Global Cyber Range (GCR)

Empowering the Cybersecurity Professional (CyPro)

NICE Conference 2014

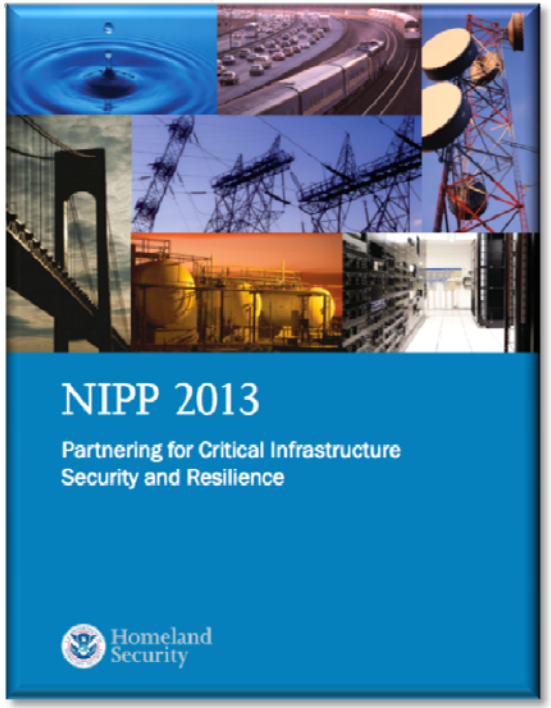
CYBERSECURITY RESILIENCE– A THREE TIERED SOLUTION

CRITICAL INFRASTRUCTURE RESILIENCE

Sector-Specific Agency (SSA)	Critical Infrastructures & Key Resources
Department Of Agriculture Department of Health & Human Services	Agriculture & Food
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health & Human Services	Healthcare & Public Health
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking & Finance
Environmental Protection Agency	Water
Department of Homeland Security (DHS) Office of Infrastructure Protection	Chemical / Commercial Facilities / Dams Critical Manufacturing /Emergency Services Nuclear Reactors, Materials and Waste
DHS Office of Cybersecurity & Communications	Information Technology Communications
DHS Transportation Security Administration	Postal and Shipping
DHS Transportation Security Administration United States Coast Guard	Transportation Systems
DHS Immigration & Customs Enforcement, Federal Protective Service	Government Facilities

Managing Risks from Significant Threats and Hazards to Critical Infrastructures

Requires an Integrated Approach Across a Trusted Diverse Community



Public/Private Collaboration…

NASA / Kennedy Space Center (KSC)

NASA / KSC Center for Lifecycle Design (CflCD)

US Department of Homeland Security (US DHS)

National Institute for Standards & Technology (NIST)

Private Sector | Government Agencies | Academia

Mission

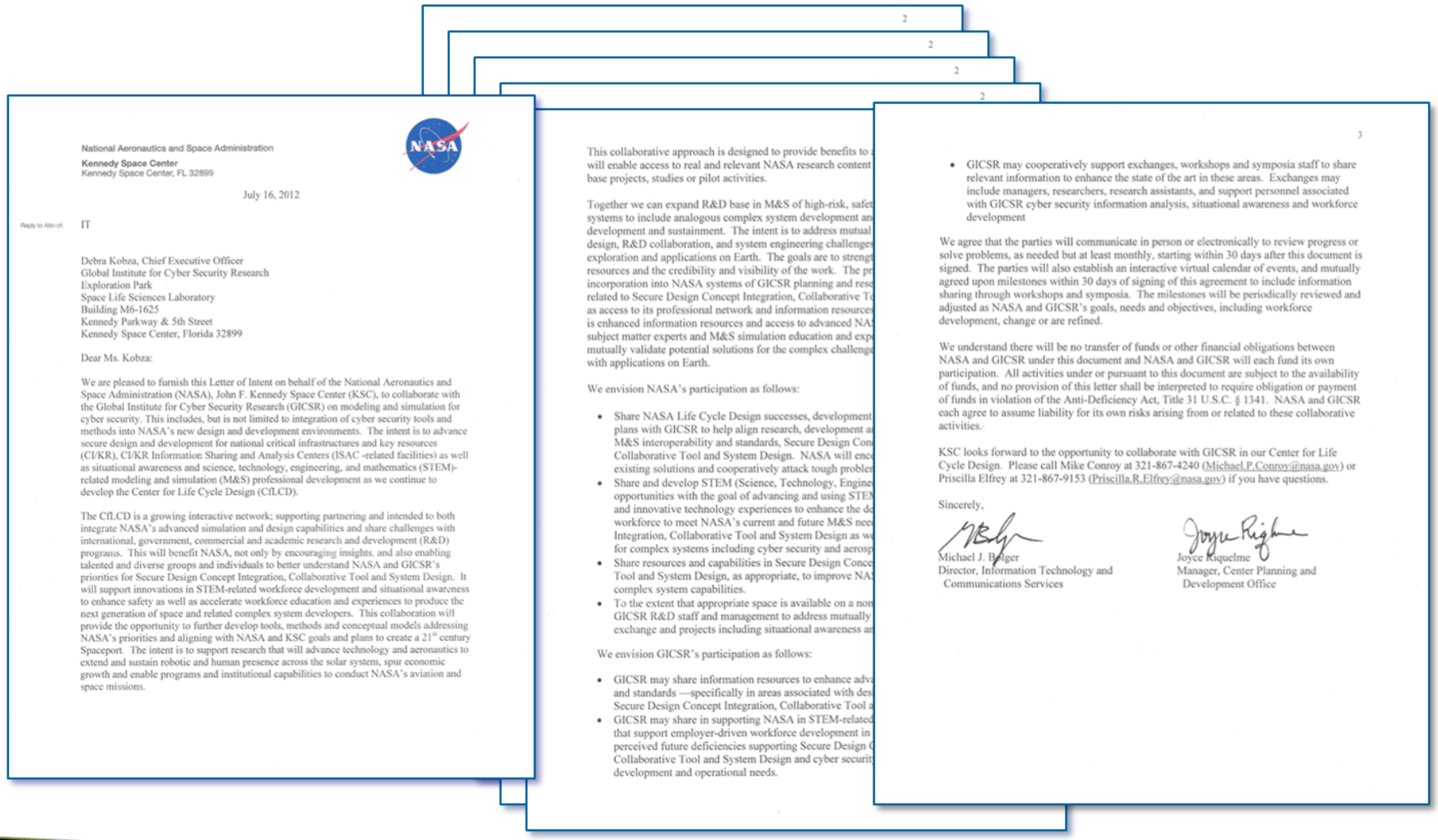
To serve as the trusted global collaborative facilitating open dialogue, critical insight and thought exchange linking critical infrastructure owners and operators, government, and academia to define and deliver scalable, flexible and adaptable cybersecurity resilience solutions.

Mission Support

Public/Private Collaboration

Government | Industry | Academia

GICSR / NASA-KSC COLLABORATIVE PARTNERSHIP



National Aeronautics and Space Administration
Kennedy Space Center
Kennedy Space Center, FL 32899

July 16, 2012

Reply to Attn of: IT

Debra Kobza, Chief Executive Officer
Global Institute for Cyber Security Research
Exploration Park
Space Life Sciences Laboratory
Building M6-1625
Kennedy Parkway & 5th Street
Kennedy Space Center, Florida 32899

Dear Ms. Kobza:

We are pleased to furnish this Letter of Intent on behalf of the National Aeronautics and Space Administration (NASA), John F. Kennedy Space Center (KSC), to collaborate with the Global Institute for Cyber Security Research (GICSR) on modeling and simulation for cyber security. This includes, but is not limited to integration of cyber security tools and methods into NASA's new design and development environments. The intent is to advance secure design and development for national critical infrastructures and key resources (CI/KR), CI/KR Information Sharing and Analysis Centers (ISAC -related facilities) as well as situational awareness and science, technology, engineering, and mathematics (STEM)-related modeling and simulation (M&S) professional development as we continue to develop the Center for Life Cycle Design (CfLCD).

The CfLCD is a growing interactive network; supporting partnering and intended to both integrate NASA's advanced simulation and design capabilities and share challenges with international, government, commercial and academic research and development (R&D) programs. This will benefit NASA, not only by encouraging insights, and also enabling talented and diverse groups and individuals to better understand NASA and GICSR's priorities for Secure Design Concept Integration, Collaborative Tool and System Design. It will support innovations in STEM-related workforce development and situational awareness to enhance safety as well as accelerate workforce education and experiences to produce the next generation of space and related complex system developers. This collaboration will provide the opportunity to further develop tools, methods and conceptual models addressing NASA's priorities and aligning with NASA and KSC goals and plans to create a 21st century Spaceport. The intent is to support research that will advance technology and aeronautics to extend and sustain robotic and human presence across the solar system, spur economic growth and enable programs and institutional capabilities to conduct NASA's aviation and space missions.

This collaborative approach is designed to provide benefits to
will enable access to real and relevant NASA research content
base projects, studies or pilot activities.

Together we can expand R&D base in M&S of high-risk, safet
systems to include analogous complex system development an
development and sustainment. The intent is to address mutual
design, R&D collaboration, and system engineering challenges
exploration and applications on Earth. The goals are to strengt
resources and the credibility and visibility of the work. The pr
incorporation into NASA systems of GICSR planning and rese
related to Secure Design Concept Integration, Collaborative To
as access to its professional network and information resources
is enhanced information resources and access to advanced NA
subject matter experts and M&S simulation education and exp
mutually validate potential solutions for the complex challenge
with applications on Earth.

We envision NASA's participation as follows:

- Share NASA Life Cycle Design successes, development
plans with GICSR to help align research, development a
M&S interoperability and standards, Secure Design Con
Collaborative Tool and System Design. NASA will enc
existing solutions and cooperatively attack tough proble
- Share and develop STEM (Science, Technology, Engine
opportunities with the goal of advancing and using STE
and innovative technology experiences to enhance the de
workforce to meet NASA's current and future M&S nee
Integration, Collaborative Tool and System Design as w
for complex systems including cyber security and aerosp
- Share resources and capabilities in Secure Design Conce
Tool and System Design, as appropriate, to improve NA
complex system capabilities.
- To the extent that appropriate space is available on a non
GICSR R&D staff and management to address mutually
exchange and projects including situational awareness a

We envision GICSR's participation as follows:

- GICSR may share information resources to enhance adv
and standards —specifically in areas associated with des
Secure Design Concept Integration, Collaborative Tool a
- GICSR may share in supporting NASA in STEM-related
that support employer-driven workforce development in
perceived future deficiencies supporting Secure Design C
Collaborative Tool and System Design and cyber securit
development and operational needs.

- GICSR may cooperatively support exchanges, workshops and symposia staff to share relevant information to enhance the state of the art in these areas. Exchanges may include managers, researchers, research assistants, and support personnel associated with GICSR cyber security information analysis, situational awareness and workforce development

We agree that the parties will communicate in person or electronically to review progress or solve problems, as needed but at least monthly, starting within 30 days after this document is signed. The parties will also establish an interactive virtual calendar of events, and mutually agreed upon milestones within 30 days of signing of this agreement to include information sharing through workshops and symposia. The milestones will be periodically reviewed and adjusted as NASA and GICSR's goals, needs and objectives, including workforce development, change or are refined.

We understand there will be no transfer of funds or other financial obligations between NASA and GICSR under this document and NASA and GICSR will each fund its own participation. All activities under or pursuant to this document are subject to the availability of funds, and no provision of this letter shall be interpreted to require obligation or payment of funds in violation of the Anti-Deficiency Act, Title 31 U.S.C. § 1341. NASA and GICSR each agree to assume liability for its own risks arising from or related to these collaborative activities.

KSC looks forward to the opportunity to collaborate with GICSR in our Center for Life Cycle Design. Please call Mike Conroy at 321-867-4240 (Michael.P.Conroy@nasa.gov) or Priscilla Elfrey at 321-867-9153 (Priscilla.R.Elfrey@nasa.gov) if you have questions.

Sincerely,

Michael J. Barger
Director, Information Technology and Communications Services

Joyce Riquelme
Manager, Center Planning and Development Office

GICSR "CORE 5"

G3 **Global Cooperation + Collaboration + Coordination**

C3i **Cybersecurity Intelligence + Information Sharing + Incident Response**

CRi **Cybersecurity Research Innovation**

CSD **Cybersecurity Secure Design**

GCR **Global Cyber Range**

Performance / Role-Based Education

Virtual Customizable Network – Applying Skills

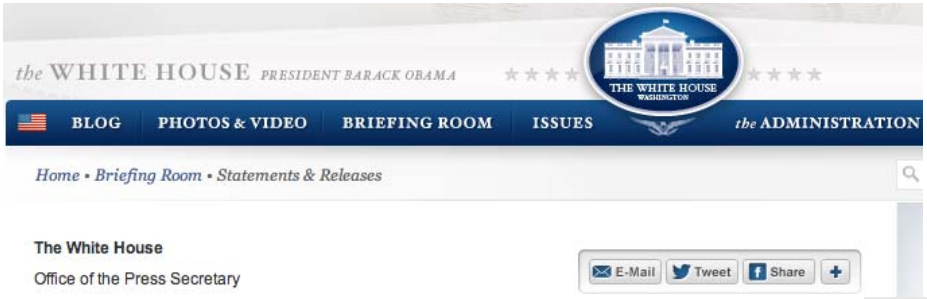
Certified Cyber First Responder – Coordinated Response

Modeling & Simulation, Exercise Simulation

Testing – Secure Design Verification and Validation

GSAC

PRESIDENTIAL POLICY DIRECTIVE | EXECUTIVE ORDER



the WHITE HOUSE PRESIDENT BARACK OBAMA

BLOG | PHOTOS & VIDEO | BRIEFING ROOM | ISSUES | the ADMINISTRATION

Home • Briefing Room • Statements & Releases

The White House
Office of the Press Secretary

E-Mail | Tweet | Share

For Immediate Release — February 12, 2013

Presidential Policy Directive -- Critical Infrastructure Security and Resilience

PRESIDENTIAL POLICY DIRECTIVE/PPD-21

SUBJECT: Critical Infrastructure Security and Resilience

The Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure.

the WHITE HOUSE PRESIDENT BARACK OBAMA

BLOG | PHOTOS & VIDEO | BRIEFING ROOM | ISSUES | the ADMINISTRATION

Home • Briefing Room • Presidential Actions • Executive Orders

The White House
Office of the Press Secretary

E-Mail | Tweet | Share

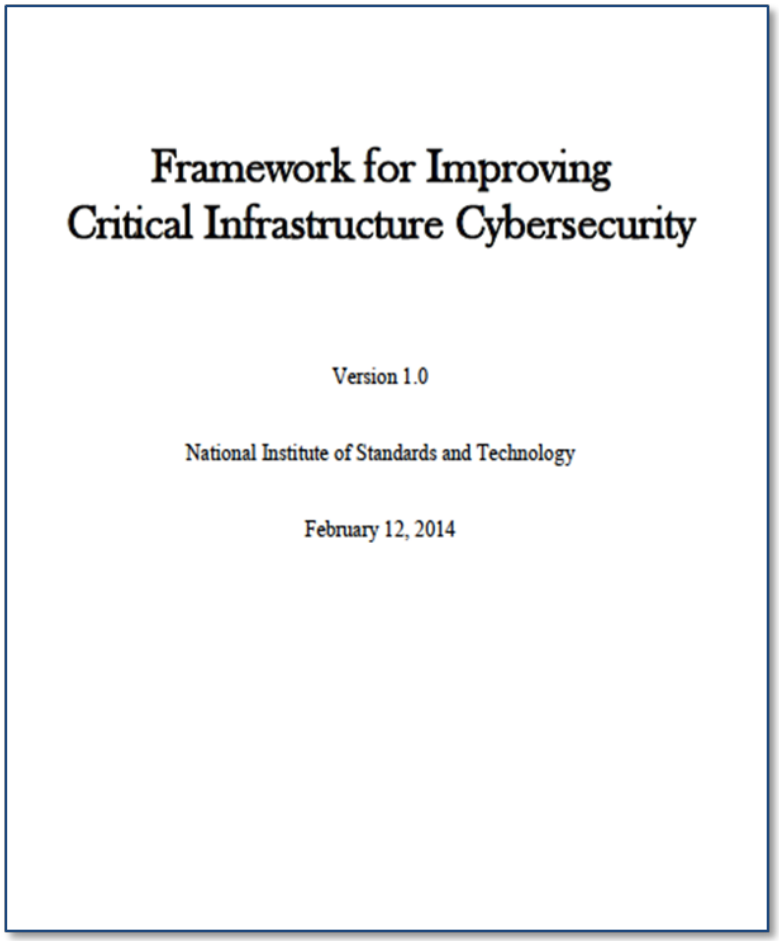
For Immediate Release — February 12, 2013

Executive Order -- Improving Critical Infrastructure Cybersecurity

EXECUTIVE ORDER

IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY

Executive Order 13636 – Improving Critical Infrastructure Cybersecurity


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

NIST Cybersecurity Framework

Framework Core

Identify | Protect | Detect | Respond | Recover

Identify (Systems, Assets, Data, Capabilities)

Protect (Develop and Implement Safeguards)

Detect (Timely Discovery of Cybersecurity Events)

Respond (Develop and Implement Appropriate Action Activities)

Recover (Develop and Implement Resilience Plans – Restore Capabilities

Categories | Subcategories | Informative References

(Categories – Access Management Control, Detection Process…)

(Subcategories – Activities Outcomes – Data at Rest is Protected…)

NIST Cybersecurity Framework

Framework Profile

Alignment of Functions, Categories and Subcategories

With Business Requirements, Risk Tolerance and Organization Resources

Establishes Reducing Cybersecurity Risk

Current Profile | Target Profile

Current Profile – Cybersecurity Outcomes Currently Being Achieved

Target Profile – Outcomes Needed to Achieve Cyber Risk Management Goals

Profile Comparison

Gap Mitigation Cost-Effective Roadmap

NIST Cybersecurity Framework

Framework Implementation Tiers

How an Organization Views Cyber Risk + Risk Management

Risk Management Process | Integrated Risk Management Program | External Participation

Tier 1: Partial – Not Formalized, Ad-Hoc, Reactive, Limited Awareness, No Processes

Tier 2: Risk Informed – Processes, Not Org. Wide, Informal Sharing, Limited Interaction

Tier 3: Repeatable – Practices Approved/Policy, Org-Wide, Knowledge/Skills, Sharing Information Internally

Tier 4: Adaptive – Continuous Improvement, Org-Wide, Active Sharing, Cyber Risk Part of Culture, Share Information Internally / Externally

NICE

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

National Initiative for Cybersecurity Education

NICE

NATIONAL INITIATIVE FOR
CYBERSECURITY EDUCATION

The Framework establishes:

- A common taxonomy and lexicon which organizes cybersecurity into 31 specialty areas within 7 categories.
- A baseline of tasks, specialty areas, and knowledge, skills and abilities (KSAs) associated with cybersecurity professionals.

The Framework assists with strategic human capital efforts, including:

- Workforce Planning
- Recruitment and Selection
- Training and Development
- Succession Planning

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

Framework Categories and Specialty Areas

- The Framework's 31 Specialty Areas (SA), organized into 7 Categories, encompass the entirety of national cybersecurity work.
- Organizations can use the SAs to identify, build, and customize cybersecurity roles based on mission requirements.

This is the tie to the OPM Data Element and EHRI.

Securely Provision	Operate and Maintain	Oversight and Development	Protect and Defend	Analyze	Collect and Operate	Investigate
Systems Requirement Planning	System Administration	Legal Advice and Advocacy	Computer Network Defense (CND)	Cyber Threat Analysis	Collection Operations	Digital Forensics
Systems Development	Network Services	Education and Training	Vulnerability Assessment and Management	All Source Intelligence	Cyber Operations Planning	Investigation
Software Assurance and Security Engineering	Customer Service and Technical Support	Strategic Planning and Policy	Incident Response	Targets	Cyber Operations	
Technology Research and Development	Systems Security Analysis	Information Systems Security Operations	CND Incident Response	Exploitation Analysis		
Test and Evaluation	Data Administration	Security Program Management (CISO)				
Systems Security Architecture	Knowledge Management					
Information Assurance (IA) Compliance						

NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

CYBERSECURITY RESILIENCE– A THREE TIERED SOLUTION

GLOBAL CYBER RANGE OBJECTIVES

Simulate systems and their complexities and advance visualization of data with the goal of improving policy, practices, technologies, operations and education to measure and strengthen cybersecurity resilience and safety, including but not limited to:

- Support Global Cyber Education – Performance/Role-Based-based Education
- Customizable Network Environments to Apply Skills (Offensive or Defensive)
- Modeling & Simulation - Cyber Drill Exercises (Gaming, Metrics, and Storytelling to Accelerate Action and “Seed” Innovation)
- KSC – Technology Test Bed - Assessment, Testing – Secure Design IV&V
- Certified Cyber First Responder – Coordinated National Cyber Response
- Supporting Retaining, Sustaining and Creating Cybersecurity Jobs – Safety, Security, Modeling and Simulation, Information Assurance, Verification and Validation.

HOW IT WORKS

Target Virtual Machine Networks – Online Virtualized Platform.

Student Logs In – Presented with Learning Objectives and Goals, Content Briefing

Student Launches the Range environment

Within 1 Minute – Full Target Range Booted in the Range Cloud Environment.

All Labs – Fully Isolated and Disconnected from the Live Internet

Student Logs In – Learning Objectives and Goals, Content Briefing

Remote Viewer Operates Through Range of Protocols for Maximum Compatibility

Provides Student with Screen View and Machine Commands for Virtual Machines

Virtual Machines (VMs) Housed – Inside Learning Environment

Includes Ability to Provide Direct Guidance, Learning Objectives, Exercises and Tasks

Advanced Feedback Models (Alerts, Recommendations, Screen Shots, Short Video Tutorials)

GLOBAL CYBER RANGE LOG-IN

https://gicsr.learnondemand.net/User/Login?ReturnUrl=%2f

The Global Institute for Cybersecurity + Research

Where Science, Technology and Innovation Excel

Contact

Welcome to the Global Cyber Range (GCR)

Are you a new user? Create an account to register you access code and get started. Make sure you have your access code handy before registering!

Already have an account with GICSR's National Cyber Range? Simply log into your existing account to register a new access code or begin a new session.

Login

Username:

Password:

Login

Create an Account

Forget Your Password?

ON-DEMAND

24/7

Global Cyber Range (GCR)

CyPro
(Cybersecurity Professional)

Training Catalog

Most Comprehensive and Feature Rich Cyber Range

Currently – Over 400 Complete Exercises

Hundreds of Fully Virtualized Operating Systems

Windows Server 2003 | Windows 7 | Windows 8 | Windows Server 2012 | ubuntu | back | track 5

GLOBAL CYBER RANGE ENVIRONMENT

On-Demand 24/7 LIVE Cyber Range Professional Development Environment

Access Anywhere - Internet Connection & Web Browser – No Plug-Ins, No Software

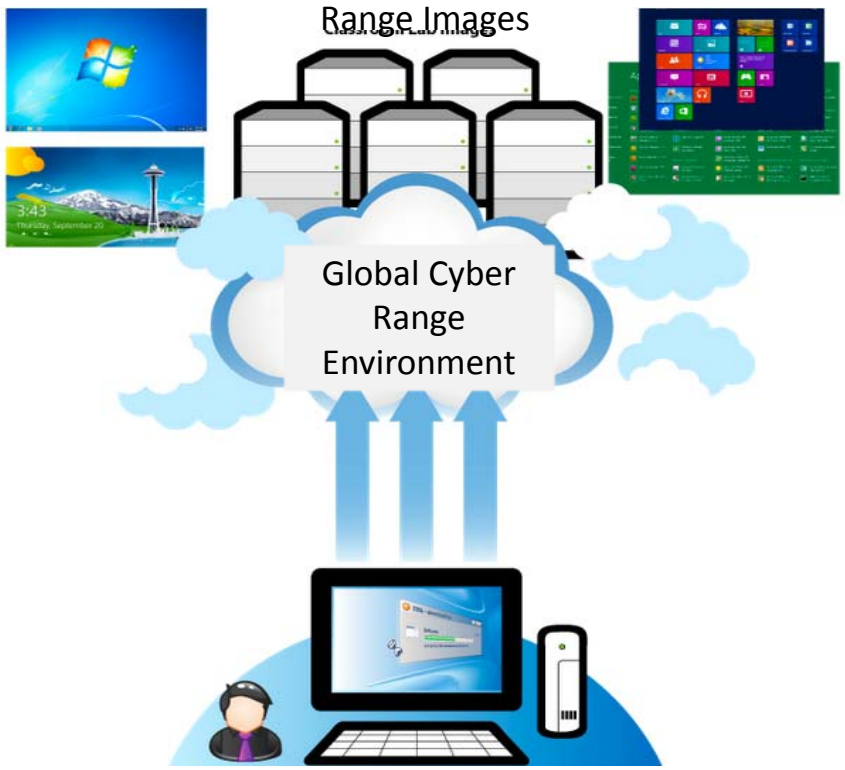
Desktop | Laptop | iPad | iPhone | Android Any Device Supporting HTML5

Launch and Dynamically Access a Host of Virtual Machines Preconfigured with Vulnerabilities, Exploits, Tools and Scripts

Target Machines – Completely Virtualized - Control and Reset Machines Quickly

Student – Has 100% Control of the Environment

Instructor – "Over-the-Shoulder" Review



Mobile Forensics: Advanced Mobile Hacking & Forensics

Hardening Your Enterprise: Advanced Network Defense

Network Exploitation Concepts and Methods (Boot Camp)

Network Forensics – Identifying and Correlating Events (Network Forensics)

Packet and Traffic Analysis (Wiretap)

Digital Media Forensics I (Basic Digital Media Forensics)

Digital Media Forensics II (Advanced Digital Media Forensics)

Understanding Machine Assembly Language (Assembly Fundamentals)

ETHICAL HACKING

Access to 75 Different Exercises – Fully Patched Operating Systems / Virtual Machines

Footprinting and Reconnaissance | Scanning Networks | Enumeration |

System Hacking | Trojans and Backdoors | Viruses and Worms | Sniffers

Social Engineering | Denial of Service | Session Hijacking | Hacking Web Servers

Hacking Web Applications | SQL Injection | Hacking Wireless Networks

Evading IDS, Firewalls & Honeypots | Buffer Overflow | Cryptography

COMPUTER FORENSICS

Access to 34 Different Exercises – Each exercise category has it's own Virtual Private Cloud preconfigured with vulnerable websites, victim machines, an environment LOADED with tools, and investigation files, hard disk clones and targets.

