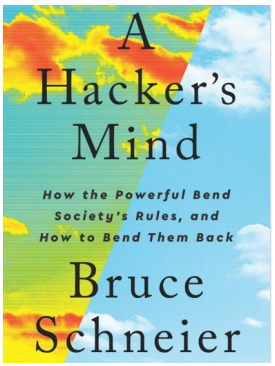
Recipes for Computing

Bespoke code in custom environments

The mission of this paper is to publicize my “Hacking as a Service” tools and sell services in support on my tools, to help you “hack”.

An attempt to create a hacking as a service business in one night.

Ethics	
Do nothing malicious.	 Hacking as generally defined by Bruce Schneier is “doing something allowed by the rules”, that is beyond original “intentions” of a systems.

Project Scope

Where it started.

Final Project was going to be execution of one system command found in a Linux Commands Cheat Sheet.

```
~$ sudo shutdown -n now
```

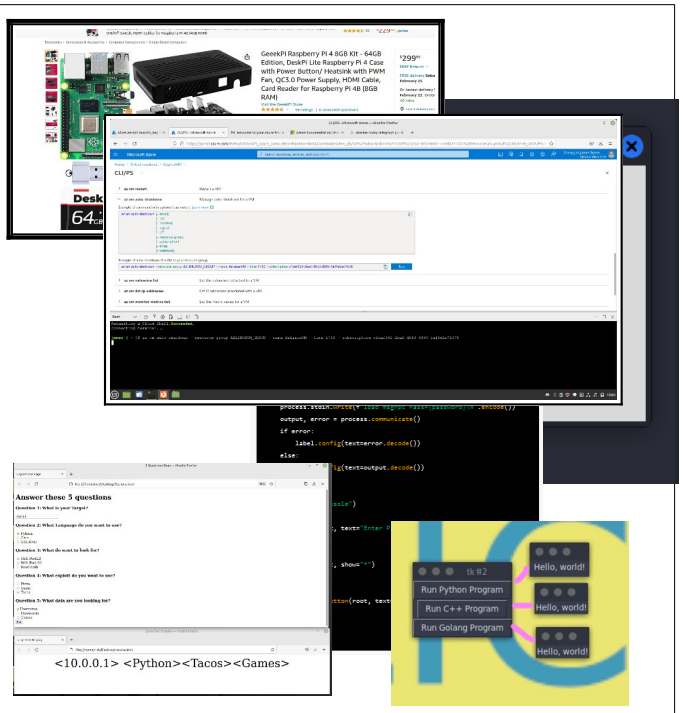
Where it’s going.

Full spectrum service form edge computers, to cloud

Easy to use Graphical User Interfaces

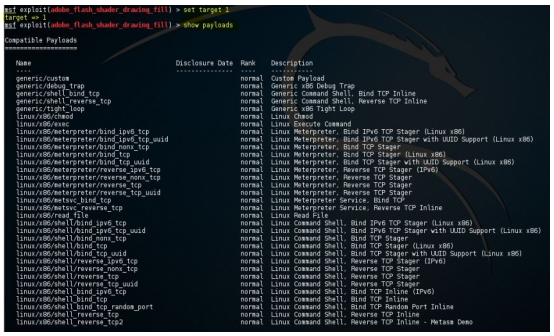
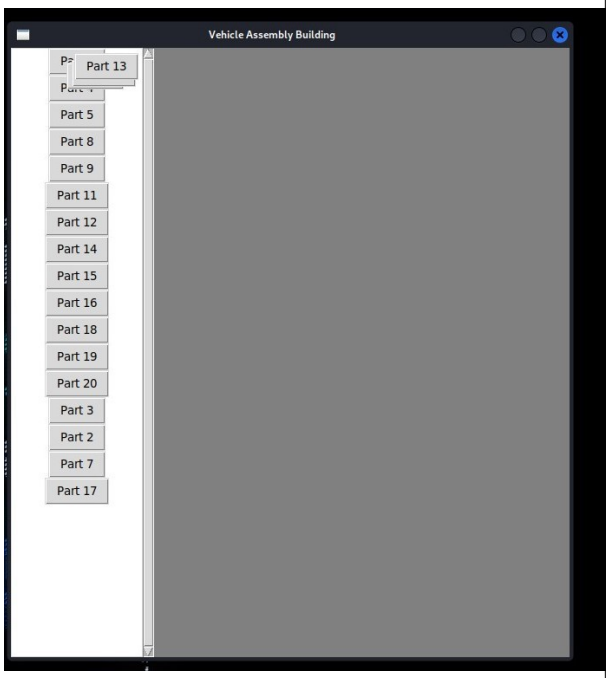
Complex Chained operations.

Unique code for each new operations prevents learned countermeasures.



Introducing “AttackEM” Multi-tool

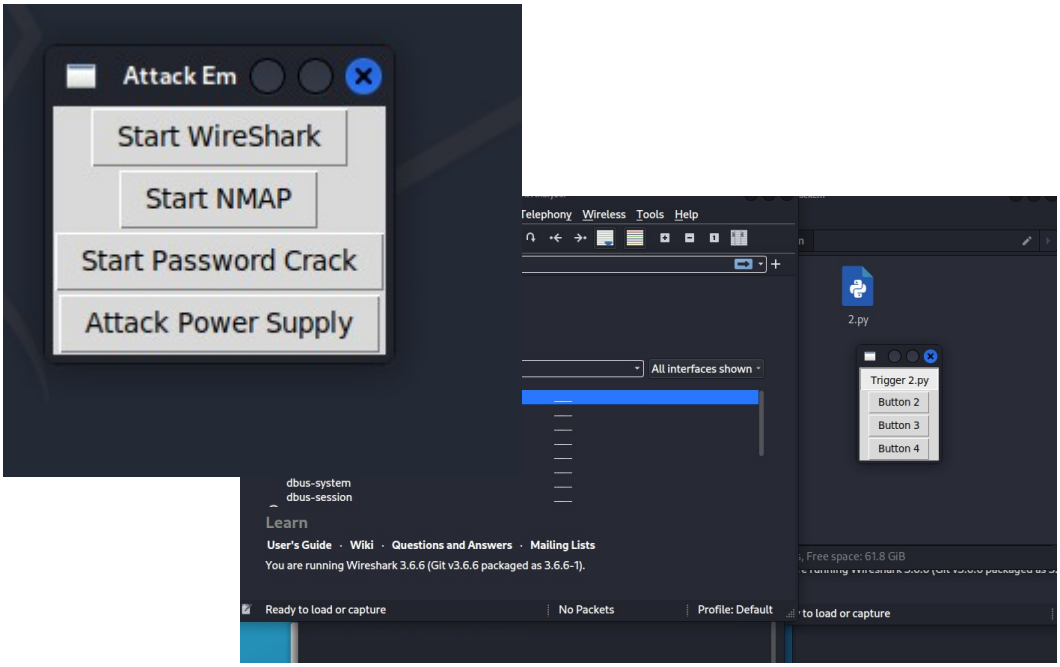
Graphical User Interface is a strategic advantage

Their tool is ugly and hard to use.	Our tool is clear to see and easy to use.
	

The way forward is clear with AttackEM

Menu's follow the logic of the Cyber Kill Chain

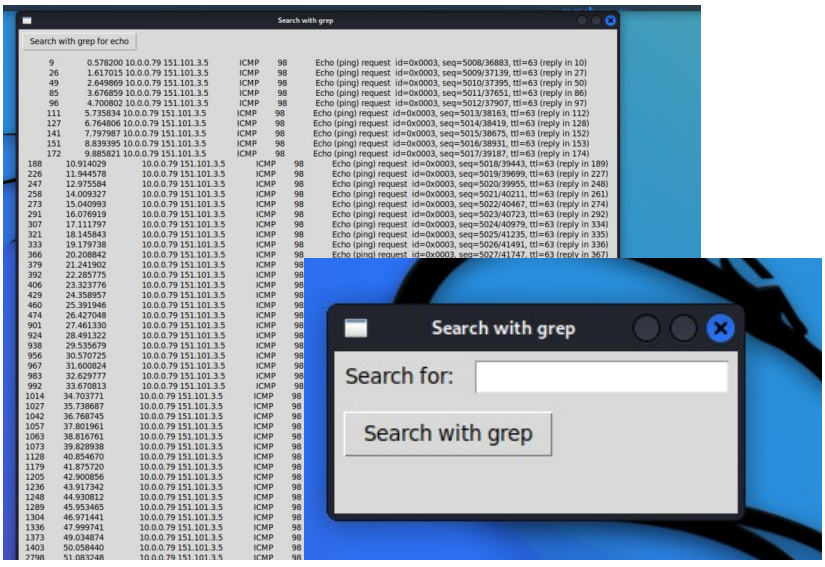
Manage Powerful Tools in an orderly environment



Find Valuable information, sort it and pass it up the chain for the next process.

