Setting up a Security Test Lab

Amherst Security Group (@AmherstSec)
July 11, 2018
Robert Hurlbut

RobertHurlbut.com • @RobertHurlbut
Robert Hurlbut

Threat Modeling Architect, Trainer
(ISC)2 CSSLP 2014-2020
Co-host with Chris Romeo – Application Security Podcast
MeetUp Leader: Boston .NET Architecture Group, Amherst Security Group

Contacts
Web Site: https://roberthurlbut.com
Twitter: @RobertHurlbut, @AppSecPodcast

© 2018 Robert Hurlbut
Acknowledgement

Special thanks to inspiration from David Boyd’s talks below for this talk:

• “Hacking Yourself: Building a Test Lab” at BSides Knoxville 2016
• “Hack Yourself: Build a Pentesting Lab” at DerbyCon 2016

You can catch videos of these on YouTube.
Agenda

• Why / how to set up the lab
  Virtualization software
  Pen testing distributions
  Vulnerable VMs
  Recommended tools

• Demo

• Resources
What is a Security Test Lab?

• Virtual environment replicating a real world network
• Sandbox used for practicing penetration testing

© 2018 Robert Hurlbut
Walk-through resources

• These books are highly recommended to walk you through:

  - The Network Security Test Lab: A Step-by-Step Guide
  - The Hacker Playbook 3: Practical Guide to Penetration Testing
Why build a lab?

- Skillset improvement
- Try out something new
- Brush up on tactics
- Proof of concept (great for customers)
- Code / Script demonstration
Who should build a lab?

• Security Personnel (Red Team / Blue Team)
• IT Personnel (Networking / SysAdmin)
• C Level Executives (great to keep skills sharp)
• Students
• Anyone wanting to learn a new skill
• YOU!
What you need - ?
What you used to need
What you (Really) need

Computer + Virtualization Software + Testing VMs Vulnerable VMs

© 2018 Robert Hurlbut
Computer Specifications

• i5 Quad Core Processor
• ~16 GB RAM
• ~250–500 GB HDD

• NOTES:
  • Make sure Virtualization is enabled in the BIOS
  • Only one hypervisor software running / enabled on a computer at a time (For example: You can’t enable both Hyper-V AND Virtual Box at the same time)
Step 1: Download file archivers

• WinRar
   https://www.rarlab.com/download.htm

• 7-Zip
   https://www.7-zip.org/

• Keka
   Mac App Store

• The Unarchiver
   Mac App Store

© 2018 Robert Hurlbut
Step 2: Install Virtualization Software (Free examples)

- VMWare Player
  [https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0](https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/vmware_workstation_player/14_0)
- Oracle Virtual Box
  [https://www.virtualbox.org/wiki/Downloads](https://www.virtualbox.org/wiki/Downloads)
- Hyper-V (not an install, but available on some Windows versions)
  Windows 10 (Enterprise, Professional, Education versions only), Windows Server 2012+
- Linux KVM
  [https://www.linux-kvm.org/page/Main_Page](https://www.linux-kvm.org/page/Main_Page)
- Linux ProxMox
  [https://www.proxmox.com/](https://www.proxmox.com/)
Step 2: Install Virtualization Software (Paid examples)

- VMWare Fusion (for Macs)
  Free Trial 30 Days
  $80 after that

- VMWare Workstation Player
  Free Trial 30 Days
  $149 after that

- Parallels Desktop (for Macs)
  Free Trial 30 Days
  $80+ after that

© 2018 Robert Hurlbut
Step 3: Install Pen Testing Platform

- Kali Linux (Lots of tools)
  [https://www.kali.org](https://www.kali.org)
- Pentoo (Lots of tools)
  [https://www.pentoo.ch](https://www.pentoo.ch)
- Backbox (Lots of tools)
  [https://backbox.org/](https://backbox.org/)
- Samurai WTF (Web App Testing)
- Samurai STFU (Utility (i.e. SCADA) Hacking)
- Deft Linux (Forensics)
  [http://www.deftlinux.net/](http://www.deftlinux.net/)
Step 3a: Use a Firewall

• pfSense
  https://www.pfsense.org/

• OPNsense
  https://opnsense.org

Firewall for your Security Test Lab environment is highly recommended in order to contain the vulnerable VMs as much as possible.
Using pfSense for firewall
Step 4: Install Vulnerable VMs (Free!)

- Metasploitable 2 or 3 (Metasploit)
- Morning Catch (Phishing)
- OWASP Broken Web Applications (Web Apps)
  - https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
  - Also, look at these separate OWASP vulnerable web projects (not VMs, though)
    - OWASP WebGoat Project
    - OWASP Juice Shop Project
    - OWASP DevSlop Project
- Vulnhub (https://www.vulnhub.com/)
- Kioptrix (Beginners)
- PwnOS
Step 4: Other Vulnerable VMs (not intentional)

- Windows XP
- Windows Server
- Microsoft Exchange
- Windows 7
Step 4: Other VM Sources

• Windows Server Evaluations
  https://www.microsoft.com/en-us/evalcenter/try (180 day trials)

• Windows Server 2016

• IE Virtual Machines
  https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/ (IE 8 to Edge – 90 day trials)
Recommended Tools

- Nmap / Masscan (Scanning)
- Nessus (Vulnerability Scanning)
- Cain (ARP Poisoning)
- Responder (MiTM)
- John The Ripper / Hashcat (Hash Cracking)
- Metasploit (Exploits)
- SET / GoPhish / SPF (Phishing)
- Discover Scripts (OSINT)
- PowerShellEmpire (PowerShell Scripts)
- CrackMapExec (Post Exploitation)
Optional (Build a Domain)

• Build a Domain
• Add users with various privileges

• Peter Kim’s article on “Setting up a Windows Lab Environment”:
  http://thehackerplaybook.com/Windows_Domain.htm

© 2018 Robert Hurlbut
Security Test Lab (example)

Computer (Windows 10 Laptop)
Virtual Box (VM Software)
pfSense (VM)
Kali Linux (VM)
Metasploitable 2 or 3 (VM)
Windows XP (VM)
Domain Controller (VM)
VM network design example from *Building Virtual Machine Labs: A Hands-On Guide* (p. 30)

- Bridged Network (bridge to external network)
- Management Network (SIEM / Splunk, IPS, etc.)
- IPS 1 Network (Test tools)
- IPS 2 Network (Vulnerable VMs)
Demo

Look at Hyper-V config

Look at VirtualBox config
Resources

  Tony Robinson

The Network Security Test Lab: A Step-By-Step Guide
  Michael Gregg

The Hacker Playbook 3: Practical Guide to Penetration Testing
  Peter Kim

© 2018 Robert Hurlbut
Resources

Metasploitable 2 Exploitability Guide
https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide

Introducing Morning Catch – A Phishing Paradise
https://blog.cobaltstrike.com/2014/08/06/introducing-morning-catch-a-phishing-paradise/

SANS Mutillidae Whitepaper

© 2018 Robert Hurlbut
Resources

• Building a PenTest Lab (Robert Musser) –
  interesting list found on the web
