Prepare your Laptop

Spinning up those disks!

Laptop requirements
("what you should have brought")

- x86-compatible or x64-compatible 2.0 GHz CPU minimum or higher
- 4 GB RAM minimum with 8 GB or higher recommended
- Internet connectivity
- 80 GB available hard-drive space
- A working copy of VMWare Workstation, Fusion or Player to run our virtual images
- USB port
- A functioning, non-intoxicated brain

Preparing your system
('what you should do now")

- Copy over the files to your hard disk
- When asked by VMWare … you have MOVED this system, not copied
- Do NOT start the virtual machine yet (or you are fscked)

SECURITY. RESEARCH. RISK.

Workshop – Incident Response

BruCON 2015

Objectives

11.00 – Briefing

11.15 – Analysis

12.15 – Update + Next Steps

13.15 – Update + Next Steps

14.15 – Update + Next Steps

15.15 – Update + Next Steps (Optional)

15.45 – Solution and Conclusions

nviso
SECURITY. RESEARCH. RISK.

Objectives

Experience a simulated real-life incident

Understand your strengths and weaknesses by practicing

Learn to ask the right questions

Analyse Threat -> Mitigate Impact -> Active Defense

Your Spiritual Guides

Pieter Danhieux

Instructor, SANS Institute

CEO, Secure Code Warrior

Strategy & Research, NVISO

Erik Van Buggenhout

Instructor, SANS Institute

Director, NVISO

Cyber Resiliency

Prepare your Laptop

Spinning up those disks!

Laptop requirements
("what you should have brought")

- x86-compatible or x64-compatible 2.0 GHz CPU minimum or higher
- 4 GB RAM minimum with 8 GB or higher recommended
- Internet connectivity
- 80 GB available hard-drive space
- A working copy of VMWare Workstation, Fusion or Player to run our virtual images
- USB port
- A functioning, non-intoxicated brain

Preparing your system
('what you should do now")

- Copy over the files to your hard disk
- When asked by VMWare … you have MOVED this system, not copied
- Do NOT start the virtual machine yet (or you are fscked)

Rules of the Workshop

Setting the stage…

We are representing your client, the meat manufacturer "Jurasic Pork"

"One of our employees, Seymour Buttz, came to us yesterday mentioning that something went wrong with his workstation. We couldn't really understand what he was saying, so we've called upon you to help sort this out as soon as possible…"

- You can ask us questions, you probably should… Just like in real-life
- We'll try to help, but we're not the most technical guys… We might not always understand or could need some time to get the stuff you need (e.g. additional data from other systems)
- We already provide you with the workstation of Seymour Buttz
- Do not attack any system without asking permission!

Guidance

How to get started?

Step 0 – Understand the context and environment of the problem

Interview with Seymour Buttz

Network diagram

Step 0 – Understand the context and environment of the problem

Interview notes with the workstation owner

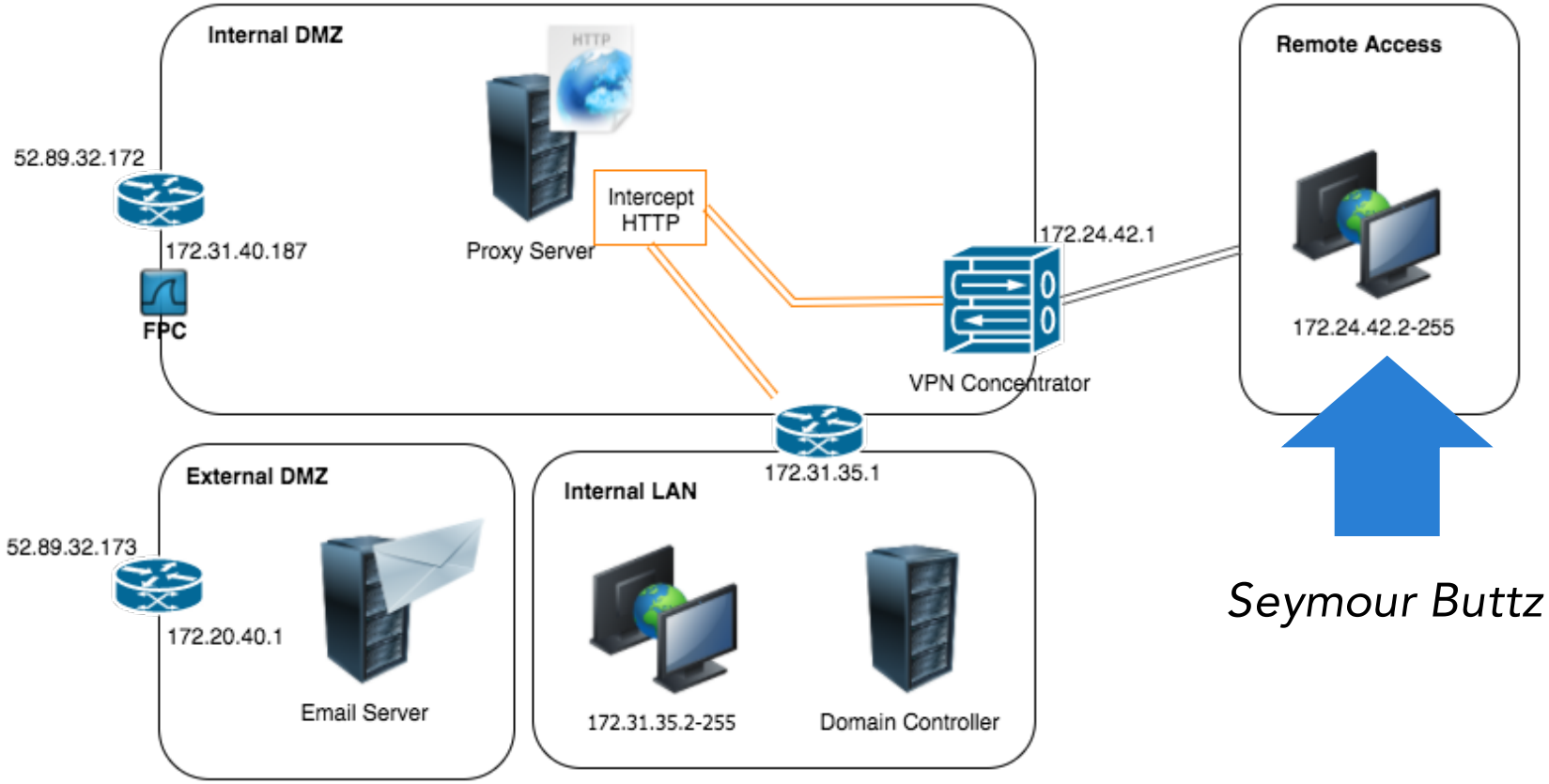
"I work in the IT department at Jurassic Pork and I was working from our home that day. I checked my emails and read some news from IT sites. I can't remember if anything special happened. My computer was a bit slow but we are working with these old machines that are running Windows 7.

