**Team Access Tutorial: GMU Honeypot EC2 Instance**

**Complete Beginner's Guide - No Linux Experience Required**

**What You'll Learn**

* How to connect to our cloud server (EC2 instance)
* Basic commands to monitor our honeypot
* How to work as a team on this project

**Step 1: Install WSL2 (Linux on Windows)**

**What is WSL?** It's a way to run Linux commands on Windows.

1. **Open PowerShell as Administrator:**    - Press Windows key + X    - Click "Windows PowerShell (Admin)" or "Terminal (Admin)"    - Click "Yes" when prompted
2. **Install WSL:**    ```powershell

   wsl --install    ```    - Wait for installation to complete    - **Restart your computer** when prompted

1. **After restart:**    - WSL will automatically open    - Create a username and password (remember these!)

**Step 2: Install VS Code (if you don't have it)**

1. Download from: <https://code.visualstudio.com/>
2. Install with default settings
3. Open VS Code
4. Install the "Remote - WSL" extension:    - Click Extensions icon (4 squares) on left sidebar    - Search "Remote WSL"    - Click "Install" on the Microsoft one

**Step 3: Open WSL in VS Code**

1. **Open VS Code**
2. **Press Ctrl + Shift + P**
3. **Type:** WSL: Connect to WSL
4. **Press Enter**
5. **A new VS Code window opens** - this is connected to Linux!

**Step 4: Get the SSH Key File**

**I will send you a file called gmu-honeypot-key.pem**

1. **Save it to your Downloads folder**
2. **In VS Code WSL terminal** (bottom panel), type:    ```bash

   mkdir ~/.ssh    ```    - This creates a hidden folder for security keys

1. **Copy the key file:**    ```bash

   cp /mnt/c/Users/YourWindowsUsername/Downloads/gmu-honeypot-key.pem ~/.ssh/    ```    - Replace YourWindowsUsername with your actual Windows username    - \*\*Example:\*\* cp /mnt/c/Users/John/Downloads/gmu-honeypot-key.pem ~/.ssh/

1. **Set correct permissions** (important for security):    ```bash

   chmod 400 ~/.ssh/gmu-honeypot-key.pem    ```

**Step 5: Test Connection to Our Server**

**Type this command exactly:**

ssh -i ~/.ssh/gmu-honeypot-key.pem ec2-user@44.222.200.1

**What this means:**

* ssh = connect to another computer
* -i ~/.ssh/gmu-honeypot-key.pem = use this key file
* ec2-user = username on the server
* 44.222.200.1 = our server's address

**If successful, you'll see:**

[ec2-user@ip-172-31-21-182 ~]$

**Congratulations! You're now connected to our cloud server!**

**Step 6: Make Connection Easier**

**Instead of typing that long command every time, let's create a shortcut:**

1. **Type:** nano ~/.bashrc    - This opens a text editor
2. **Use arrow keys to go to the bottom**
3. **Add this line:**    ```bash

   alias ec2='ssh -i ~/.ssh/gmu-honeypot-key.pem [ec2-user@44.222.200.1](mailto:ec2-user@44.222.200.1)'    ```

1. **Save and exit:**    - Press Ctrl + X    - Press Y (yes to save)    - Press Enter
2. **Activate the shortcut:**    ```bash

   source ~/.bashrc    ```

**Now you can connect with just:**

ec2

**Basic Linux Commands You'll Need**

**Navigation:**

pwd                    # Shows current folder location

ls                     # Lists files in current folder

ls -la                 # Lists all files with details

cd /path/to/folder     # Changes to a folder

cd ~                   # Goes to your home folder

**Viewing Files:**

cat filename.txt       # Shows entire file content

head filename.txt      # Shows first 10 lines

tail filename.txt      # Shows last 10 lines

tail -f filename.txt   # Shows last lines and keeps updating

**Basic Operations:**

sudo command           # Runs command as administrator

exit                   # Disconnects from server

clear                  # Clears the screen

**Honeypot Commands (Copy & Paste These)**

**Check if honeypot is running:**

sudo netstat -tlnp | grep 2222

* If you see output, it's running
* If no output, it's stopped

**View live honeypot activity:**

sudo tail -f /opt/cowrie/var/log/cowrie/cowrie.log

* Press Ctrl + C to stop viewing

**Test the honeypot (open a second terminal):**

ssh -p 2222 root@44.222.200.1

* This connects to our fake server
* Try commands like ls, whoami, cat /etc/passwd
* Type exit to disconnect

**Start/Stop honeypot (coordinate with team first!):**

# Stop honeypot

sudo -u cowrie python3.10 /opt/cowrie/src/cowrie/scripts/cowrie.py stop

# Start honeypot

sudo -u cowrie python3.10 /opt/cowrie/src/cowrie/scripts/cowrie.py start

**Understanding the Terminal Prompt**

When you see:

[ec2-user@ip-172-31-21-182 ~]$

This means:

* ec2-user = your username
* ip-172-31-21-182 = server name
* ~ = you're in your home folder
* $ = ready for your command

**Common Beginner Mistakes**

**"Permission denied" error:**

* Make sure you typed the command exactly
* Check that the key file has correct permissions: chmod 400 ~/.ssh/gmu-honeypot-key.pem

**"Connection refused" error:**

* The server might be stopped
* Contact team leader

**"No such file or directory":**

* Check your spelling
* Make sure you're in the right folder with pwd

**Stuck in a command:**

* Press Ctrl + C to cancel
* Press Ctrl + D to exit

**Team Coordination Rules**

1. **Always announce in team chat before:**    - Stopping the honeypot    - Making configuration changes    - Running tests that might affect others
2. **Share interesting findings:**    - Screenshot unusual log entries    - Document attack patterns you notice
3. **Don't panic if something breaks:**    - Take a screenshot of the error    - Ask for help in team chat    - Don't try to "fix" things you don't understand

**Getting Help**

**If you're stuck:**

1. Take a screenshot of your terminal
2. Copy the exact error message
3. Ask in team chat with context: "I was trying to [do what] and got this error: [paste error]"

**Useful keyboard shortcuts:**

* Ctrl + C = Cancel current command
* Ctrl + D = Exit/logout
* Ctrl + L = Clear screen (same as clear)
* Up arrow = Previous command
* Tab = Auto-complete file/folder names

**Project Overview**

**What we're doing:**

* Running a "honeypot" - a fake server that attracts hackers
* Monitoring who tries to break in and what they do
* Analyzing attack patterns for our cybersecurity project

**Your role:**

* Help monitor the honeypot
* Document interesting attacks
* Learn about cybersecurity through hands-on experience

**Remember:** This is a learning environment. It's okay to make mistakes - that's how we learn!

**Questions?** Contact the team leader or ask in our team chat.