Computer Forensics Investigation Process | Computer Forensics Lab

Understanding Hard Disks and File Systems | Windows Forensics

Data Acquisition and Duplication | Recovering Deleted Files and Partitions

Forensics Investigation Using AccessData FTK | Forensics Investigation Using EnCase

Steganography and Image File Forensics | Application Password Crackers

Log Capturing and Event Correlation | Investigating Wireless Attacks

Network Forensics, Investigation Logs, Investigating Network Traffic

Tracking and Investigating Email Crimes | Mobile Forensics | Investigative Reports

SECURITY ANALYST EXERCISES

Access to 15 Different Exercises – Fully Patched Operating Systems / Virtual Machines

TCPIP Packet Analysis | Information Gathering | Vulnerability Analysis

External Penetration Testing | Internal Network Penetration Testing

Firewall Penetration Testing | IDS Penetration Testing

Password Cracking Penetration Testing | Social Engineering Penetration Testing

Web Application Penetration Testing | SQL Penetration Testing

SECURE PROGRAMMING

Access to 68 Different Exercises – Fully Patched Operating Systems / Virtual Machines

Input Validation and Output Encoding

.NET Authentication and Authorization

Secure Session and State Management

.NET Cryptography

.NET Error Handling, Auditing and Logging

.NET Secure File Handling

.NET Configuration Management and Secure Code Review

INCIDENT HANDLING

Access to 75 Exercises – Fully Patched Operating Systems / Virtual Machines

Trojans and Backdoors

Computer Forensics Investigation Process

Understanding Hard Disks and File Systems

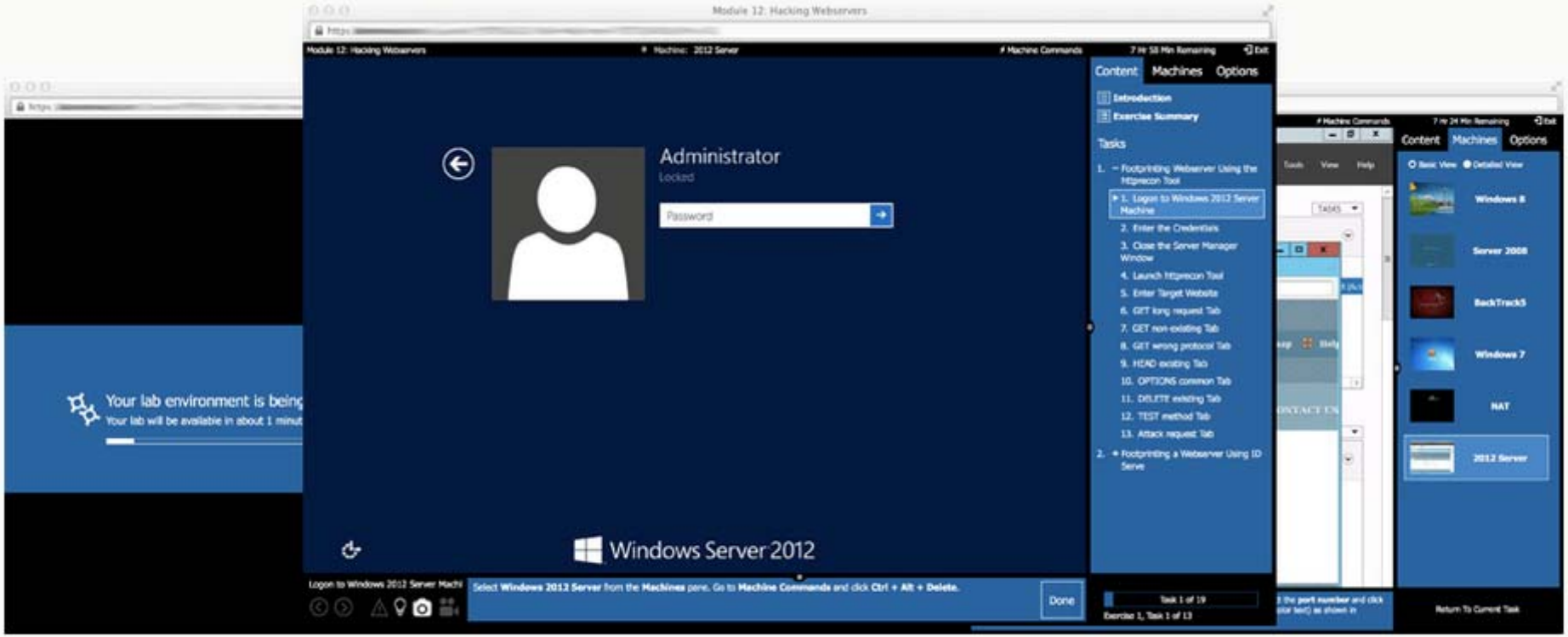
Forensics Investigation Using AccessData FTK

Forensics Investigation Using EnCase

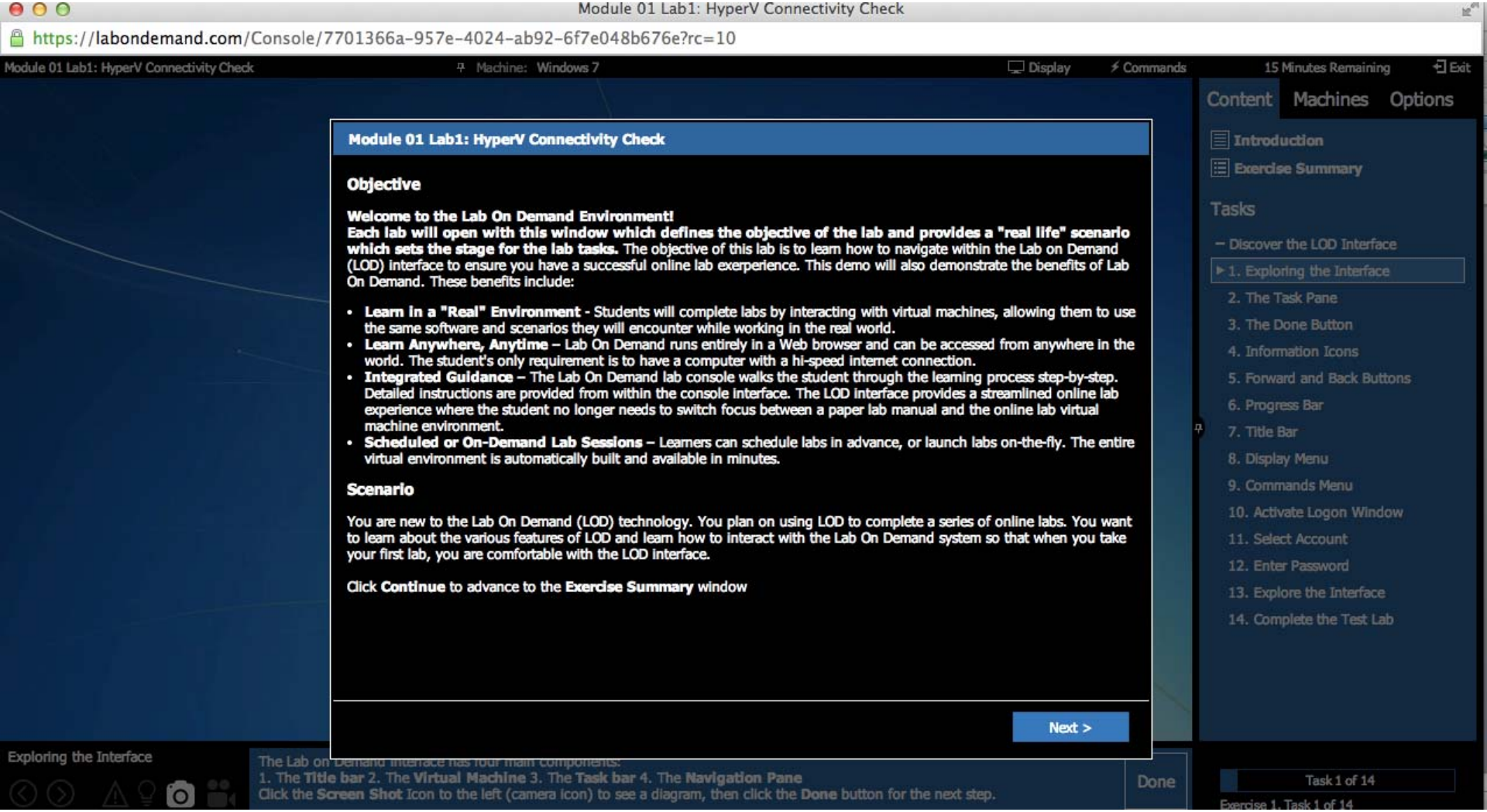
Log Capturing and Event Correlation

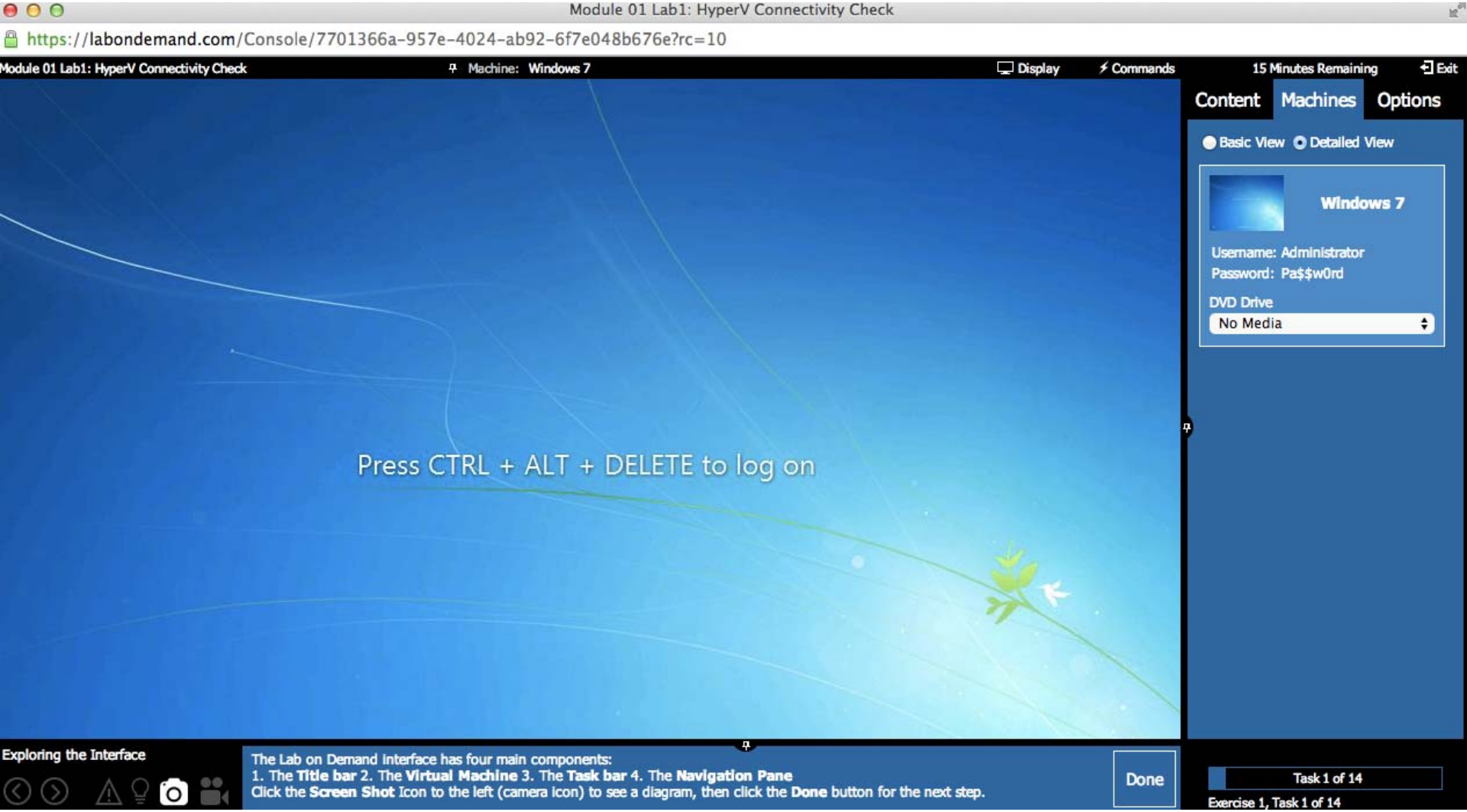
Cloud-Based | 100% Automated - 100% Virtualization
Accessible Anywhere – Via Internet Connection
Instant Connectivity to all Range Labs

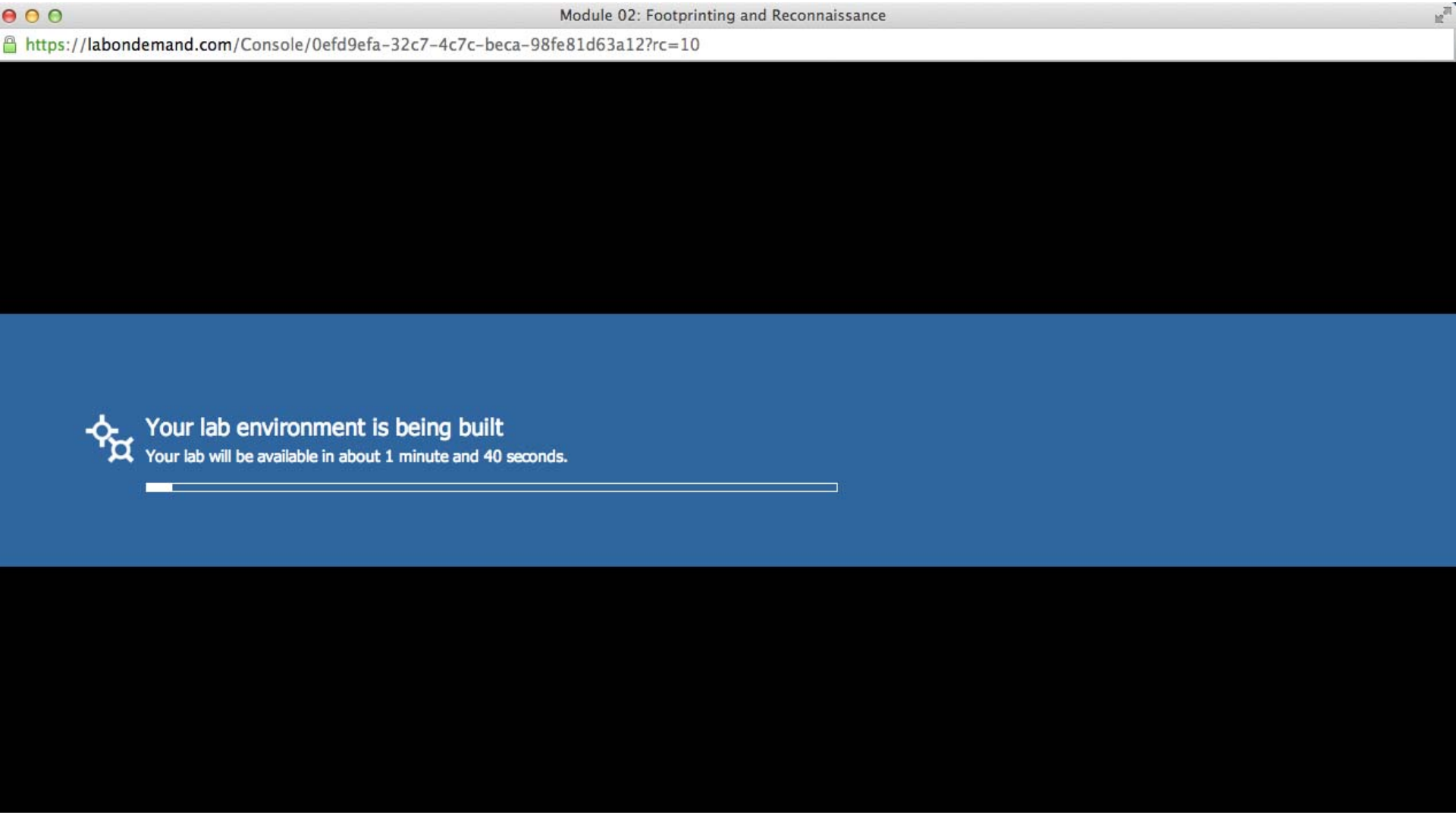
Access to Real-World Tools and Scenarios
After Log-In – Full Access to Preconfigured Targets, Networks and Attack Tools

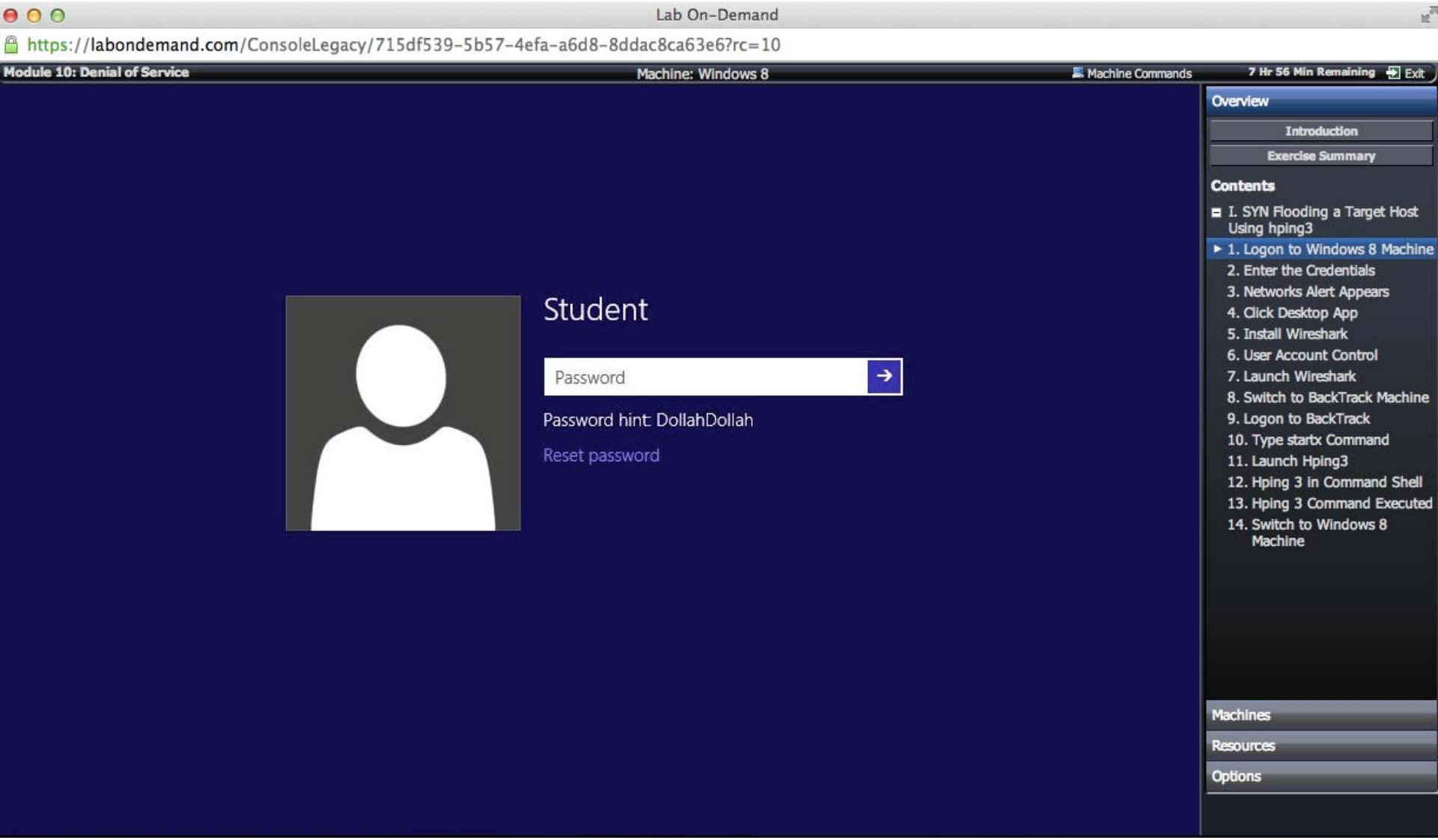


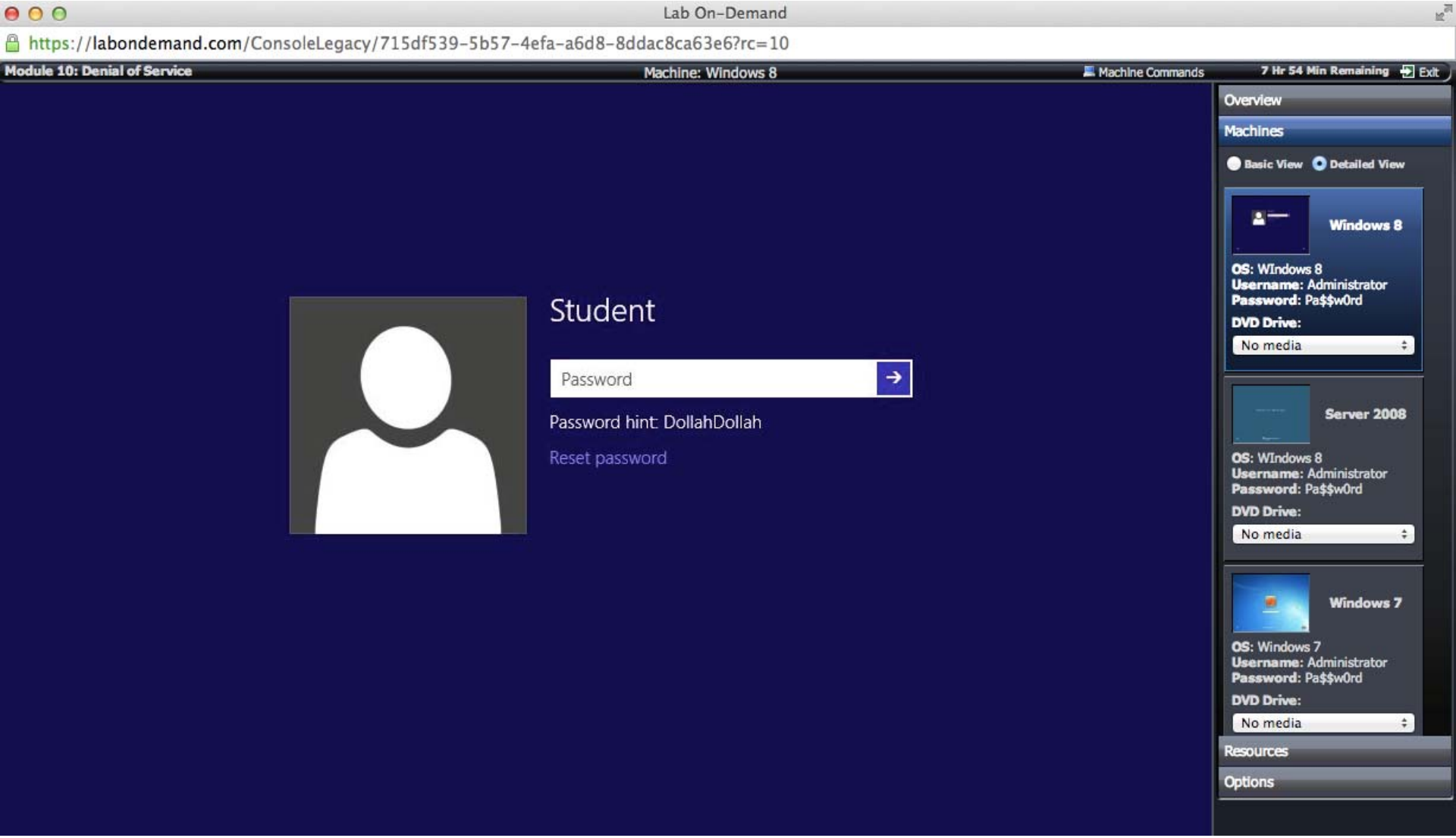
Preconfigured Vulnerable Websites
Hidden Victim Machines
Vulnerable, Unpatched Operating Systems
Fully Networked Environments
Forensic Cast Files and Hard Disks

