# CSCE48503: Information Security

## Week 2: Security Basics

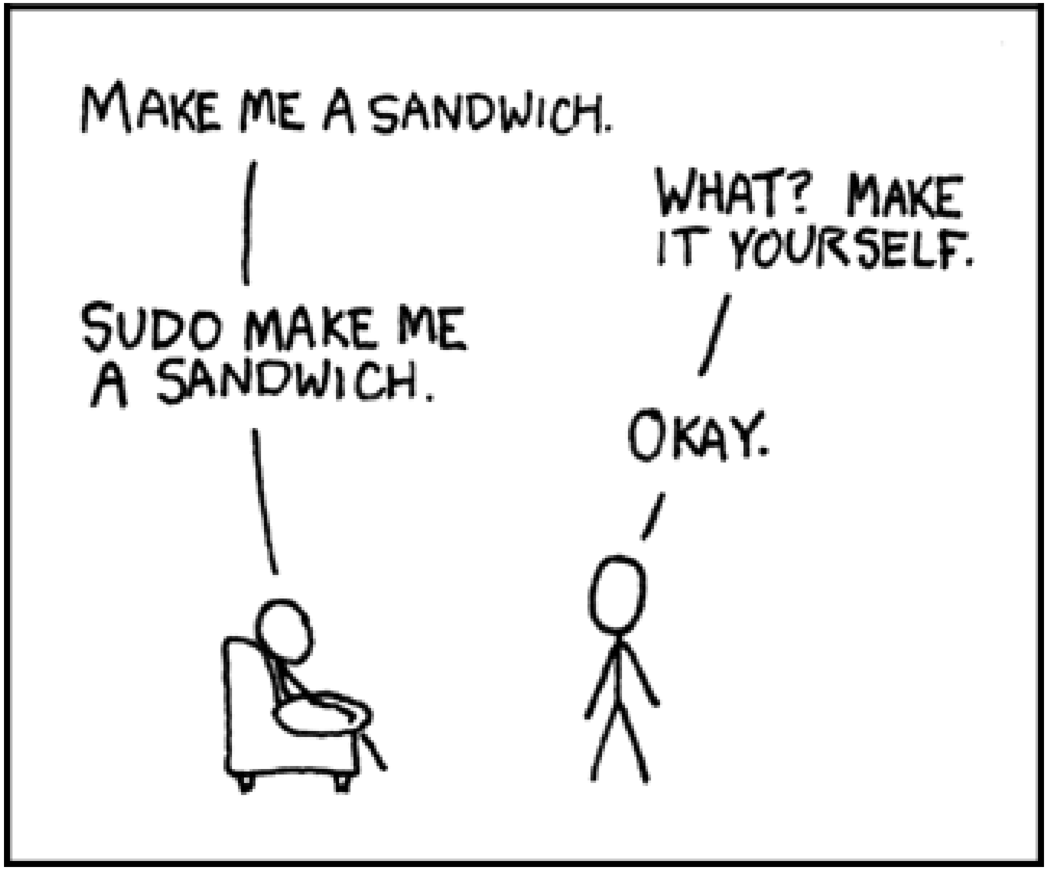
University of Arkansas

Jan 21, 2025

# Schedule [Tentative]

| | | |
|---|---|---|
| ❖ Week 1: Intro, Syllabus, CIA (Expectations) | [13Jan2025] | |
| ❖ Week 2: Security Basics | [20Jan2025] | (MLK Holiday) |
| ❖ Week 3: Access Control | [27Jan2025] | |
| ❖ Week 4: Security Policies (Week 1) | [3Feb2025] | |
| ❖ Week 5: Security Policies (Week 2) | [10Feb2025] | (S4x25 Conf) |
| ❖ Week 6: Cryptography Basics (Week 1) | [17Feb2025] | |
| ❖ Week 7: Cryptography Basics (Week 2) | [24Feb2025] | |
| ❖ Week 8: Cryptography Basics (Week 3) | [3Mar2025] | |
| ❖ Week 9: Mid-Term Review and Test | [10Mar2025] | |
| ❖ Week 10: Operating Systems Security & Malware | [17Mar2025] | |
| ❖ Week 11: Spring Break! (Be Safe) | [24Mar2025] | (Spring Break) |
| ❖ Week 12: Network Security (Week 1) | [31Mar2025] | |
| ❖ Week 13: Network Security (Week 2) | [7Apr2025] | (IEEE DC) |
| ❖ Week 14: Web Security | [14Apr2025] | |
| ❖ Week 15: Advanced Topics | [21Apr2025] | |
| ❖ Week 16: FINAL Review | [28Apr2025] | |
| ❖ Week 17: FINAL Exam Respondus and in Classroom | [7May2025 @ 10:15am] | |