Use powerful databases to find the data you need.

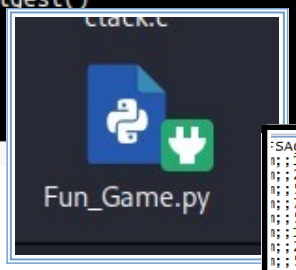
Use it for the next step.

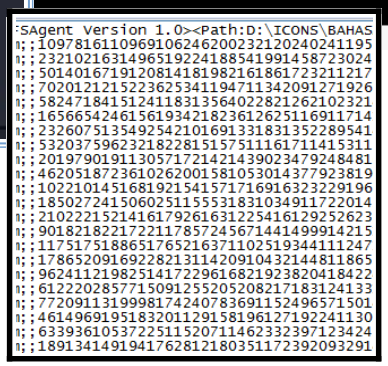


Secure Files are unreadable to others.

Powerful hash technology protects your work.

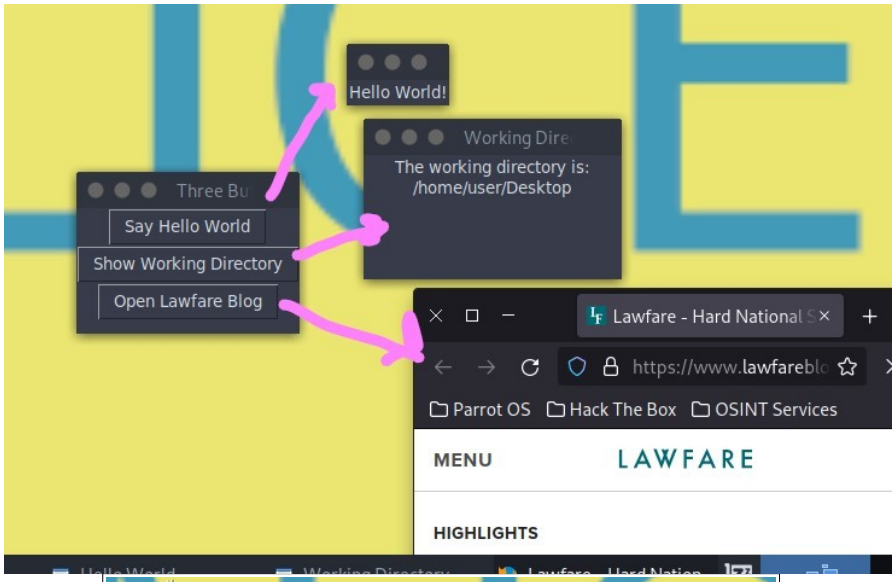
```python
import hashlib

# Open the Python file in binary mode
with open('example.py', 'rb') as f:
    # Read the contents of the file
    file_contents = f.read()
    # Hash the contents using the SHA256 algorithm
    hash_object = hashlib.sha256(file_contents)
    # Get the hex representation of the hash value
    hex_dig = hash_object.hexdigest()
    # Print the hash value
    print(hex_dig)
```

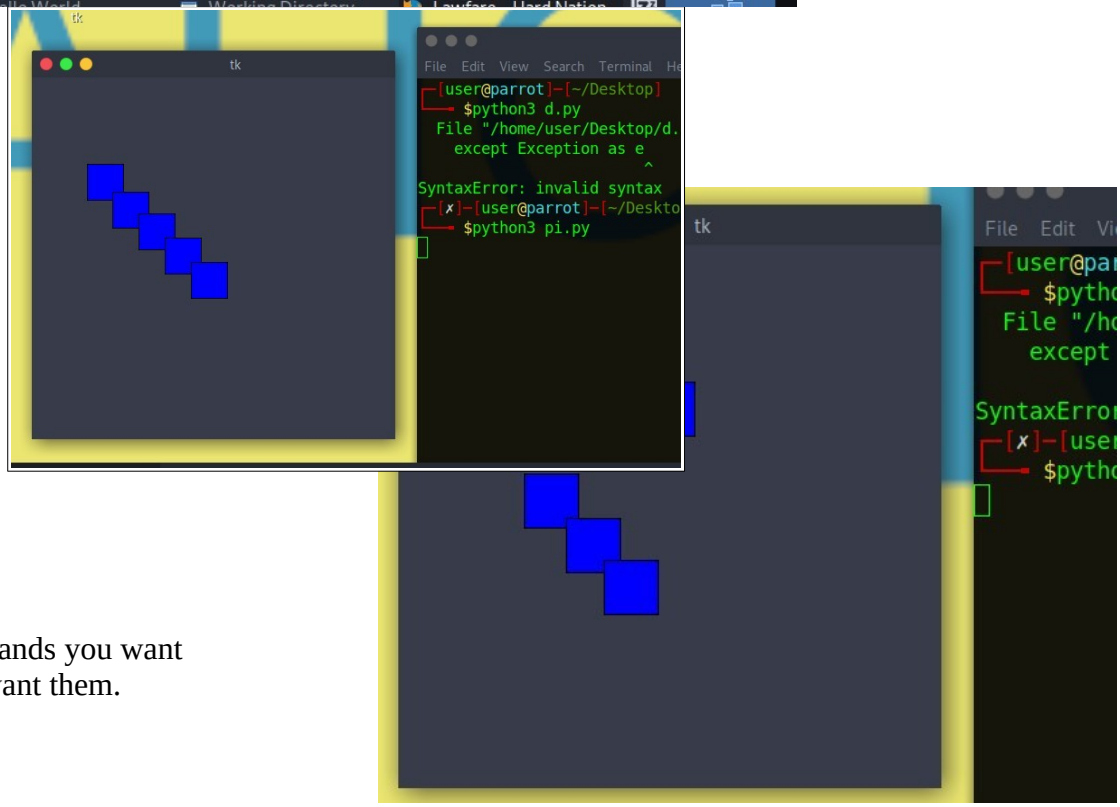



SAgent Version 1.0><Path:D:\ICONS\BAHAS
109781611096910624620023212024024119
232102163149651922418854199145872302
501401671912081418198216186172321121
702012121522362534119471134209127192
582471841512411831356402282126210232
165665424615619342182361262511691171
232607513549254210169133183135228954
532037596232182281515751116171141531
201979019113057172142143902347924848
462051872361026200158105301437792381
102210145168192154157171691632292196
185027241506025115553183103491172201
210222152141617926163122541612925262
901821822172211785724567144149991421
117517518865176521637110251934411124
178652091692282131142091043214481186
962411219825141722961682192382041842
612220285771509125520520821718312413
772091131999817424078369115249657150
461496919518320112915819612719224113
633936105372251152071146233239712342
189134149194176281218035117239209329
```
```

A Pallet for Computer Artists

Think more about what you want to do the “how to” is now easy.





The commands you want how you want them.

Generate Unique Code

AttackEM helps you use unique code for each new operation.

```python
print("Hello World!")
```

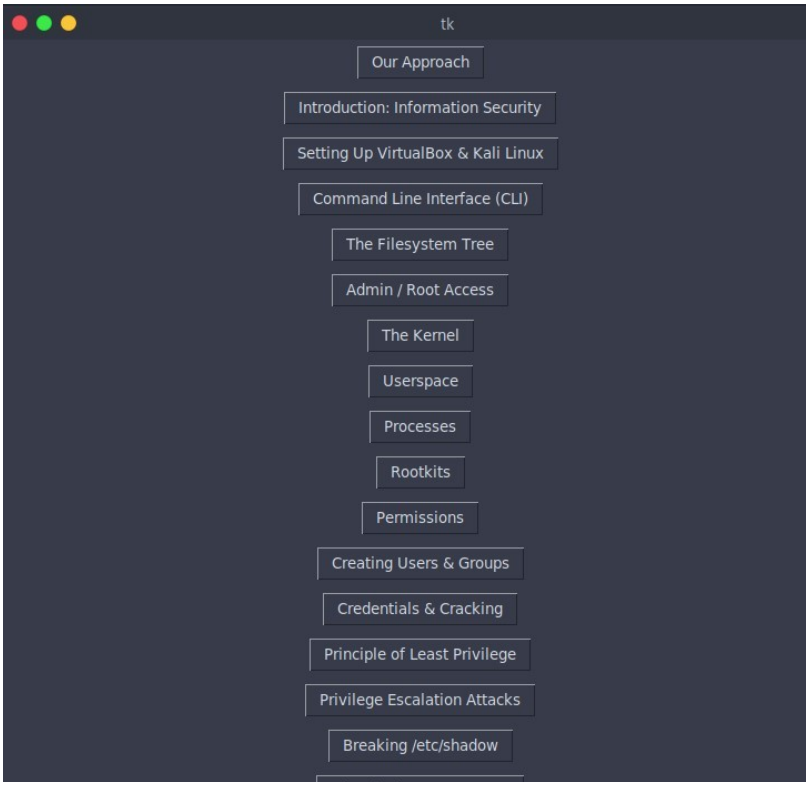
```python
message = "Hello, World!"
print(message)
```