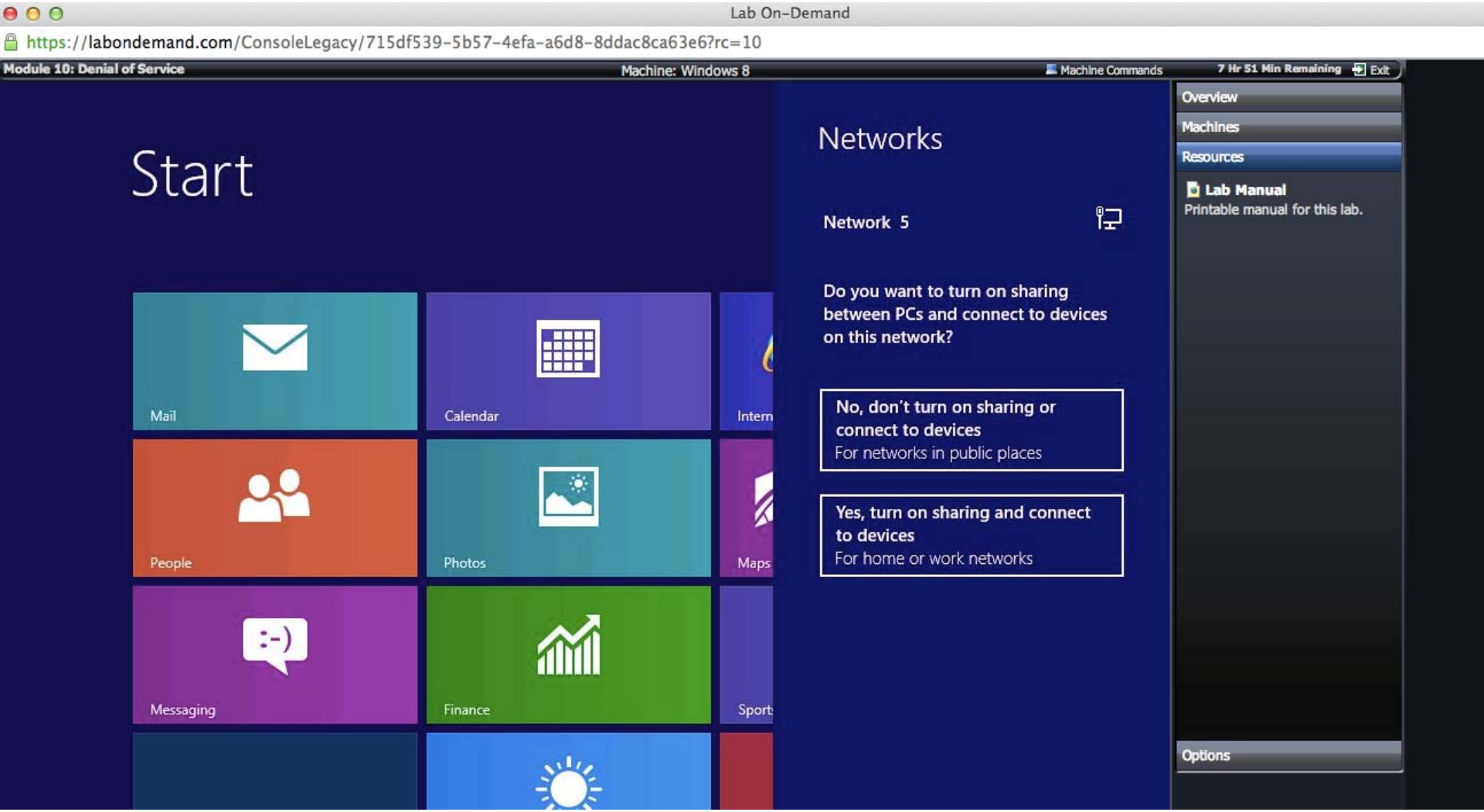

Module 01 Lab1: HyperV Connectivity Check
https://labondemand.com/Console/7701366a-957e-4024-ab92-6f7e048b676e?rc=10
Module 01 Lab1: HyperV Connectivity Check
Machine: Windows 7
Display
Commands
15 Minutes Remaining
Exit
Content
Machines
Options
Introduction
Exercise Summary
Tasks
– Discover the LOD Interface
1. Exploring the Interface
2. The Task Pane
3. The Done Button
4. Information Icons
5. Forward and Back Buttons
6. Progress Bar
7. Title Bar
8. Display Menu
9. Commands Menu
10. Activate Logon Window
11. Select Account
12. Enter Password
13. Explore the Interface
14. Complete the Test Lab
Module 01 Lab1: HyperV Connectivity Check
Objective
Welcome to the Lab On Demand Environment!
Each lab will open with this window which defines the objective of the lab and provides a "real life" scenario which sets the stage for the lab tasks. The objective of this lab is to learn how to navigate within the Lab on Demand (LOD) interface to ensure you have a successful online lab exerperience. This demo will also demonstrate the benefits of Lab On Demand. These benefits include:
• Learn in a "Real" Environment - Students will complete labs by interacting with virtual machines, allowing them to use the same software and scenarios they will encounter while working in the real world.
• Learn Anywhere, Anytime – Lab On Demand runs entirely in a Web browser and can be accessed from anywhere in the world. The student's only requirement is to have a computer with a hi-speed internet connection.
• Integrated Guidance – The Lab On Demand lab console walks the student through the learning process step-by-step. Detailed instructions are provided from within the console interface. The LOD interface provides a streamlined online lab experience where the student no longer needs to switch focus between a paper lab manual and the online lab virtual machine environment.
• Scheduled or On-Demand Lab Sessions – Learners can schedule labs in advance, or launch labs on-the-fly. The entire virtual environment is automatically built and available in minutes.
Scenario
You are new to the Lab On Demand (LOD) technology. You plan on using LOD to complete a series of online labs. You want to learn about the various features of LOD and learn how to interact with the Lab On Demand system so that when you take your first lab, you are comfortable with the LOD interface.
Click Continue to advance to the Exercise Summary window
Next >
Exploring the Interface
1. The Title bar 2. The Virtual Machine 3. The Task bar 4. The Navigation Pane
Click the Screen Shot Icon to the left (camera icon) to see a diagram, then click the Done button for the next step.
Done
Task 1 of 14
Exercise 1, Task 1 of 14

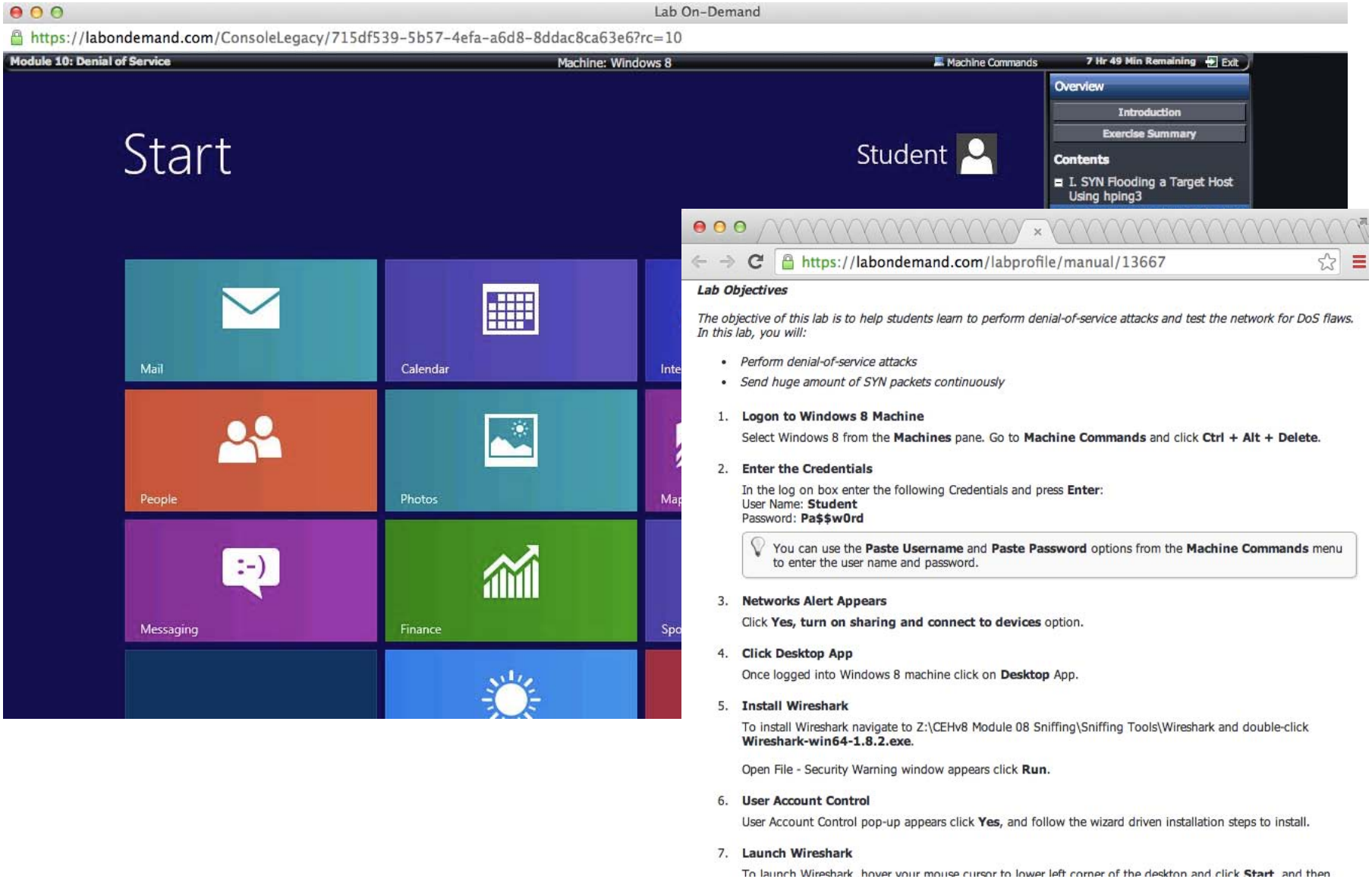

Module 01 Lab1: HyperV Connectivity Check
https://labondemand.com/Console/7701366a-957e-4024-ab92-6f7e048b676e?rc=10
Module 01 Lab1: HyperV Connectivity Check
Machine: Windows 7
Display
Commands
15 Minutes Remaining
Exit
Content
Machines
Options
Basic View
Detailed View
Windows 7
Username: Administrator
Password: Pa$$w0rd
DVD Drive
No Media
Press CTRL + ALT + DELETE to log on
Exploring the Interface
The Lab on Demand interface has four main components:
1. The Title bar 2. The Virtual Machine 3. The Task bar 4. The Navigation Pane
Click the Screen Shot Icon to the left (camera icon) to see a diagram, then click the Done button for the next step.
Done
Task 1 of 14
Exercise 1, Task 1 of 14

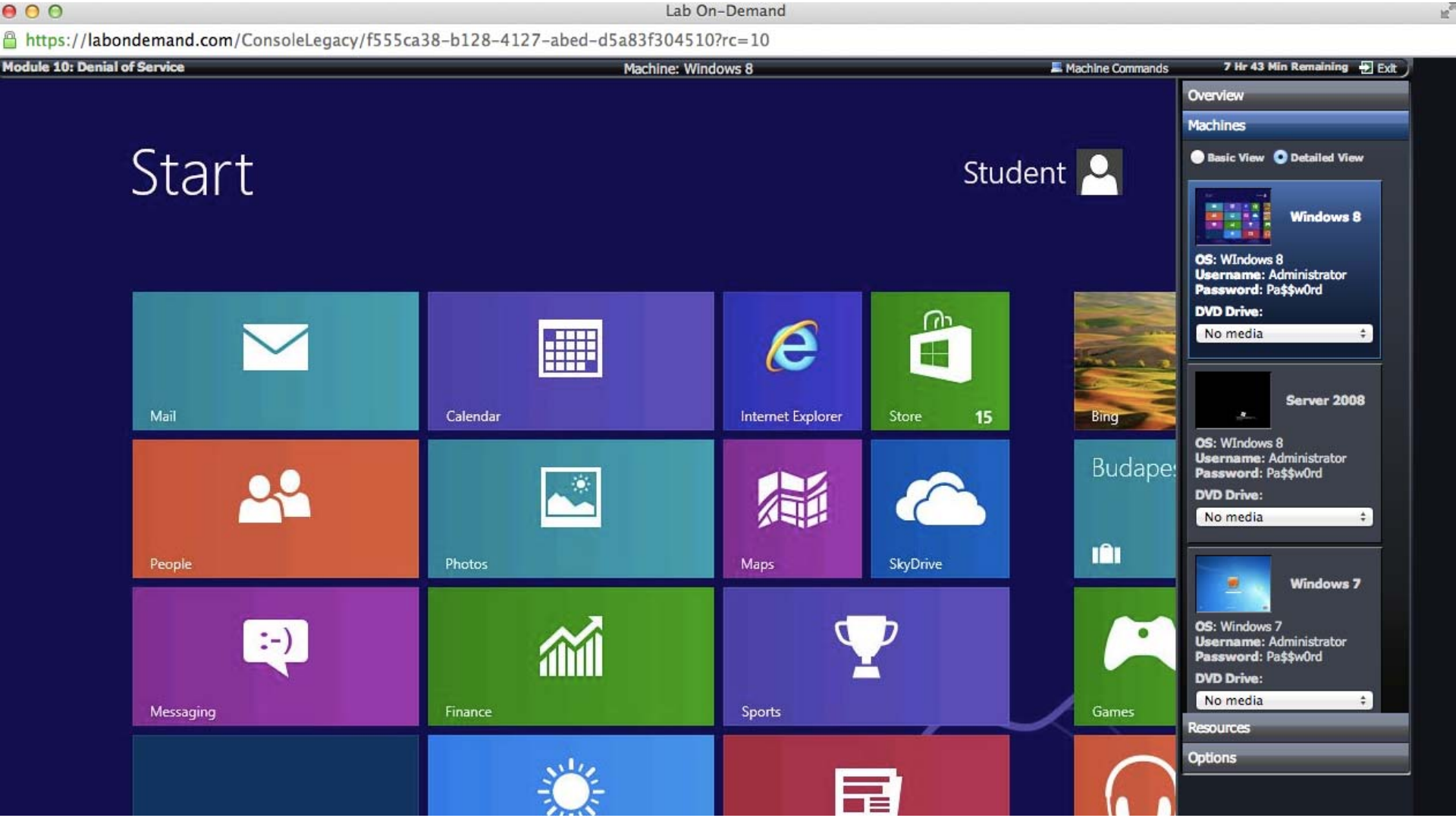

Module 02: Footprinting and Reconnaissance
https://labondemand.com/Console/0efd9efa-32c7-4c7c-beca-98fe81d63a12?rc=10
Your lab environment is being built
Your lab will be available in about 1 minute and 40 seconds.

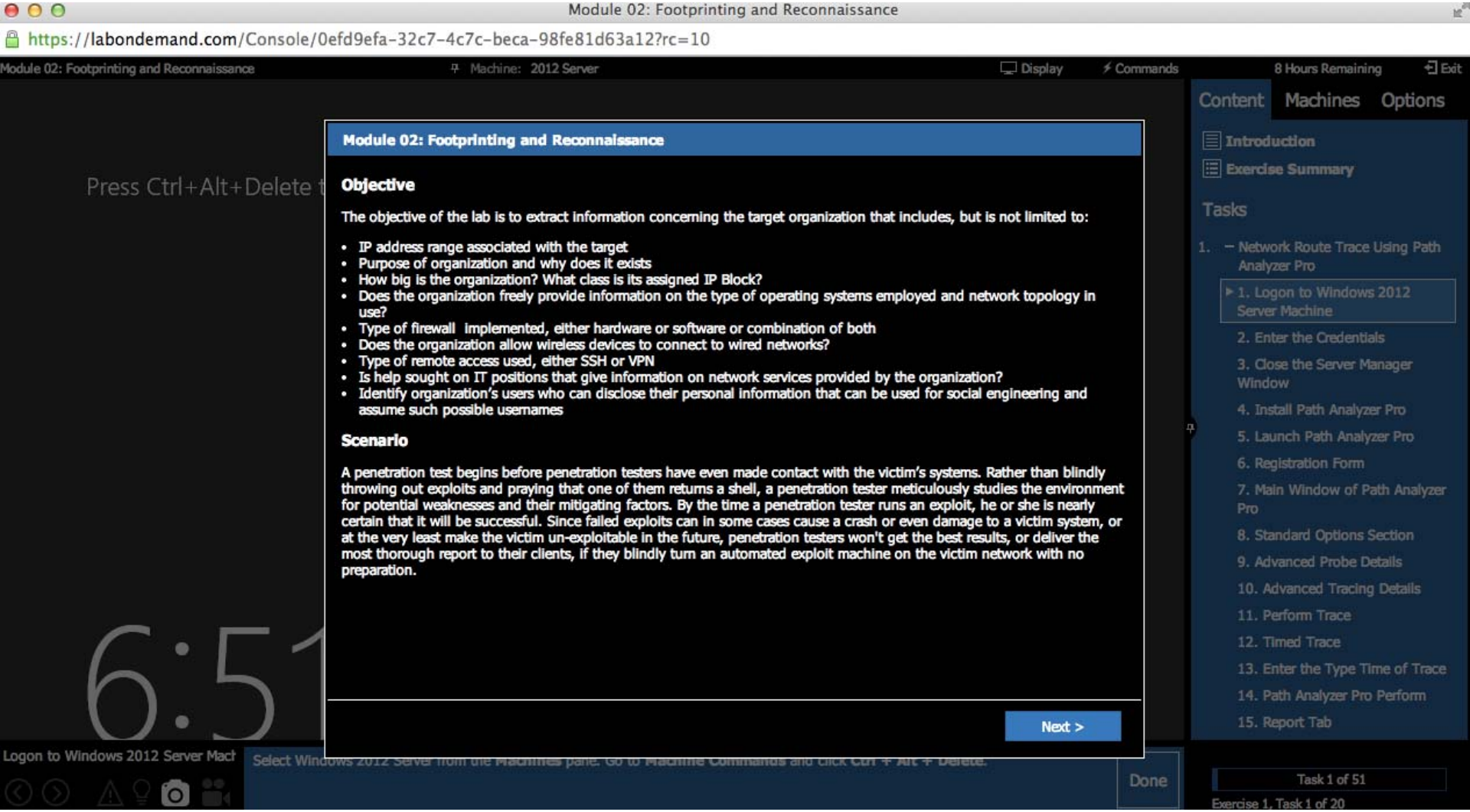

Lab On-Demand
https://labondemand.com/ConsoleLegacy/715df539-5b57-4efa-a6d8-8ddac8ca63e6?rc=10
Module 10: Denial of Service
Machine: Windows 8
Machine Commands
7 Hr 56 Min Remaining
Exit
Student
Password
Password hint: DollahDollah
Reset password
Overview
Introduction
Exercise Summary
Contents
I. SYN Flooding a Target Host Using hping3
1. Logon to Windows 8 Machine
2. Enter the Credentials
3. Networks Alert Appears
4. Click Desktop App
5. Install Wireshark
6. User Account Control
7. Launch Wireshark
8. Switch to BackTrack Machine
9. Logon to BackTrack
10. Type startx Command
11. Launch Hping3
12. Hping 3 in Command Shell
13. Hping 3 Command Executed
14. Switch to Windows 8 Machine
Machines
Resources
Options

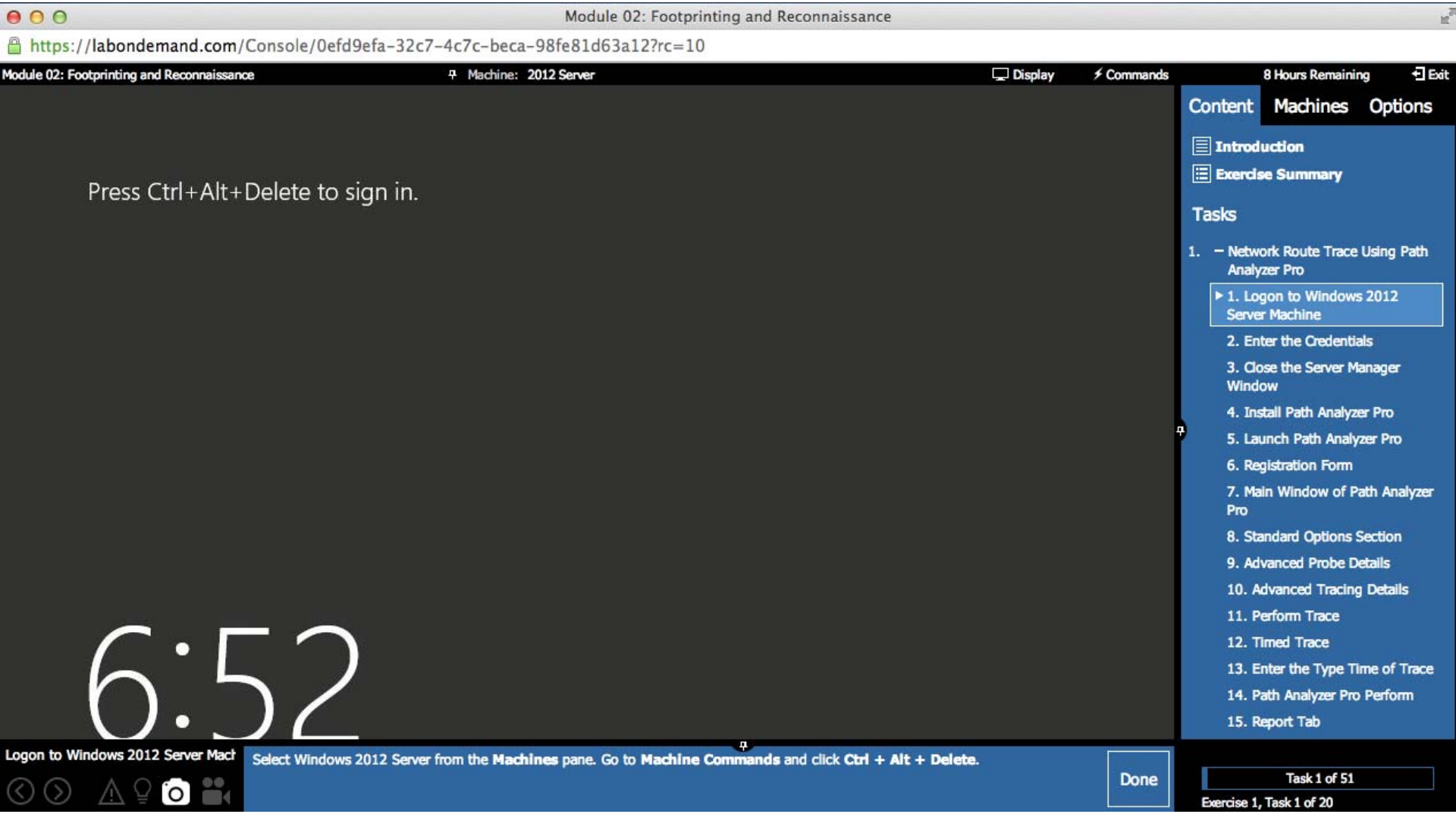

Lab On-Demand
https://labondemand.com/ConsoleLegacy/715df539-5b57-4efa-a6d8-8ddac8ca63e6?rc=10
Module 10: Denial of Service
Machine: Windows 8
Machine Commands
7 Hr 54 Min Remaining
Exit
Student
Password
Password hint: DollahDollah
Reset password
Overview
Machines
Basic View
Detailed View
Windows 8
OS: WIndows 8
Username: Administrator
Password: Pa$$w0rd
DVD Drive:
No media
Server 2008
OS: WIndows 8
Username: Administrator
Password: Pa$$w0rd
DVD Drive:
No media
Windows 7
OS: Windows 7
Username: Administrator
Password: Pa$$w0rd
DVD Drive:
No media
Resources
Options

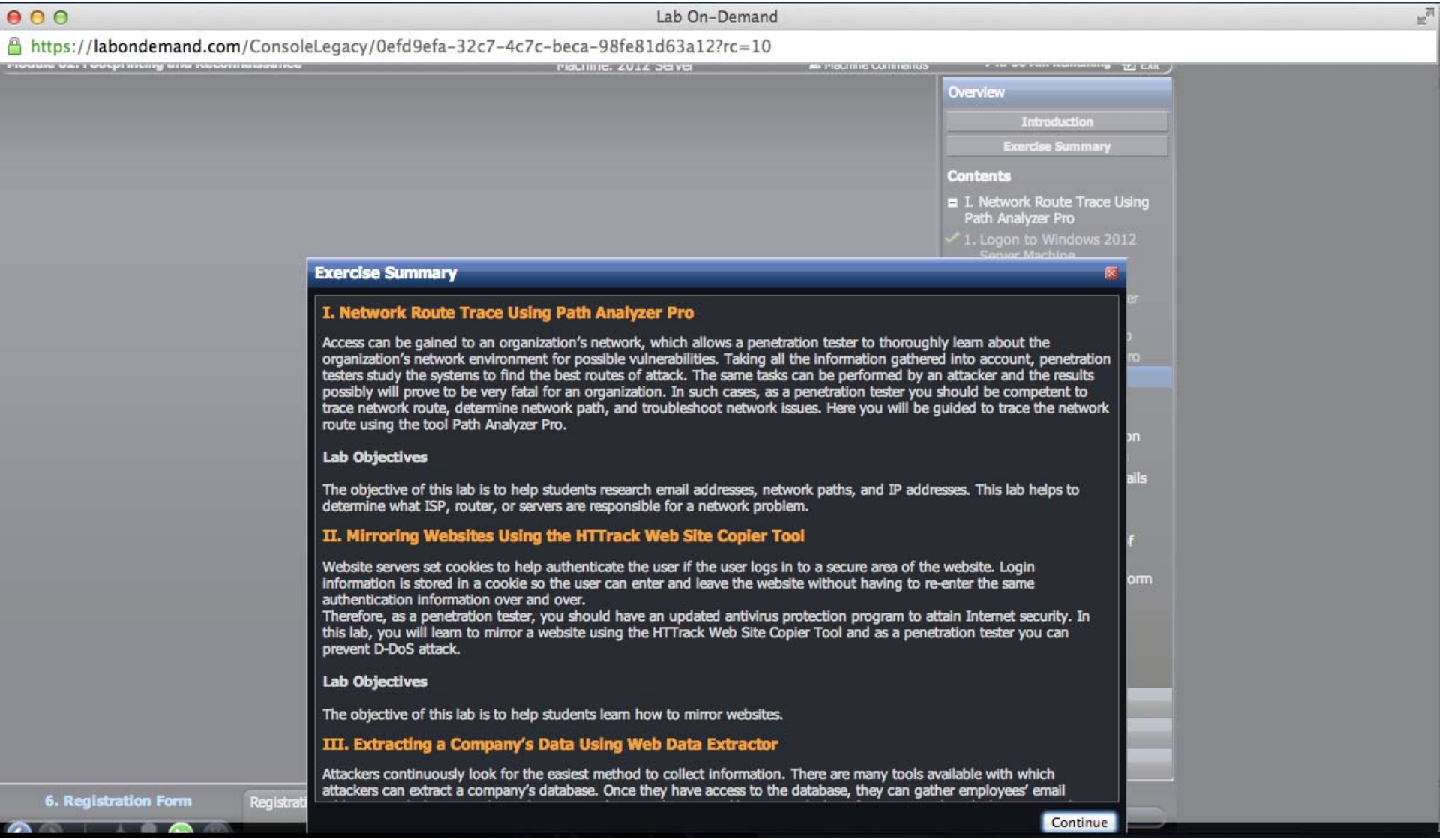

Lab On-Demand
https://labondemand.com/ConsoleLegacy/715df539-5b57-4efa-a6d8-8ddac8ca63e6?rc=10
Module 10: Denial of Service
Machine: Windows 8
Machine Commands
7 Hr 51 Min Remaining
Exit
Start
Mail
Calendar
People
Photos
Maps
Messaging
Finance
Networks
Network 5
Do you want to turn on sharing between PCs and connect to devices on this network?
No, don't turn on sharing or connect to devices
For networks in public places
Yes, turn on sharing and connect to devices
For home or work networks
Overview
Machines
Resources
Lab Manual
Printable manual for this lab.
Options

