King of the Packet

Florida Tech IoT Security & Privacy Lab

What is Hacking?

Hackers

Hacking involves a different way of looking at problems that no one’s thought of.

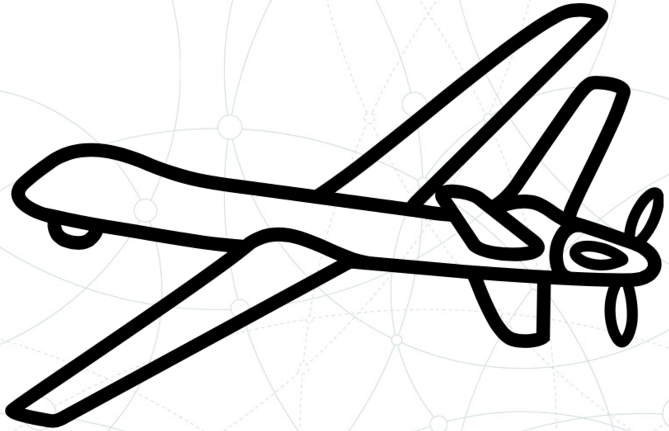
US RQ-170 Drone Compromise

- 5 December 2011 – Iranian forces captured a Lockheed Martin RQ-170 Sentinel Drone

- Iranian Cyberwarfare Forces crashed the drone near Kashmar with minimal damage by compromising either GPS or telemetry

- By 2016, Iranian forces had reverse engineered the drone technology

- In 2018, Israeli forces shot down an advanced Iranian drone that borrowed several technologies from the captured RQ-170



Text copied from: https://en.wikipedia.org/wiki/Iran–U.S._RQ-170_incident

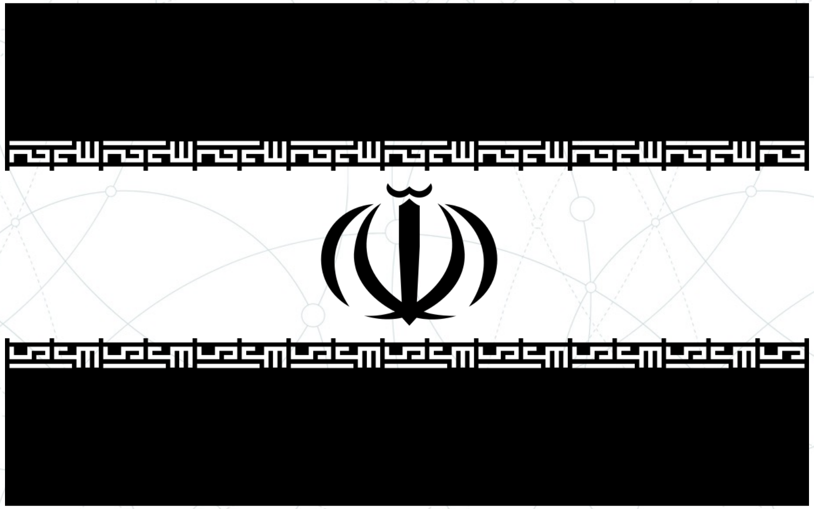
[redacted]

How Does One Hack Something?

- Break a problem into **manageable steps.**
- Research each step to find **border-cases.**
- Attempt to **exploit the border** case.
- Repeat until you observe an **unintended result.**

How the Iranians Hacked The Drone

- First, they determined that the RQ-170 drone leveraged different types of traffic to fly.
  - Video: Captures the drone camera.
  - Telemetry: Relays commands to the drone
  - GPS: Determines locations, altitude, speed.
- Then they began experimenting with different conditions for each type of traffic.