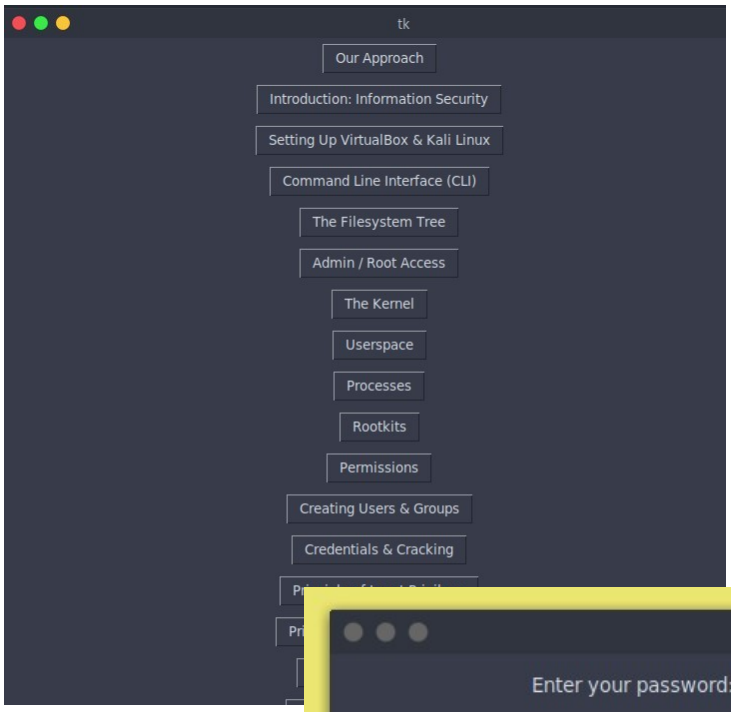
When your adversary adapts to one string of code AttackEM helps you develop a new axis of attack with unique signatures.

Developed from the academic work of the ‘Best of the Best”

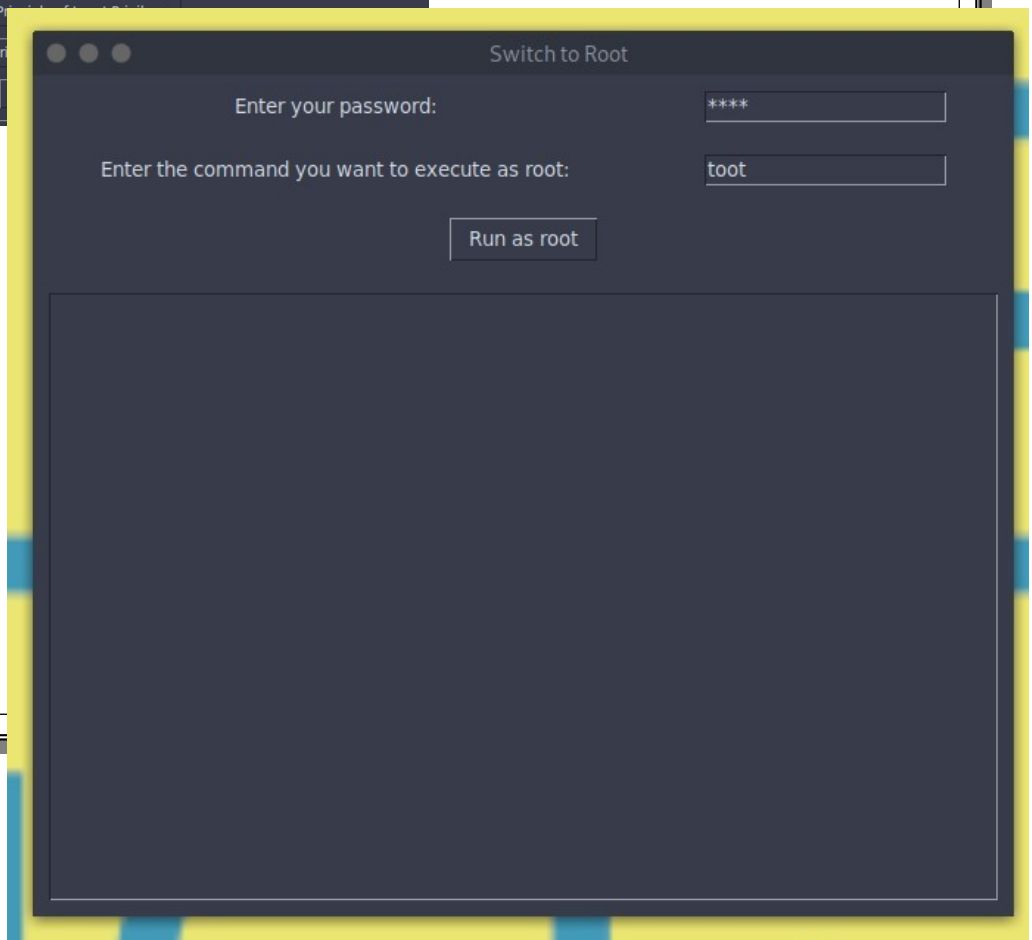
Based on the academic work of the best hacking teachers in the world.

Fancy Scott and Cozy Sean.

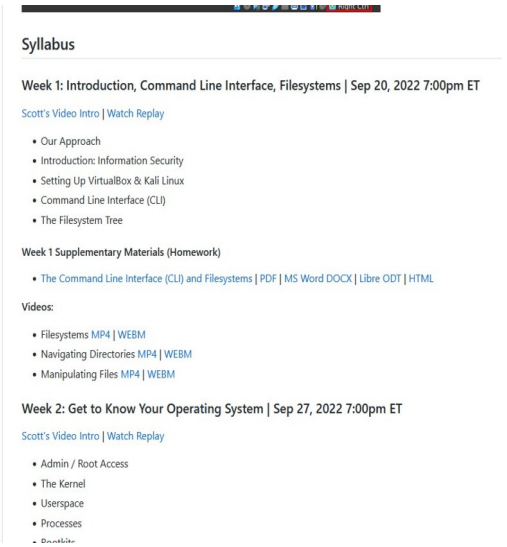




The cyber chain of action is built right in.



AttackEM can work with unstructured data and extract and format chaos into actionable commands.



Syllabus

Week 1: Introduction, Command Line Interface, Filesystems | Sep 20, 2022 7:00pm ET

Scott's Video Intro | Watch Replay

- Our Approach
- Introduction: Information Security
- Setting Up VirtualBox & Kali Linux
- Command Line Interface (CLI)
- The Filesystem Tree

Week 1 Supplementary Materials (Homework)

- The Command Line Interface (CLI) and Filesystems | PDF | MS Word DOCX | Libre ODT | HTML

Videos:

- Filesystems MP4 | WEBM
- Navigating Directories MP4 | WEBM
- Manipulating Files MP4 | WEBM

Week 2: Get to Know Your Operating System | Sep 27, 2022 7:00pm ET

Scott's Video Intro | Watch Replay

- Admin / Root Access
- The Kernel
- Userspace
- Processes

```
import tkinter as tk

# Define the list of bulleted points
bullets = [
    "Our Approach",
    "Introduction: Information Security",
    "Setting Up VirtualBox & Kali Linux",
    "Command Line Interface (CLI)",
    "The Filesystem Tree",
    "Admin / Root Access",
    "The Kernel",
    "Userspace",
    "Processes",
    "Rootkits",
    "Permissions",
    "Creating Users & Groups",
    "Credentials & Cracking",
    "Principle of Least Privilege",
    "Privilege Escalation Attacks",
    "Breaking /etc/shadow",
    "Historical & Current OS's",
    "Unix",
```

