



Security 504: Hacker Techniques, Exploits, and
Incident Handling
Introduction to Lab Exercises

Get the most out of the tools and
techniques that you will learn in the course

© 2017 SANS Institute

If you have any questions while working through your labs, please do not hesitate to contact our online Subject Matter Experts (SMEs) by sending an e-mail to online-sme@sans.org.

Setting the Stage

- Have fun with the course, but it is critical that you follow the instructions provided to maximize your learning experience.
- Do not use a computer with sensitive data stored on it. Assume that all your data could be lost.
- You must have local administrator access to the host operating system. Changes will need to be made to host-based software (antivirus, firewall, etc.) in order for the labs to work.
- We recommend that you keep your computer disconnected from the Internet while your security software is disabled.

© 2017 SANS Institute

This section is intentionally left blank.

System Requirements

- A properly configured system is critical for the lab exercises.
- You will need a Windows, Linux, or Mac computer with the following:
 - 16 GB of RAM minimum (more memory is recommended)
 - 70 GB of available disk space (more space is recommended)
 - Networking capability
 - USB Port
 - Wireless Adapter Required
 - VMware Player 6, Workstation 10, or Fusion 5, or higher (**Software is provided by SANS**)
 - 7-Zip or WinZip
- If you are using Linux or Mac, you must also have a Windows VMware virtual machine.

© 2017 SANS Institute

Windows

- Windows Vista, 7, or 8 (excluding Home editions) either as a real system or a virtual machine.
 - Home editions will NOT work for the course as they do not include all of the built-in capabilities we need for comprehensive analysis of the system.

VMware Software

- SANS provides software licenses to VMware with your course.
- Directions for obtaining your software can be obtained from the **VMware Software License Handout**

7-Zip or WinZip

- [7-Zip](http://www.7-zip.org/) is free software.
- [WinZip](http://www.winzip.com/) is available for a free trial.

URL References

[7-Zip](http://www.7-zip.org/) <http://www.7-zip.org/>

[Winzip](http://www.winzip.com/) <http://www.winzip.com/>

Overview (1)

The following index identifies where the lab exercises will be performed during the course.
All lab exercises are local except the section 6 CTF exercise which is remote.

Section 1: p.7 - 504 VM Setup p.78 - Windows Cheat Sheet p.145 - Enterprise-wide Identification and Analysis p.185 - Analyzing the Evil Insider p.245 - Linux Cheat Sheet	Section 2: p.76 - InSSIDer p.106 - Nmap p.122 - Nessus p.147 - SMB Sessions, smbclient, and rpcclient	Section 3: p.29 - Netcat on Windows and Linux p.80 - ARP and MAC Analysis	Section 4: p.158 - Metasploit Attack & Analysis p.46 - John the Ripper - Linux p.51 - John the Ripper - Windows p.130 - XSS and SQLi p.176 - Counting Resources to Evaluate DoS Attacks	Section 5: p.28 - Memory Analysis of a Windows Attack p.86 - Analysis a Shell History File p.102 - Alternate Data Streams on Windows p.130 - Covert Channels	Section 6: Final Workshop (Remote)
---	--	--	---	---	---

© 2017 SANS Institute

This section is intentionally left blank.

Overview (2)

- The course **USB** is full of attack tools to experiment with during the course. You do not need to bring a Linux system; we will provide you with a Linux virtual machine with all of our tools pre-installed.
 - Setup instructions for the course virtual machine can be found on **page 7** of your **SEC504.1 course book**.
 - Setup instructions for VMware networking can be found starting on **page 194** of your **SEC504.1 course book**.
 - Use the following login credentials for the Linux virtual machine:
 - User ID: **sec504**
 - Password: **sec504**
 - For root access, at the command prompt type **sudo su** – followed by the password **sec504**

© 2017 SANS Institute

This section is intentionally left blank.

Overview (3)

- The following **handouts** will be referenced in the course as needed:
 - [Intrusion Discovery Cheat Sheet](#)
 - [Windows Intrusion Discovery Cheat Sheet - Pocket Reference Guide](#)
 - [Lab Errata](#)
- You will receive poster(s) with your course to reference as you progress throughout the content
- The following URL contains **SEC504 extras** that can be downloaded:
 - <http://tinyurl.com/504extra2>

© 2017 SANS Institute

SEC504 Extras

- [SEC504 extras](#) that can be downloaded.

Overview (4)

- When this course is taught at a SANS live training event, the Capture the Flag (CTF) exercise in **Section 6** is performed over a wired network in the classroom.
- For SANS Online Training, we have a **Virtual Lab** for this exercise to replicate the live classroom environment.
 - You will access the **Virtual Lab** over the Internet through OpenVPN.
 - For instructions on accessing the **Virtual Lab** for the CTF exercise in **Section 6**, reference the following **two e-mails** that you received from virtual-labs-support@sans.org after you paid for your course:
 - **SEC504 Virtual Lab Access**
 - **SEC504 Virtual Lab Targets**

© 2017 SANS Institute

This section is intentionally left blank.

Common Lab Issues You May Experience (1)

- **Section 1 - Initial Setup:** In **Section 1** when setting up up your virtual machine and importing the .ovf file into VMWare, you may get a **consistency error** from VMWare. This is because the OVF was not created with the same version of VMWare you have. Just **select Retry** and it should import just fine.
- **Section 1 – Lab: Windows Cheat Sheet:** Part of the lab asks the student to look at "HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx". This registry key may or may not be present on different versions of windows.
- **Section 3 – Netcat on Windows and Linux:** On page 40 of this lab the courseware incorrectly states to **su student** where it should state **su sec504**.
- **Section 5 – Covert Channels:** On p.133, step 3 '**service nginx start**' may not be necessary. If you receive an error, simply enter '**systemctl restart nginx**' to restart the HTTP server.

© 2017 SANS Institute

This section is intentionally left blank.

Common Lab Issues You May Experience (2)

- **Section 6 – Final Workshop:** In the **Section 6 Final Workshop**, you will not follow the instructions for getting networked, instead follow the instructions you received from virtual-labs-support@sans.org
 - The IP addresses for your Windows and course Linux virtual machine will be automatically assigned using DHCP
 - Your email will contain the download location for your SSL certificates for OpenVPN authentication
 - Your email will also contain the URL <https://labs.sans.org/> which contains instructions for configuring OpenVPN for both your course Linux virtual machine, and a Windows operating system.
 - Under the VMware settings, configure your network connection for NAT or Bridged, and ensure that the Device status is "Connected"

© 2017 SANS Institute

This section is intentionally left blank.

Common Lab Issues You May Experience (3)

- In the **Section 6 Final Workshop**, once you have your OpenVPN connection configured and running, you will need to address the correct network interface when using commands like tcpdump. You can identify your OpenVPN network interface by using the command **ifconfig -a**. It will be associated with the 10.10.75.0/24 network and normally be tap0.
 - For example, to look at tcpdump data going across the OpenVPN connection, you will issue the command **tcpdump -i tap0 -nn**.
- The Virtual Machines (VMs) in the **Section 6 Virtual Lab** revert to a known state every hour at 30 minutes past the hour. If you are in the middle of something when this happens, you may not receive the result that you are expecting.

Remember to contact the online Subject Matter Experts if you become stuck while participating in the lab exercises and need some hints to help you continue.

© 2017 SANS Institute

This section is intentionally left blank.