I have complained about that to my boss for a few months now. They need to invest some more time and money in IT. Since they installed that anti-virus system, my laptop is slower that the computer of my wife.

I did download some files during the day that I needed and I connected to other systems in the network to do my work. Suddenly, I needed some files that I stored in C:\secrets.txt and noticed I couldn't open it anymore. Weird stuff. That's when I called the helpdesk. I know that file was there and I could use it the day before."

Step 0 – Understand the context and environment of the problem

Network diagram



Step 1 – Analyse the workstation to obtain a basic understanding of the issue

We have provided you with the live system as a VMware image. Note that the VMware image has been shut down to prevent "suspend" / "resume" difficulties. In order to obtain access to the "live" state when Seymour Buttz was last using the image, please revert to the Snapshot that has been created.

Feel free to use the workstation as you see fit. Note that the workstation has been disconnected from the network for obvious reasons.

Your Turn

Next Guidance – 12h15

Objective: find out what's going on with C:\secrets.txt and if it's an incident

Guidance

How to get started?

Step 0 – Understand the context and environment of the problem

Interview with Seymour Buttz

Network diagram

Step 1 – Analyse the workstation to obtain a basic understanding of the issue

Disk image?

Browser history?

Memory analysis?

…

Have a look at archive Evidence-003.7z

Use password **NVISO@BruCON!**

Your Turn

Next Guidance – 13h15

Objective: help recovering the c:\secrets.txt file

Guidance

How to get started?

Step 0 – Understand the context and environment of the problem

Interview with Seymour Buttz

Network diagram

Step 1 – Analyse the workstation to obtain a basic understanding of the issue

Disk image?

Browser history?

Memory analysis?

…

Step 2 – Request additional information?

What are you missing? What more would you like?
ASK US

Have a look at archive Evidence-001.7z
Use password **ErikIsTheGreatest!**

Your Turn

Next Guidance – 14h15

Objective: help recovering the c:\secrets.txt file

Guidance

How to get started?

Step 0 – Understand the context and environment of the problem

Interview with Seymour Buttz

Network diagram

Step 1 – Analyse the workstation to obtain a basic understanding of the issue

Disk image?

Browser history?

Memory analysis?

…

Step 2 – Request additional information?

What are you missing? What more would you like?
ASK US

Have a look at archive Evidence-002.7z
Use password **PieterIsAlsoQuiteOK!**

Your Turn

Next Guidance – 15h15

(Optional) Objective: find out who our threats are

Walkthrough

How you could have solved it…

- From the interview and the workstation, you could have guessed it would have been something ransomware-related (the secrets.txt file looks encrypted / obfuscated / …). If you know how ransomware works, you probably know it means that an **encryption key** was used to encrypt the information, but the encryption key will most likely be stored remotely by an attacker… Let's try finding it!

- By using notepad and reviewing the proxy logs, you could have spotted there is one request where an actual **IP address** is used instead of a hostname. There is also a "**hiw**" parameter being sent across (which, after URL decoding, looks awfully lot like a **MAC address**). Could this be the seed for the encryption algorithm?

- In the memory dump, you could have spotted the **video_viewer.exe** executable, with the cunning process description of "PoC ransomware". By extracting this executable from the memory dump (e.g. using volatility) and analyzing it in a sandbox, you could identify the **IP address of the C&C.**

- By analyzing all traffic in the network capture (PCAP) towards the malicious IP address, you could have found the **encryption key** being sent in the response to the request where the MAC address was being sent through.