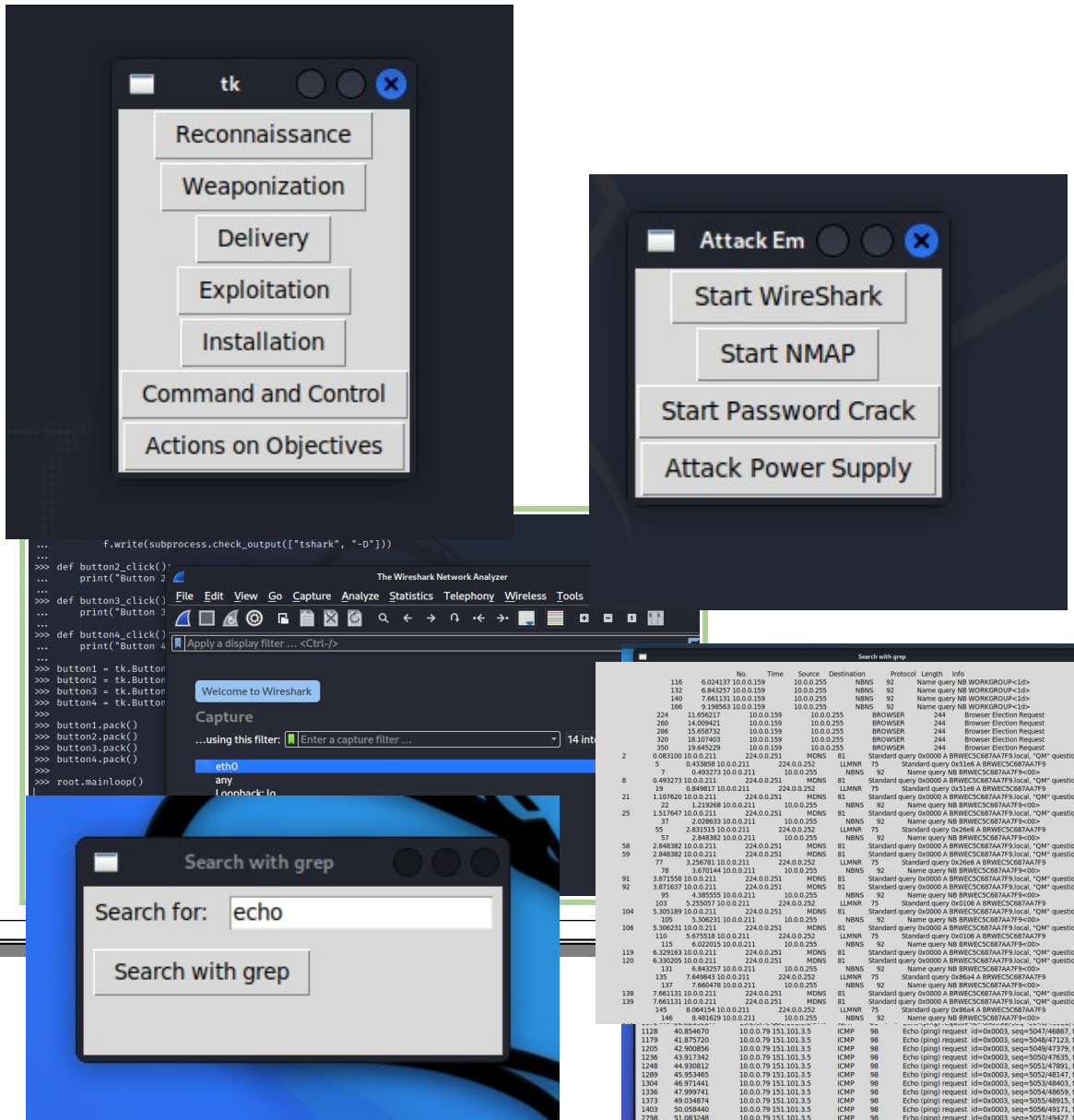
CASE STUDY

Using AttackEM to attack the cooling system of a computer

My final final project evolved from trying to launch one system command to trying to build a malware tool for launching a complex attack on the physical hardware of a computer through the protections of a virtual machine.

Recon

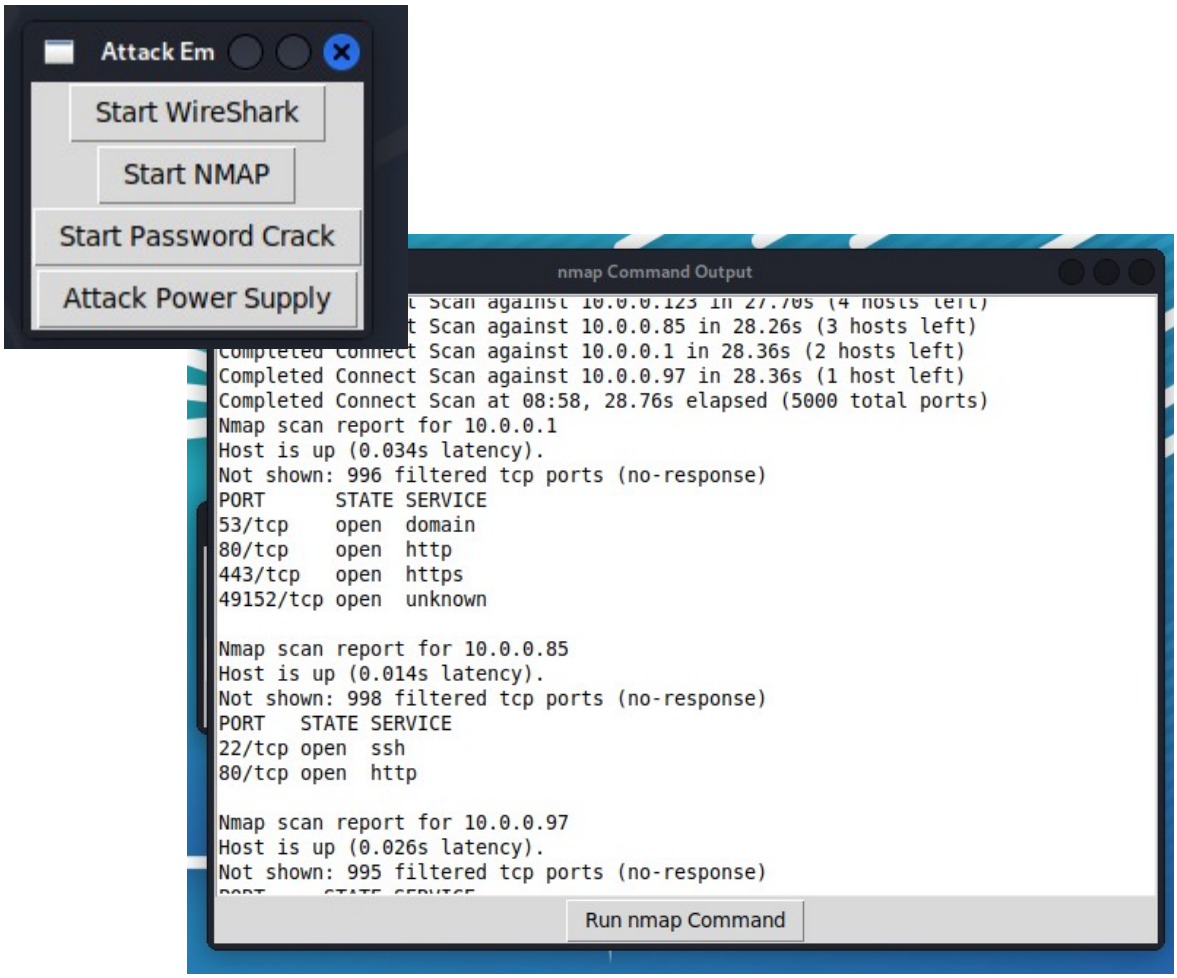
Search a network and then turn unstructured output about that network into structure data you can use.



Work your way down the menu.

