VIRTUALIZATION - DARK WEB FORENSICS USING CSI LINUX

Deborah K. Wells, Lecturer, CWU

Introduction

In today's world, virtualization is something that many companies and industries are migrating their environments in order to save on physical appliances.

Welcome to this afternoon's workshop…today we are going to discuss virtualization and then how to conduct some forensics on the Dark Web…using a VM and CSI Linux

AGENDA

What is virtualization?

Introduction to CSI Linux

Dark Web Explained

Using CSI Linux to Investigate the Dark Web

VIRTUALIZATION

Subtitle

What is virtualization?

- Virtualization uses software to create an **abstraction layer** over computer hardware that allows the hardware elements of a single computer—processors, memory, storage and more—to be divided into multiple virtual computers, commonly called virtual machines

- Sharing computing power, saves resources

Pros/Cons of Virtualization

- **Pros of Virtualization**
  - **Uses Hardware Efficiently**
  - **Available at all Times**
  - **Recovery is Easy**
  - **Quick and Easy Setup**
  - **Cloud Migration is Easier**
- **Cons of Virtualization**
  - **High Initial Investment**
  - **Data Can be at Risk**
  - **Quick Scalability is a Challenge**
  - **Performance Witnesses a Dip**
  - **Unintended Server Sprawl**

Types of Virtualization

- OS Virtualization—aka Virtual Machines
- Application-Server Virtualization
- Application Virtualization
- Administrative Virtualization
- Network Virtualization
- Hardware Virtualization
- Storage Virtualization

An Overview of Virtual Machine Forensics

- Virtual machines are important in today's networks.
- Investigators must know how to analyze virtual machines and use them to analyze other suspect drives
- The software that runs virtual machines is called a "hypervisor"
- Two types of hypervisor:
  - Type 1 - loads on physical hardware and doesn't require a separate OS
  - Type 2 - rests on top of an existing OS

An Overview of Virtual Machine Forensics

- Type 2 hypervisors are usually the ones you find loaded on a suspect machine
- Type 1 hypervisors are typically loaded on servers or workstations with a lot of RAM and storage – you may have heard the term “bare metal” before…

Type 2 Hypervisors

- Before installing a type 2 hypervisor, enable virtualization in the BIOS before attempting to create a VM
- Virtualization Technology (VT) - Intel's CPU design for security and performance enhancements that enable the BIOS to support virtualization
- Virtualization Machine Extensions (VMX) - instruction sets created for Intel processors to handle virtualization

Type 2 Hypervisors

- Most widely used type 2 hypervisors:
  - Parallels Desktop - created for Macintosh users who also use Windows applications
  - KVM (Kernel-based Virtual Machine) - for Linux OS
  - Microsoft Virtual PC - the most recent version supports only VMs that run Windows
  - VMware Workstation and Player - can be installed on almost any device, including tablets
    - Can install Microsoft Hyper-V Server on it
    - Can support up to 16 CPUs, 8 TB storage, and 20 VM

Type 2 Hypervisors

File extension	Description
.vmx	Stores configuration files
.log	Contains logs of information such as when a VM was powered off, virtual appliances added, and so on
.nvram	Keeps track of the state of a VM's BIOS
.vmdk	Stores the virtual hard drive's contents
.vmem	Stores VM paging files, which serve as RAM
.vmsd	Contains information about snapshots

Source: VMware, *www.vmware.com*

Type 2 Hypervisors

- Most widely used type 2 hypervisors (cont'd):
  - VirtualBox - supports all Windows and Linux OSs as well as Macintosh and Solaris
    - Allows selecting types associated with other applications, such as VMware VMDK type or the Parallels HDD type
- Type 2 hypervisors come with templates for different OSs

Type 2 Hypervisors

File extension	Description
`.ova` or `.ovf`	File used to create a virtual machine; OVF stands for "Open Virtualization Format"
`.vdi`	Disk image file
`.r0`	Default libraries
`.vbox`	Saved settings of virtual hard drives
`.vbox-extpack`	Plug-ins
`.vbox-prev`	Backups of VMs
`.xml-prev`	Backups of XML settings
`.log`	Log files containing information such as a VM being powered on and off, whether it's in hibernation mode, virtual appliances added, and so on

Conducting an Investigation with Type 2 Hypervisors

- Begin by acquiring a forensic image of the host computer as well as network logs
  - By linking the VM's IP address to log files, you may determine what Web sites the VM accessed
- To detect whether a VM is on a host computer:
  - Look in the Users or Documents folder (in Windows) or user directories (in Linux)
  - Check the host's Registry for clues that VMs have been installed or uninstalled
  - Existence of a virtual network adapter

