# Hacking Introduction

**Eli the Computer Guy - November 11, 2024**
Version 1

## What is Hacking?

Using systems in undocumented ways...

## Why Do People Hack?

- Curiosity
- Criminal Intentions
- Vandalism
- Pen Testing
- Access
- Hacktivism

### Hacking Hats

- Black Hat
- White Hat
- Grey Hat

## Legality and Legal Agents

Know when to stop!

Legal Agents are representatives of an organization that have the legal right to authorize the organization to enter into binding contracts.

Verify anyone you are dealing with has the authorization to allow you to "test" their systems.

In some jurisdictions personal privacy trumps organization ownership.

https://www.cnbc.com/2019/11/12/iowa-paid-coalfire-to-pen-test-courthouse-then-arrested-employees.html

## Consequences

https://www.justice.gov/usao-ndtx/pr/man-receives-maximum-sentence-ddos-attack-legal-news-aggregator

https://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html

# Zero Day Exploits

Zero Day exploits are simply attacks that use vulnerabilities that are no known before the attack.

# Command an Control Systems

Command and Control Systems allow bots or nefarious servers to take actions, send a report to a controlling server, and then wait for a command on what to do next.

# Hacking Attacks

## Social Engineering

Social Engineering is pretending to be someone you're not to gain access to systems.

Act like you belong.

- Ask for Password to be reset
- Gain access to sensitive facilities

## Hard Drive Access

Hard Drives can be accessed using Live Flash Drives, or by pulling them out and using USB connections.

## Network Scanners

Network Scanners such as NMAP can map a LAN and determine open ports and services on specific systems.

## Key Loggers and Screen Capture

Key loggers log keystrokes on a computer or device.  They can be software or hardware based.

https://www.keelog.com/airdrive-keylogger/

- Captures username/ passwords
- Captures sensitive information

## Phishing and Spear Phishing

Sending emails pretending to be a trusted party.  Phishing is a mass email, Spear Phishing is attacking a specific target like a CTO.

```php
<?php
$to = "recipient@example.com";
$subject = "Subject of the Email";
$message = "Hello, this is a hacking attack email sent using PHP!";
$headers = "From: boss@mycompany.com\r\n";
$headers .= "Reply-To: boss@mycompany.com\r\n";
$headers .= "X-Mailer: PHP/" . phpversion();

if (mail($to, $subject, $message, $headers)) {
    echo "Email sent successfully!";
} else {
    echo "Failed to send the email.";
}
?>
```

## Spoofing

Spoofing is pretending to be a legitimate service such as a web site, or telephone number.

Websites may either look similar to legitimate URLs, or use a shortener to try to hide the actual URL

```
BankOfEngland.hackyou.com
```

https://www.recordiapro.com/

## Poisoning

Poisoning involves adding or modifying values in caching systems so that the end user receives  a response other than the correct one.

DNS Poisoning means that DNS will return an IP Address other than the one it should.

Cache Poisoning means that a file that is retrieved from cache will not be the correct one.

```
Example: hosts
```

## Ransomeware

Ransomeware seeks to encrypt data and then extort the user to regain access.

## Man in the Middle Attacks

Man in the Middle attacks are where the attacker is able to read the traffic that you are sending or receiving from a remote system.

## Injection

Injection attacks involve escaping a legitimate command to a system and then adding additional commands.  This can be SQL injection in web apps, or even OS Command Injection.

```
ping –c 1 cnn.com; touch YOUBE.HACKED
```

## DoS and DDoS

Denial of Service is using a system to use all the resources of a target system so legitimate traffic will fail.

Distributed Denial Of Service is simply DoS using multiple attack systems.

## Cross Site Scripting

Cross Site Scripting is adding scripts to a web app platform that point back to servers the attacker owns.

## Supply Chain Attacks

Supply Chain Attacks involve compromising systems or services at the vendor or before the reach the customer.

## Honey Pots

Honey Pots are systems that are setup to attract the attention of users to compromise.  Kitty Pictures, or access of pirated movies for a $1 credit card transaction.

## Bad USB - Rubber Ducky

Bad USB devices act as USB keyboards as far as the computer is concerned and are able to launch keystroke injection attacks.

https://shop.hak5.org/products/usb-rubber-ducky

## USBKill

USB Kill destroys the motherboard by sending electricity into the USB port.

https://usbkill.com/