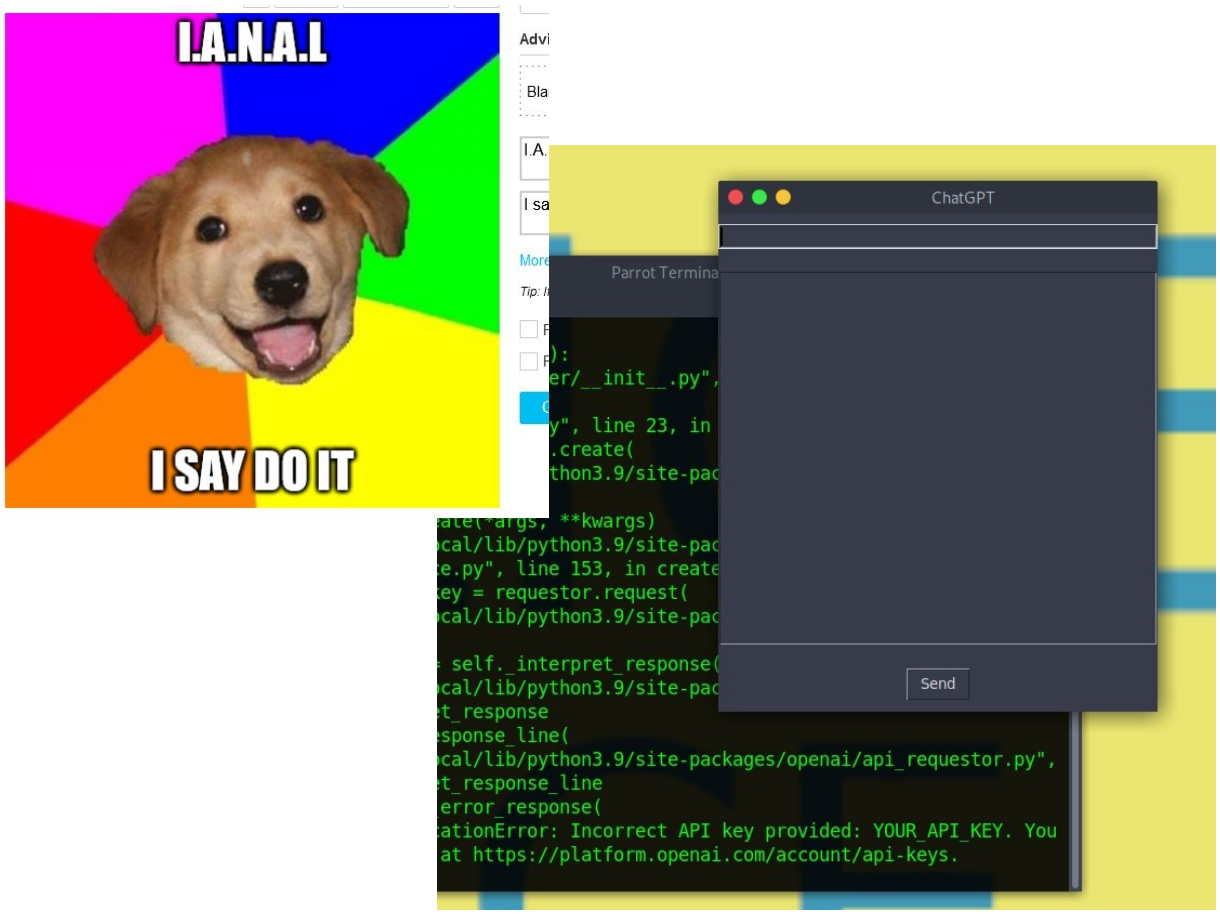
After a computer is found, and information about it has been formatted for easy use.

Look for an opening with one click.

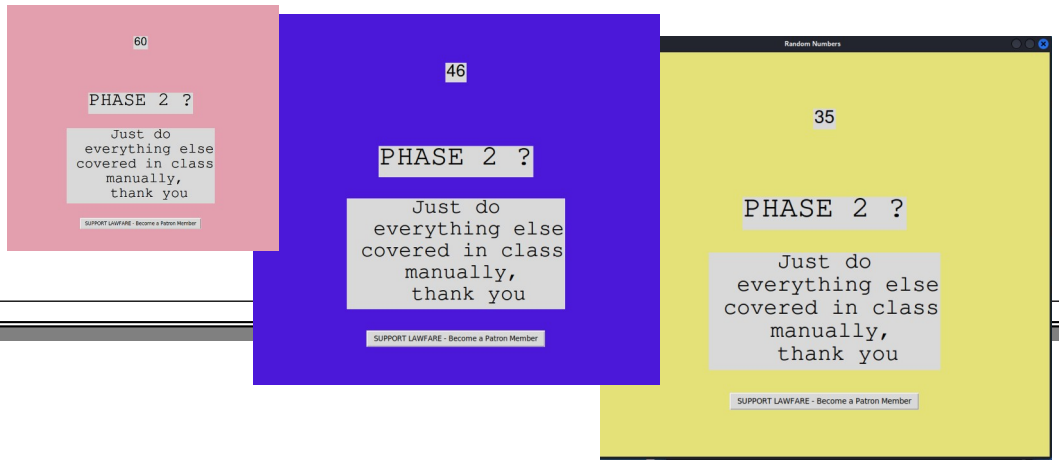


AttackEM is a full spectrum tool, for hacking every system.
If it has rules, we can help you hack it.

While AttackEM is all like “I.A.N.A.L’ it can provide you with tons of advice about the law



Phase II



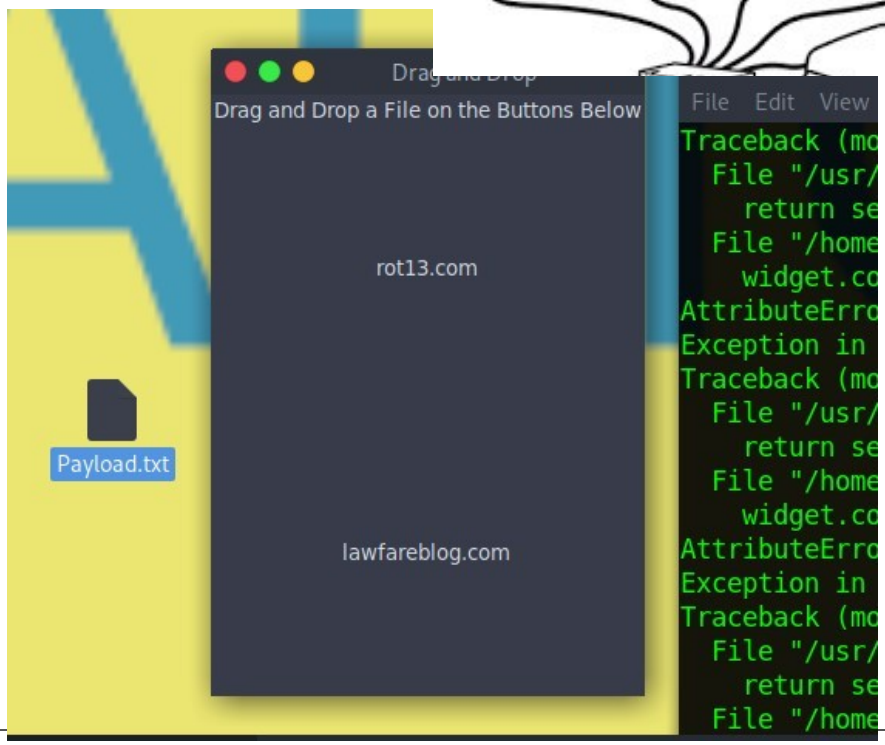
< INTENTIONALLY LEFT BLANK >

For security reason I can't demonstrate that I learned some topics.
For a full demonstration of what I learned in class
upgrade to AttackEM (BLUE).

AttackEM helps you daisy chain an attack to hide origins.

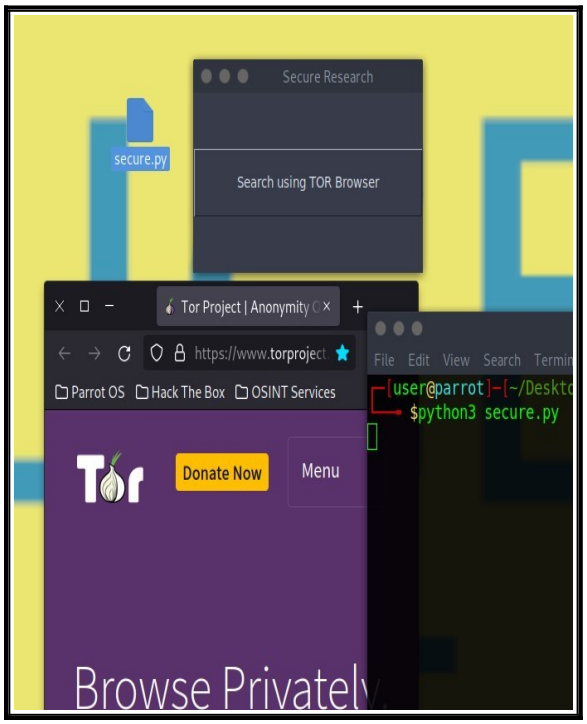
Build tools on other compromised computers to attack your target.