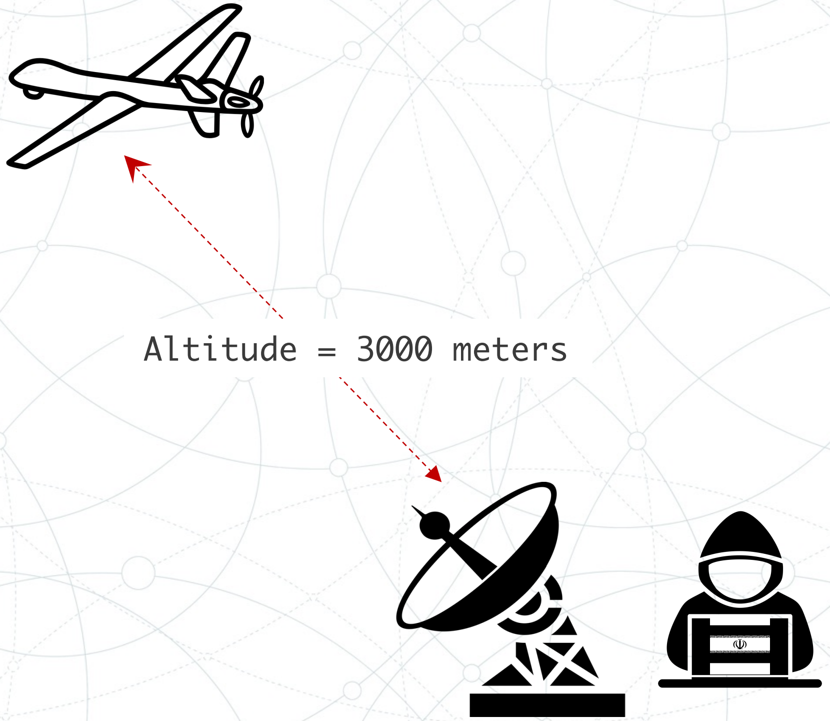
Spoofing Conditions

First, they examined if the different types of traffic used **encryption**. Encryption is a complex math formula that translates the traffic into something only understandable by the parties that set it up.

- Is the video encrypted?
  ✓ Yes.

- Is the telemetry encrypted?
  ✓ Yes.

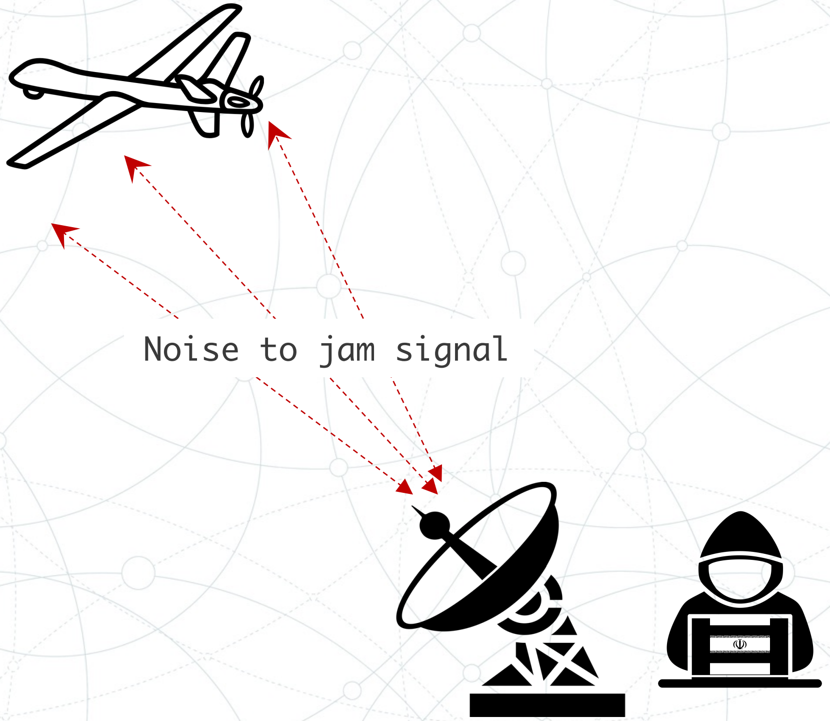
- Is the GPS encrypted?
  ✗ **No.** This is interesting, maybe we could forge fake GPS signals.



Jamming Conditions

Next, they determined if they could jam the traffic. Jamming is a technique that overpowers a signal.

- What happens if you jam video?
  - *Operators controlling the drone can no longer fly via sight, but position is still relayed to operators.*
- What happens if you jam telemetry?
  - *Drone recognizes that it is no longer under operator control and returns to base.*
- What happens if you jam GPS?
  - *Drone doesn't know its speed, location, or altitude (its flying blind.)*



How do you think they hacked it?

