



Conversation with:
Itzel Coba Espinosa
Computer Network Defense Auditor

Vulnerability Analysis Challenge Chat Transcript

Itzel sent:

Hello, @playerone! I'm Itzel, I'm a Computer Network Defense Auditor here at TryCyber University.

Welcome to the team! I'll be your mentor while you're interning here. 🎓

Itzel sent:

I'll introduce you to some of the core **Vulnerability Analysis** tasks. Today, I'm going to have you assist me with a few of my simpler tasks on the **Ubuntu 22.04 Linux** workstation you are looking at now.

Itzel sent:

The tasks we will be doing today will be completed using the **Terminal** and the **Report Form**. The Terminal can be intimidating if you have not used it before. So let me know if you want a brief tutorial on it.

Itzel sent:

So, are you ready to get started? 😊

Participant sent:
Terminal tutorial, please!

Itzel sent:

The **Terminal** is primarily used to access an application called a shell. We interact with shells via a **command-line interface (CLI)** where we input and execute text-based commands on a system.

Itzel sent:

Let's open the Terminal on this system now and run a few basic commands so you get the hang of it. You can open the **Terminal** by double-clicking the icon on the desktop named **Terminal Emulator**. It should look like this once you have it open...

Itzel sent:

```
Terminal - playerone@workstation: ~
File Edit View Terminal Tabs Help
playerone@workstation:~$
```

Participant sent:
I've opened the Terminal.

Itzel sent:

Great. Basically, you type commands into the shell within the Terminal and then hit `Enter` or `Return` on the keyboard to run the command.

Itzel sent:

To properly utilize any CLI command, you must understand its format, options, and other arguments. The **format** defines the structure and order of options and other arguments, the **options** define or modify behavior, and the **arguments** are command defined input types (e.g., files, directories, users, software packages, etc.).

Itzel sent:

Additionally, all CLI commands on this system are case-sensitive, so pay close attention to the capitalization of letters.

Itzel sent:

The basic command format is...

```
command [OPTIONS] [ARGUMENTS]
```

However, it varies a lot from command to command, and options and other arguments are not always required.

Itzel sent:

An example of a command that does not require any options or other arguments is `whoami`. If you type `whoami` into the shell and then hit `Enter` or `Return` on the keyboard, the `whoami` command will output the name of the user running the command into the Terminal. It should look like this if you run that command...

Itzel sent:

```
playerone@workstation:~$ whoami  
playerone
```

Participant sent:

What's a more involved example?

Itzel sent:

I'll give you a more complex example using the `ls` command.

Itzel sent:

In this example, we will use the `ls` command to list detailed information about the entire contents of the `Templates` directory (i.e., folder) in your (playerone's) `home` directory. Our example `ls` command will use the following format...

```
ls [OPTIONS] [DIRECTORY]
```

Note that in this case, the command's argument requires the input to be a directory.

Itzel sent:

The actual command we want to run is...

```
ls -a -l /home/playerone/Templates
```

Itzel sent:

The `-a` and the `-l` are both options that modify the `ls` command's behavior, and `/home/playerone/Templates` is our argument which is a directory provided in the form of a path.

Itzel sent:

For this command's argument, we must provide the **path** to the directory from the root of the file system; otherwise, the system won't know which directory named `Templates` we are referring to.

Itzel sent:

And finally, when you run that command, the output should look like this...

Itzel sent:

```
playerone@workstation:~$ ls -a -l /home/playerone/Templates/
total 24
drwxr-xr-x  2 playerone playerone 4096 Jul 12 21:36 .
drwxr-x--- 14 playerone playerone 4096 Jul 12 21:36 ..
-rw-r--r--  1 playerone playerone 6859 Apr  9 2022 'OpenDocument Spreadsheet.ods'
-rw-r--r--  1 playerone playerone 7388 Apr  9 2022 'OpenDocument Text.odt'
-rw-r--r--  1 playerone playerone   0 Apr  9 2022 'Plain Text.txt'
```

Participant sent:
Got it. Any extra notes?

Itzel sent:

The Terminal and shells are incredibly powerful and versatile tools. Not all commands and programs follow the general structure I've provided you with here. Unfortunately, we only have time to cover the basics, but I do have a few last things I'd like to mention.

Itzel sent:

Some commands will not print visual output to the Terminal in normal operation, such as the `cp` command, which is used to copy files and directories.