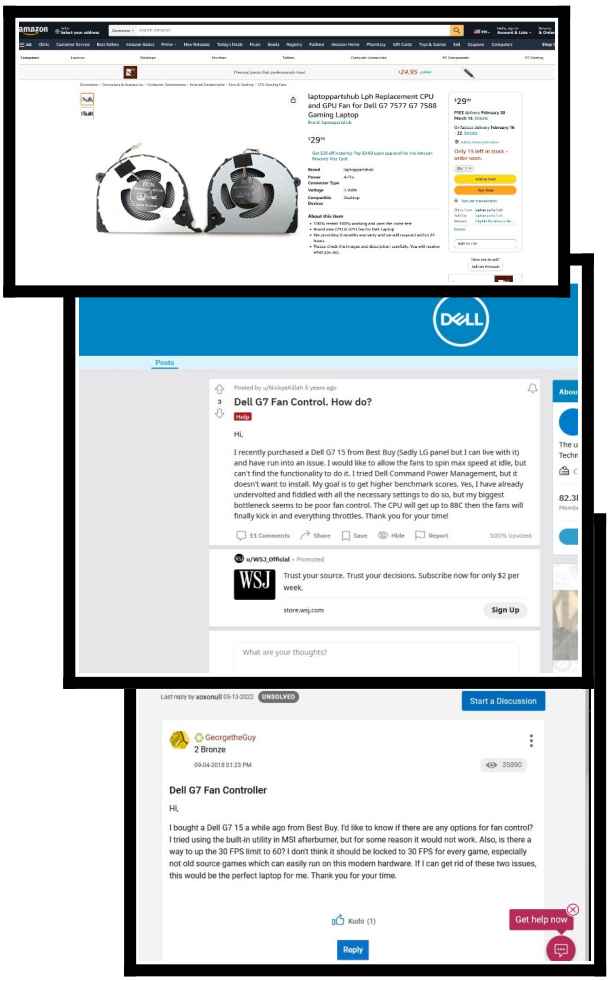
Easy to use just "Drag and Drop" payloads onto your targets.



Research your operation with stealth.

AttackEM uses a secure chain code technology to search for exploits.



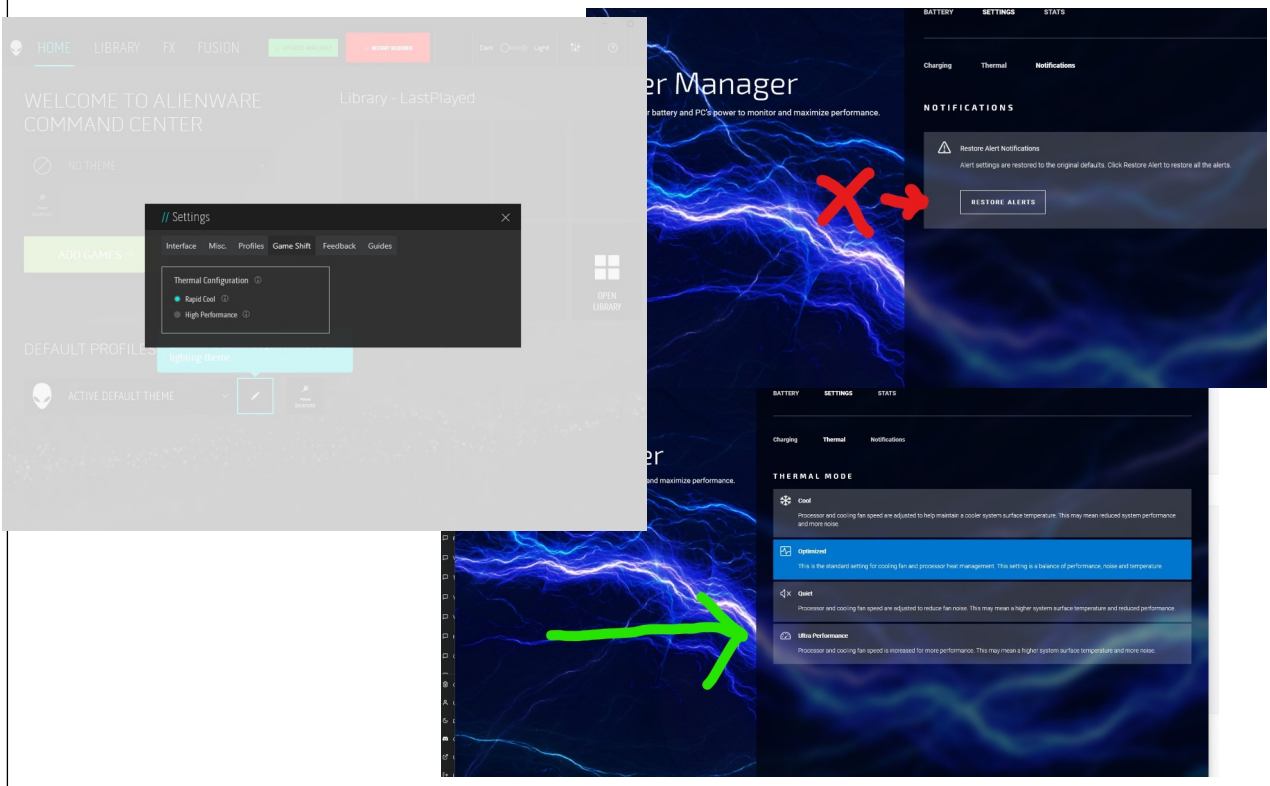


Upgrade to AttackEM PRO for access to Password and other Brute force tools in action.

[Upgrade to AttackEM (PRO).]

The Attack

Use existing tools in found on this computer and operating system to turn off heat notification.
Turn Graphics performance up to full power with less heat safeguards.