Spoofing (Sending Fake Signals)	
Video	✗ Not Possible
Telemetry	✗ Not Possible
GPS	✓ Possible

Jamming (Blocking Signals)	
Video	✓ Possible
Telemetry	✓ Possible
GPS	✓ Possible

What actions should we take?	
Video	(**Spoof** or **Jam**)
Telemetry	(**Spoof** or **Jam**)
GPS	(**Spoof** or **Jam**)

FLORIDA TECH

How do you think they hacked it?

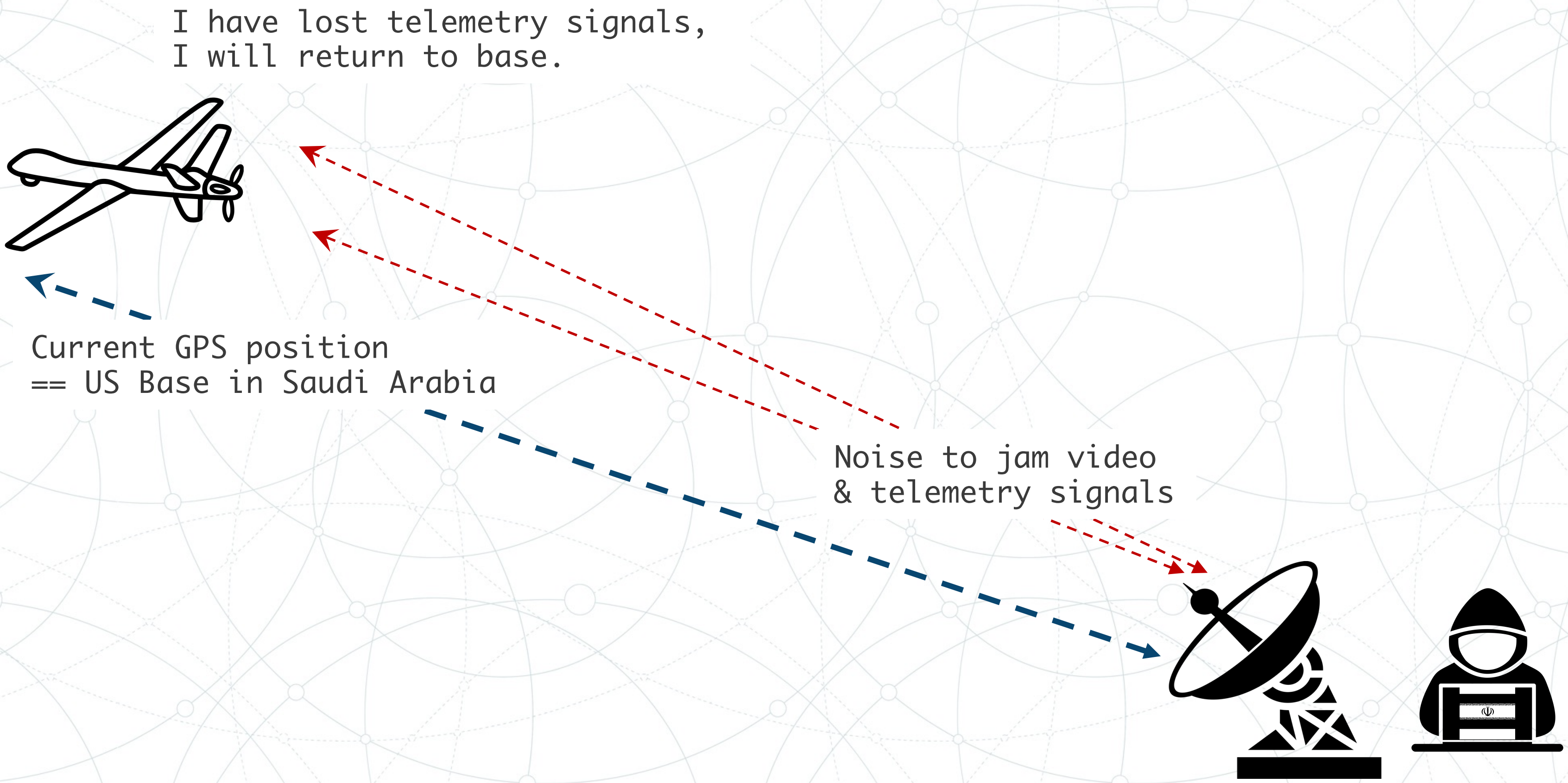
Spoofing (Sending Fake Signals)	
Video	✗ Not Possible
Telemetry	✗ Not Possible
GPS	✓ Possible

Jamming (Blocking Signals)	
Video	✓ Possible
Telemetry	✓ Possible
GPS	✓ Possible

What actions should we take?	
Video	(**Jam**)
Telemetry	(**Jam**)
GPS	(**Spoof**)

FLORIDA TECH

Iranian Drone Attack



I have lost telemetry signals,
I will return to base.