Itzel sent:

Many commands can use multiple arguments, handle multiple input types for arguments (e.g., file and/or directory paths), or have options that will have their own arguments.

Itzel sent:

Some options can, or must be, written in a long-form format (e.g., `ls --all [DIRECTORY]` is the same as `ls -a [DIRECTORY]`).

Itzel sent:

Options without arguments can often be provided together and in any order (e.g., `ls -la [DIRECTORY]` is the same as `ls -a -l [DIRECTORY]`).

Itzel sent:

And last, but certainly not least, you can almost always reference a command's format, options, and other arguments using the command `man [COMMAND]` (e.g., `man cp`) to view the provided command's manual page in the Terminal.

Itzel sent:

Hopefully that was not too much information! I know it seems like a lot, but it gets easier the more you use it. For today's tasks, I'll be sure to provide you with more details for any commands and programs you'll need.

Participant sent:

Sounds good! I'm ready to get started!

Itzel sent:

Perfect!

Itzel sent:

Today, we are going to use one of the university's simpler policy documents to perform a basic audit on this Ubuntu Workstation.

Itzel sent:

Performing vulnerability audits and reporting the results of those audits are some of the most common Vulnerability Analysis tasks!

Itzel sent:

Before we get into the audit, let's briefly discuss the university's **cybersecurity policies**.

Itzel sent:

Here at the university, we have numerous cybersecurity policies that, *when followed*, enhance our computer systems' availability, integrity, and confidentiality. Many of our cybersecurity policies, like the one we will be looking at today, include and reference matching **Vulnerability Identifiers (Vul IDs)** from applicable **Security Technical Implementation Guides (STIGs)**.

Itzel sent:

STIGs, which are created by the Defense Information Systems Agency (DISA), are essentially guides that help us check our systems for known vulnerabilities.

Itzel sent:

We use the STIGs embedded in our cybersecurity policies to audit the university's computer systems and ensure the policies are being followed. When a policy is not being followed, and a vulnerability is found, it's called a **finding**.

Itzel sent:

If there are any findings during our audit, we need to add the details of the finding to our audit report.

Participant sent:
Got it.

Itzel sent:

Now that we've covered some of the basics, let's start our audit!

Itzel sent:

The policy document you will need to reference for today's audit is in the `Materials` folder on the workstation desktop. It is a one-page PDF document named `security_policy.pdf`.

Itzel sent:

To open this PDF document, you will want to double-click the `Materials` folder on the desktop, then double-click the `security_policy.pdf` file. This will open the PDF in the default PDF viewer on the workstation. It should look something like this once you have it open...

Itzel sent:

security_policy.pdf - 1/1 (96 dpi)

Default Filesystem Permissions, and Password Encryption Policy

Policy Statement: This policy establishes guidelines for default filesystem permissions and password encryption on the Ubuntu operating system. It aims to enhance the security and integrity of our organization's information systems by enforcing appropriate file access controls and encrypting stored passwords.

1. Password Encryption with FIPS 140-2 Approved Algorithm (SHA512) (Vul ID: V-238325):

1.1. The Ubuntu operating system must encrypt all stored group passwords using the SHA512 cryptographic hashing algorithm.

1.2. Encryption is crucial for protecting passwords from unauthorized access and compromise.

1.3. Use the following information pulled from DISA Security Technical Implementation Guides to assess the current hashing algorithm for group passwords and to resolve any issues found.

Vul ID: V-238325
Check Content: Check the hashing algorithm that is being used to hash passwords with the following command: <pre>\$ cat /etc/login.defs grep -i encrypt_method</pre> If "ENCRYPT_METHOD" is not set to SHA512 this is a finding and will need to be resolved
Fix Text: Edit/modify the following line in the "/etc/login.defs" file and set "ENCRYPT_METHOD" to

Participant sent:
I've got it open!

Itzel sent:

Great!

Itzel sent:

As you can see, this policy document has two sections, and while I'd encourage you to review the whole policy, we need to focus on the STIG Vul excerpts to audit the workstation.

Itzel sent:

Each policy section contains a matching STIG Vul excerpt embedded at the bottom of the policy within a box with a black outline. The STIG Vul excerpts start with the Vul ID (e.g., Vul ID: V-###), which is then followed by details on how to check for and fix the corresponding vulnerability.

Itzel sent:

For each policy section, we will be using the information and Terminal command in the STIG Vul excerpt's **Check Content** section to audit a specific setting on the workstation.