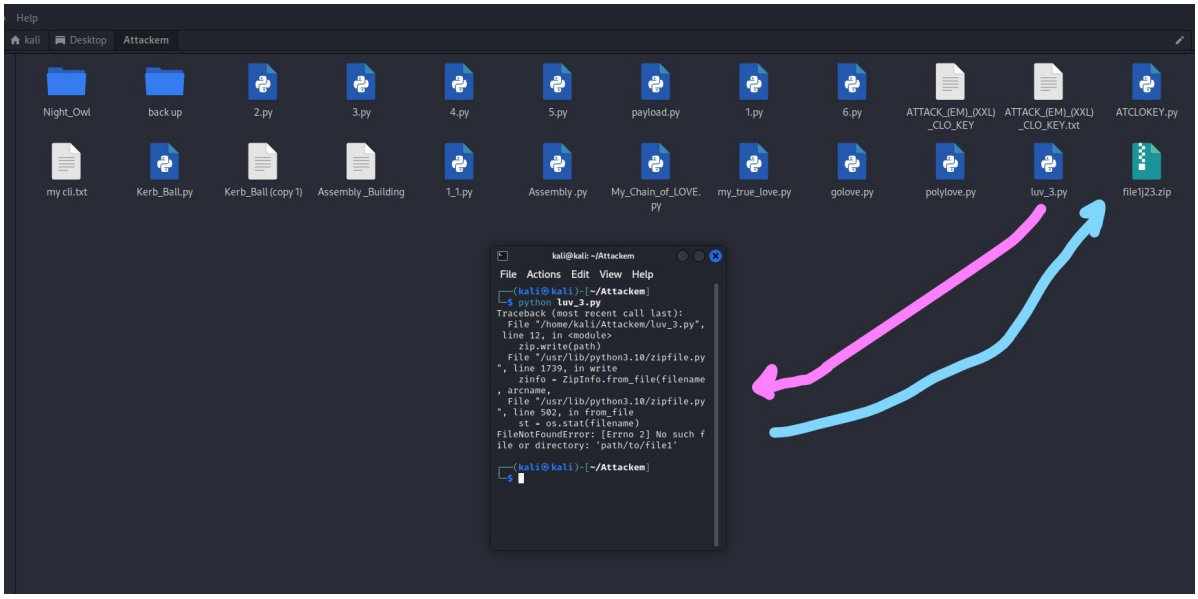


The Payload

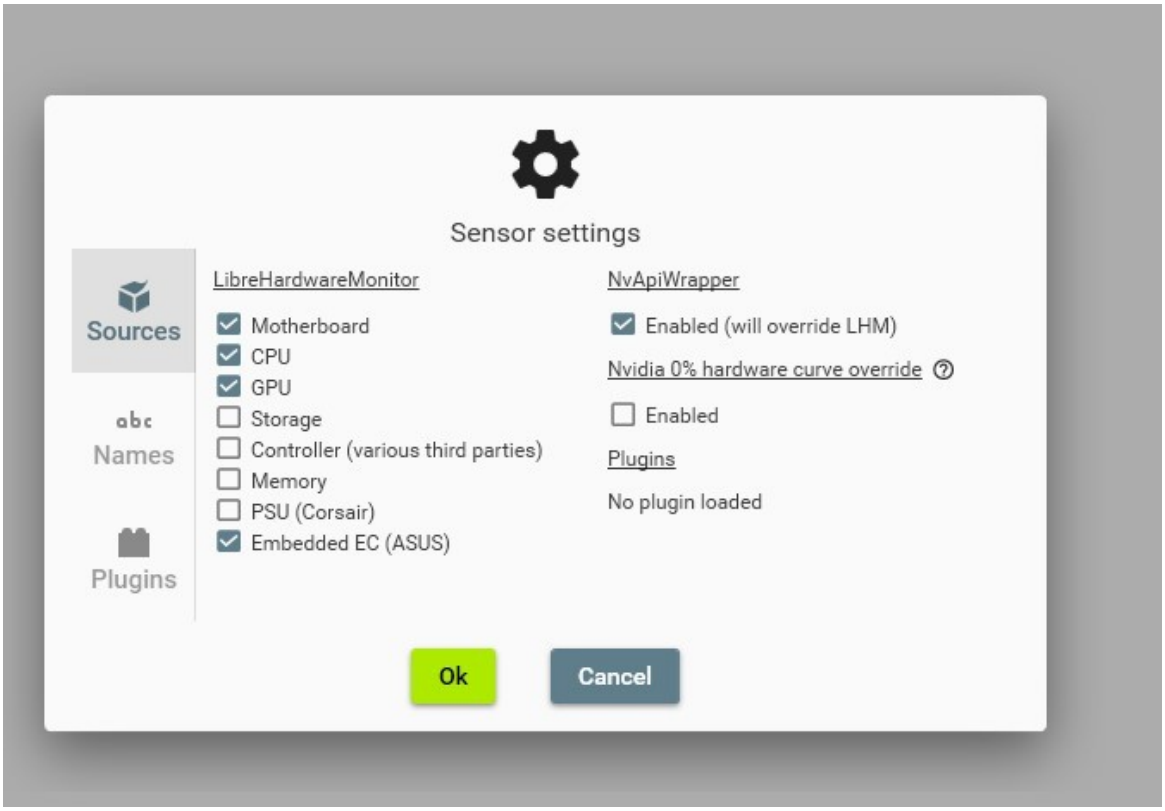
The sharp end of this attack
is a Third Party Application
for monitoring system preform ace.

The payload is an archive for **FanControl**

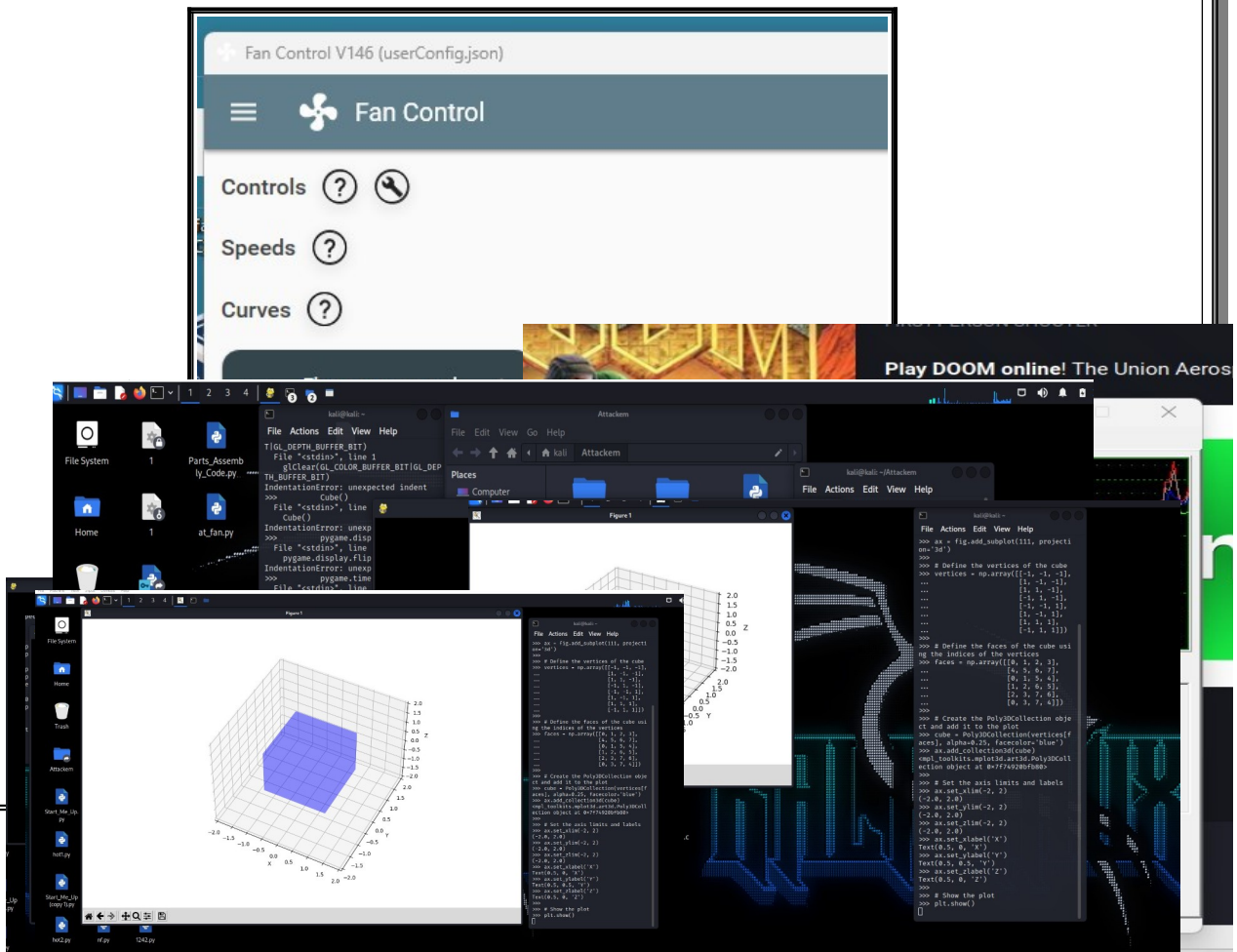
AttackEM can help you move files like our payload easily with automatic scripts.



FanControl looks for fans



Use our payload to turn fan down to 1%



4. How to turn off Azure Virtual Machine.

Microsoft | Learn Documentation Training Certifications Q&A Code Samples Assessments Shows Events Search

Azure Product documentation Architecture Learn Azure Develop Resources

Filter by title

Power Off
Reapply
Redeploy
Reimage
Restart
Retrieve Boot Diagnostics Data
Simulate Eviction
Start
Update
Confluent
Consumption
Container Instances
Container Registry
Cosmos DB
Cosmos DB Resource Provider
Cost Management
Custom Providers
Data Box Edge/Data Box Gateway
Data Catalog
Download PDF

Learn / Compute / Virtual Machines /

Virtual Machines - Power Off

Reference Feedback

Service: Compute

API Version: 2022-11-01

The operation to power off (stop) a virtual machine. The virtual machine can be restarted with the same provisioned resources. You are still charged for this virtual machine.

HTTP Copy Try It

```
POST https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups
```

With optional parameters:

HTTP Copy

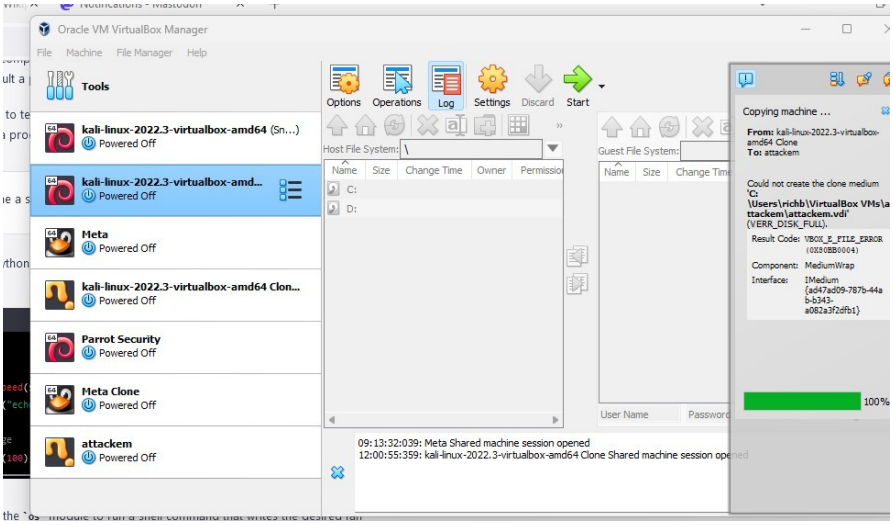
```
POST https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups
```