Current GPS position
== US Base in Saudi Arabia

Noise to jam video
& telemetry signals

Let’s Hack Something Today

Please note, I attempted to borrow a US Military Drone, but they are currently not able to be lent out for high school experiments. So, I got the next best legal thing.

How Does One Hack Something?

- Break a problem into **manageable steps.**
- Research each step to find **border-cases.**
- Attempt to **exploit the border** case.
- Repeat until you observe an **unintended result.**

FLORIDA TECH

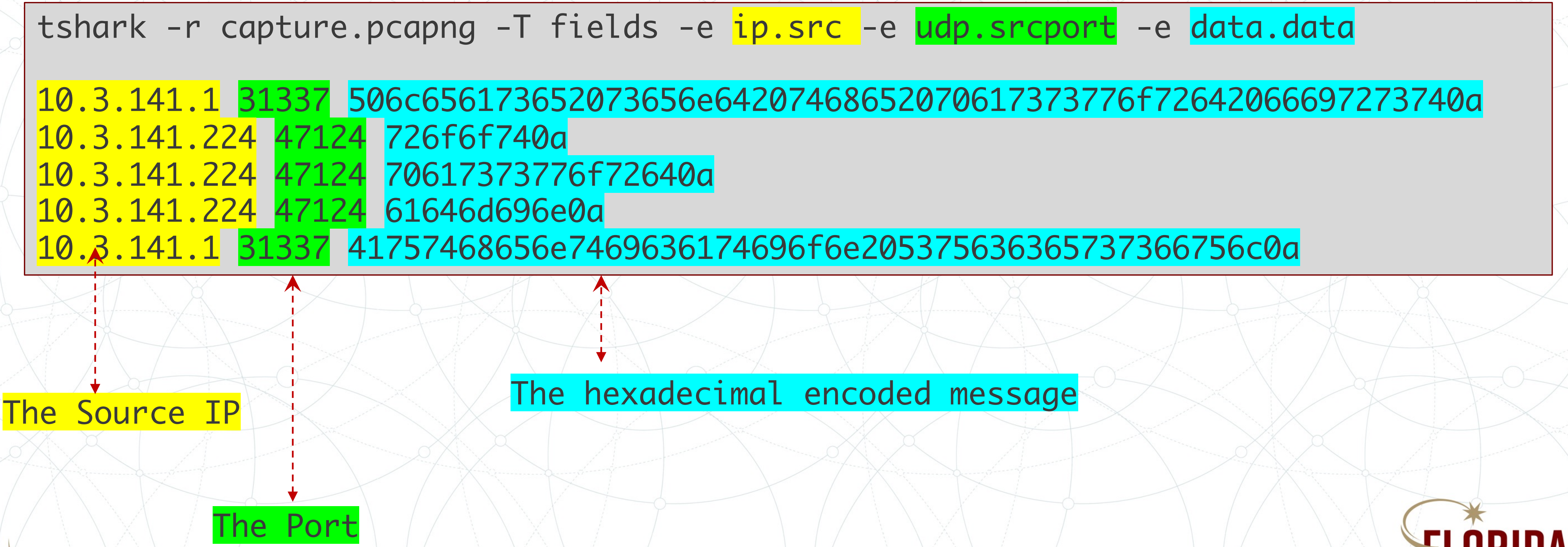
Manageable Steps

1. Examine the traffic capture from the car
2. Determine the cars IP Address and port and **Connect to It**
3. Examine the **traffic payloads for commands.**
4. Spoof the replicated commands to the car.

Hacker Tools for Today

1. Tshark – allows us to investigate previously recorded network packets.
2. Netcat – allows us to connect to a service and send commands.

