Project Companion Document

Ex1 - Forensic Analysis: Local Incident Response

5. Environment Preparation

Mac users with Apple Silicon (M1/M2) CPUs:

- Due to the fact that VirtualBox does not support macOS hosts running Arm64 chips (they currently have a beta version, but we had some issues using it) we opted to use an alternative. Although there are several of them, we opted to use **UTM**. You can download it directly from the UTM website (https://mac.getutm.app/).
- UTM is based on QEMU and thus does not support OVA/OVF. Students should instead use the provided **Caine_v1.4.qcow2** to set up their VMs. You can follow this brief tutorial on how to do it (how to import qcow2 to utm). **But before that:**
    - We recommend those who can use at least **8GB** of RAM to do so, as some tasks can be very time consuming otherwise (some will take long regardless).
    - In addition, we recommend changing the emulated display card to **VGA** and and the VGA device RAM to at least **64MB**. This can be done by first selecting the VM and navigating to (Edit > Display).
- The evidence file you should use is the **Evidence_1.qcow2**. You can import it just as you did with Caine_v1.4.qcow2 (in Edit > Drives > New) and you should end up with both drives installed simultaneously.
- You can adjust the keyboard layout and screen resolution from within the VM.

All others:

- Use **VirtualBox** (https://www.virtualbox.org/wiki/Downloads) and set up the virtual machine using the provided **Caine_v1.4.ova**.
- We would like to note that it would be beneficial to increase the display memory to at least **64MB**, you can do so after first setting up the virtual machine in (Settings > Display). In addition, we recommend those who can use at least **8GB** of RAM to do so, as some tasks can be very time consuming otherwise (some will take long regardless).
- The evidence file you should use is **Evidence_1.vmdk**.
- The handbook provides a username and a password although they are not necessary to login.
- You can adjust the keyboard layout and screen resolution from within the VM.

7. Disk Analysis

Just a brief note to acknowledge that some of the **Autopsy** related exercises can take a very long time.

7.2 Antivirus Scan

This exercise also takes a very long time, sometimes more than 30 minutes depending on your VM’s configuration.

7.7 System Logs Analysis

If you attempt to lookup Event IDs on the website that is mentioned in the handbook you will find that most of them do not return any results. In fact, only the events logged by the “Microsoft-Windows-Security-Auditing” provider (or the ones corresponding to the “Security” channel) are present. It might be a good idea to focus on those.

The handbook also suggests searching the logs between 14:03:00 and 14:05:00 based on the execution time of THC Hydra. Feel free to explore results outside this timeframe and see if you find any events that could be relevant. It is not guaranteed you will find anything but the idea is for you to put yourself in an investigator’s shoes and explore all avenues that make sense to you.

8.2 Inspecting Registry Timeline

The portion of the exercise that requires the executing **RegRipper** does not work properly and you will not get the same results as the ones referenced in the figures. You should pretend you got a similar result and proceed normally.

8.3 User Assist

The same issue regarding **RegRipper** occurs. Although you will be able to extract some information from executing the provided commands, you’ll find that you will not get the same output as shown in the figures. Yet again, just assume the pictured results are true and move along.

Ex2 - Forensic Analysis: Network Incident Response

1. Introduction to the Training

The “Review from previous training” section lacks a bit of context that you might find interesting. Here is the “background story” that is referenced as well as more detailed results from the first part of the training:

Story

“The customer’s organization has found out that some of its sensitive data has been detected in an online text sharing application. Due to the legal obligations and for business continuity purposes the CSIRT team has been tasked to conduct an incident response and incident investigation to mitigate the threats.

The breach contains sensitive data and includes a threat notice that in a short while more data will follow. As the breach leads to a specific employee’s computer then the CSIRT team, tasked to investigate the incident, follows the leads.

Below is presented a simplified overview of the training technical setup.”