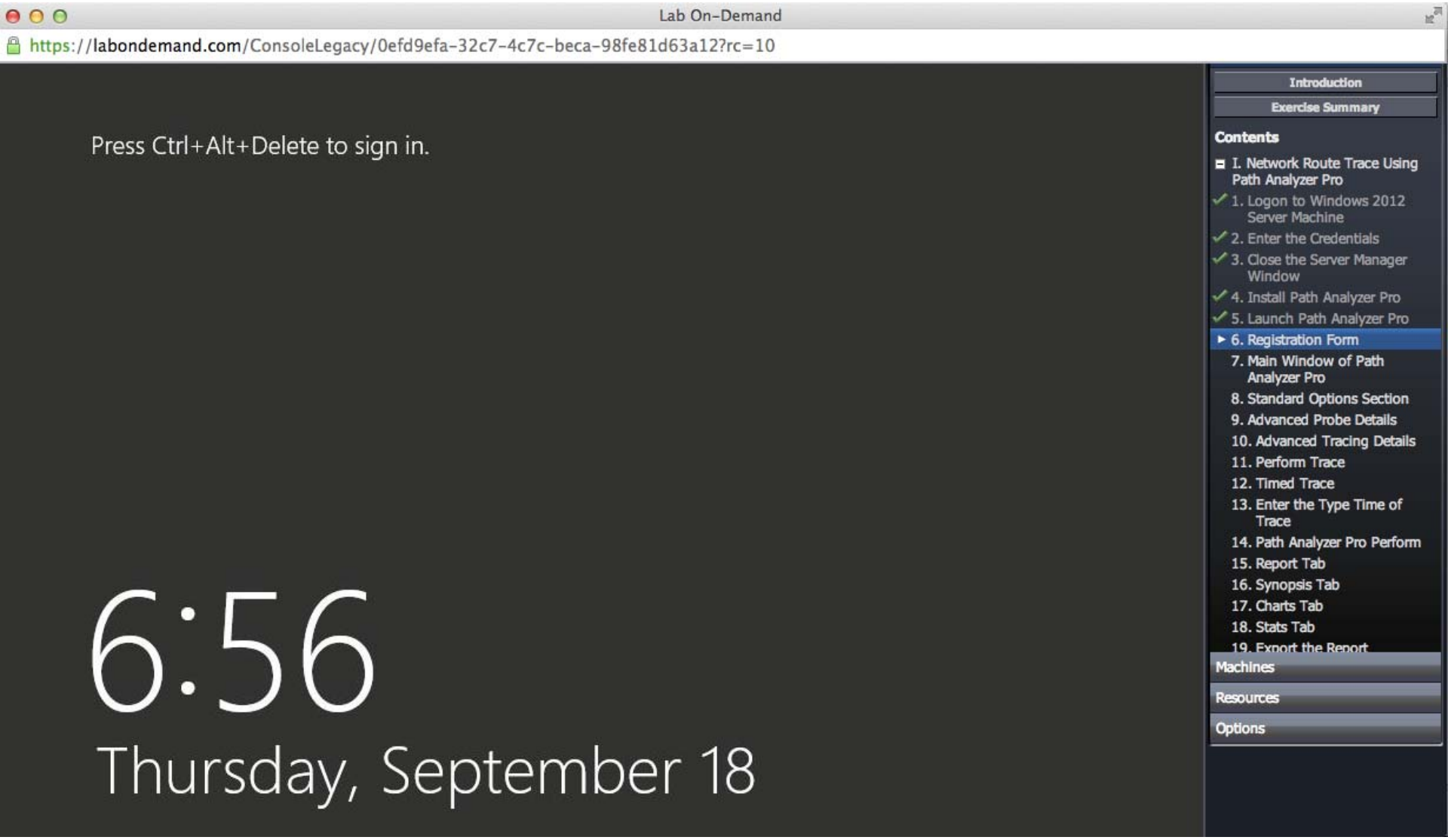

Lab On-Demand
https://labondemand.com/ConsoleLegacy/715df539-5b57-4efa-a6d8-8ddac8ca63e6?rc=10
Module 10: Denial of Service
Machine: Windows 8
Machine Commands
7 Hr 49 Min Remaining
Exit
Start
Student
Mail
Calendar
People
Photos
Messaging
Finance
Overview
Introduction
Exercise Summary
Contents
I. SYN Flooding a Target Host Using hping3
https://labondemand.com/labprofile/manual/13667
Lab Objectives
The objective of this lab is to help students learn to perform denial-of-service attacks and test the network for DoS flaws. In this lab, you will:
Perform denial-of-service attacks
Send huge amount of SYN packets continuously
1. Logon to Windows 8 Machine
Select Windows 8 from the Machines pane. Go to Machine Commands and click Ctrl + Alt + Delete.
2. Enter the Credentials
In the log on box enter the following Credentials and press Enter:
User Name: Student
Password: Pa$$w0rd
You can use the Paste Username and Paste Password options from the Machine Commands menu to enter the user name and password.
3. Networks Alert Appears
Click Yes, turn on sharing and connect to devices option.
4. Click Desktop App
Once logged into Windows 8 machine click on Desktop App.
5. Install Wireshark
To install Wireshark navigate to Z:\CEHv8 Module 08 Sniffing\Sniffing Tools\Wireshark and double-click Wireshark-win64-1.8.2.exe.
Open File - Security Warning window appears click Run.
6. User Account Control
User Account Control pop-up appears click Yes, and follow the wizard driven installation steps to install.
7. Launch Wireshark

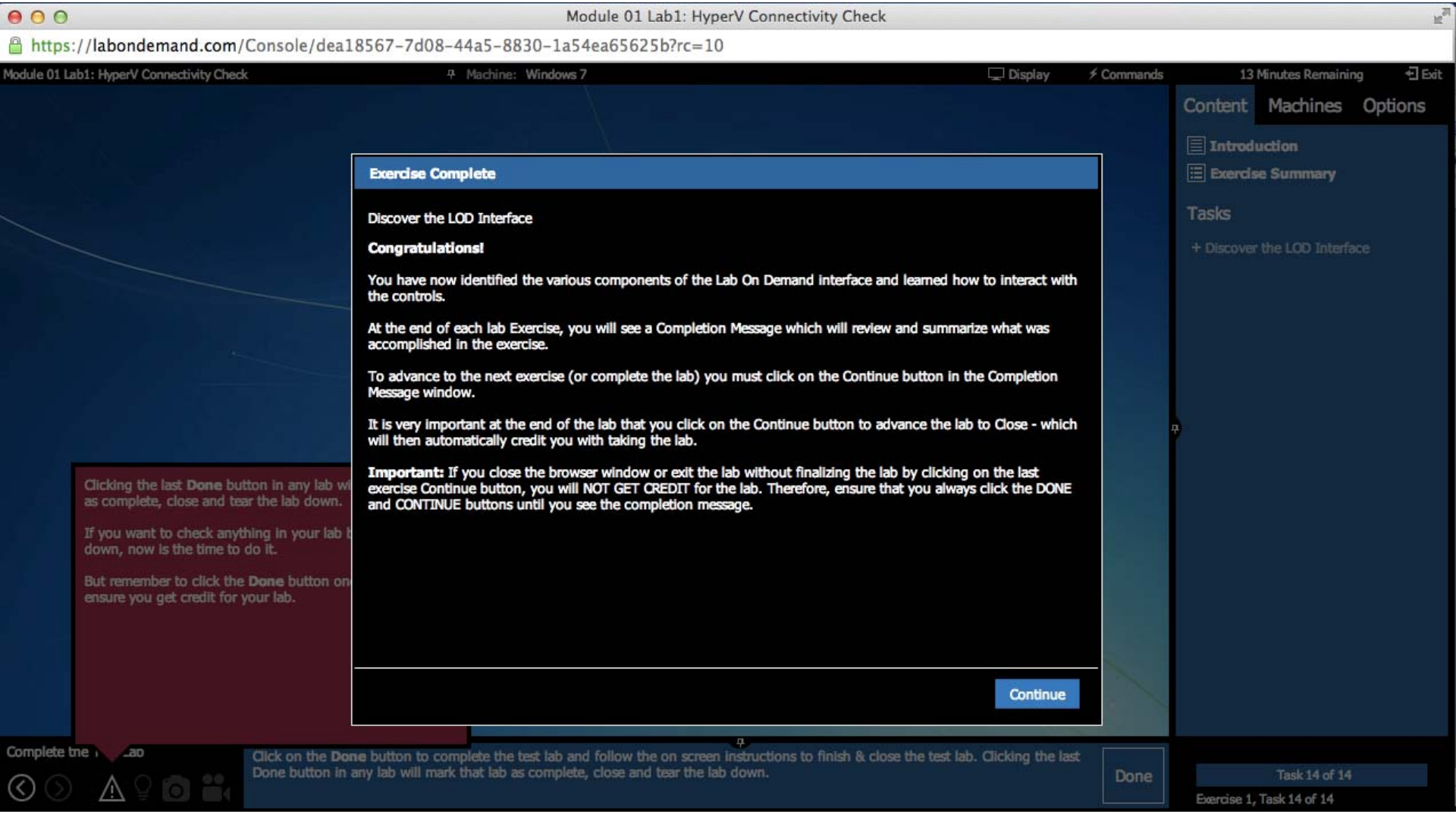

Lab On-Demand
https://labondemand.com/ConsoleLegacy/f555ca38-b128-4127-abed-d5a83f304510?rc=10
Module 10: Denial of Service
Machine: Windows 8
Machine Commands
7 Hr 43 Min Remaining
Exit
Start
Student
Mail
Calendar
Internet Explorer
Store
15
Bing
People
Photos
Maps
SkyDrive
Budape
Messaging
Finance
Sports
Games
Overview
Machines
Basic View
Detailed View
Windows 8
OS: WIndows 8
Username: Administrator
Password: Pa$$w0rd
DVD Drive:
No media
Server 2008
OS: WIndows 8
Username: Administrator
Password: Pa$$w0rd
DVD Drive:
No media
Windows 7
OS: Windows 7
Username: Administrator
Password: Pa$$w0rd
DVD Drive:
No media
Resources
Options

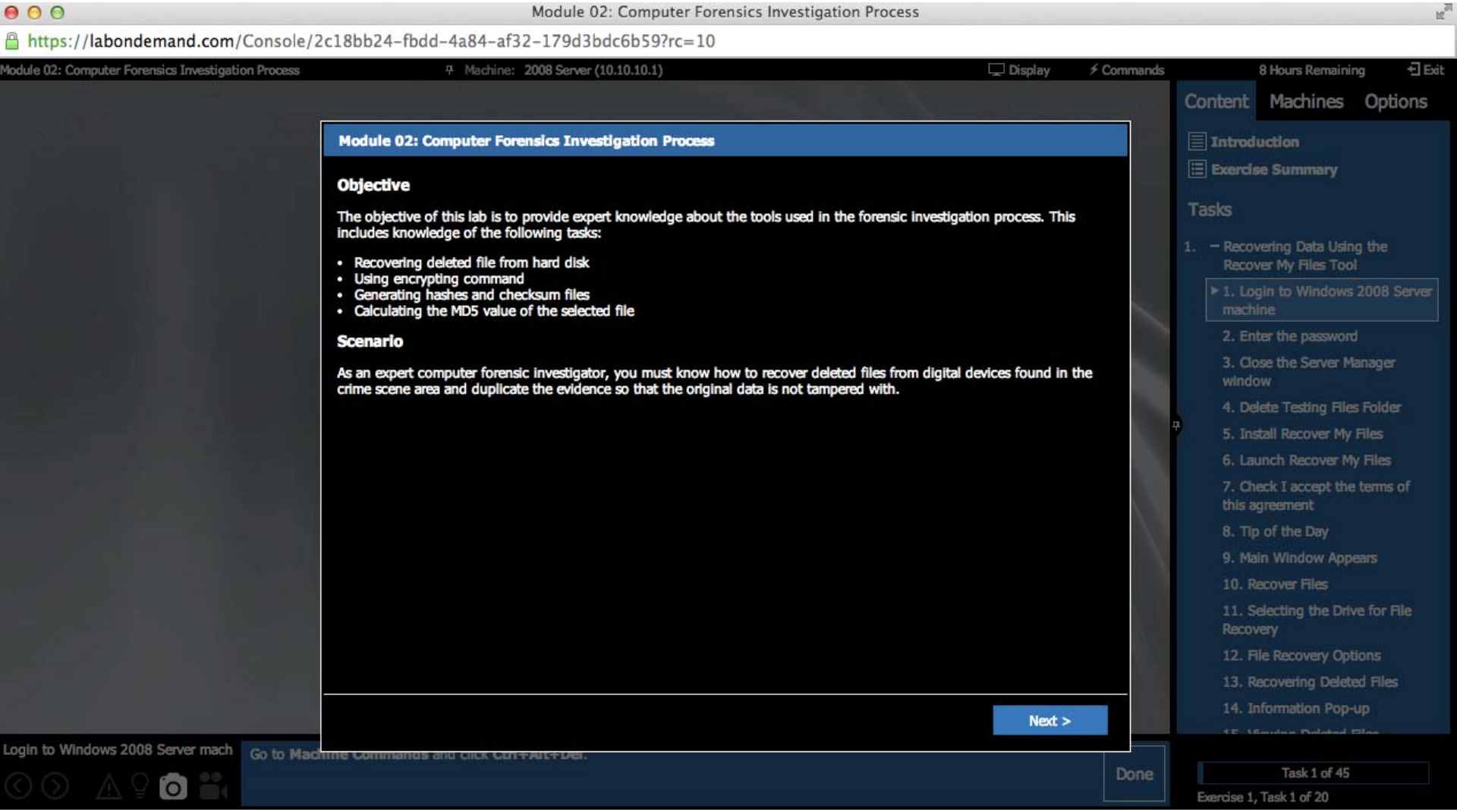

Module 02: Footprinting and Reconnaissance
https://labondemand.com/Console/0efd9efa-32c7-4c7c-beca-98fe81d63a12?rc=10
Module 02: Footprinting and Reconnaissance
Machine: 2012 Server
Display
Commands
8 Hours Remaining
Exit
Content
Machines
Options
Introduction
Exercise Summary
Tasks
1. – Network Route Trace Using Path Analyzer Pro
1. Logon to Windows 2012 Server Machine
2. Enter the Credentials
3. Close the Server Manager Window
4. Install Path Analyzer Pro
5. Launch Path Analyzer Pro
6. Registration Form
7. Main Window of Path Analyzer Pro
8. Standard Options Section
9. Advanced Probe Details
10. Advanced Tracing Details
11. Perform Trace
12. Timed Trace
13. Enter the Type Time of Trace
14. Path Analyzer Pro Perform
15. Report Tab
Module 02: Footprinting and Reconnaissance
Objective
The objective of the lab is to extract information concerning the target organization that includes, but is not limited to:
IP address range associated with the target
Purpose of organization and why does it exists
How big is the organization? What class is its assigned IP Block?
Does the organization freely provide information on the type of operating systems employed and network topology in use?
Type of firewall implemented, either hardware or software or combination of both
Does the organization allow wireless devices to connect to wired networks?
Type of remote access used, either SSH or VPN
Is help sought on IT positions that give information on network services provided by the organization?
Identify organization's users who can disclose their personal information that can be used for social engineering and assume such possible usernames
Scenario
A penetration test begins before penetration testers have even made contact with the victim's systems. Rather than blindly throwing out exploits and praying that one of them returns a shell, a penetration tester meticulously studies the environment for potential weaknesses and their mitigating factors. By the time a penetration tester runs an exploit, he or she is nearly certain that it will be successful. Since failed exploits can in some cases cause a crash or even damage to a victim system, or at the very least make the victim un-exploitable in the future, penetration testers won't get the best results, or deliver the most thorough report to their clients, if they blindly turn an automated exploit machine on the victim network with no preparation.
Next >
Logon to Windows 2012 Server Mach
Done
Task 1 of 51
Exercise 1, Task 1 of 20

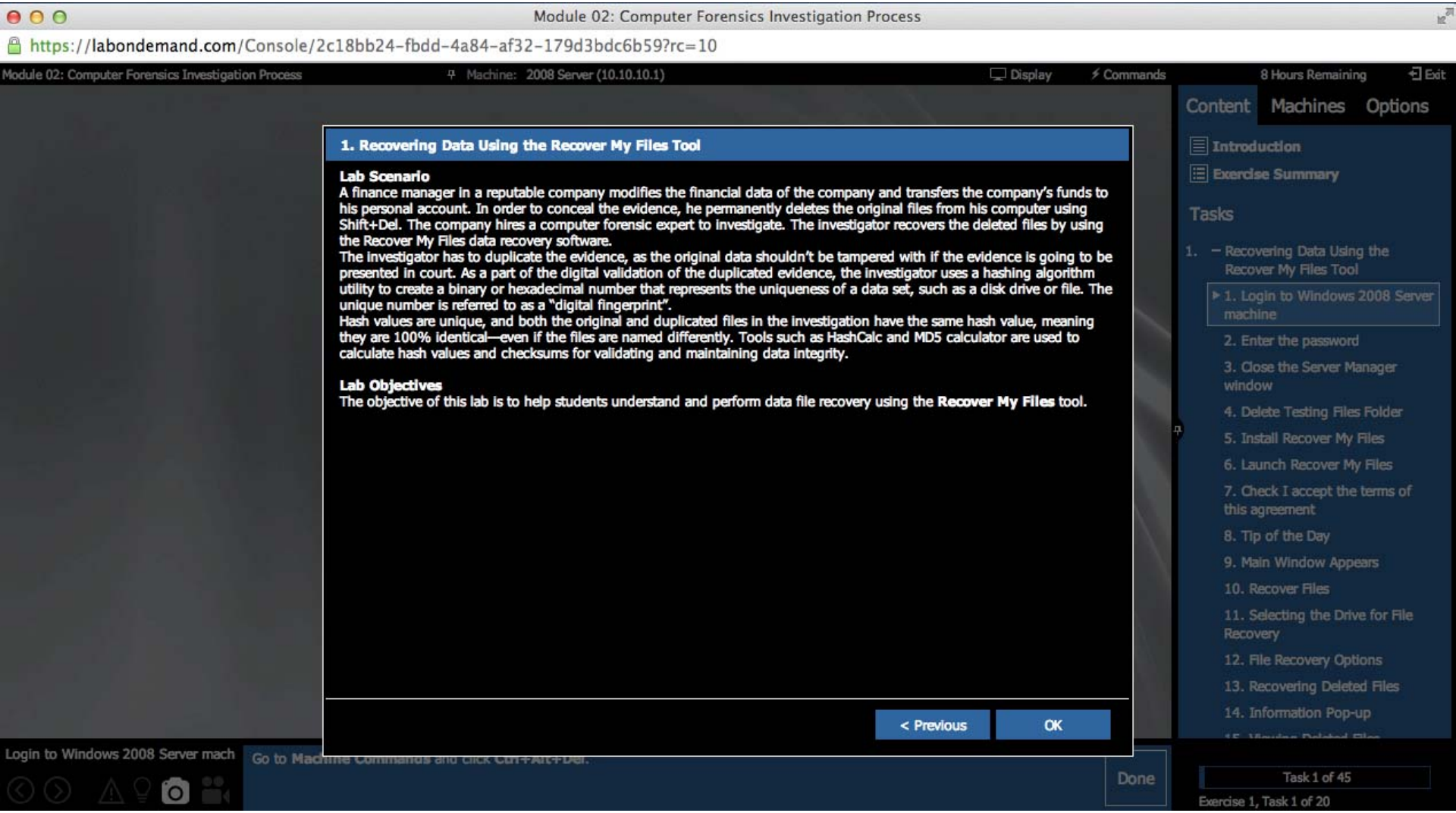

Module 02: Footprinting and Reconnaissance
https://labondemand.com/Console/0efd9efa-32c7-4c7c-beca-98fe81d63a12?rc=10
Module 02: Footprinting and Reconnaissance
Machine: 2012 Server
Display
Commands
8 Hours Remaining
Exit
Press Ctrl+Alt+Delete to sign in.
6:52
Content
Machines
Options
Introduction
Exercise Summary
Tasks
1. – Network Route Trace Using Path Analyzer Pro
1. Logon to Windows 2012 Server Machine
2. Enter the Credentials
3. Close the Server Manager Window
4. Install Path Analyzer Pro
5. Launch Path Analyzer Pro
6. Registration Form
7. Main Window of Path Analyzer Pro
8. Standard Options Section
9. Advanced Probe Details
10. Advanced Tracing Details
11. Perform Trace
12. Timed Trace
13. Enter the Type Time of Trace
14. Path Analyzer Pro Perform
15. Report Tab
Logon to Windows 2012 Server Mach
Select Windows 2012 Server from the Machines pane. Go to Machine Commands and click Ctrl + Alt + Delete.
Done
Task 1 of 51
Exercise 1, Task 1 of 20

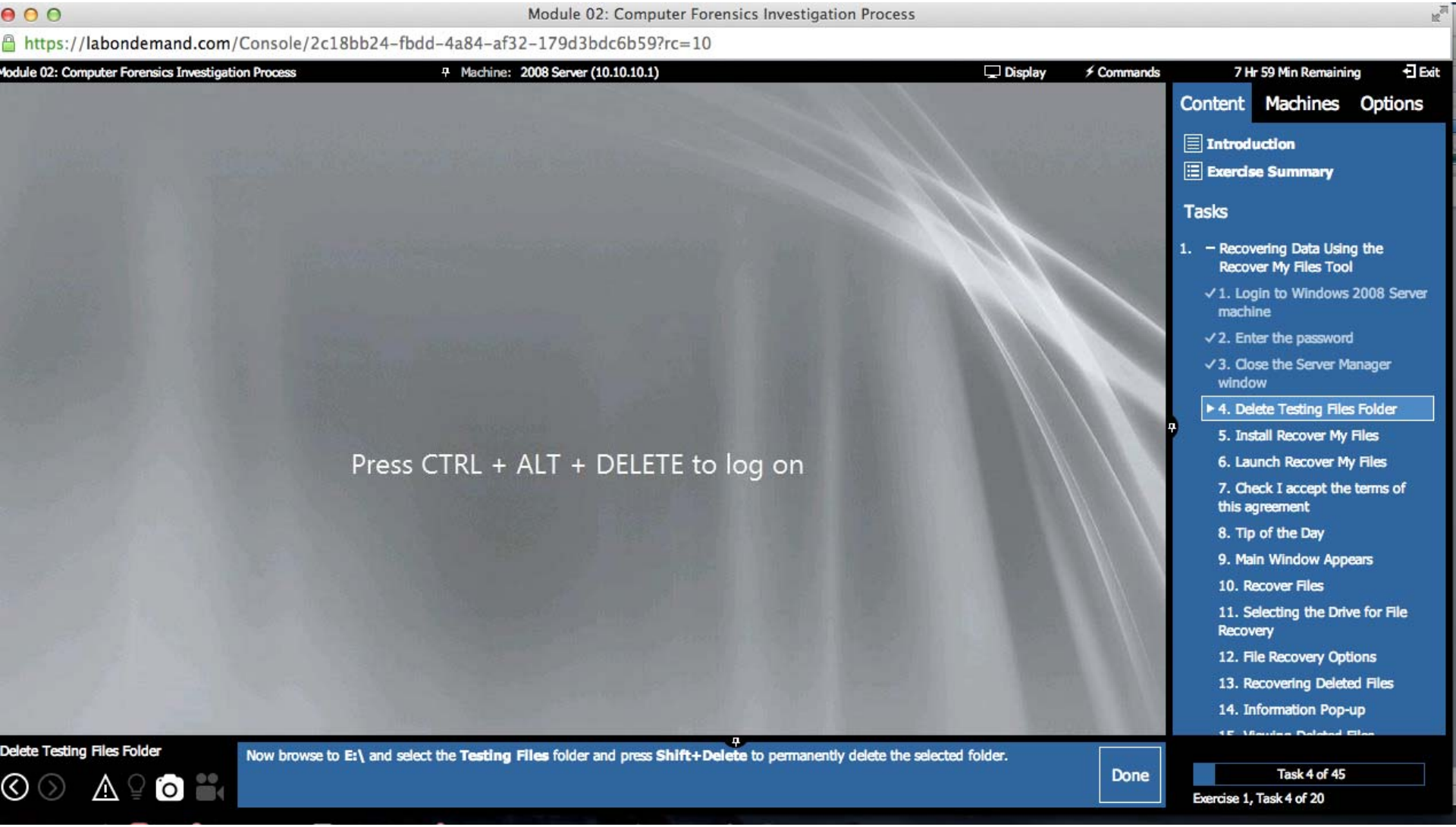

Lab On-Demand
https://labondemand.com/ConsoleLegacy/0efd9efa-32c7-4c7c-beca-98fe81d63a12?rc=10
Overview
Introduction
Exercise Summary
Contents
I. Network Route Trace Using Path Analyzer Pro
1. Logon to Windows 2012
Exercise Summary
I. Network Route Trace Using Path Analyzer Pro
Access can be gained to an organization's network, which allows a penetration tester to thoroughly learn about the organization's network environment for possible vulnerabilities. Taking all the information gathered into account, penetration testers study the systems to find the best routes of attack. The same tasks can be performed by an attacker and the results possibly will prove to be very fatal for an organization. In such cases, as a penetration tester you should be competent to trace network route, determine network path, and troubleshoot network issues. Here you will be guided to trace the network route using the tool Path Analyzer Pro.
Lab Objectives
The objective of this lab is to help students research email addresses, network paths, and IP addresses. This lab helps to determine what ISP, router, or servers are responsible for a network problem.
II. Mirroring Websites Using the HTTrack Web Site Copier Tool
Website servers set cookies to help authenticate the user if the user logs in to a secure area of the website. Login information is stored in a cookie so the user can enter and leave the website without having to re-enter the same authentication information over and over.
Therefore, as a penetration tester, you should have an updated antivirus protection program to attain Internet security. In this lab, you will learn to mirror a website using the HTTrack Web Site Copier Tool and as a penetration tester you can prevent D-DoS attack.
Lab Objectives
The objective of this lab is to help students learn how to mirror websites.
III. Extracting a Company's Data Using Web Data Extractor
Attackers continuously look for the easiest method to collect information. There are many tools available with which attackers can extract a company's database. Once they have access to the database, they can gather employees' email
Continue
6. Registration Form