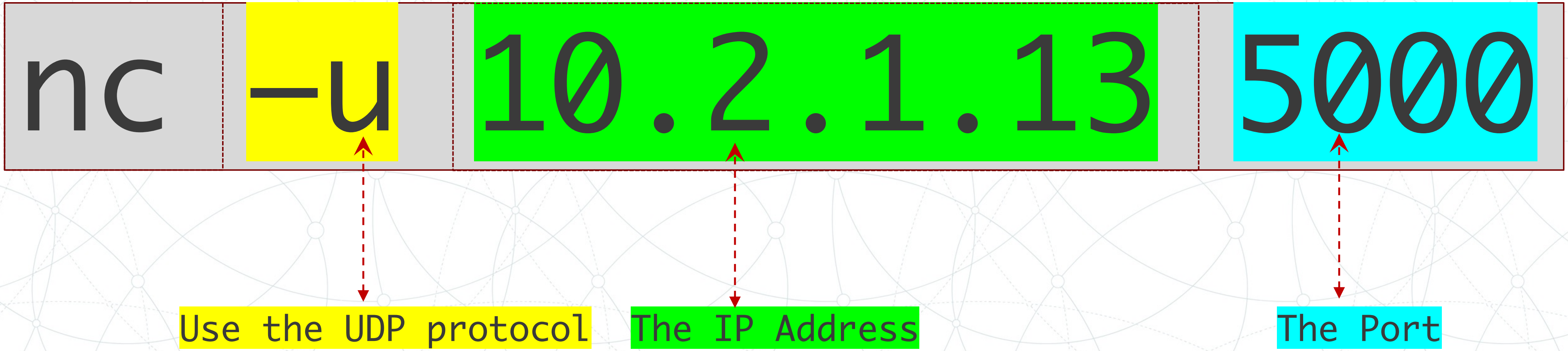
Tshark



```
tshark -r capture.pcapng -T fields -e ip.src -e udp.srcport -e data.data

10.3.141.1 31337 506c656173652073656e64207468652070617373776f72642066697273740a
10.3.141.224 47124 726f6f740a
10.3.141.224 47124 70617373776f72640a
10.3.141.224 47124 61646d696e0a
10.3.141.1 31337 41757468656e7469636174696f6e205375636365737366756c0a
```

Netcat



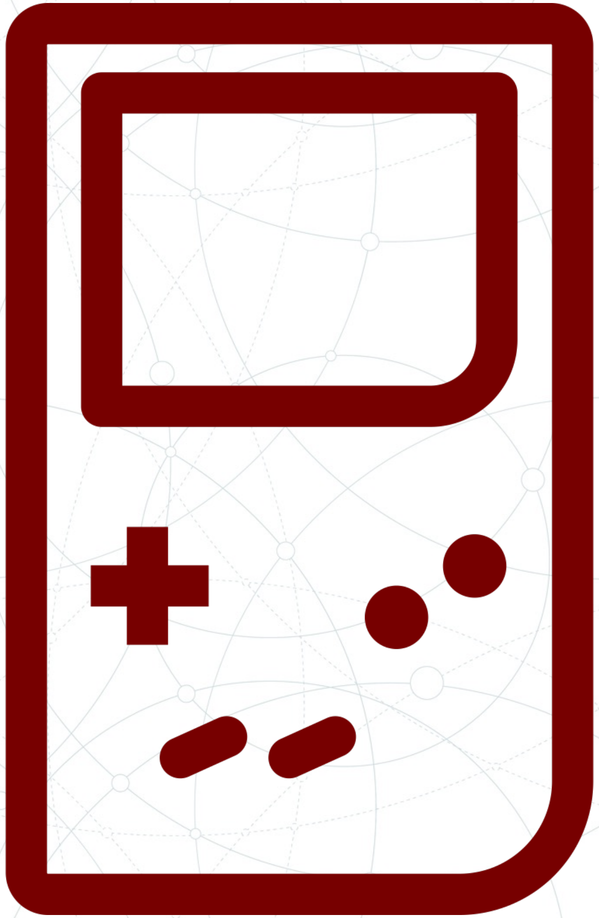
```
nc -u 10.2.1.13 5000
```

Let the King of the Hill Begin

(1) Connect to your wireless car via RCCTF-<car id>
(2) Browse to http://10.3.141.1
(3) Read and follow the instructions

Next Lesson

Attack Oriented Programming



Thank you.