Conducting an Investigation with Type 2 Hypervisors

- In addition to searching for network adapters, you need to determine whether USB drives have been attached to the host
  - They could have live VMs running on them
- A VM can also be nested inside other VMs on the host machine or a USB drive
  - Some newer Windows systems log when USB drives are attached
  - Search the Windows Registry or the system log files

Conducting an Investigation with Type 2 Hypervisors

- Follow a consistent procedure:
  - 1. Image the host machine
  - 2. Locate the virtualization software and VMs, using information learned about file extensions and network adapters
  - 3. Export from the host machine all files associated with VMs
  - 4. Record the hash values of associated files
  - 5. Open a VM as an image file in forensics software and create a forensic image or mount the VM as a drive

Conducting an Investigation with Type 2 Hypervisors

- Live acquisitions of VMs are often necessary
  - They include all snapshots, which records the state of a VM at a particular moment (records only changes in state, not a complete backup)
- When acquiring an image of a VM file, snapshots might not be included
  - In this case, you have only the original VM
- Doing live acquisitions of VMs is important to make sure snapshots are incorporated

Conducting an Investigation with Type 2 Hypervisors

- Other VM Examination Methods
  - FTK Imager and OSForensics can mount VMs as an external drive
    - By mounting a VM as a drive, you can make it behave more like a physical computer
    - Allows you to use the same standard examination procedures for a static hard drive
  - Make a copy of a VM's forensic image and open the copy while it's running
    - Start it as a live VM so that forensics software can be used to search for clues

Working with Type 1 Hypervisors

- This section is meant to help you understand the impact Type 1 hypervisors have on forensic investigations
  - Having a good working relationship with network administrators and lead technicians can be helpful
- Type 1 hypervisors are installed directly on hardware
  - Can be installed on a VM for testing purposes
  - Capability is limited only by the amount of available RAM, storage, and throughput

Working with Type 1 Hypervisors

- Common type 1 hypervisors:
  - VMware vSphere
  - Microsoft Hyper-V 2012
  - Citrix XenServer
  - IBM PowerVM
  - Parallels Bare Metal

CSI LINUX

Subtitle

CSI Linux

“CSI Linux is a focused Linux distribution for digital forensics. We (Jeremy Martin and his team) developed an open-source 'theme park' for the cyber security industry. It has tons of capabilities for investigations, analysis and response! CSI Linux is available in both a Virtual Machine Appliance and Bootable distro to use as a daily driver.”

https://csilinux.com/download

Walk through CSI Linux

- When you go through all the tools available with this Linux distribution, I would say “Cornucopia”
- All types of tools
  - Regular Forensics
  - VM Forensics
  - Malware Analysis
  - Network Forensics
  - Threat Intelligence tools

Walk through CSI Linux

- When you first launch the OS, I recommend looking at your IP addresses
- Then you can ensure you are being anonymized!
- You can go out and download the files you need – like the CFREDS – Rhino file for the lab.

THE DARK WEB

Subtitle

The Deep Web

The Public Web

Only 4% of Web content (~8 billion pages) is available via search engines like Google

The Deep Web

Approximately 96% of the digital universe is on Deep Web sites protected by passwords

Deep Web

- Think databases or academic journals
- Use it especially when working on papers…
  - Your Library Resources

The Dark Web

- The "dark web" is the encrypted network that exists between TOR servers and their clients, whereas the "deep web" is simply the content of databases and other web services that for one reason or another cannot be indexed by conventional search engines
- Dark Web is something that's encrypted, or purposely hidden
- The Silk Road website is an example of a site on the Dark Web
  - All of those are located on the dark web; you need Tor to access them, plus there's a 3-step verification in order to log into the sites

Welcome! | Silk Road | State of the Road Address

silkroadvb5piz3r.onion

Silk Road

anonymous marketplace

Welcome **OzFreelancer!**

messages(0) | orders(0) | account(฿0.00) | settings | log out

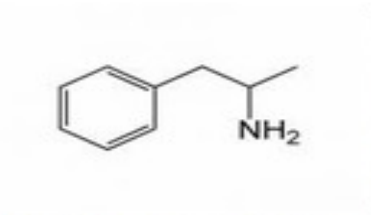
search | (0)

Shop by category:

- Drugs(1582)
  - Cannabis(271)
  - Dissociatives(33)
  - Ecstasy(217)
  - Opioids(106)
  - Other(65)
  - Prescription(274)
  - Psychedelics(306)
  - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)
- Erotica(165)
- Fireworks(1)
- Food(1)
- Forgeries(34)
- Hardware(1)
- Home & Garden(5)
- Lab Supplies(5)
- Medical(3)
- Money(89)
- Musical instruments(2)
- Packaging(1)

10 Grams high grade MDMA 80+%

฿61.17



Amphetamines sulfate / Speed freebase...