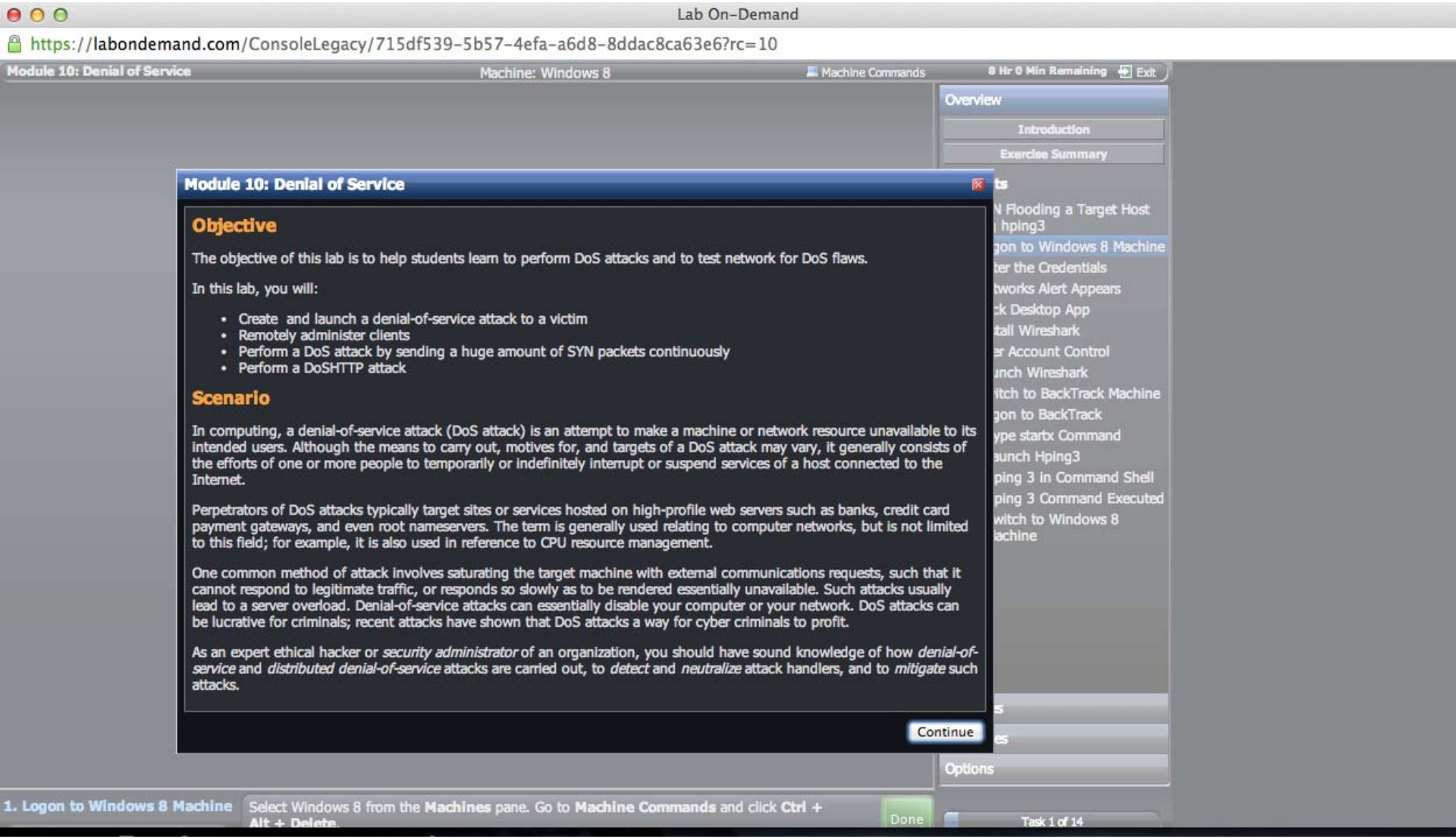

Lab On-Demand
https://labondemand.com/ConsoleLegacy/0efd9efa-32c7-4c7c-beca-98fe81d63a12?rc=10
Press Ctrl+Alt+Delete to sign in.
6:56
Thursday, September 18
Introduction
Exercise Summary
Contents
I. Network Route Trace Using Path Analyzer Pro
1. Logon to Windows 2012 Server Machine
2. Enter the Credentials
3. Close the Server Manager Window
4. Install Path Analyzer Pro
5. Launch Path Analyzer Pro
6. Registration Form
7. Main Window of Path Analyzer Pro
8. Standard Options Section
9. Advanced Probe Details
10. Advanced Tracing Details
11. Perform Trace
12. Timed Trace
13. Enter the Type Time of Trace
14. Path Analyzer Pro Perform
15. Report Tab
16. Synopsis Tab
17. Charts Tab
18. Stats Tab
19. Export the Report
Machines
Resources
Options

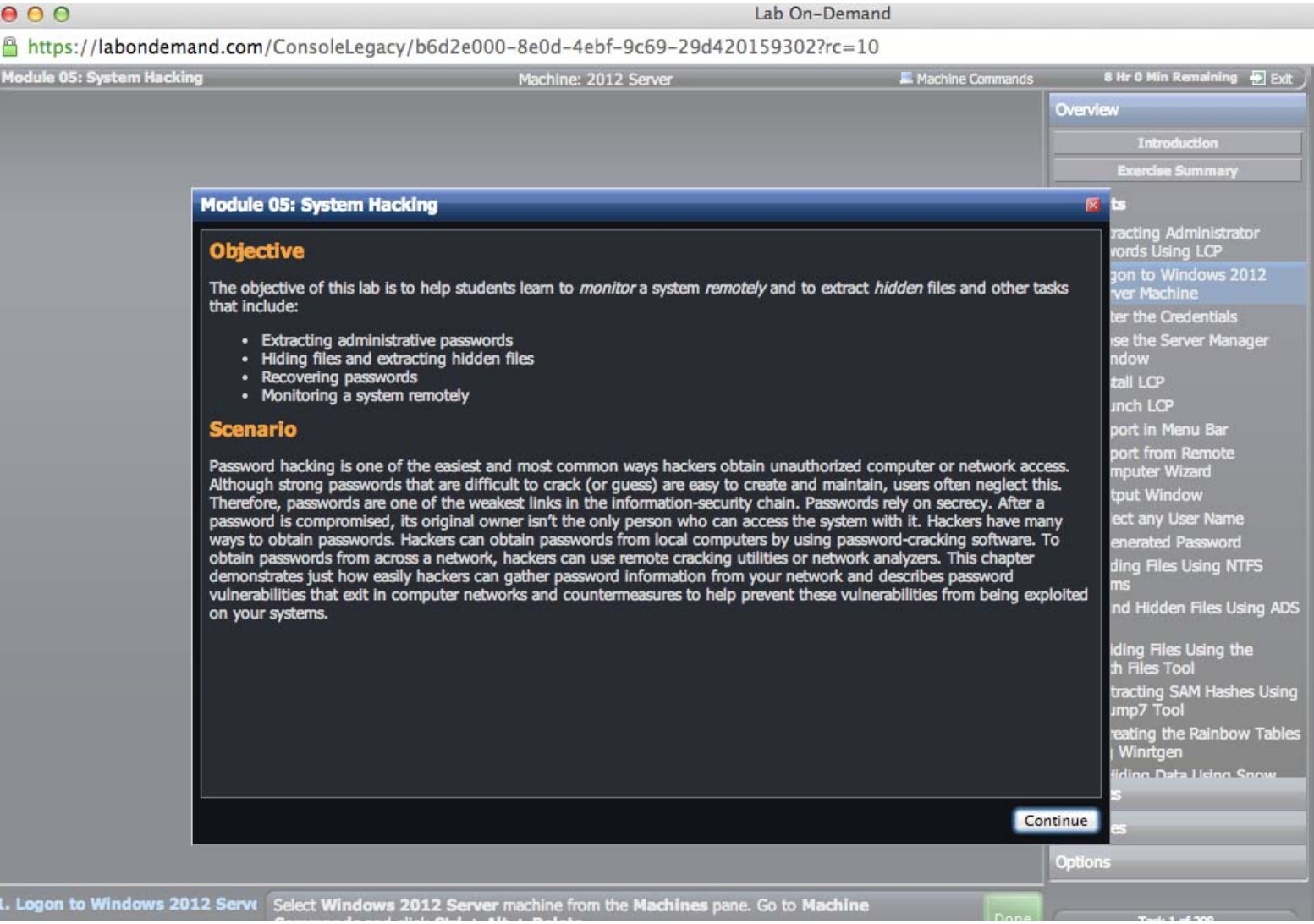

Module 01 Lab1: HyperV Connectivity Check
https://labondemand.com/Console/dea18567-7d08-44a5-8830-1a54ea65625b?rc=10
Module 01 Lab1: HyperV Connectivity Check
Machine: Windows 7
Display
Commands
13 Minutes Remaining
Exit
Content
Machines
Options
Introduction
Exercise Summary
Tasks
+ Discover the LOD Interface
Exercise Complete
Discover the LOD Interface
Congratulations!
You have now identified the various components of the Lab On Demand interface and learned how to interact with the controls.
At the end of each lab Exercise, you will see a Completion Message which will review and summarize what was accomplished in the exercise.
To advance to the next exercise (or complete the lab) you must click on the Continue button in the Completion Message window.
It is very important at the end of the lab that you click on the Continue button to advance the lab to Close - which will then automatically credit you with taking the lab.
Important: If you close the browser window or exit the lab without finalizing the lab by clicking on the last exercise Continue button, you will NOT GET CREDIT for the lab. Therefore, ensure that you always click the DONE and CONTINUE buttons until you see the completion message.
Continue
Clicking the last Done button in any lab wi
as complete, close and tear the lab down.
If you want to check anything in your lab
down, now is the time to do it.
But remember to click the Done button on
ensure you get credit for your lab.
Click on the Done button to complete the test lab and follow the on screen instructions to finish & close the test lab. Clicking the last Done button in any lab will mark that lab as complete, close and tear the lab down.
Done
Task 14 of 14
Exercise 1, Task 14 of 14

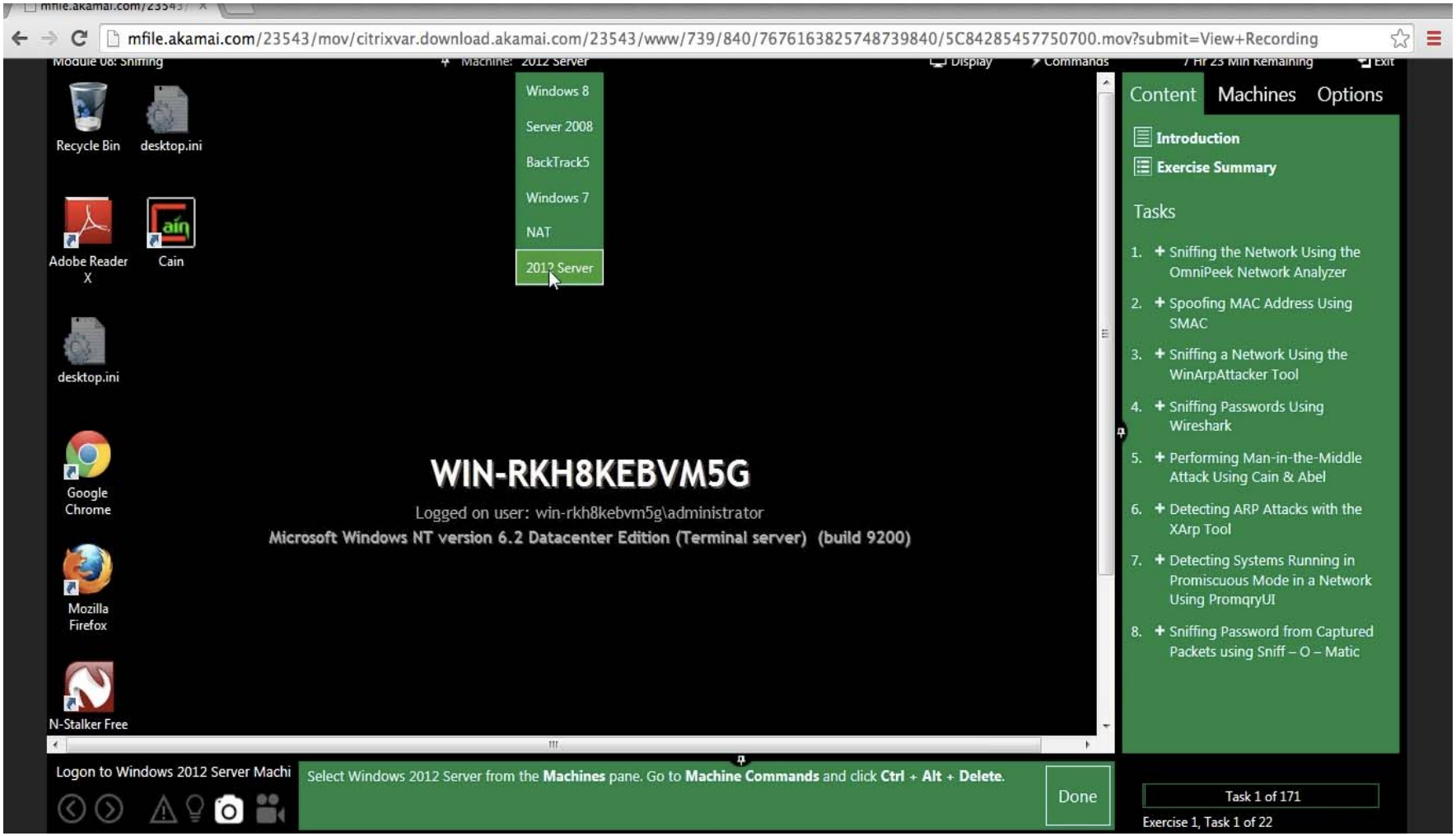

Module 02: Computer Forensics Investigation Process
https://labondemand.com/Console/2c18bb24-fbdd-4a84-af32-179d3bdc6b59?rc=10
Module 02: Computer Forensics Investigation Process
Machine: 2008 Server (10.10.10.1)
Display
Commands
8 Hours Remaining
Exit
Content
Machines
Options
Introduction
Exercise Summary
Tasks
1. – Recovering Data Using the Recover My Files Tool
1. Login to Windows 2008 Server machine
2. Enter the password
3. Close the Server Manager window
4. Delete Testing Files Folder
5. Install Recover My Files
6. Launch Recover My Files
7. Check I accept the terms of this agreement
8. Tip of the Day
9. Main Window Appears
10. Recover Files
11. Selecting the Drive for File Recovery
12. File Recovery Options
13. Recovering Deleted Files
14. Information Pop-up
Module 02: Computer Forensics Investigation Process
Objective
The objective of this lab is to provide expert knowledge about the tools used in the forensic investigation process. This includes knowledge of the following tasks:
• Recovering deleted file from hard disk
• Using encrypting command
• Generating hashes and checksum files
• Calculating the MD5 value of the selected file
Scenario
As an expert computer forensic investigator, you must know how to recover deleted files from digital devices found in the crime scene area and duplicate the evidence so that the original data is not tampered with.
Next >
Login to Windows 2008 Server mach
Done
Task 1 of 45
Exercise 1, Task 1 of 20


Module 02: Computer Forensics Investigation Process
https://labondemand.com/Console/2c18bb24-fbdd-4a84-af32-179d3bdc6b59?rc=10
Module 02: Computer Forensics Investigation Process
Machine: 2008 Server (10.10.10.1)
Display
Commands
8 Hours Remaining
Exit
Content
Machines
Options
Introduction
Exercise Summary
Tasks
1. Recovering Data Using the Recover My Files Tool
1. Login to Windows 2008 Server machine
2. Enter the password
3. Close the Server Manager window
4. Delete Testing Files Folder
5. Install Recover My Files
6. Launch Recover My Files
7. Check I accept the terms of this agreement
8. Tip of the Day
9. Main Window Appears
10. Recover Files
11. Selecting the Drive for File Recovery
12. File Recovery Options
13. Recovering Deleted Files
14. Information Pop-up
1. Recovering Data Using the Recover My Files Tool
Lab Scenario
A finance manager in a reputable company modifies the financial data of the company and transfers the company's funds to his personal account. In order to conceal the evidence, he permanently deletes the original files from his computer using Shift+Del. The company hires a computer forensic expert to investigate. The investigator recovers the deleted files by using the Recover My Files data recovery software.
The investigator has to duplicate the evidence, as the original data shouldn't be tampered with if the evidence is going to be presented in court. As a part of the digital validation of the duplicated evidence, the investigator uses a hashing algorithm utility to create a binary or hexadecimal number that represents the uniqueness of a data set, such as a disk drive or file. The unique number is referred to as a "digital fingerprint".
Hash values are unique, and both the original and duplicated files in the investigation have the same hash value, meaning they are 100% identical—even if the files are named differently. Tools such as HashCalc and MD5 calculator are used to calculate hash values and checksums for validating and maintaining data integrity.
Lab Objectives
The objective of this lab is to help students understand and perform data file recovery using the Recover My Files tool.
< Previous
OK
Login to Windows 2008 Server mach
Done
Task 1 of 45
Exercise 1, Task 1 of 20


Module 02: Computer Forensics Investigation Process
https://labondemand.com/Console/2c18bb24-fbdd-4a84-af32-179d3bdc6b59?rc=10
Module 02: Computer Forensics Investigation Process
Machine: 2008 Server (10.10.10.1)
Display
Commands
7 Hr 59 Min Remaining
Exit
Content
Machines
Options
Introduction
Exercise Summary
Tasks
1. – Recovering Data Using the Recover My Files Tool
✓1. Login to Windows 2008 Server machine
✓2. Enter the password
✓3. Close the Server Manager window
▸4. Delete Testing Files Folder
5. Install Recover My Files
6. Launch Recover My Files
7. Check I accept the terms of this agreement
8. Tip of the Day
9. Main Window Appears
10. Recover Files
11. Selecting the Drive for File Recovery
12. File Recovery Options
13. Recovering Deleted Files
14. Information Pop-up
Press CTRL + ALT + DELETE to log on
Delete Testing Files Folder
Now browse to E:\ and select the Testing Files folder and press Shift+Delete to permanently delete the selected folder.
Done
Task 4 of 45
Exercise 1, Task 4 of 20

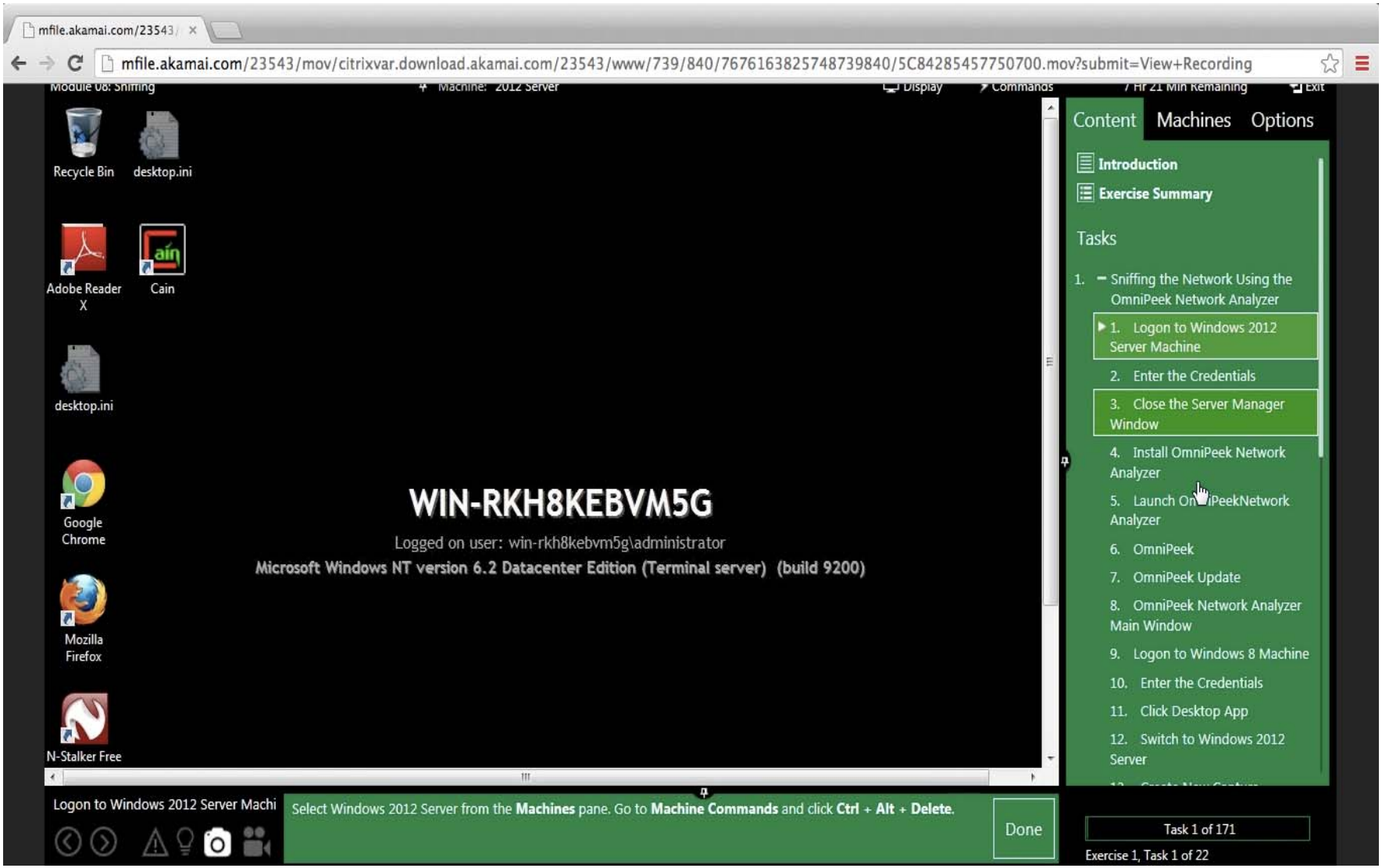

Lab On-Demand
https://labondemand.com/ConsoleLegacy/715df539-5b57-4efa-a6d8-8ddac8ca63e6?rc=10
Module 10: Denial of Service
Machine: Windows 8
Machine Commands
8 Hr 0 Min Remaining
Exit
Overview
Introduction
Exercise Summary
Module 10: Denial of Service
Objective
The objective of this lab is to help students learn to perform DoS attacks and to test network for DoS flaws.
In this lab, you will:
Create and launch a denial-of-service attack to a victim
Remotely administer clients
Perform a DoS attack by sending a huge amount of SYN packets continuously
Perform a DoSHTTP attack
Scenario
In computing, a denial-of-service attack (DoS attack) is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the efforts of one or more people to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.
Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.
One common method of attack involves saturating the target machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. Denial-of-service attacks can essentially disable your computer or your network. DoS attacks can be lucrative for criminals; recent attacks have shown that DoS attacks a way for cyber criminals to profit.
As an expert ethical hacker or security administrator of an organization, you should have sound knowledge of how denial-of-service and distributed denial-of-service attacks are carried out, to detect and neutralize attack handlers, and to mitigate such attacks.
Continue
Options
1. Logon to Windows 8 Machine
Select Windows 8 from the Machines pane. Go to Machine Commands and click Ctrl + Alt + Delete.
Done
Task 1 of 14


Lab On-Demand
https://labondemand.com/ConsoleLegacy/b6d2e000-8e0d-4ebf-9c69-29d420159302?rc=10
Module 05: System Hacking
Machine: 2012 Server
Machine Commands
8 Hr 0 Min Remaining
Exit
Overview
Introduction
Exercise Summary
Module 05: System Hacking
Objective
The objective of this lab is to help students learn to monitor a system remotely and to extract hidden files and other tasks that include:
Extracting administrative passwords
Hiding files and extracting hidden files
Recovering passwords
Monitoring a system remotely
Scenario
Password hacking is one of the easiest and most common ways hackers obtain unauthorized computer or network access. Although strong passwords that are difficult to crack (or guess) are easy to create and maintain, users often neglect this. Therefore, passwords are one of the weakest links in the information-security chain. Passwords rely on secrecy. After a password is compromised, its original owner isn't the only person who can access the system with it. Hackers have many ways to obtain passwords. Hackers can obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, hackers can use remote cracking utilities or network analyzers. This chapter demonstrates just how easily hackers can gather password information from your network and describes password vulnerabilities that exit in computer networks and countermeasures to help prevent these vulnerabilities from being exploited on your systems.
Continue
Options
Select Windows 2012 Server machine from the Machines pane. Go to Machine
Done



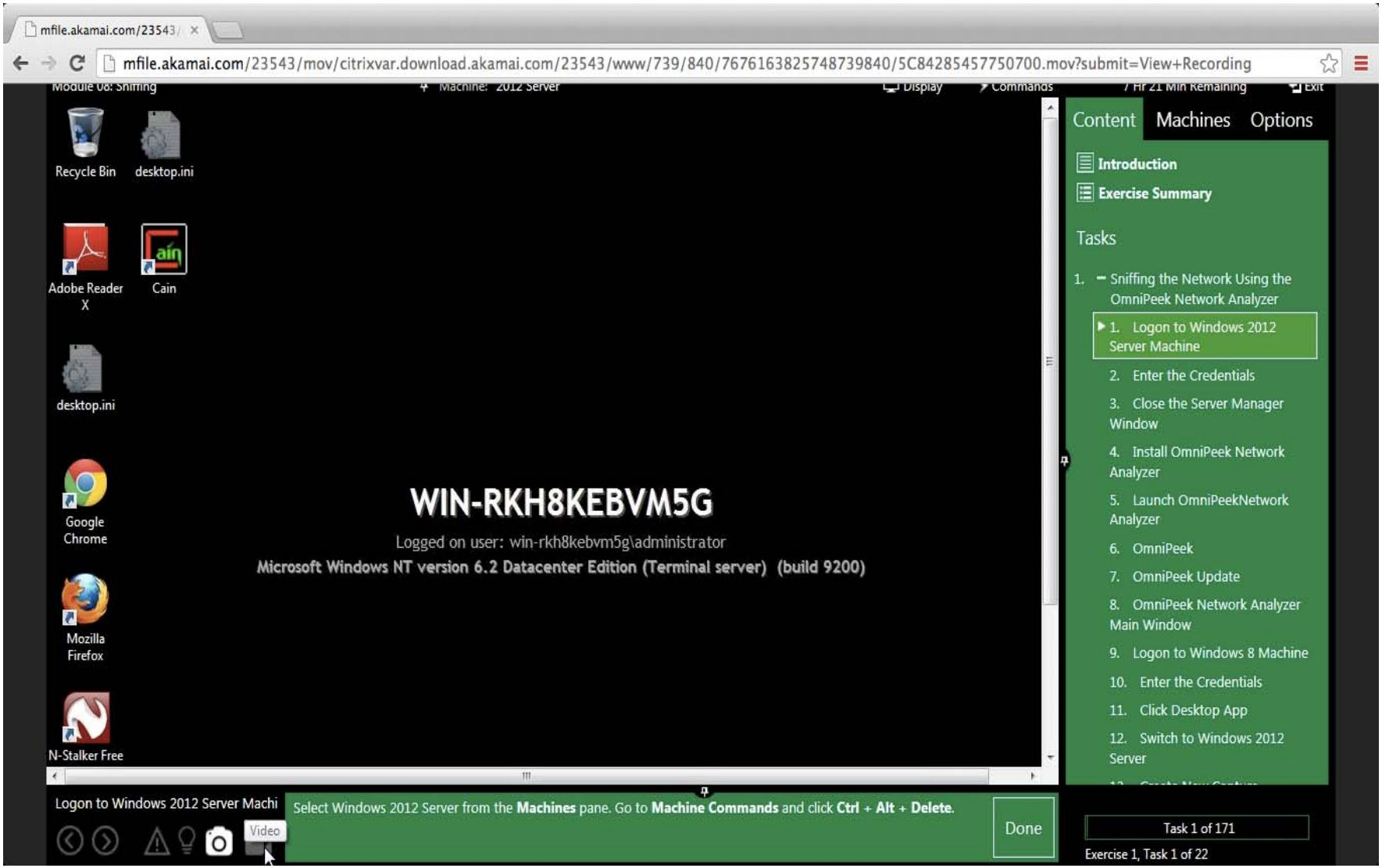
Active (Live) Machines – Interchangeable at any time.