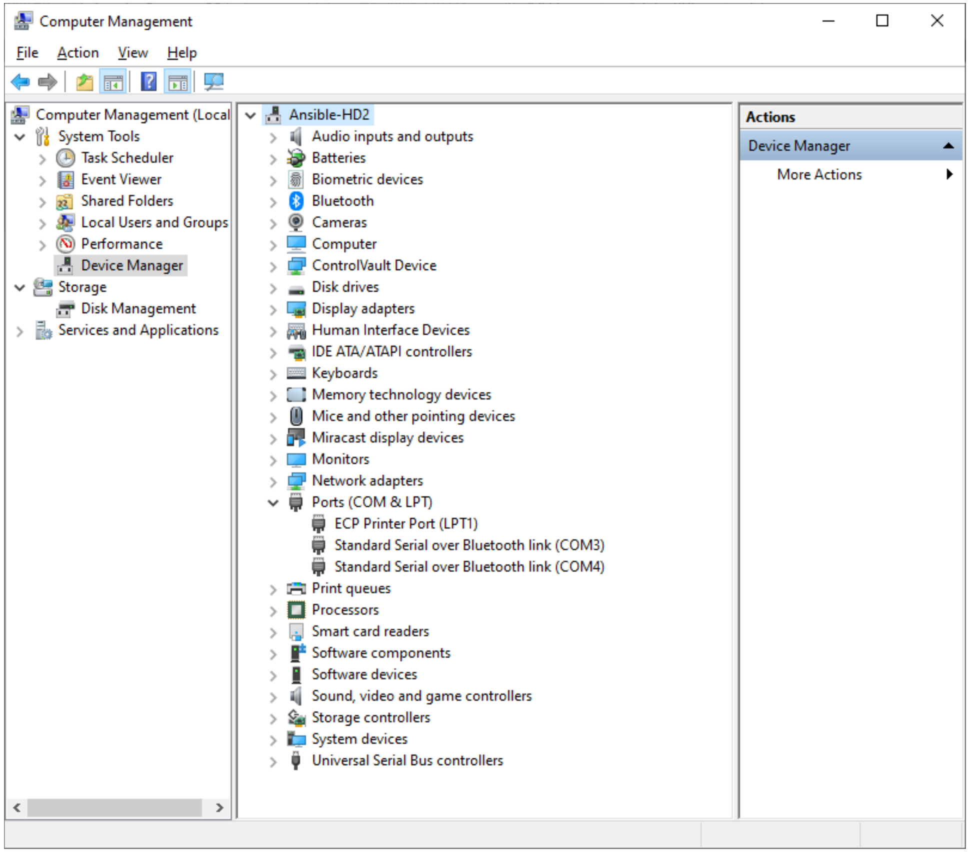
# Make Me a Sandwich



*Source: https://xkcd.com/149/

# Windows Configuration (GUI)

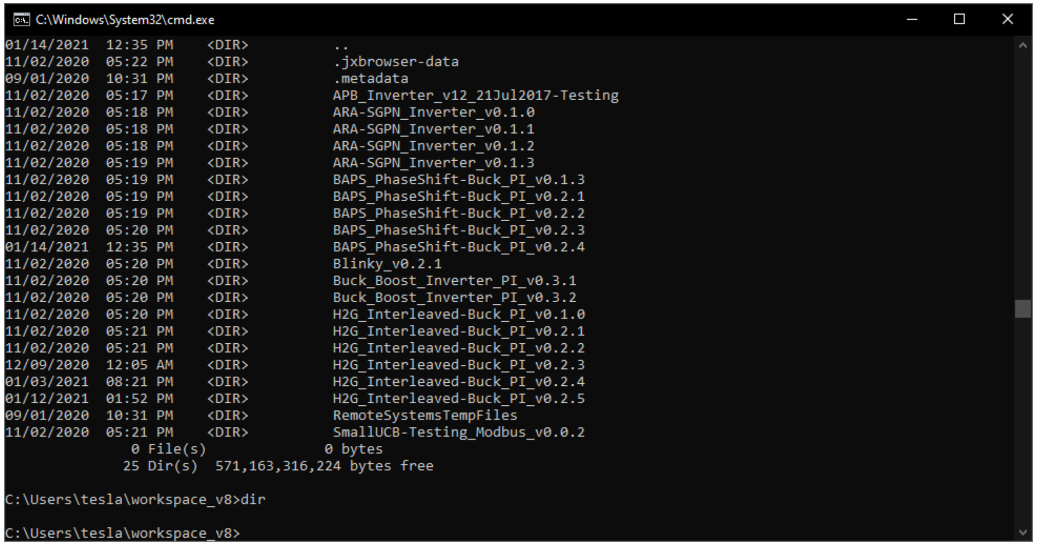
- **Computer Management**
  - **Drivers**
  - **Ports**
  - **Users**
  - **Disk**
- **System Properties**
  - **Configuration**
  - **Remote Setting**
  - **Advanced**
    - **Performance**
    - **Environment Variables**
- **Task Manager**
  - **Performance**
  - **Resource Monitor**
- **Control Panel**
  - **Most Everything Else**



# Windows Configuration (Cmd)

## Review Common Commands

- dir
- pwd
- cd
- mkdir
- rmdir
- copy
- del
- ping
- echo
- echo %HOME%
- ipconfig
- systeminfo
- shutdown /p
- shutdown /r