฿28.59

2g Jack Frost (weed) *420 SALE****

฿8.54

5 Grams of pure MDMA crystals

฿42.04

100 red Y tablets 111mg (lab tested)...

฿97.77

Michael Jackson Discography 1971-2009...

฿2.52

3.5g Albino Rhino (weed)

฿12.37

10mg Flexeril (muscle relaxant)...

฿3.22

***10gr. Amphetamine Sulphate...

฿33.19

News:

- The gift that keeps on **giving**
- Who's your **favorite**?
- Acknowledging **Heroes**
- A new annonymous market **The Armory**!
- **State of the Road Address**

Dark Web activity

- Sites that exist in dark nets today, while not illegal in and of themselves, tend to be a haven for illegal activity
- Agencies such as the NSA, FBI, and ICE have been trying to de-anonymize dark websites and crack down on the crime aspect, but it looks as though they've only made a chip in the proverbial iceberg


The Internet
(more or less)
You can turn a computer on. Yay.
Digg
reddit
LiveLeak
tumblr.
random wikis and blogs
Gaia
808chan, 7chan, 420chan
2channe
4chan
You must be really bored.
sTORage
PedoPlanet
KindzazaChan
Hard Candy
TorChan
Hidden Wiki
Tor P.M.
OnionChan
OnionIB
Either use a proxy, or say hi to the FBI.

Who invented the dark w | Tor Project | Privacy Onlir | So what is a torrent exac

Secure | https://www.torproject.org/index.html.en

Home | About Tor | Documentation | Press | Blog | Newsletter | Contact

Download | Volunteer | Donate

We're hiring! »

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.

Download Tor

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android

What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

Learn more about Tor »

Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, and it prevents the sites you visit from learning your physical location.

Get involved with Tor »

Our Projects

Tor Browser
Tor Browser contains everything you need to safely browse the Internet.

Orbot
Tor for Google Android devices.

Tails
Live CD/USB operating system preconfigured to use Tor safely.

Nyx
Terminal (command line) application for monitoring and configuring Tor.

Relay Search
Site providing an overview of the Tor network.

Pluggable Transports
Pluggable transports help you circumvent censorship.

Stem

OONI

Recent Blog Posts

Tor Browser 8.0a2 is released
Fri, 23 Feb 2018 Posted by: *boklm*

We've Launched a Search for Our ...
Thu, 22 Feb 2018 Posted by: *steph*

Tor + Outreachy: Internships for...
Wed, 21 Feb 2018 Posted by: *t0mmy*

Volunteer Spotlight: Meejah Help...
Tue, 20 Feb 2018 Posted by: *t0mmy*

Italian Anti-Corruption Authorit...
Tue, 13 Feb 2018 Posted by: *steph*

View all blog posts »

Who Uses Tor?

Family & Friends
People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

Businesses
Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal accountability.

Activists
Activists use Tor to anonymously report abuses from danger zones. Whistleblowers use Tor to safely report on corruption.

Media
Journalists and the media use Tor to protect their research and sources online.

Military & Law Enforcement
Militaries and law enforcement use Tor to protect their communications

History of The onion router

- Like other areas of the Internet, the Deep Web began to grow with help from the U.S. military
- They were looking for ways to communicate with intelligence assets and Americans stationed abroad without being detected
- Paul Syverson, David Goldschlag and Michael Reed, mathematicians at the Naval Research Laboratory, began working on the concept of “onion routing” in 1995
- Their research soon developed into The Onion Router project, better known as Tor, in 1997

tor

- The Tor network is a group of volunteer-operated servers that allows people to improve their privacy and security on the Internet
- Tor's users employ this network by connecting through a series of virtual tunnels rather than making a direct connection, thus allowing both organizations and individuals to share information over public networks without compromising their privacy
- Tor can also be used as a building block for software developers to create new communication tools with built-in privacy features

tor

- Individuals use Tor to keep websites from tracking them and their family members, or to connect to news sites, instant messaging services, or the like when these are blocked by their local Internet providers
- Tor’s onion services let users publish web sites and other services without needing to reveal the location of the site. Individuals also use Tor for socially sensitive communication: chat rooms and web forums for rape and abuse survivors, or people with illnesses
- Using Tor protects you against a common form of Internet surveillance known as "traffic analysis"
- Tor is supported solely by sponsors

