDUMP • Lab 9: OpenVAS vulnerability scanner • Lab 10: Enumerating users • Lab 11: LDAP enumeration update • Lab 12: SNMP enumeration • Lab 13: NTP enumeration • Lab 14: NMAP Footprinting • Lab 15: Netcat

Password Cracking & Stego	• Lab 16: Sniffing Password with Wireshark • Lab 17: Hacking Cisco Routers with Hydra • Lab 18: Cracking Windows and Linux password with Hydra • Lab 19: Bypass firewall with Netcat redirection • Lab 20: Using John the Ripper to crack windows and Linux password • Lab 21: Password hash attack • Lab 22: Rainbow table password attack • Lab 23: Concealing a file with Steganography • Lab 24: Windows 7, 8, 10, 2012 password cracking with Cain & Abel • Lab 25: Resetting Windows password with CHNTPW

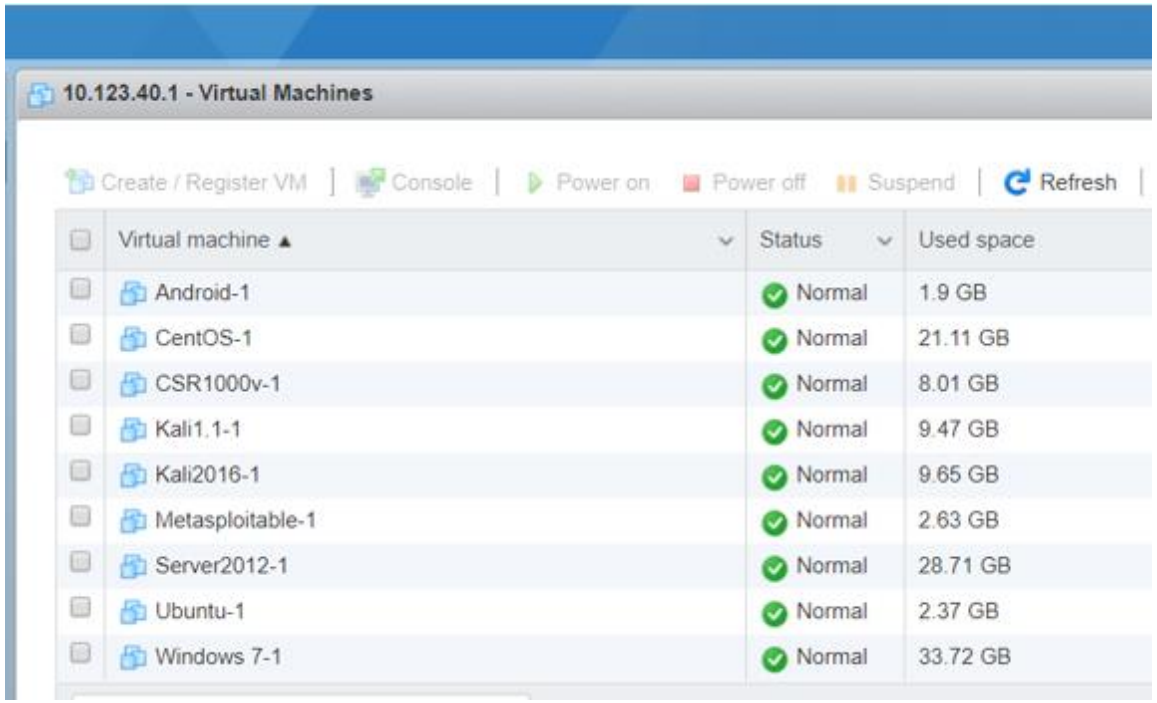
Network Attacks & Social Engineering	• Lab 26: Facebook social engineering • Lab 27: Creating a Trojan & backdoor with Metasploit • Lab 28: Hash file verification • Lab 29: Denial of Service attack • Lab 30: DHCP starvation attack • Lab 31: Man-in-the-Middle attack • Lab 32: XSS attack
SQL Injection & Buffer Overflow	• Lab 33: SQL injection • Lab 34: Buffer overflow