URI Parameters

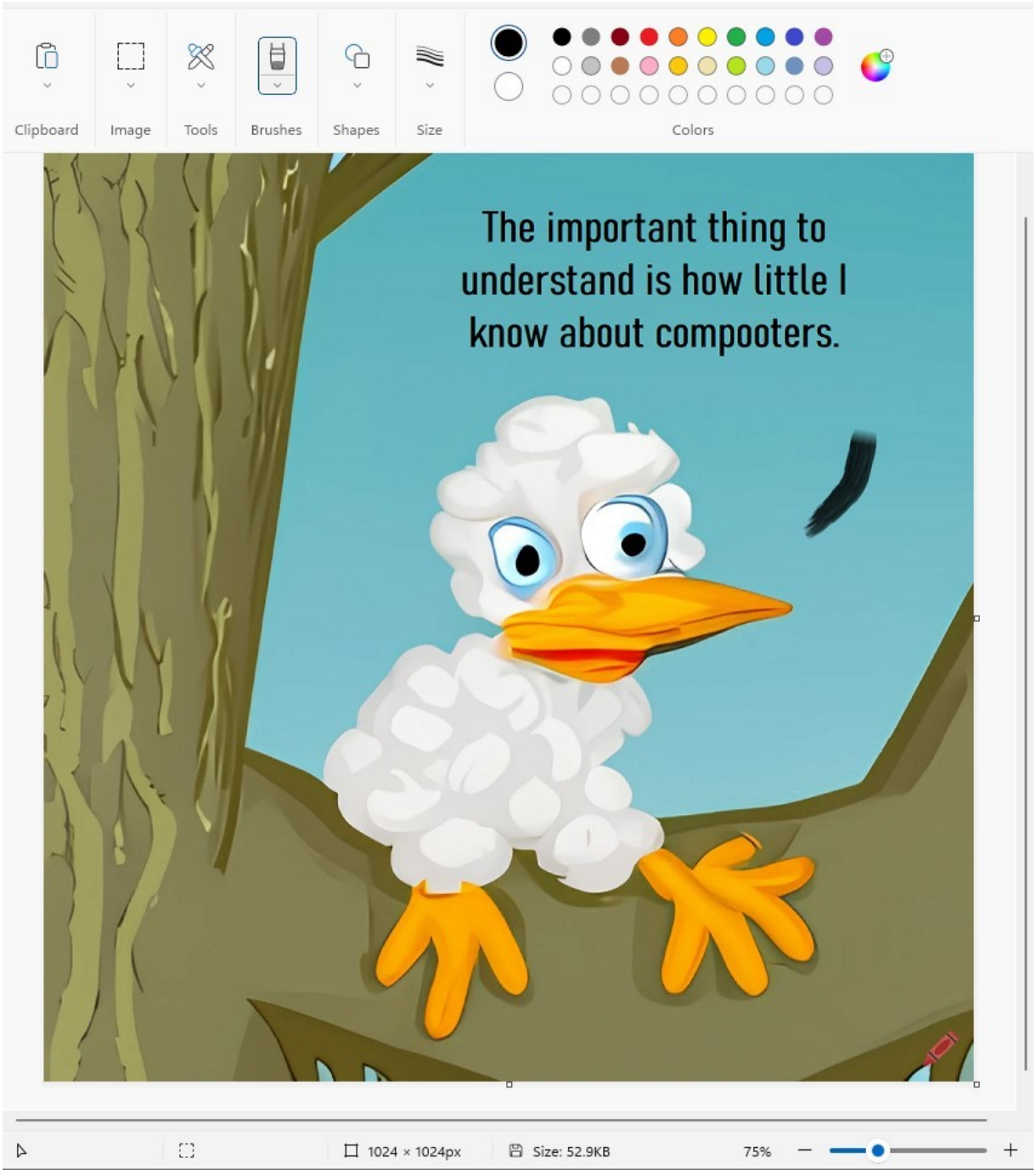
Name	In	Required	Type	Description

In this art
URI Parameters
Responses
Security
Examples

5. Set up a more realistic testing environment and learn more about virtual machines.



CONCLUSION :



Less than 30 Days ago I was doing this in python

```
>>> 2+2
4
```

Scott and Sean have definalty infomred my artistic practice.

Thank you

Contact Jimmy: https://mastodon.social/@jimmy_jim_James
Support Lawfare: https://www.lawfareblog.com/support-lawfare
Buy Merchandiz: www.lawflair.com
Buy Scott's book: https://us.macmillan.com/books/9780374601171/fancybeargoesphishing

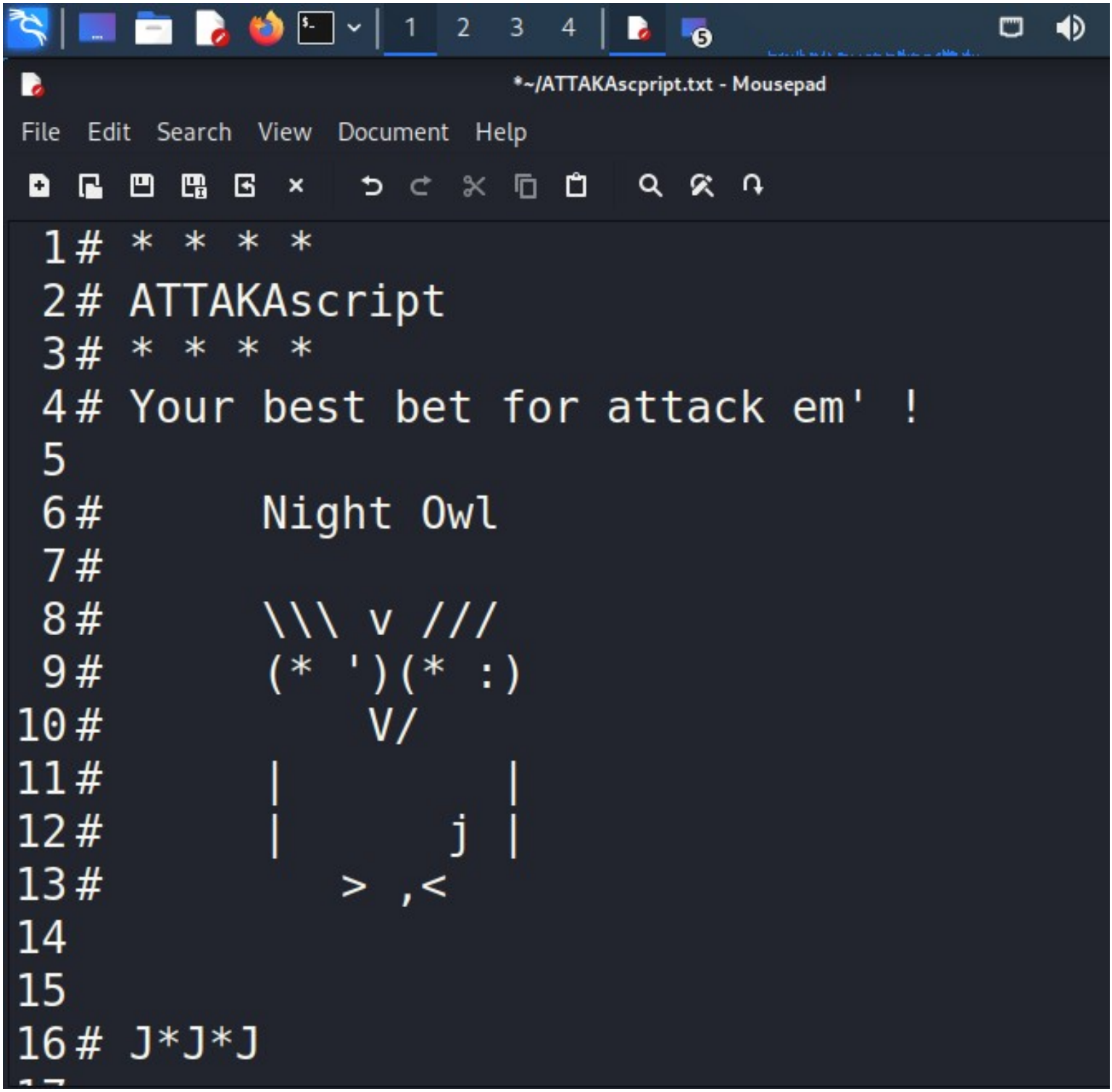
Footnotes:

(1) The Lawfare Podcast: ChatGPT Tells All

⁂⁂⁂

MY FILE

```
                    ////////////
<<<<<<<<<<<(X)  (X)
            V              V
            V              V
            V              V
              --   --
```


1 2 3 4
*~/ATTAKAscript.txt - Mousepad
File Edit Search View Document Help
1# * * * *
2# ATTAKAscript
3# * * * *
4# Your best bet for attack em' !
5
6# Night Owl
7#
8# \\\ v ///
9# (* ')(* :)
10# V/
11# | |
12# | j |
13# > ,<
14
15
16# J*J*J