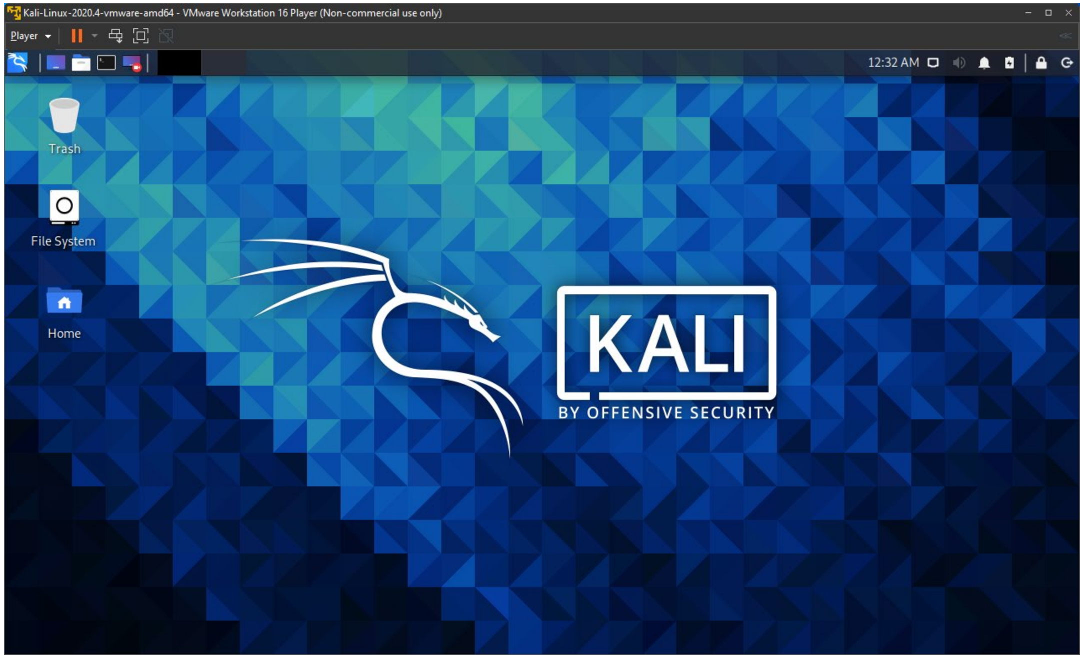
```
01/14/2021  12:35 PM    <DIR>          ..
11/02/2020  05:22 PM    <DIR>          .jxbrowser-data
09/01/2020  10:31 PM    <DIR>          .metadata
11/02/2020  05:17 PM    <DIR>          APB_Inverter_v12_21Jul2017-Testing
11/02/2020  05:18 PM    <DIR>          ARA-SGPN_Inverter_v0.1.0
11/02/2020  05:18 PM    <DIR>          ARA-SGPN_Inverter_v0.1.1
11/02/2020  05:18 PM    <DIR>          ARA-SGPN_Inverter_v0.1.2
11/02/2020  05:19 PM    <DIR>          ARA-SGPN_Inverter_v0.1.3
11/02/2020  05:19 PM    <DIR>          BAPS_PhaseShift-Buck_PI_v0.1.3
11/02/2020  05:19 PM    <DIR>          BAPS_PhaseShift-Buck_PI_v0.2.1
11/02/2020  05:19 PM    <DIR>          BAPS_PhaseShift-Buck_PI_v0.2.2
11/02/2020  05:20 PM    <DIR>          BAPS_PhaseShift-Buck_PI_v0.2.3
01/14/2021  12:35 PM    <DIR>          BAPS_PhaseShift-Buck_PI_v0.2.4
11/02/2020  05:20 PM    <DIR>          Blinky_v0.2.1