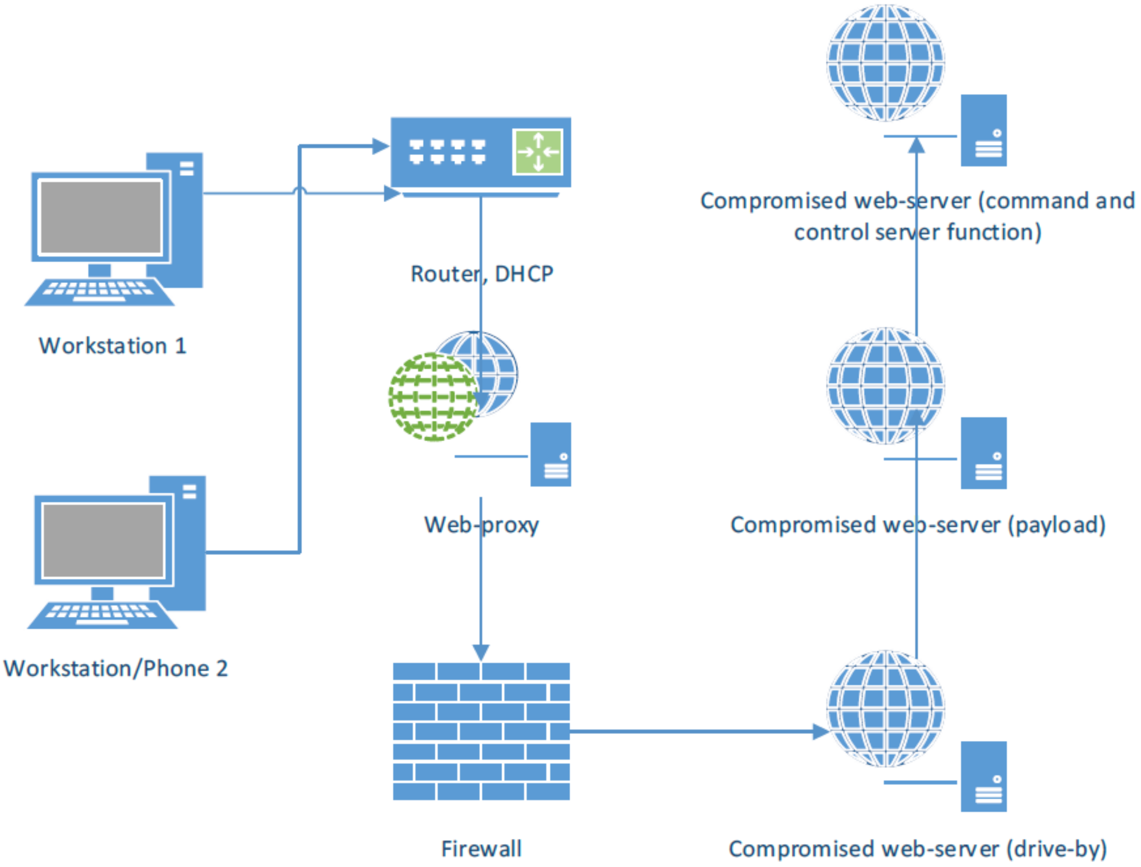
Workstation 1
Workstation/Phone 2
Router, DHCP
Web-proxy
Firewall
Compromised web-server (command and control server function)
Compromised web-server (payload)
Compromised web-server (drive-by)