Display – Full Screen, Dual Monitors, Machine Commands

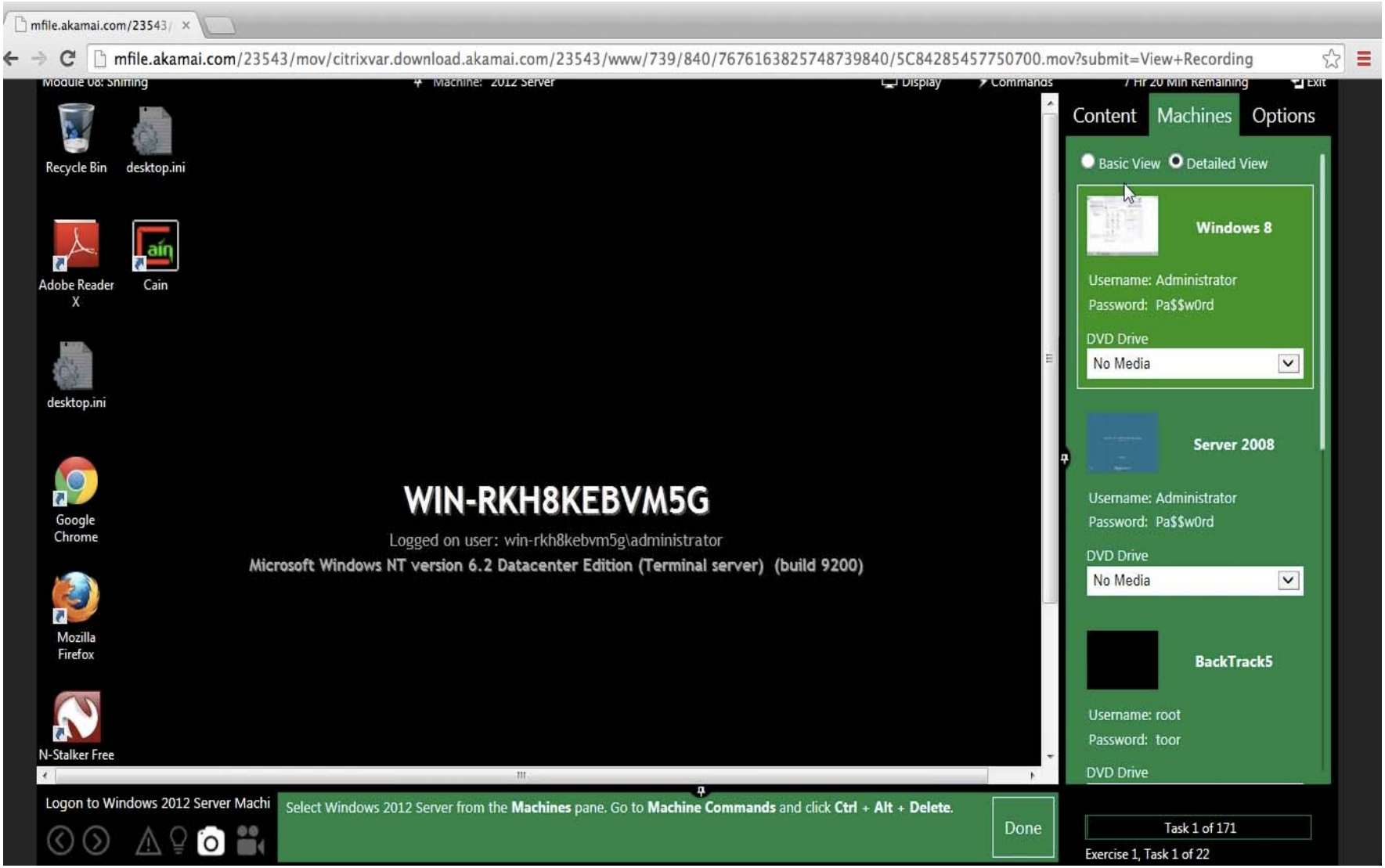


Real-Life Scenarios - Tasks – Group of Exercises to Complete

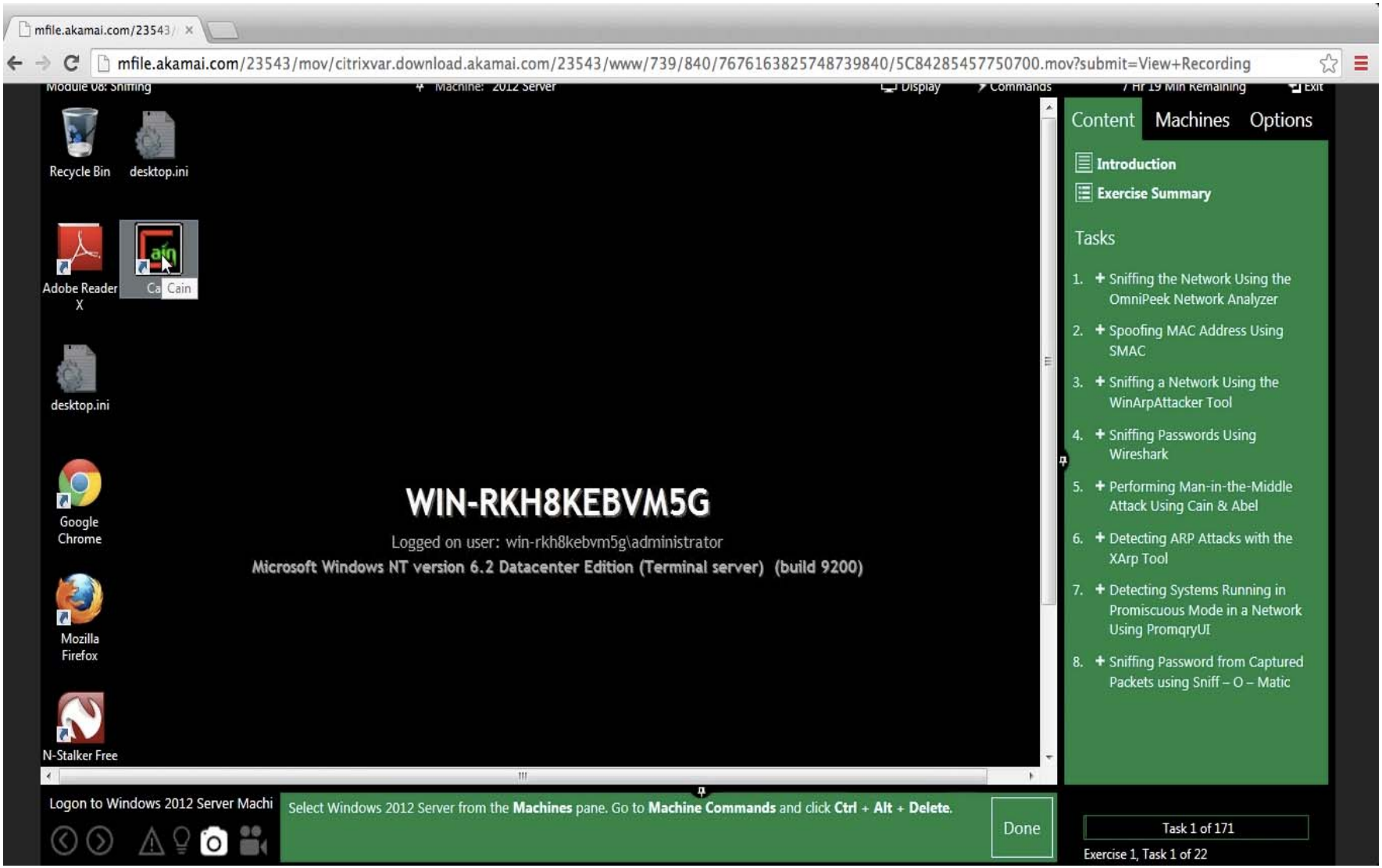
Bottom Task Bar – Helpful Ideas, Screen Shots, Video, Instruction



Log-On to Windows Server Machine

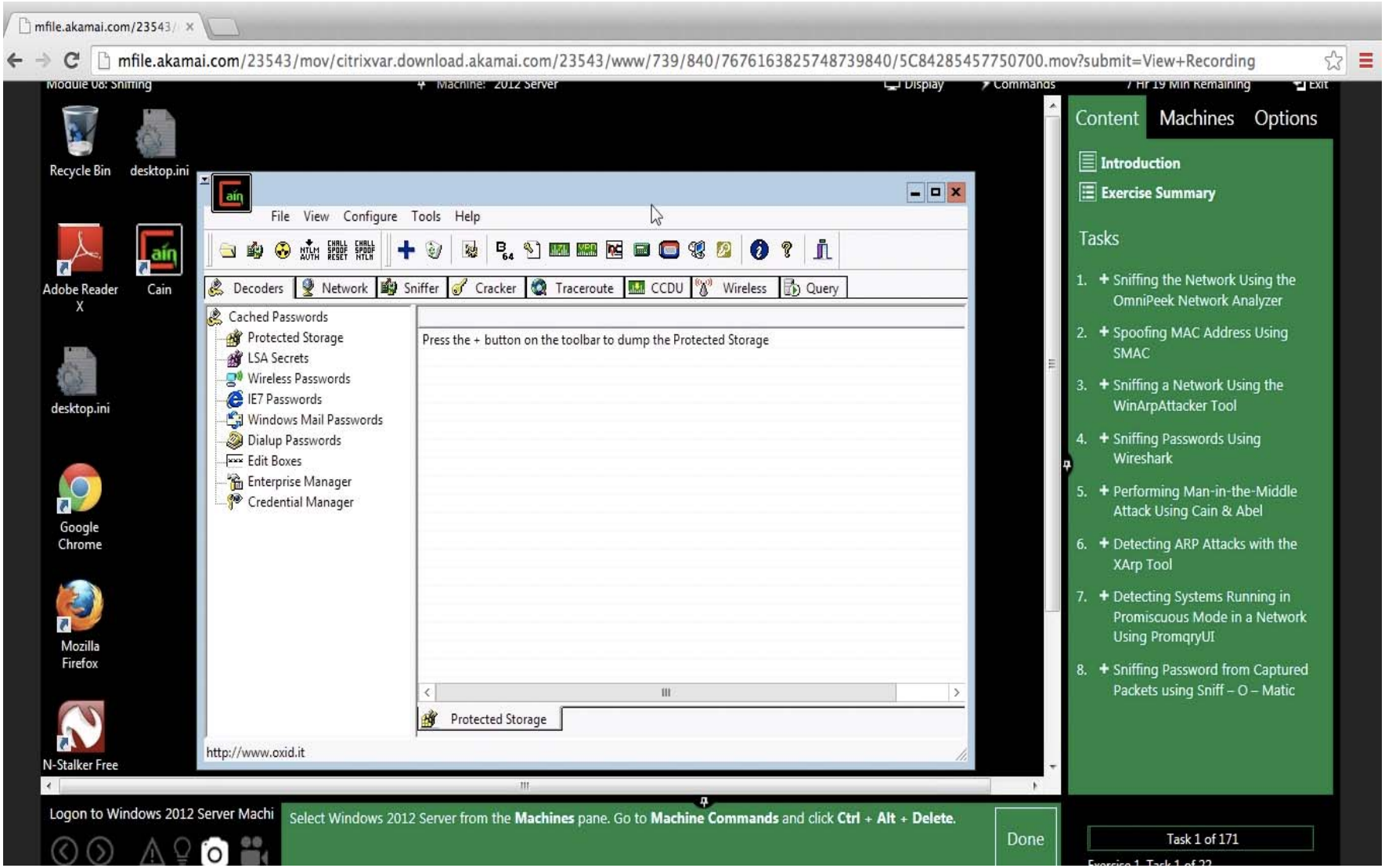


Active Machines – Interchangeable At Any Time

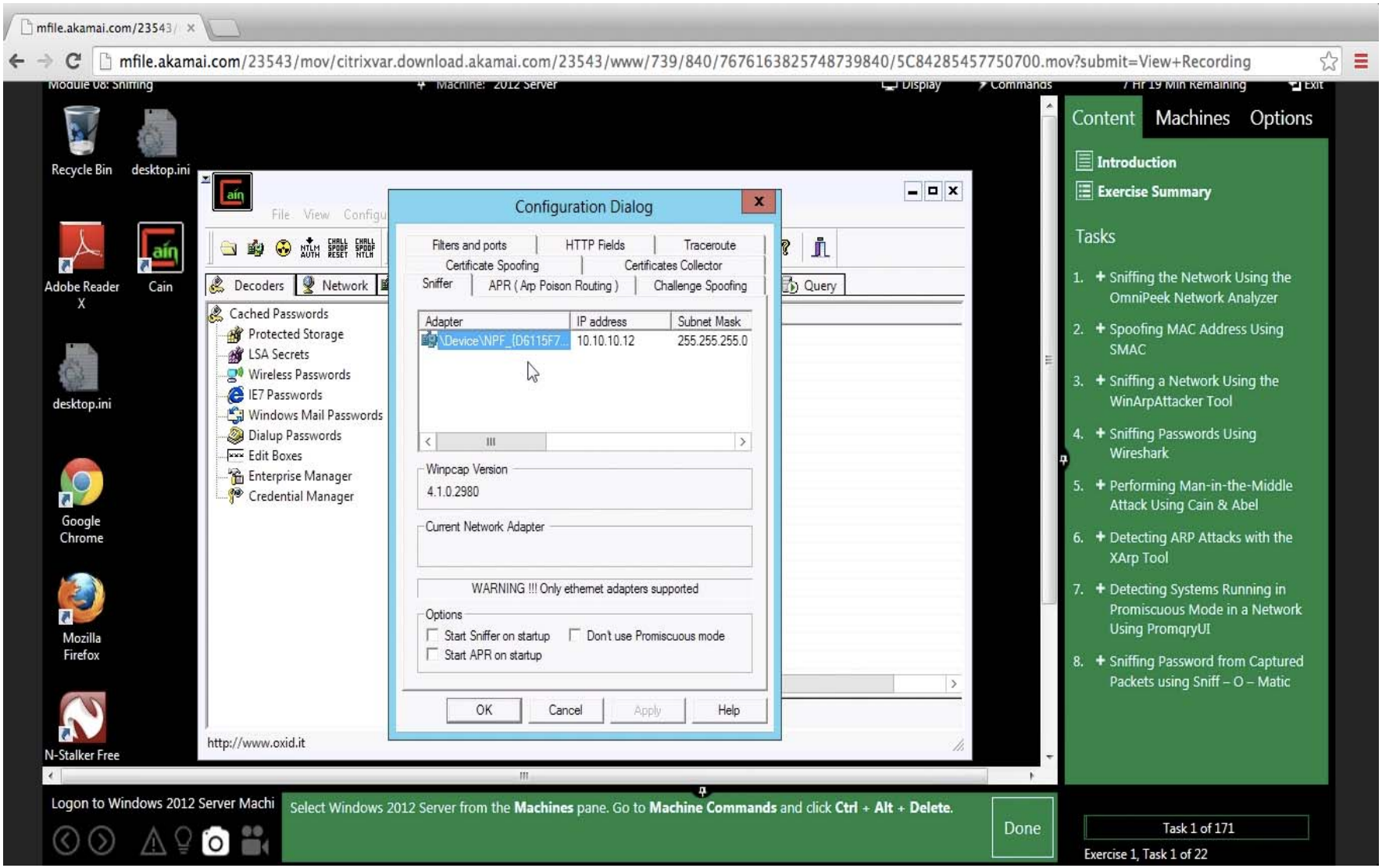


Access Open Source Attacker Tool – **Cain & Able**, Playing the Attacker – Against Victims

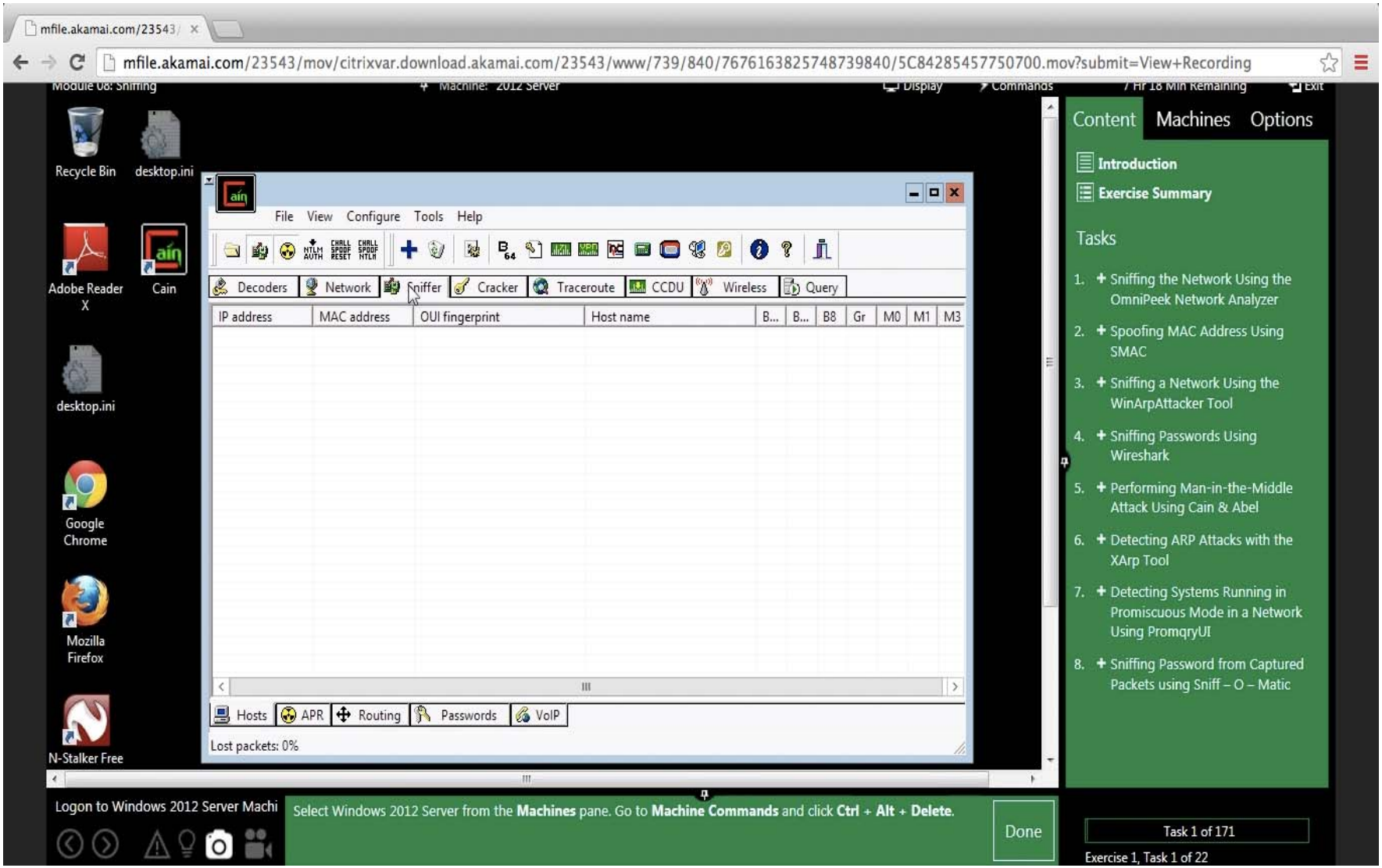
Sniff the Network within the Range, Access IP Addresses, Monitor, Access Password



What we'll see – IP Addresses related to Machines in the Range



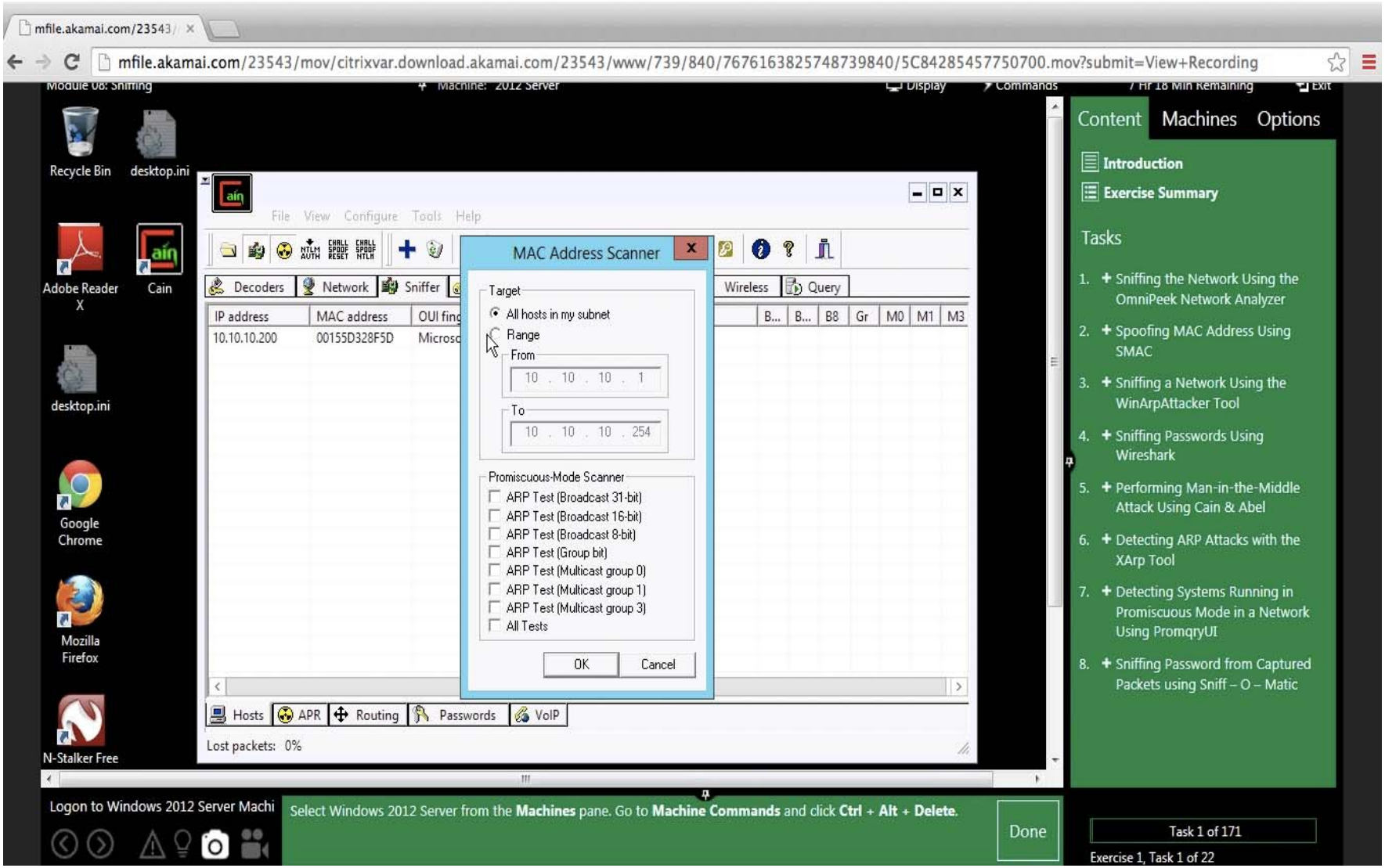
Cain and Able – Sniffing Configuration



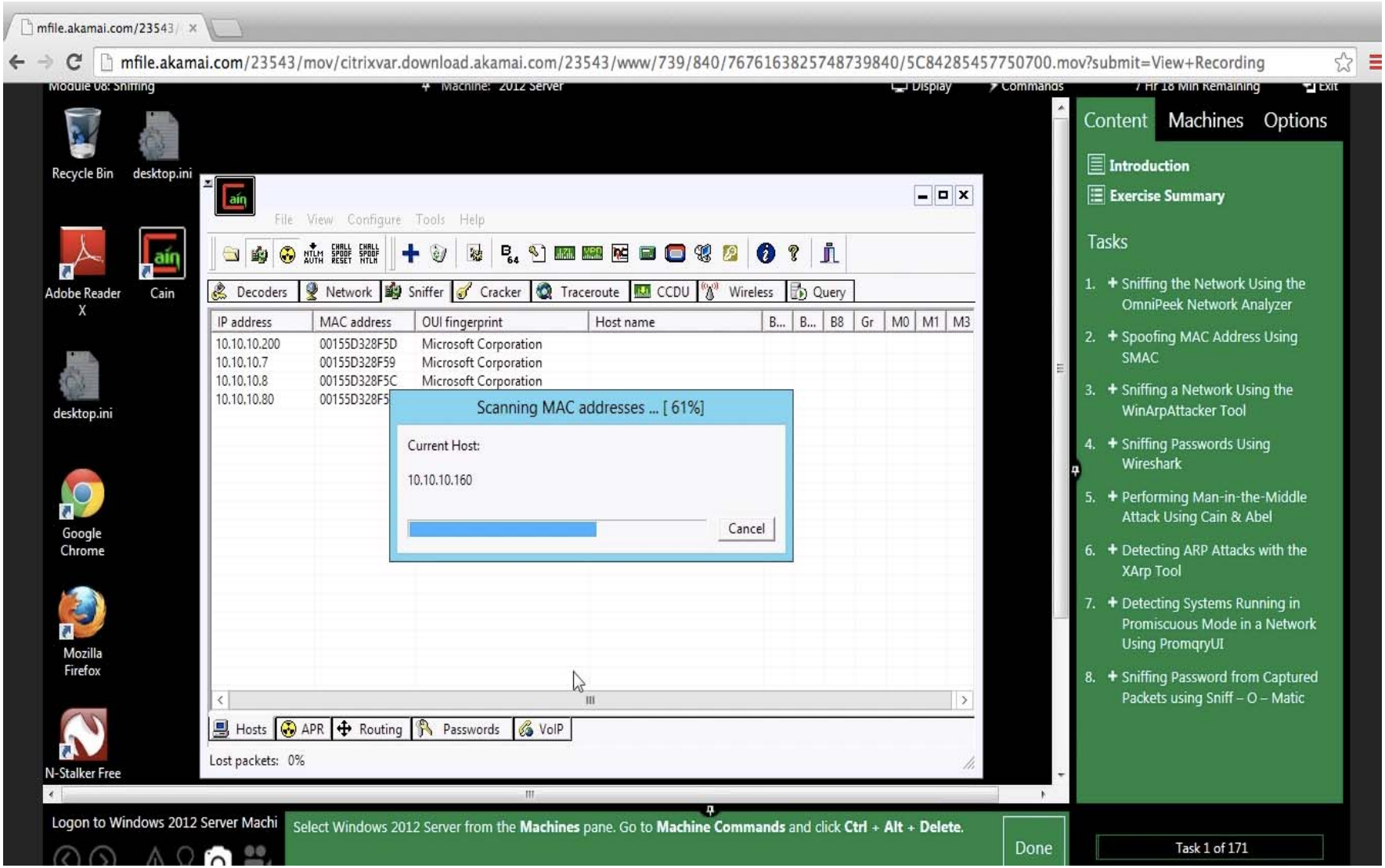
Scanning for IP Addresses

Global Institute *for* Cybersecurity + Research (GICSR)