Wireless, Voice, Cloud Computing, IoT, & Mobile Devices	• Lab 35: Hacking WPA/WPA2 • Lab 36: Finding a hidden SSID • Lab 37: Telephone wiretapping • Lab 38: Root exploits for Android • Lab 39: Jailbreaking iOS • Lab 40: Hacking an IoT device • Lab 41: Hacking from AWS Cloud • Lab 42: Hacking the Cloud
Post Exploitation	• Lab 43: Transferring the files • Lab 44: Privilege Escalation • Lab 45: Covering the tracks



VMWare Workstation

ESXi


10.123.40.1 - Virtual Machines
Create / Register VM
Console
Power on
Power off
Suspend
Refresh
Virtual machine
Status
Used space
Android-1 Normal 1.9 GB
CentOS-1 Normal 21.11 GB
CSR1000v-1 Normal 8.01 GB
Kali1.1-1 Normal 9.47 GB
Kali2016-1 Normal 9.65 GB
Metasploitable-1 Normal 2.63 GB
Server2012-1 Normal 28.71 GB
Ubuntu-1 Normal 2.37 GB
Windows 7-1 Normal 33.72 GB


vmware
User name
user1
Password
Log in
vmware ESX

Virtual Machine Username & Password

Virtual Machine	User Name	Password	IP Address
Windows Server 2012 R2	Administrator	Pa$$w0rd	
Windows 7 Professional	Administrator	Pa$$w0rd	
Ubuntu 11.10	advsec	Pa$$w0rd	
CentOS 7	advsec	Pa$$w0rd	
Kali 2016.2	advsec	Pa$$w0rd	
Metasploitable 2	advsec	Pa$$w0rd	
Cisco CSR 1000v	advsec	Pa$$w0rd	
Android 4.4	advsec	Pa$$w0rd	
Kali 1	advsec	Pa$$w0rd	

Lab 1: Virtual Machine IP Address Discovery

Lab Description

In this lab, you will discover and document the IP addresses for all virtual machines.

Lab Objectives

The lab teaches you how to:

- Discover the IP address of each virtual machine.

Lab Environment

This lab requires:

- All the virtual machines

Lab Duration

Time: 20 minutes

Lab 4: Websites Copy with HTTrack

Lab Description

In this lab, you will learn how to make an offline copy of a website.

Lab Objectives

The lab shows you how to use HTTrack to:

- Download a website to a local directory
- Build recursively all directories, HTML, images, videos, etc

Lab Environment

This lab requires:

- Kali Linux 2016.2

Lab 14: Nmap Footprinting

Lab Description

In this lab, you will learn how to use Nmap to scan and audit a network.

Lab Objectives

The lab teaches you how to use Nmap to:

- Scan TCP and UDP ports
- Enumerate services
- Enumerate operating systems

Lab Environment

This lab requires:

- Metasploitable-2
- Kali 2016.2

Lab Duration

Time: 20 minutes

Lab 15: Netcat

Lab Description

In this lab, you will learn how to use Netcat to read and write to TCP and UDP ports.

Lab Objectives

The lab teaches you how to use Netcat to:

- Connect to a remote system
- Chat between two VMs
- Transfer files
- Reverse shell
- Create a backdoor

Lab Environment

This lab requires:

- Metasploitable-2
- Kali 2016.2
- Windows 7

Lab Duration

Time: 30 minutes

Lab 16: Sniffing Passwords with Wireshark

Lab Description

In this lab, you will sniff telnet and SSH packets and analyze traffic with Wireshark to discover the telnet password.

Lab Objectives

The lab teaches you how to use Wireshark to:

- Capture packets
- Filter packets
- Analyze packets

Lab Environment

This lab requires:

- CentOS
- Windows 7

Lab Duration

Time: 30 minutes

Lab 17: Hacking Cisco Routers with Hydra

Lab Description

In this lab, you will learn how to crack Cisco Router passwords with Hydra.

Lab Objectives

The lab teaches you how to use Hydra:

- Crack Cisco Cloud Router's SSH password
- Crack Cisco Cloud Router's HTTP password

Lab Environment

This lab requires:

- Cisco Cloud Router (CSR1000v)
- Kali 2016.2

Lab Duration

Time: 30 minutes

Lab 19: Bypassing Firewall with Netcat Redirection

Lab Description

In this lab, you will learn how to use Netcat to redirect SSH traffic through port 4444 bypassing the SSH deny firewall rule.