11/02/2020  05:20 PM    <DIR>          Buck_Boost_Inverter_PI_v0.3.1
11/02/2020  05:20 PM    <DIR>          Buck_Boost_Inverter_PI_v0.3.2
11/02/2020  05:20 PM    <DIR>          H2G_Interleaved-Buck_PI_v0.1.0
11/02/2020  05:21 PM    <DIR>          H2G_Interleaved-Buck_PI_v0.2.1
11/02/2020  05:21 PM    <DIR>          H2G_Interleaved-Buck_PI_v0.2.2
12/09/2020  12:05 AM    <DIR>          H2G_Interleaved-Buck_PI_v0.2.3
01/03/2021  08:21 PM    <DIR>          H2G_Interleaved-Buck_PI_v0.2.4
01/12/2021  01:52 PM    <DIR>          H2G_Interleaved-Buck_PI_v0.2.5
09/01/2020  10:31 PM    <DIR>          RemoteSystemsTempFiles
11/02/2020  05:21 PM    <DIR>          SmallUCB-Testing_Modbus_v0.0.2
               0 File(s)              0 bytes
              25 Dir(s)  571,163,316,224 bytes free

C:\Users\tesla\workspace_v8>dir

C:\Users\tesla\workspace_v8>
```

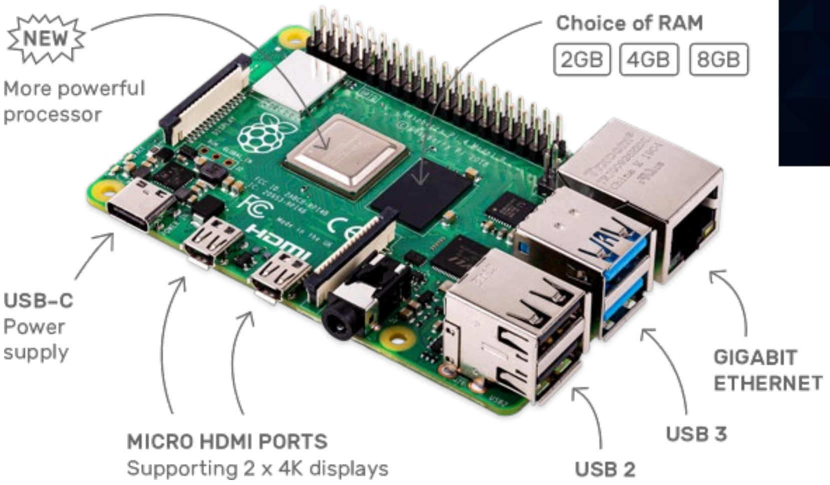
## Software downloads:

- Microsoft Office 365 Student Download
- **MSDNAA**

# Linux Configuration (GUI)

- VMWare
- Ubuntu
- Redhat
- CentOS
- KALI
- Raspian

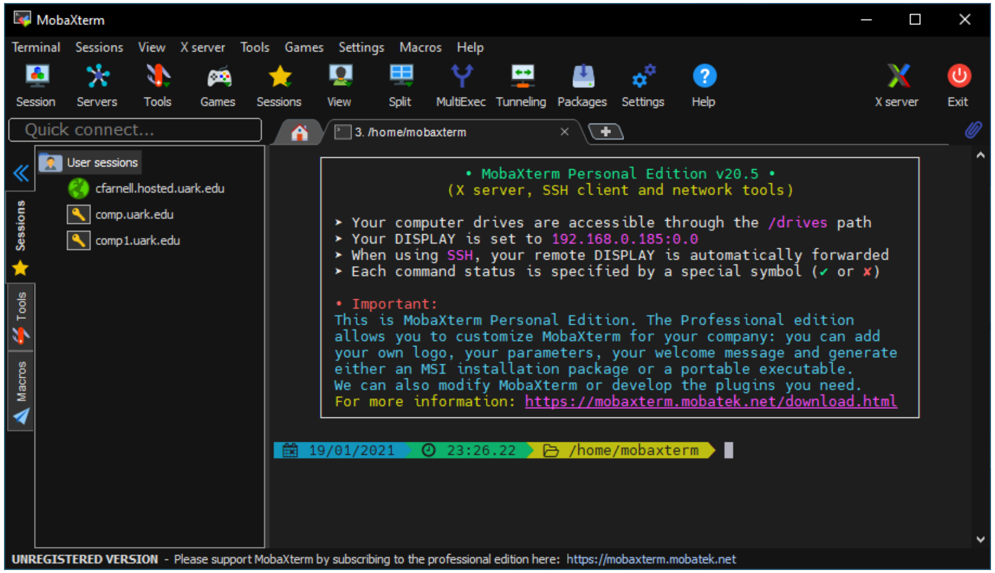

Kali-Linux-2020.4-vmware-amd64 - VMware Workstation 16 Player (Non-commercial use only)
Player
12:32 AM
Trash
File System
Home
KALI
BY OFFENSIVE SECURITY



# Linux Configuration (Cmd)

## ❖ Review Common Commands

- pwd
- cd
- ls
- ls –la
- uname
- mkdir
- cp
- chmod a+x
- rm –rf (Extreme caution)
- cat
- vim
- ping
- ifconfig
- sudo (Extreme caution)
- apt-get install



MobaXterm
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help X server Exit
Quick connect...
3. /home/mobaxterm
User sessions
cfarnell.hosted.uark.edu
comp.uark.edu
comp1.uark.edu
Sessions
Tools
Macros

```
• MobaXterm Personal Edition v20.5 •
(X server, SSH client and network tools)

➤ Your computer drives are accessible through the /drives path
➤ Your DISPLAY is set to 192.168.0.185:0.0
➤ When using SSH, your remote DISPLAY is automatically forwarded
➤ Each command status is specified by a special symbol (✓ or ✗)

• Important:
This is MobaXterm Personal Edition. The Professional edition
allows you to customize MobaXterm for your company: you can add
your own logo, your parameters, your welcome message and generate
either an MSI installation package or a portable executable.
We can also modify MobaXterm or develop the plugins you need.
For more information: https://mobaxterm.mobatek.net/download.html

19/01/2021  23:26.22  /home/mobaxterm
```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