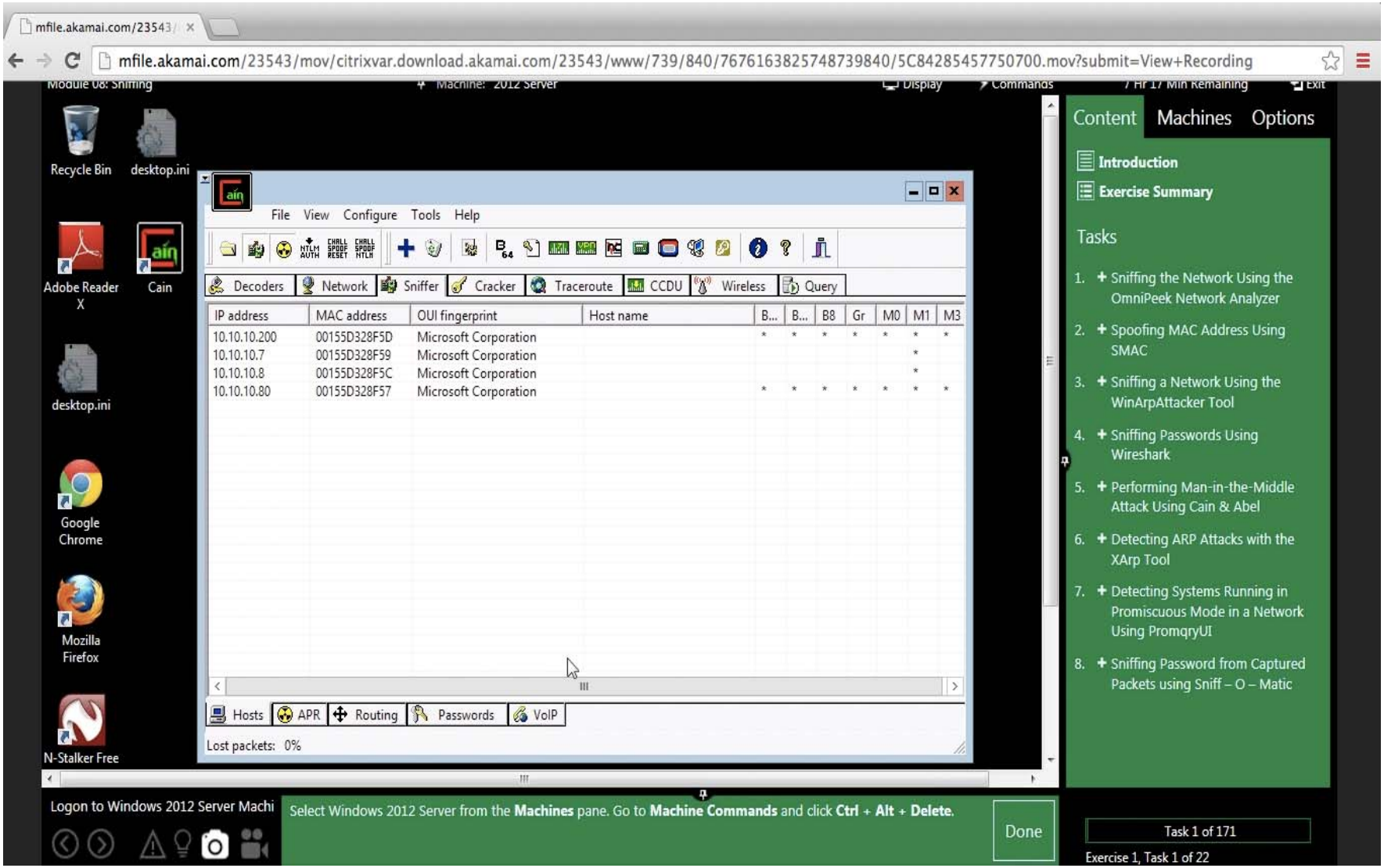
NICE Conference 2014



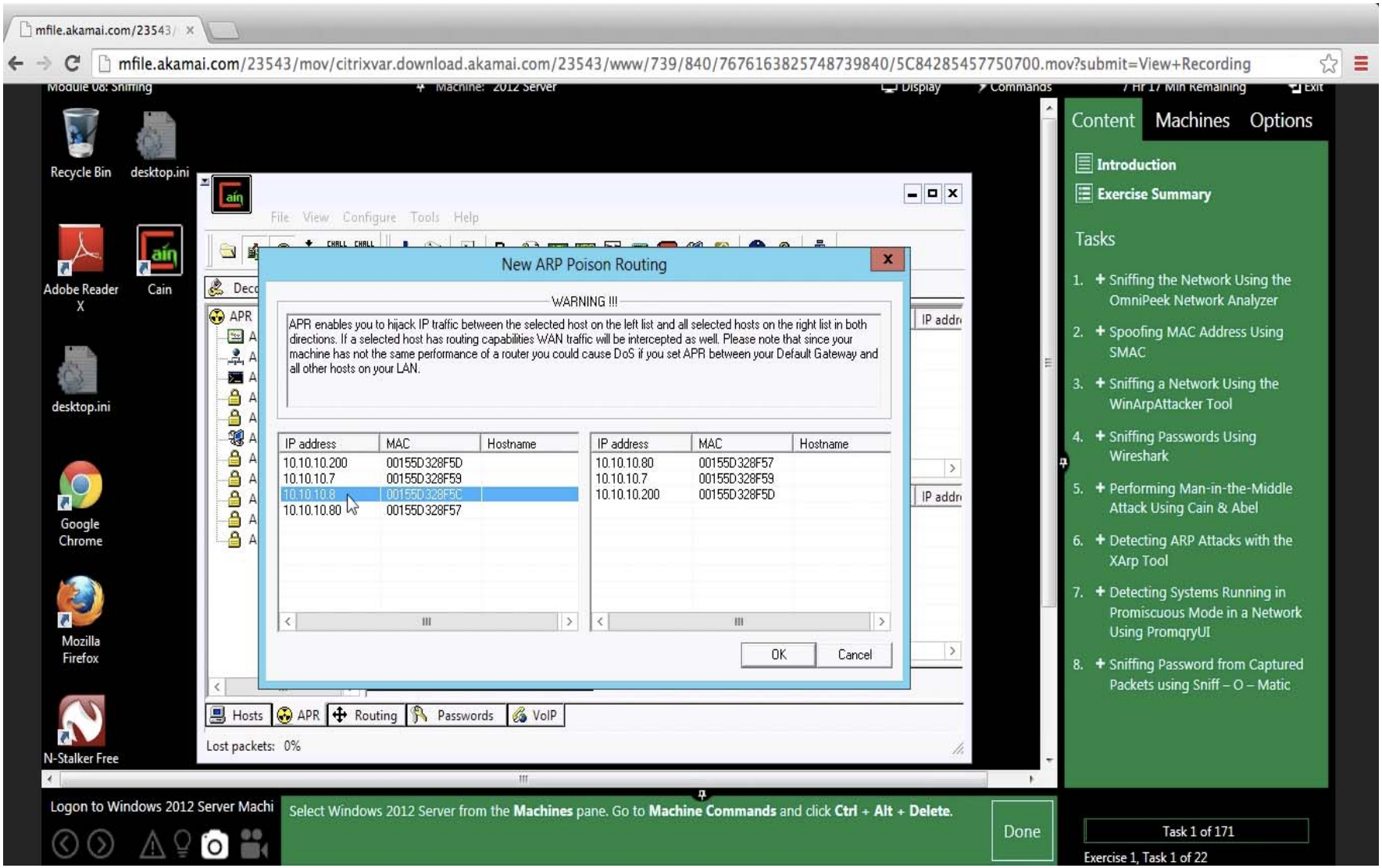
IP Address Scanning


mfile.akamai.com/23543/mov/citrixvar.download.akamai.com/23543/www/739/840/7676163825748739840/5C84285457750700.mov?submit=View+Recording
Module 08: Sniffing
Machine: 2012 Server
Display
Commands
7 Hr 18 Min Remaining
Exit
Recycle Bin
desktop.ini
Adobe Reader X
Cain
desktop.ini
Google Chrome
Mozilla Firefox
N-Stalker Free
File View Configure Tools Help
Decoders
Network
Sniffer
Cracker
Traceroute
CCDU
Wireless
Query
IP address
MAC address
OUI fingerprint
Host name
10.10.10.200 00155D328F5D Microsoft Corporation
10.10.10.7 00155D328F59 Microsoft Corporation
10.10.10.8 00155D328F5C Microsoft Corporation
10.10.10.80 00155D328F5
Scanning MAC addresses ... [61%]
Current Host:
10.10.10.160
Cancel
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%
Content
Machines
Options
Introduction
Exercise Summary
Tasks
1. + Sniffing the Network Using the OmniPeek Network Analyzer
2. + Spoofing MAC Address Using SMAC
3. + Sniffing a Network Using the WinArpAttacker Tool
4. + Sniffing Passwords Using Wireshark
5. + Performing Man-in-the-Middle Attack Using Cain & Abel
6. + Detecting ARP Attacks with the XArp Tool
7. + Detecting Systems Running in Promiscuous Mode in a Network Using PromqryUI
8. + Sniffing Password from Captured Packets using Sniff – O – Matic
Logon to Windows 2012 Server Machi
Select Windows 2012 Server from the Machines pane. Go to Machine Commands and click Ctrl + Alt + Delete.
Done
Task 1 of 171

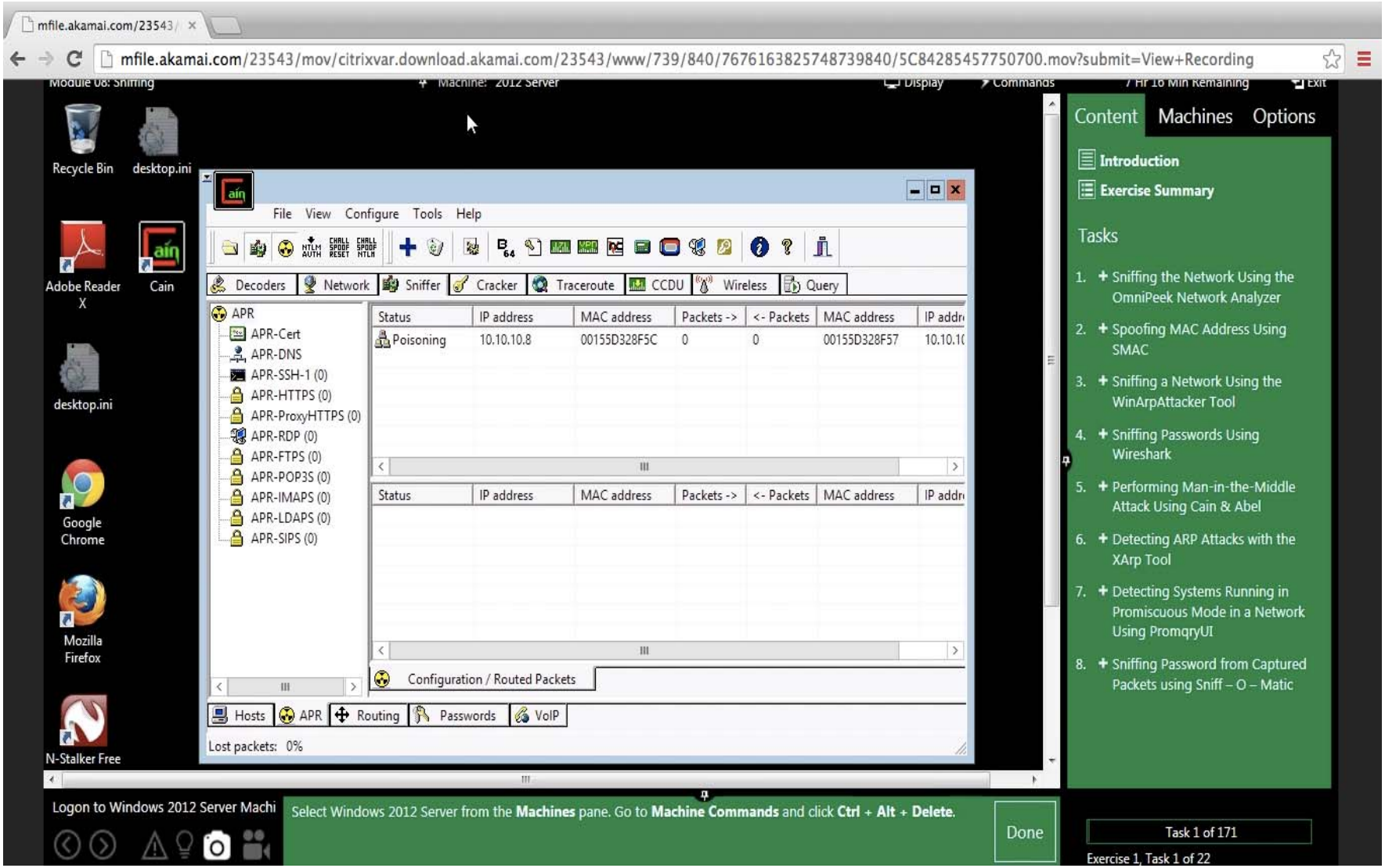
Scanning



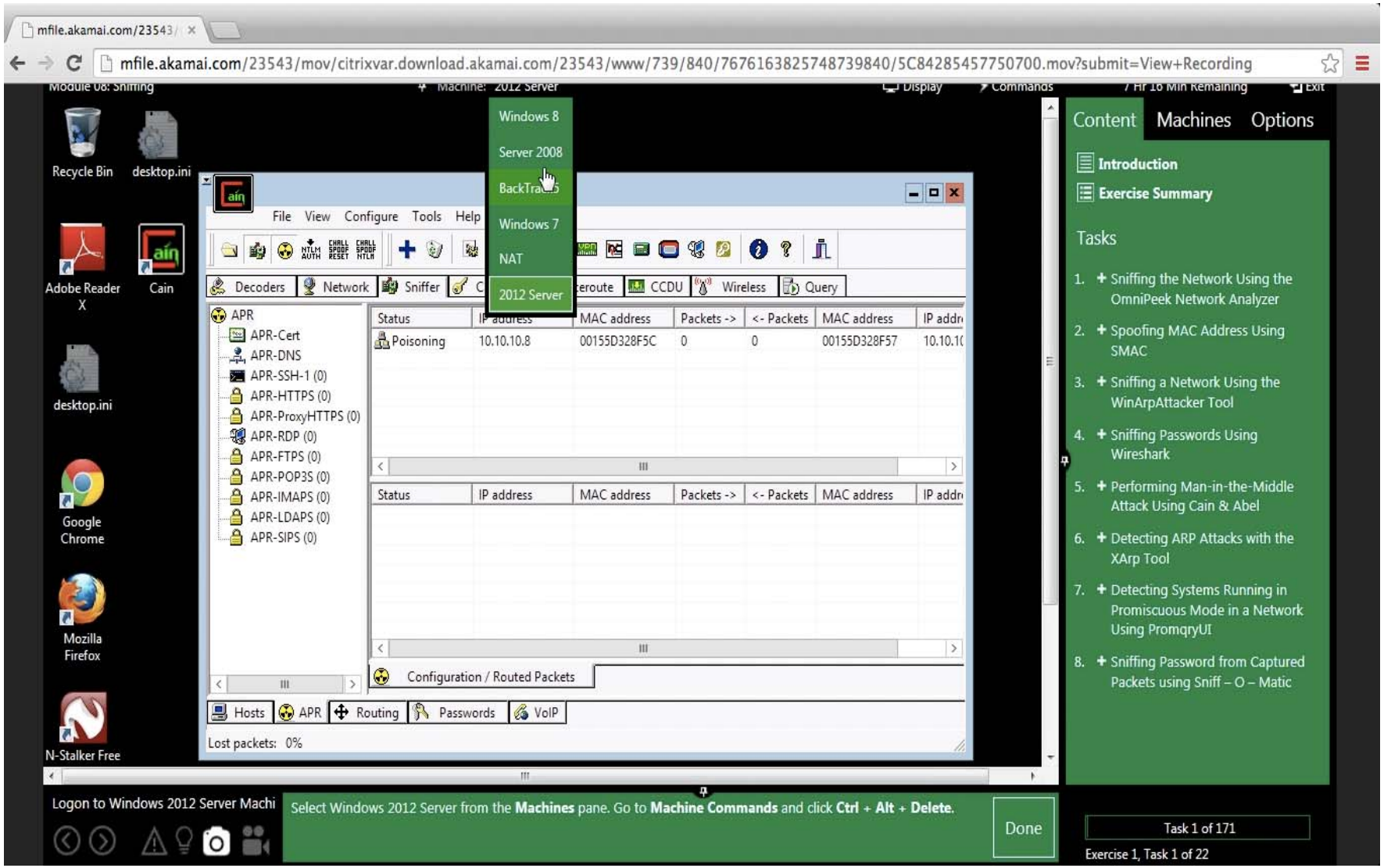
Displays IP Addresses



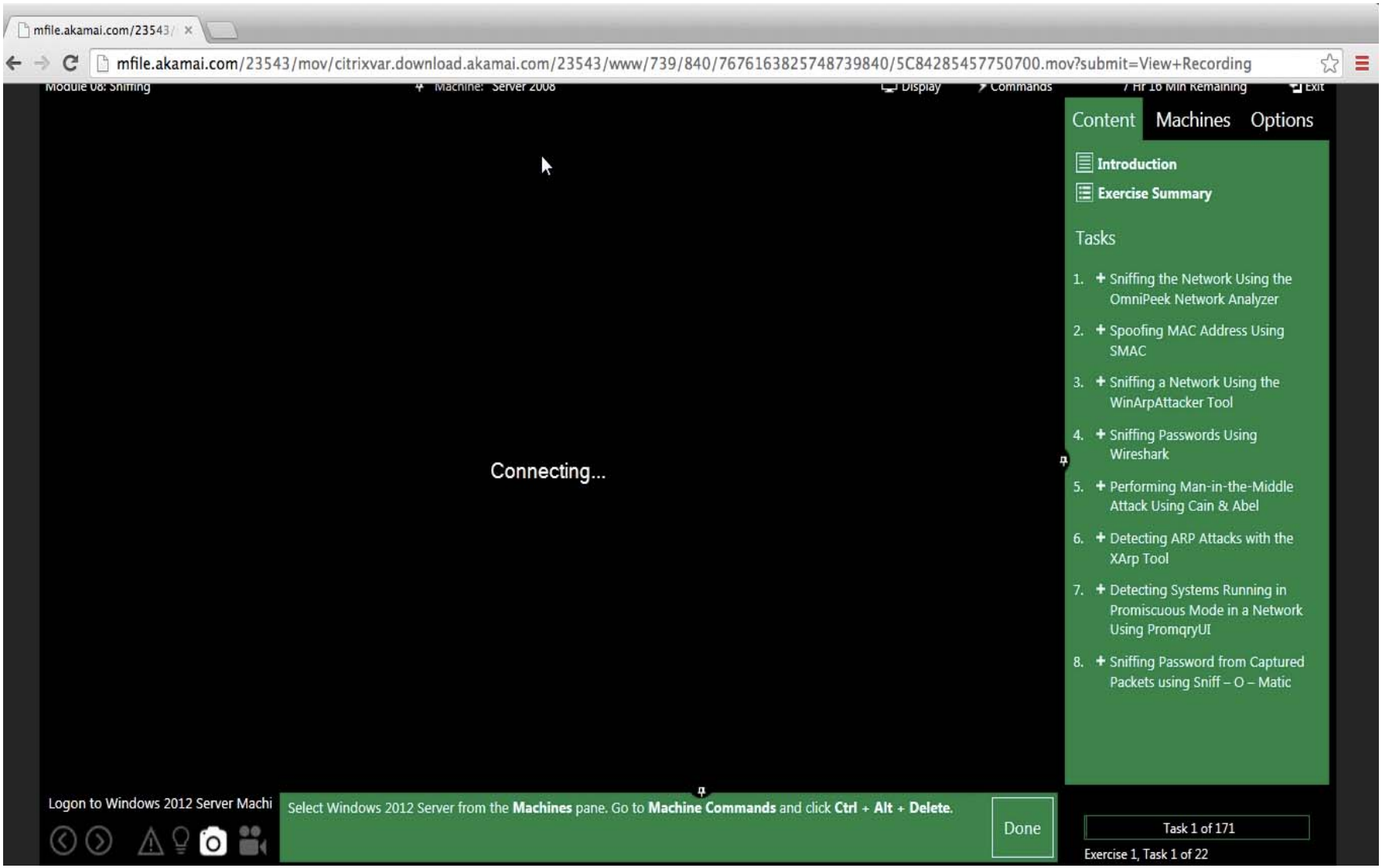
Selecting an IP Address to “Poison”