Lab Objectives

The lab teaches you how to:

- Create a firewall rule in Linux system to block the SSH traffic
- Use Netcat to redirect SSH traffic bypassing the SSH deny firewall rule

Lab Environment

This lab requires:

- Metasploitable-2
- Windows 7

Lab Duration

Time: 30 minutes

Lab 22: Rainbow Table Password Attack

Lab Description

In this lab, you will learn how to use a rainbow table to crack password hashes.

Lab Objectives

The lab teaches you how to use Ophcrack:

- Load a Vista free rainbow table
- Crack password hashes

Lab Environment

This lab requires:

- Windows 7 with Ophcrack

Lab Duration

Time: 30 minutes

Lab 23: Concealing a file with Steganography

Lab Description

In this lab, you will learn how to conceal a message or file with steganography.

Lab Objectives

The lab teaches you how to use steghide

- Conceal a file, message, image, or video within another file, message, image, or video

Lab Environment

This lab requires:

- Kali **1.1.0**

Lab Duration

Time: 20 minutes

Lab 26: Facebook Social Engineering Attack

Lab Description

In this lab, you will learn how to conduct a social engineering attack with Facebook.

Lab Objectives

The lab teaches you how to conduct:

- A phishing attack with Social Engineering Toolkit (SET) built into Kali Linux

Lab Environment

This lab requires:

- Kali 2016.2
- Windows 7

Lab Duration

Time: 30 minutes

Lab 27: Creating a Trojan/Backdoor with Metasploit

Lab Description

In this lab, you will learn how to create a Trojan or backdoor using Metasploit.

Lab Objectives

The lab teaches you how to use Metasploit:

- Create a Meterpreter payload
- Create a Trojan/backdoor

Lab Environment

This lab requires:

- Kali 2016.2
- Windows 7

Lab Duration

Time: 30 minutes

Lab 29: A SYN Flood Denial of Service Attack

Lab Description

In this lab, you will learn how to conduct a SYN Flood Denial of Service (DoS) attack with Hping3.

Lab Objectives

The lab teaches you how to use Hping3:

- Craft packets
- Conduct a SYN Flood DoS attack

Lab Environment

This lab requires:

- Windows Server 2012
- Kali 2016.2

Lab Duration

Time: 30 minutes

Lab 30 DHCP Starvation Attack

Lab Description

In this lab, you will learn how to conduct a DHCP starvation attack.

Lab Objectives

The lab teaches you how to use Versinia:

- Conduct a DHCP starvation or DHCP DoS attack

Lab Environment

This lab requires:

- Kali 2016.2
- Cisco CSR 1000v

Lab Duration

Time: 30 minutes

2nd workshop on April 4 – 5, 2019

Lab 1: Cracking a WPA/WPA2 WiFi Password

Lab Description

WPA/WPA2 cracking is a technique used to figure out the pre-shared key for a wireless network. Once a hacker has this key, they will be able to connect to and potentially steal private information as well as use the network for nefarious purposes. Depending on how complex the password is will determine how long it will take to crack the key.

Lab Objectives

This lab teaches you how to use Aircrack to:

- Scan wireless environments
- Locate target SSID
- De-authenticate connected clients
- Capture the four-way handshake between client & access point
- Use a password list to crack a WPA/WPA2 password

Lab Environment

This lab requires:

- Kali Linux

Lab 2: Finding & Authenticating to a Hidden SSID

Lab Description

In this lab, you will learn how to find an SSID that is not actively broadcasting itself. A built-in Kali Linux tool called Aircrack will be utilized to scan all surrounding WiFi networks. The hidden WiFi network does not require a password, but will only allow devices with a specific MAC address to connect. This means you will have to spoof the MAC of a client that is already connected and authenticated.

Lab Objectives

This lab teaches you how to use Kali Linux to:

- Scan wireless environments
- Locate hidden SSID's
- De-authenticate connected clients
- Recover the name of a hidden SSID
- Spoof the MAC address of connected devices

Lab Environment

This lab requires:

- Kali Linux

Lab 3: Wiretapping Voice over IP Calls

Lab Description

In this lab, you will learn how to configure a Cisco switch to monitor traffic traversing a voice VLAN. This voice VLAN will have an IP phone call on it and actively using it. Wireshark will be used to capture this traffic. Once the voice traffic is captured, you will attempt to re-assemble the voice packets and listen to the phone call.