Figure 1: Network setup

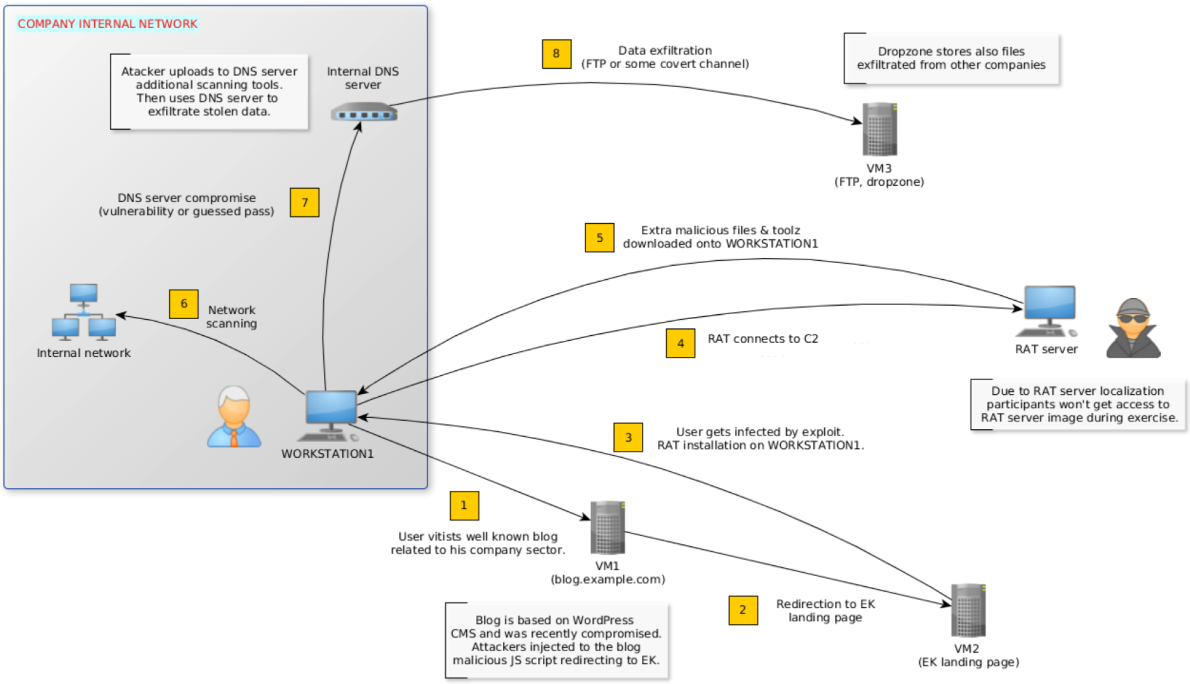
COMPANY INTERNAL NETWORK
Atacker uploads to DNS server additional scanning tools. Then uses DNS server to exfiltrate stolen data.
Internal DNS server
DNS server compromise (vulnerability or guessed pass)
7
6
Network scanning
Internal network
WORKSTATION1
8
Data exfiltration (FTP or some covert channel)
Dropzone stores also files exfiltrated from other companies
VM3 (FTP, dropzone)
5
Extra malicious files & toolz downloaded onto WORKSTATION1
4
RAT connects to C2
RAT server
Due to RAT server localization participants won't get access to RAT server image during exercise.
3
User gets infected by exploit. RAT installation on WORKSTATION1.
1
User vitists well known blog related to his company sector.
VM1 (blog.example.com)
Blog is based on WordPress CMS and was recently compromised. Attackers injected to the blog malicious JS script redirecting to EK.
2
Redirection to EK landing page
VM2 (EK landing page)

Figure 2: Compromise scope

Training 1 Results:

Timeline:

TIMESTAMP [UTC]	OBSERVATION	EVIDENCE SOURCE
12:54:24	Start of System process	Memory analysis
12:54:31	Start of Event log service	System logs
12:55:53	Start of firefox.exe	Prefetch files UserAssist keys
13:02:46	**User visits http://blog.mycompany.ex/**	Firefox history
13:02:50 - 13:03:17	**Browser downloads pages from http://blog.mysportclub.ex/wp-content/uploads/hk/ (EK)**	Firefox history, Filesystem analysis
13:02:53	Creation of Firefox cache file possibly containing exploit code (CVE-2012-3993)	AV scan Filesystem analysis
13:02:56	**Creation of 3568226350[1].exe file (referred in one of the cache files)**	AV scan Filesystem analysis
13:02:57	Creation of svchost.exe binary in %TEMP% directory	Filesystem analysis
13:02:57	Start of svchost.exe process containing Xtreme RAT code	Memory analysis
13:02:57	Modification of Run and RunOnce keys	Registry analysis
13:02:58	Start of second explorer.exe process containing Xtreme RAT code (possible Run PE)	Memory analysis
13:03:04	Start of update.exe process with Xtreme RAT code	Memory analysis
13:03:10	Modification of GhCtxq8t registry key (update.exe)	Registry analysis
13:03:16	Firefox flash plugin crash report	Firefox crash reports
13:07:36	Start of some cmd.exe process	Memory analysis
13:10:03	Creation of 54948tp.exe executable in %TEMP% directory	Filesystem analysis
13:10:13	Execution of 54948tp.exe	Prefetch files
13:10:13-13:14:47	**Time period when http://blog.mysportclub.ex/wp-content/uploads/hk/files/data_32.bin was downloaded**	Python decompilation