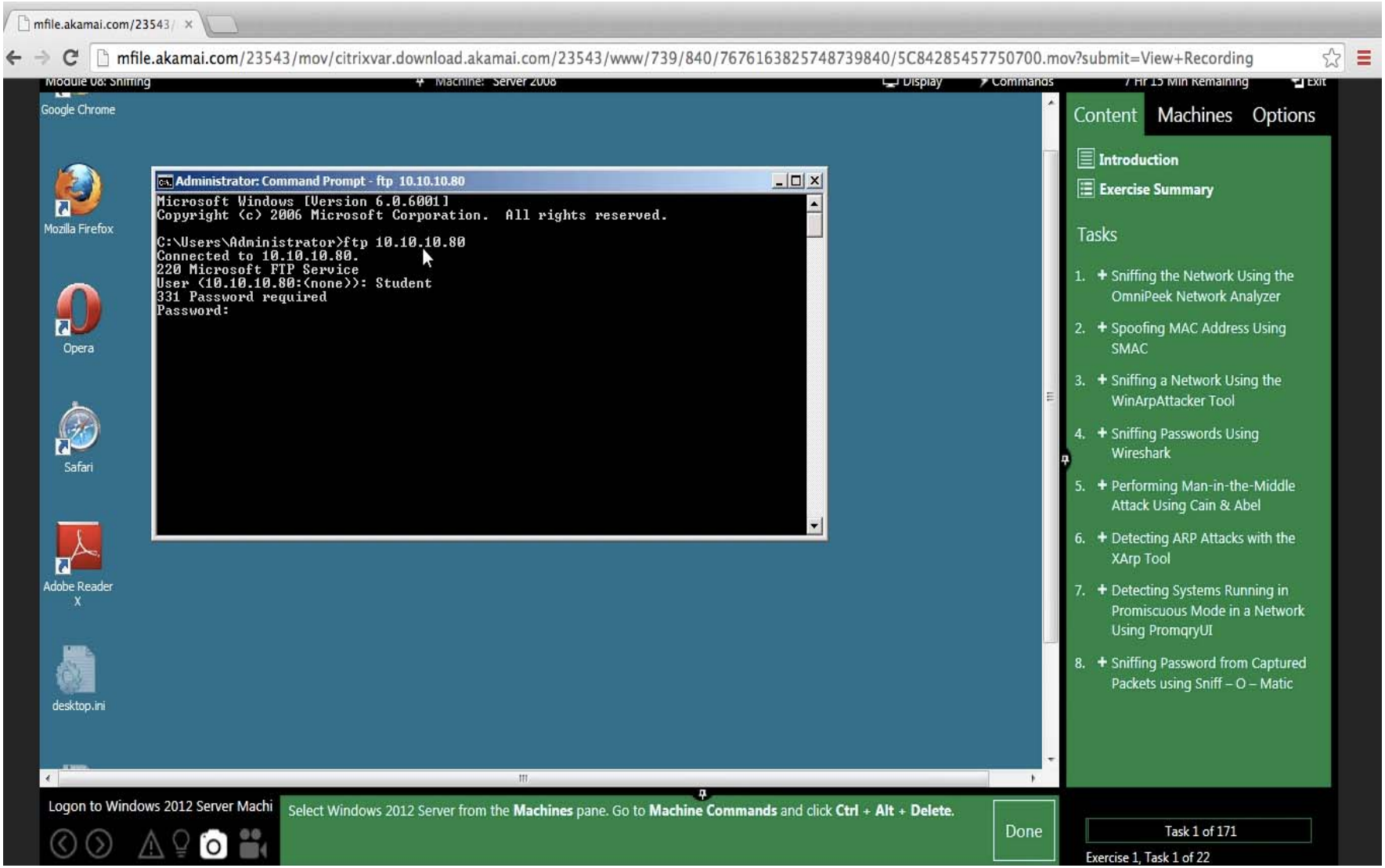
Poisoning Machine



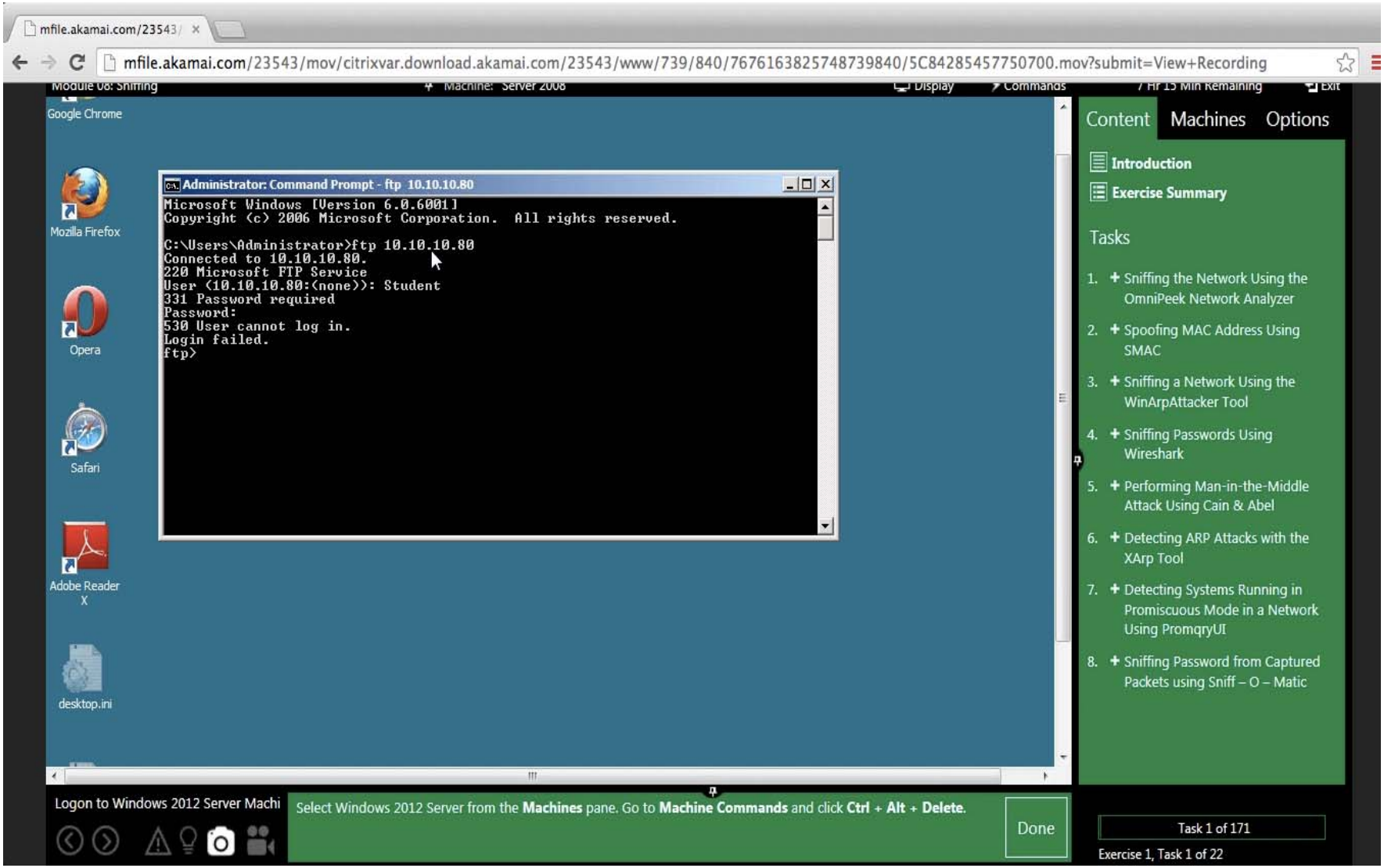
Switching Machine



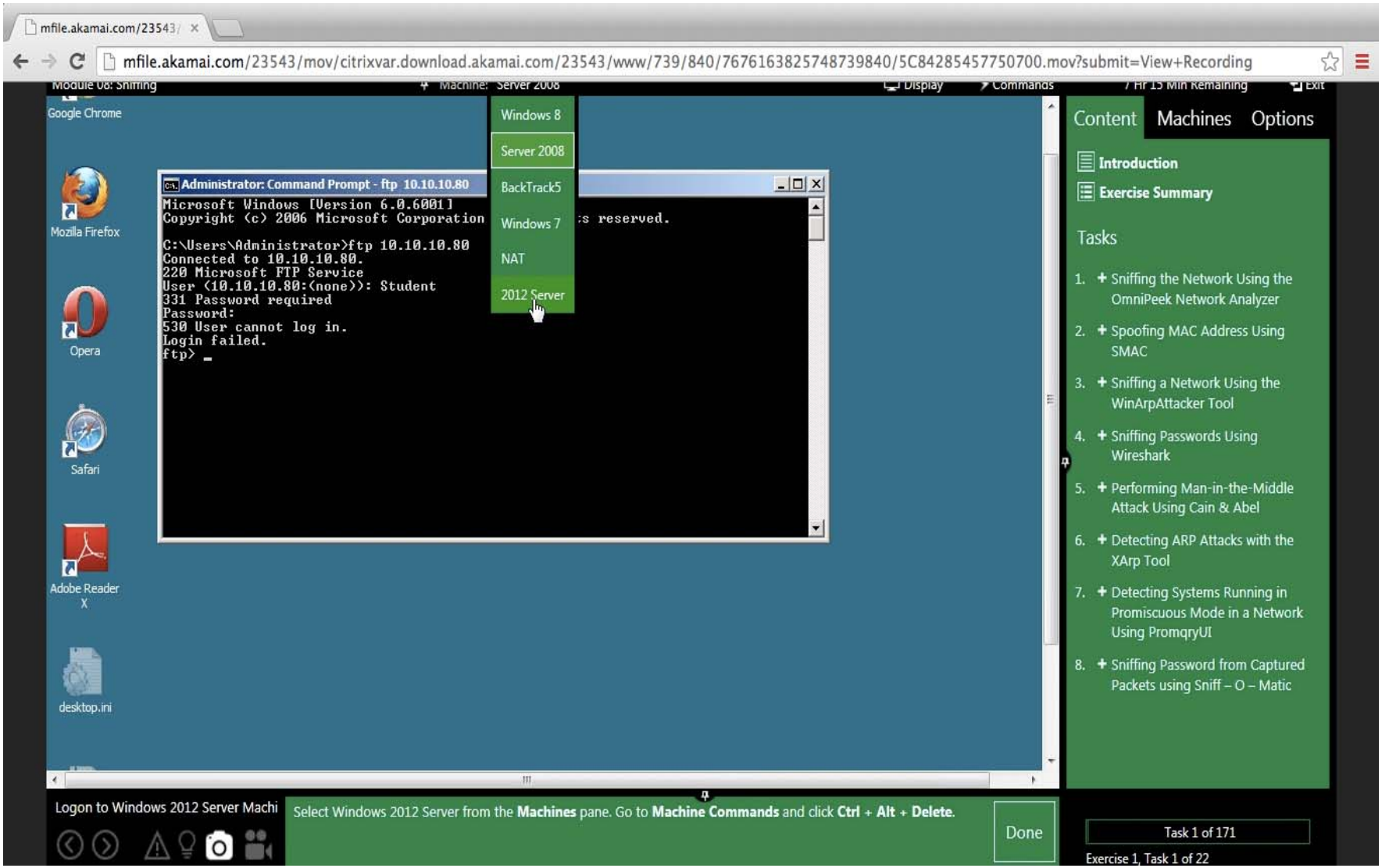
Connecting to Machine



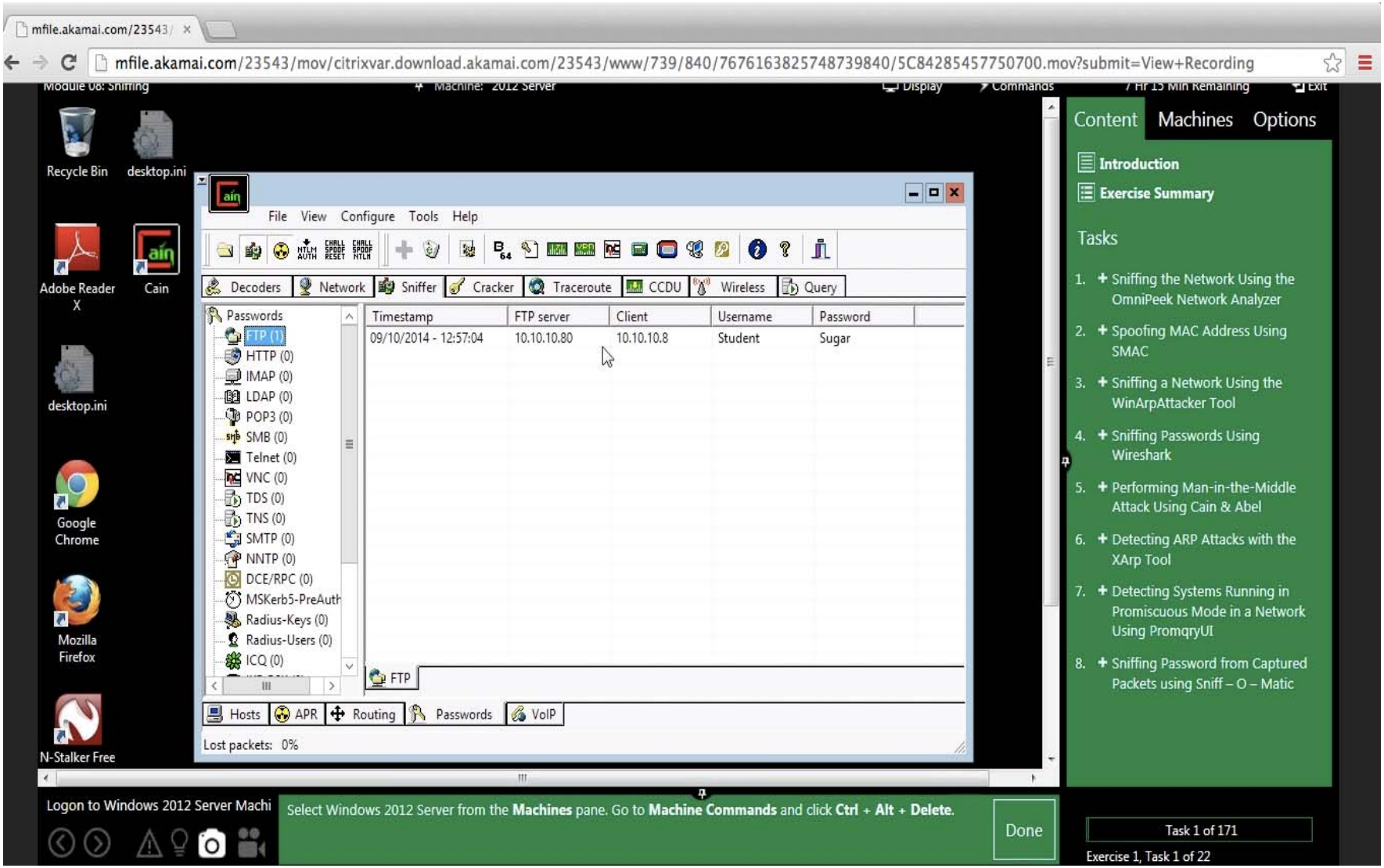
Entering Access Information – Trying to Log-In



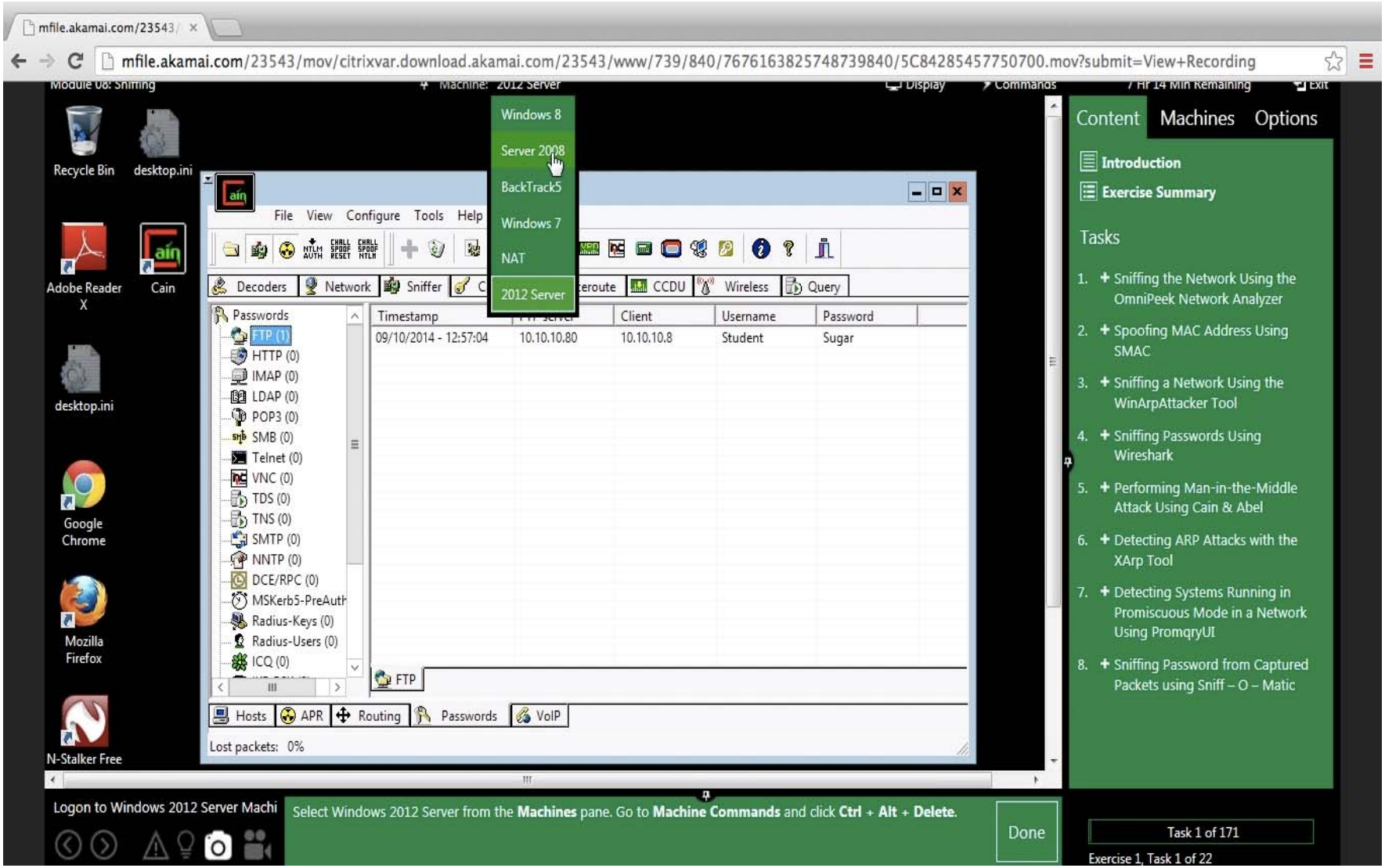
Log-in Failed



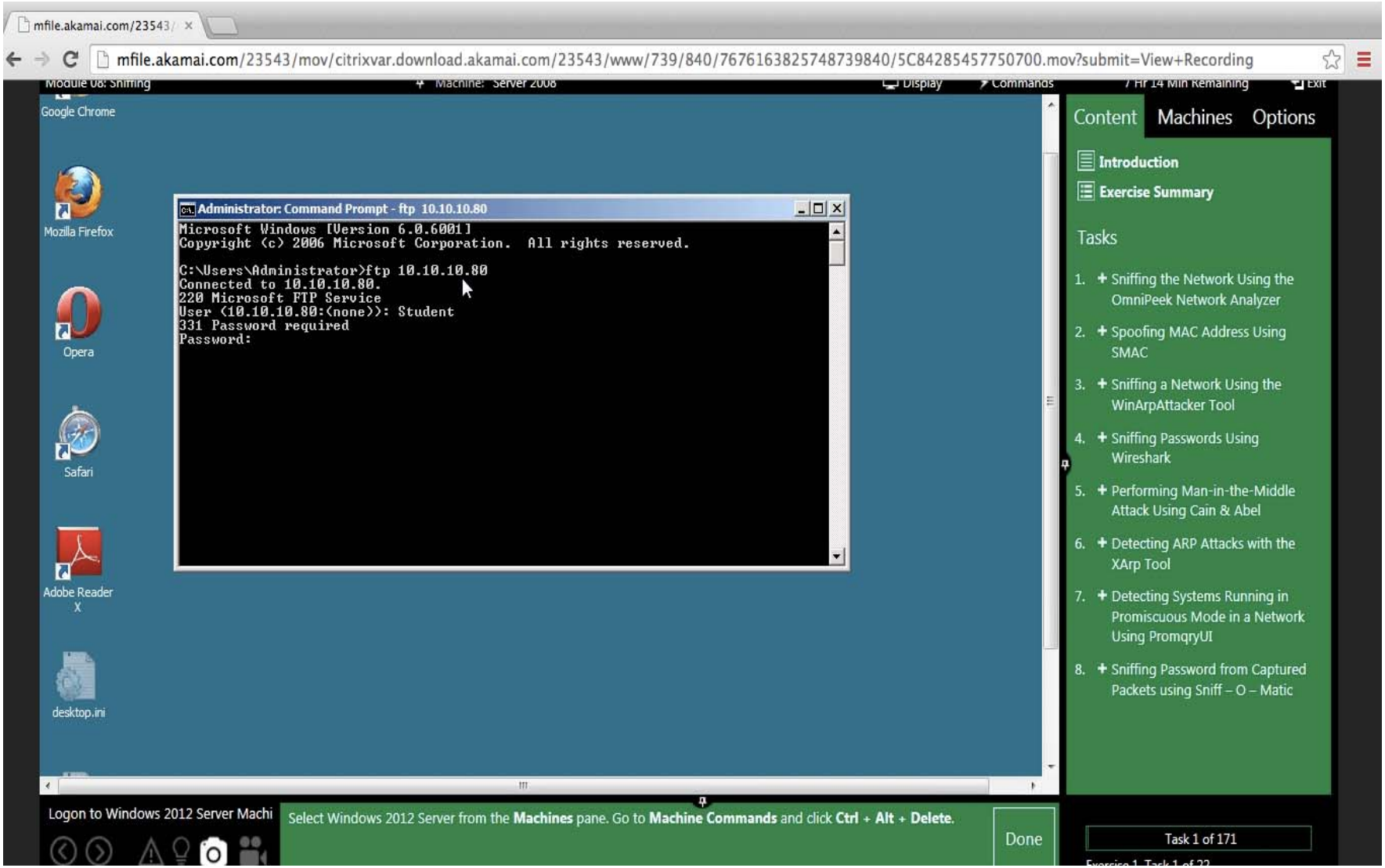
Switch To Server



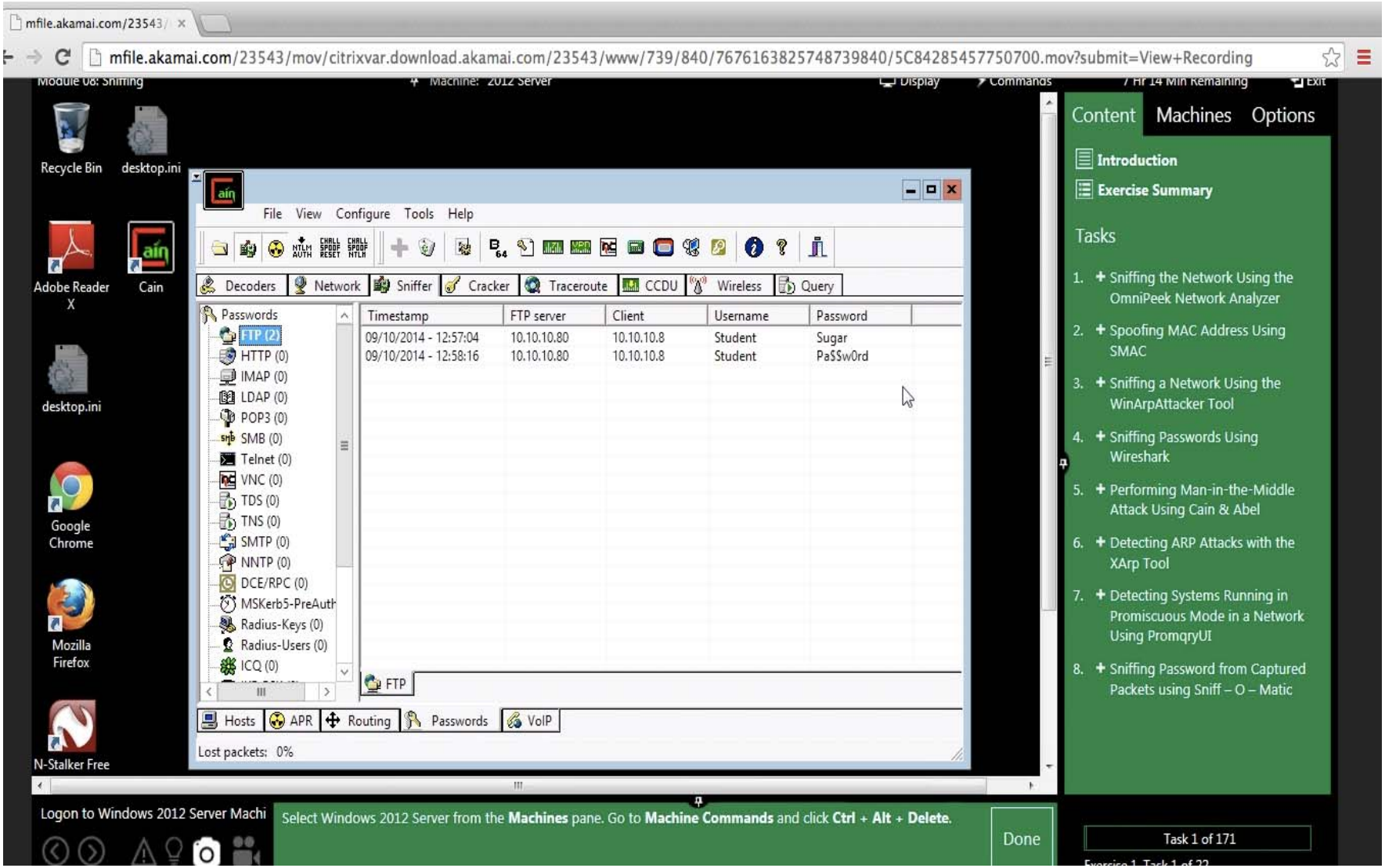
Access Timestamp, FTP Server, Client, User Name, Password Attempt



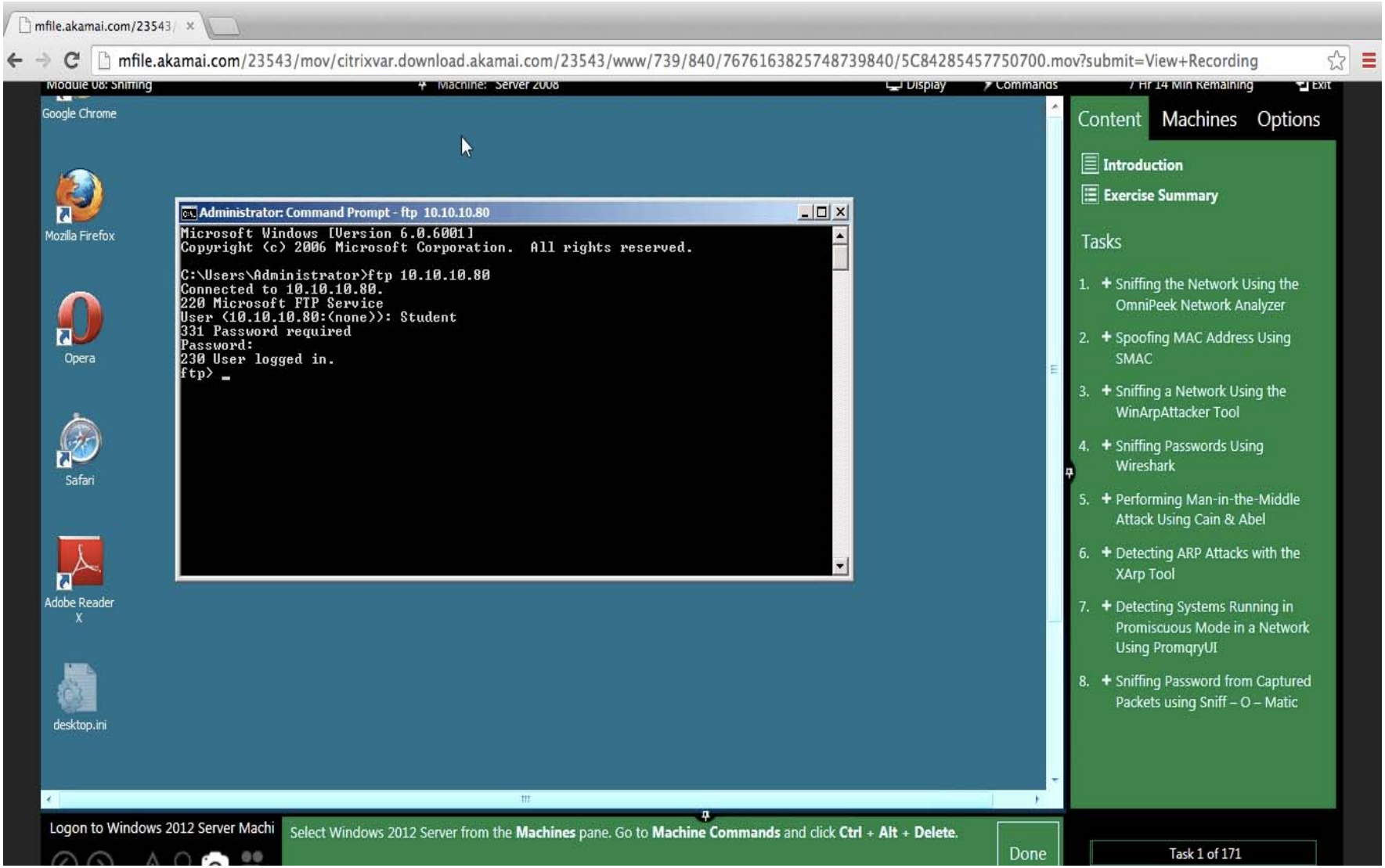
Switch Back to Server 2008



Entering Access Information – Trying to Log-In



Capturing Actual Password



Success User Log-In = Complete User Access

GOVERNMENT | ACADEMIA | PRIVATE INDUSTRY

Alignment – Global Cyber Range to Cybersecurity Education

Access – Monday, November 10, 2014


A Sustainable
Cybersecurity Workforce
Cybersecurity Resilience