More about TOR

- Tor instead uses, at a minimum, three servers to pass your traffic on, each encapsulated with its own layer of encryption
- This provides the anonymity that Tor is so famous for!
- All that these servers see is the IP that sent them the packet, and that's it.
  - The first server sees your real IP, but not your content or destination
- Only the final server knows your true destination, but doesn't know who you are

DARK WEB-FORENSICS

Subtitle

How to go to dark web using CSI Linux

- Check your IP on your host machine before starting…jot it down.
- Launch your Virtual Box
- Build a CSI Linux VM
  - When building it,
- Launch your VM
- Before you begin, go up to the top right upper corner to see your IP on your machine
- Put CSI Linux on a USB or save to your host disk drive
- Load up the CSI Linux on your VM

How to go to dark web using tails OS

- You will want to use Linux OS, Other Linux or Debian (64-bit)
- Have as much data as you can go towards the computing power
- Launch the VM

Once you are on the dark web

- Some of these directories include:
  - Hidden Wiki | Tor .onion urls directories
  - HiddenWiki Deep Web Links
  - The uncensored hidden wiki is up: http://kpvz7kpmcmne52qf.onion/wiki/index.php/Main_Page • /r/TOR

Summary

Today you were exposed to 3 different concepts:

--virtualization

-- CSI Linux

-- Dark Web

Now we will put them all together in a brief practice lab

THANK YOU

Deborah Wells

Deborah.wells@cwu.edu

DARK WEB LAB

USE THE DARK WEB AT YOUR OWN RISKDO NOT GO TO SITES HAVING CHILD PORNOGRAPHY, IT IS ILLEGAL TO EVEN GO TO THE SITE!!

IF YOU DO NOT FEEL COMFORTABLE WITH THIS LAB, JUST WORK ON THE FIRST SCENARIO

Scenario #1

- Install this on your AWS workstation
  - Virtual Box
  - CSI Linux
  - Add Rhino Hunt from https://cfreds.nist.gov/
-
- **Scenario:** *The city of New Orleans passed a law in 2004 making possession of nine or more unique rhinoceros' images a serious crime. The network administrator at the University of New Orleans recently alerted police when his instance of RHINOVORE flagged illegal rhino traffic. Evidence in the case includes a computer and USB key seized from one of the University's labs. Unfortunately, the computer had no hard drive. The USB key was imaged and a copy of the dd image is on the CD-ROM you've been given. In addition to the USB key drive image, three network traces are also available—these were provided by the network administrator and involve the machine with the missing hard drive. The suspect is the primary user of this machine, who has been pursuing his Ph.D. at the University since 1972.*
-

Tasks

- Recover at least nine rhino pictures from the available evidence and include them in a brief report. In your report, provide answers to as many of the following questions as possible:
    - Who gave the accused a telnet/ftp account?
    - What's the username/password for the account?
    - What relevant file transfers appear in the network traces?
    - What happened to the hard drive in the computer? Where is it now?
    - What happened to the USB key?
    - What is recoverable from the dd image of the USB key?

Scenario #2

- Install this on your AWS workstation
  - Virtual Box
  - CSI Linux
  - You will go out to the Dark Web from CSI Linux

- **Scenario: Scenario:** *ACME University was faced with a large exfiltration of intellectual property (IP) from a new cyber education and research program that had just started this year – of all things, the program just so happened to be Cybersecurity Education and Research (CySER)!*
- *The CySER directors call your forensics company, No FEAR, and wanted to hire you to go out and investigate where the IP was exfiltrated to and who did such a dastardly crime!*
- *During the initial intake from the CySER lead director, you have a fairly good suspicion that the data was being sold on the Dark Web.*

Tasks

- You are tasked to go out to the Dark Web or use the Dark Web Search feature…and using some of the tools in CSI Linux try and find out if indeed the data was sold to the Dark Web.
    - If it was, then try to find out as much as you can about who might have stolen the credentials and who they are selling the information to.
- **For exercise purposes you will need to search for higher education credentials from another university or college (not ACME University – that was a fictitious name).**
- Provide a screenshot or 2 from what you found.