Lab Objectives

This lab teaches you how to:

- Configure a traffic SPAN session on a Cisco switch
- Use Wireshark to capture and compile traffic
- Review captured traffic and listen to phone call

Lab Environment

This lab requires:

- Kali Linux
- USB to serial adapter with console cable

Lab 4: Conducting A Penetration Test From AWS

Lab Description

In this lab, you will create a new AWS account. After you login to the AWS account, you will set up a Kali Linux image in the cloud. Once the Kali Linux VM is deployed, you will run some tools and scans against your other Linux instance to conduct a pen test.

Lab Objectives

This lab teaches you how to:

- Create a new AWS account
- Setup Kali Linux in the Cloud
- Deploy a resource from the AWS Marketplace
- Conduct a Penetration Test

Lab Environment

This lab requires:

- Internet access
- CC for account authorization
- An email address to associate to an AWS accounts

Lab 5: Hacking Android OS

Lab Description

With such a connected world, nearly everyone has a smart phone and relies on it for communication, work, finance, and the many other resources it provides. A significant amount of these devices run Android OS and most of the users are standard consumers with little experience in networking or security. Therefore, it is not unusual for someone's device to get compromised without them even knowing it. In this lab, you will work with a tool built into Kali Linux called msfvenom to take control of an Android virtual machine. You will begin by starting up msfvenom and the necessary services that allow it to function.

Lab Objectives

This lab teaches you how to use Kali Linux to:

- Effectively use msfvenom
- Run an apache web service
- Run a postgresql service
- Execute Metasploit commands
- Navigate Android OS

Lab Environment

This lab requires:

- Kali Linux
- Android VM

Lab 6: Buffer Overflow Attack

Lab Description

Stack buffer overflows are longstanding problems for C programs that lead to all manner of ills, many of which are security vulnerabilities. The biggest problems have typically been with string buffers on the stack coupled with bad or missing length tests. A programmer who mistakenly leaves open the possibility of overrunning a buffer on a function's stack may be allowing attackers to overwrite the return pointer pushed onto the stack earlier.

In this lab, we will simply exploit the buffer by smashing the stack and modifying the return address of the function. This will be used to call some other function. You can also use the same technique to point the return address to some custom code that you have written, thereby executing anything you want.

Lab Objectives

This lab teaches you how to use Kali Linux to:

- Understand how a buffer overflow works
- Exploit a buffer

Lab Environment

This lab requires:

- Kali Linux

Lab 7: MySQL SQL Injections

Lab Description

SQL Injection is a common web vulnerability found in dynamic sites that is caused by un-sanitized user input, which is then passed on to a database. This user input can then be manipulated to "break out" of the original query made by the developers, to include more malicious actions.

These types of vulnerabilities can lead to a database information leakage and depending on the environment, could also lead to complete server compromise. In this lab, you will use Metasploitable-2's DVWA instance to experiment with MySQL SQL injection.

Lab Objectives

This lab teaches you how to use Kali Linux and Metasploit to:

- Create SQL Injections
- Learn about content in databases
- Use John the Ripper

Lab Environment

This lab requires:

- Kali Linux
- Metasploitable-2

Feedback

- *Great selection of labs, very enjoyable! Very well done.*
- *Great labs! Slow equipment was frustrating at times.*
- *Nicely done. Simple steps for students. Enjoyed 30 minute "nugget" design.*
- *Really liked binder format and lab layout, good structure.*
- *Thanks for having us! Would be fun to do a software development one too.*
- *Labs were thorough and easy to follow.*
- *Excellent, labs work well.*
- *I enjoyed it, you should put a "Stout" notebook in binder to take notes in, practical and also advertising.*
- *Appreciated the opportunity to participate.*
- *The workshop was very well organized. I enjoyed the layout of the days and very thoughtful accommodations. It helped us focus on the task and not worry about the details.*
- *The workshop was a well-run event.*
- *Networking & CAE info was excellent, as well as facility and accommodations.*
- *Great first session. The labs were well done.*
- *Very well done! Our instructors need more security specific training!*