Itzel sent:

Oh, and this is very important, if we do have a finding during this audit, it is very important that you DO NOT attempt to fix the issue. Our job is to assess the state of the system and report on its compliance.

Itzel sent:

Alright, with that out the way, let's start our audit with the first policy section listed in this document, **Password Encryption with FIPS 140-2 Approved Algorithm (SHA512) (Vul ID: V-238325)**. Let me know once you've reviewed it.

Participant sent:

I've reviewed it.

Itzel sent:

Sweet!

Itzel sent:

For this first policy section, we need to check that the hashing algorithm used on this workstation to hash passwords is **set to SHA512**. To do that, we need to run the command provided in the **Check Content** section of the STIG Vul excerpt in the Terminal. The provided command being...

```
cat /etc/login.defs | grep -i encrypt_method
```

Note that the character between the end of the `cat` command and the beginning of the `grep` command is a pipe character (i.e., `|`) and not the letter `l` or the number `1`. You can usually find the pipe character on your keyboard on the key above your `Enter` or `Return` key.

Itzel sent:

The command the STIG Vul is having us run basically outputs all lines within the configuration file `login.defs` (which resides in the `etc` directory) that contain the case-insensitive pattern `encrypt_method`. While this is going to return some lines we don't care about (e.g., lines containing comments, which start with `#`), it will also have the line we do care about, which is formatted `ENCRYPT_METHOD [HASHING ALGORITHM]`.

Itzel sent:

You should see it when you run the command, which has output that looks like this...

Itzel sent:

```
Terminal - playerone@workstation: ~
File Edit View Terminal Tabs Help
playerone@workstation:~$ cat /etc/login.defs | grep -i encrypt_
method
# This variable is deprecated. You should use ENCRYPT_METHOD.
ENCRYPT_METHOD MD5
# Only used if ENCRYPT_METHOD is set to SHA256 or SHA512.
playerone@workstation:~$
```

Itzel sent:

Uh oh! It looks like `ENCRYPT_METHOD` isn't configured per the policy! Instead of using the `SHA512` hashing algorithm, this workstation is currently using the `MD5` hashing algorithm. It looks like we've got our first finding!

Participant sent:
What do we do now?

Itzel sent:

Every time we audit a policy section, finding or no finding, we need to **add an entry** to the audit report. You will need to use the **Report Form** to add an entry to the audit report. (Note: You can find the Report Form on the Report Tab)

Itzel sent:

Using the Report Form, you will document the results of your policy section audit, including the **policy section's title**, if there was a **finding**, and, in the case of a finding, what **improper configuration** was found.

Itzel sent:

Let me know when you've successfully added the entry to the report with the Report Form or if you'd like some extra help. 😊

Participant sent:
Help, please!

Itzel sent:

Of course!

Itzel sent:

Let's quickly review the details of our audit so far. We audited the policy section **Password Encryption with FIPS 140-2 Approved Algorithm (SHA512) (Vul ID: V-238325)**. When we ran the Terminal command in the **Check Content** section of this policy section, we found a line in the `login.defs` configuration file that read `ENCRYPT_METHOD MD5`, which means the `ENCRYPT_METHOD` setting is set to `MD5` rather than what the policy calls for. This resulted in a finding for this policy section.

Itzel sent:

So, for this policy section's entry in our audit report, you need to input the following via the Report Form...

Which policy section is this submission for?: **Password Encryption**

Does this submission include a finding?: **Yes**

If there is a finding, provide the contents of the line in the configuration file that resulted in the finding. `ENCRYPT_METHOD MD5`

Itzel sent:

Let me know once you've successfully added this policy section's entry so we can keep going.

Participant sent:
I'm done.

Itzel sent:

Nice Job! 🎉

Itzel sent:

Crud... I just got called into an important meeting. So, I won't be able to finish this audit with you.



Itzel sent:

However, I'm sure you can handle auditing and reporting on the second and last policy section in the `security_policy.pdf` document, the **Default Filesystem Permissions (Vul ID: V-238209)** policy section.

Itzel sent:

I checked the policy section already, and I'm sure you can do it. The **Check Content** section of the STIG Vul for the **Default Filesystem Permissions (Vul ID: V-238209)** policy uses a simpler Terminal command than the previous policy, and whatever the result of the policy section audit you need only add one more entry to the audit report via the **Report Form**.

Itzel sent:

Alright, I'm headed out. Good luck!

TRY
CYBER

© 2023 Try Cyber - Sponsored by CISA

TRY
CYBER