## ❖ ELEG Linux Server

- ssh -X username@aperturescience.uark.edu

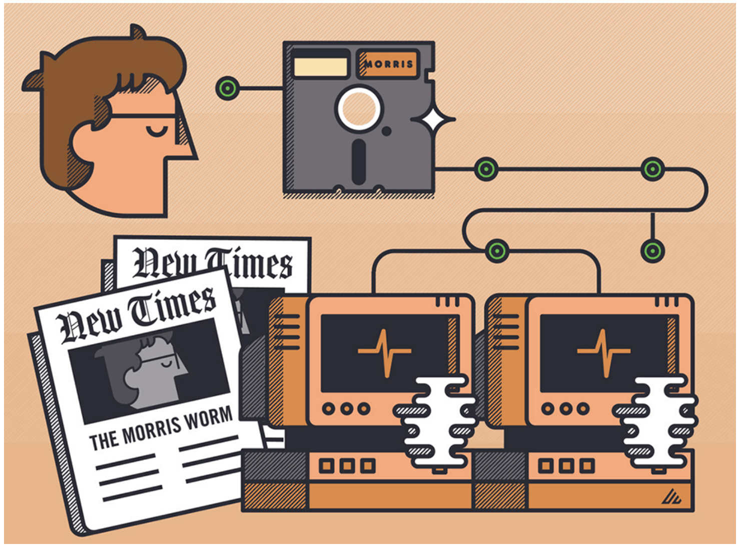
## ❖ Further Reading

- https://ubuntu.com/tutorials/command-line-for-beginners#1-overview
- https://maker.pro/linux/tutorial/basic-linux-commands-for-beginners
- https://www.hostinger.com/tutorials/linux-commands

# With any new technology comes people trying to exploit it…

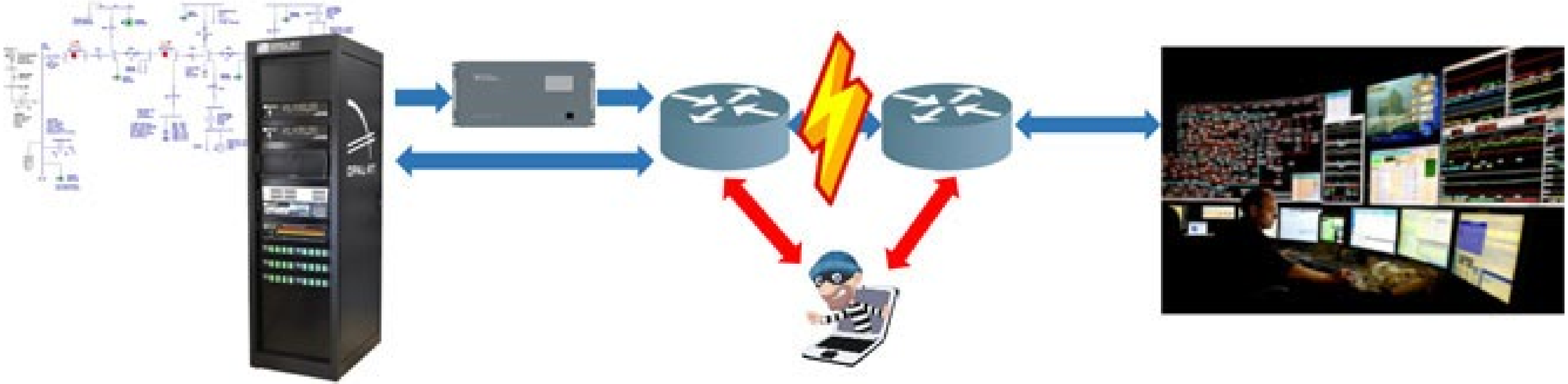
## The Morris Worm

- **First computer worm to be distributed by internet**
  - **A worm is malware that replicates itself to spread to other systems**
- **Used three different exploits to gain access to computers**
- **Worm duplicated every seventh instance, but still its growth was exponential**
- **Robert Morris was the first individual to be charged under the Computer Fraud and Abuse Act**
- **He would go on to become a professor at MIT…**



