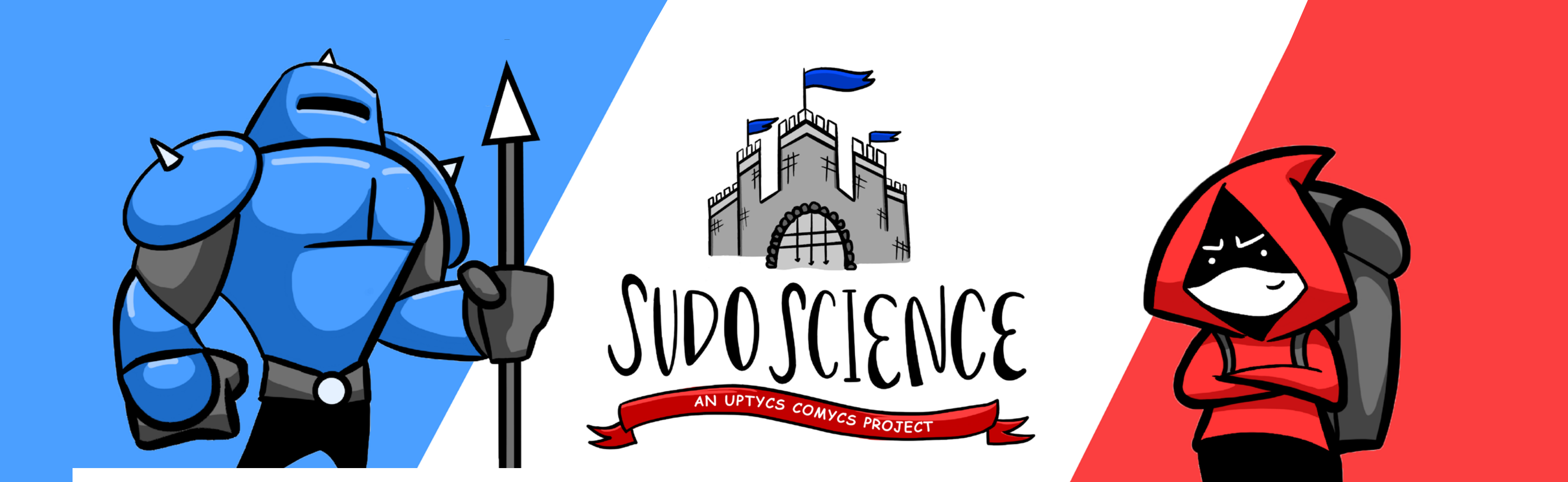

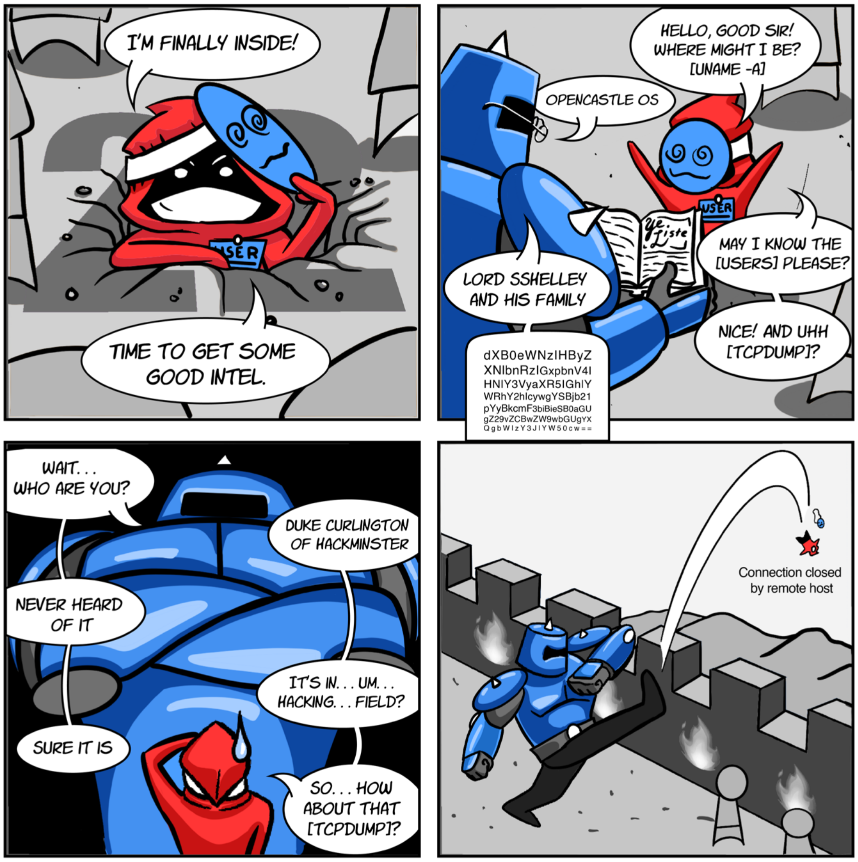
I'M FINALLY INSIDE!
USER
TIME TO GET SOME GOOD INTEL.
HELLO, GOOD SIR! WHERE MIGHT I BE? [UNAME -A]
OPENCASTLE OS
USER
MAY I KNOW THE [USERS] PLEASE?
LORD SSHELLEY AND HIS FAMILY
dXB0eWNzIHByZ
XNlbnRzIGxpbnV4I
HNlY3VyaXR5IGhlY
WRhY2hlcywgYSBjb21
pYyBkcmF3biBieSB0aGU
gZ29vZCBwZW9wbGUgYX
QgbWlzY3JlYW50cw==
NICE! AND UHH [TCPDUMP]?
WAIT... WHO ARE YOU?
DUKE CURLINGTON OF HACKMINSTER
NEVER HEARD OF IT
IT'S IN... UM... HACKING... FIELD?
SURE IT IS
SO... HOW ABOUT THAT [TCPDUMP]?
Connection closed by remote host

Deep Dive

Discovery techniques can be quite the headache when it comes to securing Linux Servers. During this phase, adversaries are trying to figure out the environment. However, some of the commands they run can be similar to what benign users may use to gain information about the system. Techniques like T1082 - System Information Discovery is a commonly used technique that "cannot be easily mitigated with preventative controls since it is based on the abuse of system features" according to MITRE.

So how can we detect malicious activity? The answer lies in understanding the behavior in context with each other. Instead of looking at each command individually, we can detect potential adversarial behavior by looking at the string of commands run.

Scenario

This comic has Curly, our Red Team character, making their way into a server via SSH (shown by the faint 22 in the first panel). Somehow, they have made their way in with some privileged credentials and now need to figure out where they are. To do this, they will implement the same discovery techniques attackers may use. They run

```
uname -a
users
tcpdump
```

However, Linus, our Blue Team character, who is always watchful of intruders becomes suspicious of the questions they are asked. They are inclined to answer Curly's first two questions since these can be very normal questions that any regular user would ask. However, they know that adversaries may try to sniff network traffic in order to capture information about their environment.

So when Curly asks for the tcpdump output, Linus becomes suspicious and asks for authentication. Curly, clearly not knowing how to answer, is caught in the act and then literally kicked off the server.