13:14:47	Creation of %APPDATA%\EpUpdate folder containing multiple hacking tools	Filesystem analysis
13:14:47	Creation of %TEMP%\SystemProfile folder containing results of execution various commands	Filesystem analysis
13:14:47	Execution of mimikatz.exe and creation of mimikatz.log file	Prefetch files Filesystem analysis
13:14:50	Execution of browserpassworddump.exe and creation of bpd.log	Prefetch files Filesystem analysis
13:34:25	Creation of sysinfo.txt in %TEMP%\SystemProfile	Filesystem analysis
13:42:12	Start of some cmd.exe process	Memory analysis
13:50:29	Start of winpcap-nmap-4.13.exe	UserAssist
13:59:29	**Port scan of 192.168.5.1**	Filesystem analysis
13:59:34	**Port scan of 192.168.5.10**	Filesystem analysis
13:59:36	**Port scan of 192.168.5.15**	Filesystem analysis
14:02:04	**Execution of hydra.exe process (possible dictionary attack)**	System logs
14:04:44	**Execution of Hydra.exe (possible dictionary attack)**	Prefetch files System logs
14:08:30	Start of some cmd.exe process	Memory analysis
14:10:49	**Possible login to some remote host (Plink.exe execution)**	Prefetch files
14:11:20	**Possible login to some remote host (Plink.exe execution)**	Prefetch files
14:11:26	Modification of PuTTY SshHostKeys (RSA key pointing to 192.168.5.10)	Registry analysis
14:17:45	**Possible login to some remote host (Plink.exe execution)**	Prefetch files
14:18:48	Start of some cmd.exe process	Memory analysis
14:20:44	**Possible login to some remote host (Plink.exe execution)**	Prefetch files
14:22:45	**Possible login to some remote host (Plink.exe execution)**	Prefetch files
14:23:02	Start of some cmd.exe process	Memory analysis
14:23:31	**Possible login to some remote host (Plink.exe execution)**	Prefetch files
14:23:46	Start of some cmd.exe process	Memory analysis
14:47:12	**Execution of PSCP tool, possibly to download/upload some data from remote host**	Prefetch files
14:47:54	**execution of PSCP tool, possibly to download/upload some data from remote host**	Prefetch files
14:50:09	**execution of PSCP tool, possibly to download/upload some data from remote host**	Prefetch files

Summary:

“(...)

During the analysis, it was determined that the system was most likely compromised on 2016-08-16 at 13:02:46 after user visited infected website http://blog.mycompany.ex/ which was redirecting to another domain (blog.mysportclub.ex) hosting some exploit kit. As a result, the operating system was infected with Xtreme RAT malware. At 13:10:03, 54948tp.exe executable was created on disk and then executed. As a result, an additional tools pack was downloaded from blog.mysportclub.ex and then unpacked in the local filesystem (%APPDATA%\EpUpdate). An additional directory SystemProfile was created in %TEMP% location.

Among the tools were tools like Nmap, THC-Hydra, Mimikatz, BrowserPasswordDump, Plink and Pscp. This suggests that the attacker’s intention was to gather information about the local system and then possibly compromise other hosts on the network. At 13:59:00, a port scan of three hosts on the local network was performed: 192.168.5.1, 192.168.5.10, 192.168.5.15. Shortly after that, THC-Hydra was executed, possibly to perform some dictionary attack. Then plink/pscp was executed a few times. The RSA key found in the registry suggests that the attacker might have been trying to login to 192.168.5.10 host.

To continue the investigation and find additional information, forensic evidence found on the Windows workstation should be correlated with evidence obtained from other systems, especially network logs, and, if possible, evidence preserved from blog.mysportclub.ex and blog.mycompany.ex.”

2.5 Environment Preparation

Please follow the instructions given for training 1 on how to set up the VMs as they are the same **except** for the fact that you should use **Evidence_2.vmdk (or .qcow2)** as your evidence file.

2.6.1 Task 1: Solution

The **clog** command does not work, you can focus on the log files shown to be “ASCII text”.

2.7.1 Task 2: Solution

This lead has not been referenced before, don’t worry if it is completely new to you.

In the first paragraph of page 16 of the handbook it is said “some flows are MDNS (5353)” but it should say “some flows are LLMNR (5355)”. It can also be interesting to see what services use the other ports not mentioned explicitly in the text.

3.2.1.2 Analysis

Mounting dhcpsrv disc image

- The process starts on page 27 of Exercise1's handbook.
- Make sure to decompress the file before proceeding.
- When issuing the mount command you should **omit the -t optional argument.** You should also **omit "ro" from the -o optional arguments**. It should end up looking something like "sudo mount -o offset=<determine offset> <disk> <mounting_location>".

Timezone

Throughout this section be aware the times may not be in UTC (in fact they are not).

Page 26 - Postfix crashing

On page 26 it is said that the postfix pickup service crashes but none of the shown log segments proves that. In fact this information can be obtained from one of the log files, try to identify which.

Page 28 - Copy of /etc/group

A certain "/etc/cron.hourly/.chkrootkit.swp" is mentioned. Is this the correct file? If not, find the correct file(s).

3.2.1.3 Analysis of ssh and sshd

You will not be able to recover **sshd.OLD**.

Page 30

The analysis of these files will not feel "superficial" unless you know exactly what to look for, don't worry if you need to take your time doing so.

After recovering John's password you can **skip** to the next section as you will not be able to run the v25 command.

3.2.1.4 Analysis of libsecurity.so

Due to **issues concerning volatility** you will be performing this section either but we encourage you to read it nonetheless.

Ex3 - Forensic Analysis: Webserver Analysis

2.1 Case Materials

In case you are running on a Mac with Apple Silicon (M1/M2) processors you should not use the mentioned **.ova** files but instead opt for the **.qcow2** files we provide.

2.2 Forensic Linux distribution

We **highly recommend** using the **ENISA CAINE VM** mentioned in the handbook instead of the Live DVD. Be aware that **the download link does not work**, use the files we provide instead.

To set up the Caine VM please follow the instructions given for Exercise1 on how to set up the VMs. Don't import evidence files for now but make sure you know how to do it for later.

2.3 Using .ova files

Mac users with Apple Silicon hardware may skip this section.

3.3.1 Task 1

Mac users with Apple Silicon hardware may skip the "Import the .ova files working copy into VirtualBox in a way that the image is network isolated" task. The others can import the appliances with default settings (even memory and storage).

You can **ignore the Trainer-related portion** of this task **until page 24** where the handbook goes over how to import the appliances into VirtualBox. Students running on anything other than Apple Silicon hardware can use this section to perform the last task of the student list.

3.4 Part 4: Examination

In order to examine the virtual machines you will be treating each respective disk image as if they were the **evidence files** mentioned in the setting up phase (one at a time in the subsequent tasks). Therefore, each time you want to investigate a different machine you should:

- Unmount the previous evidence disk, if there is one.
- Edit the VM's settings either in VirtualBox or UTM (according to your hardware):
    - Remove the previous evidence disk.
    - Add the new evidence disk (**.vdi or .vmdk** for VirtualBox and **.qcow2** for UTM).
    - Boot up the VM and mount the evidence disk as per the instructions.

Note that instead of a single device (shown in the tutorial) there will be several you need to mount (the ones named **/dev/mapper/***).

In order to get the memory dump file in the VM you can either try using shared folders (sharing the working copy you made) or download it directly from the link in the course's page from within the VM (this is a workaround, you can treat the newly downloaded file as if it were the working copy you made).

The information pertaining to "Evidence summary.docx" can be found here.

Throughout this exercise you may find yourself struggling to make sense of the timestamps, don't waste too much time on that, your questions will, most likely, be answered later.

3.4.1 Task 2

If you are using the **ENISA CAINE VM**, as we recommend, you can skip the trainer portion **until page 30** (in fact, you will be ignoring everything that mentions the **CAINE ISO** as you are not using it). On page 30, if you have already mounted the evidence devices you don't need to do it again.

3.4.3 Task 4

If you are using the **ENISA CAINE VM** you don't need to install Volatility as it is already installed. You can find it in "~/training/tools/volatility/". The "LinuxDebian84x86" profile should also be installed already.