https://www.exabeam.com/information-security/cybersecurity-calendar-morris-worm/

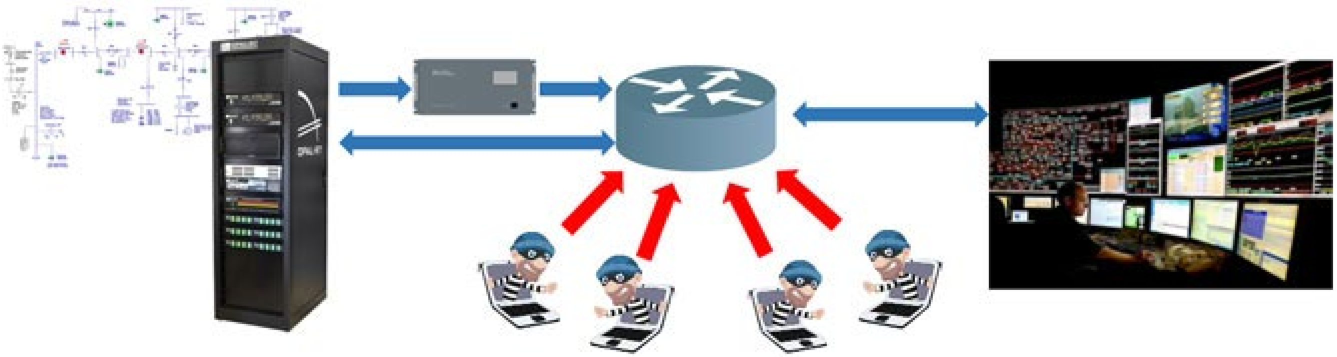
# Attack Scenario I



Man-in-the-Middle attack diagram. Credit: OPAL-RT

**Man-in-the-Middle (MitM)**
**A MitM situation occurs when an external attacker is capable of intercepting, modifying, suppressing or replaying network packets undetected by tricking two communication nodes to believe they are still communicating normally.**

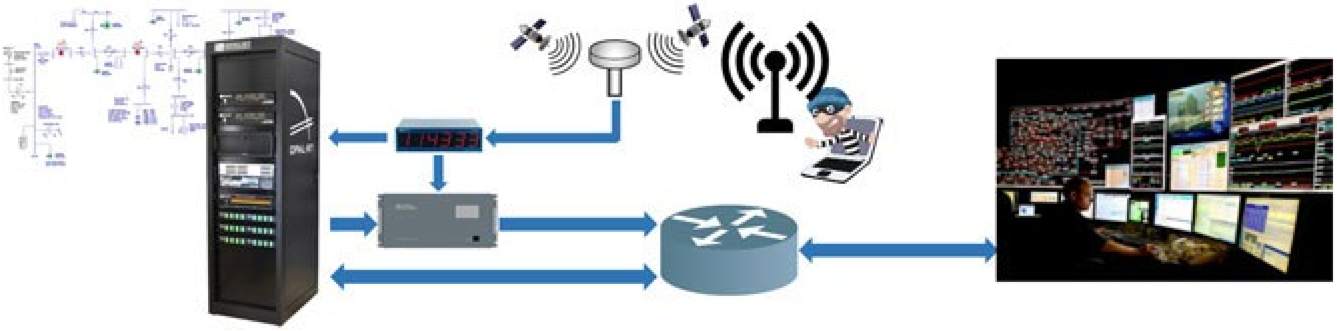
# Attack Scenario II



Denial-of-Service attack diagram. Credit: OPAL-RT

**Denial-of-Service (DoS)**
**DoS can render a service unavailable either through a direct or indirect attack. It also refers to physical attacks on communication infrastructure, such as the cutting of wires or wireless jamming.**

# Attack Scenario III



GPS Spoofing attack diagram. Credit: OPAL-RT

**GNSS Spoofing/Meaconing**

**The act of causing Global Navigation Satellite System (GNSS) receivers to lock onto simulated or replayed satellite signals instead of real ones, effectively causing the receiver to locate itself at the wrong position and/or time. This class of attack is a major threat to PMU and synchrophasor systems, which are heavily reliant on time synchronization.**

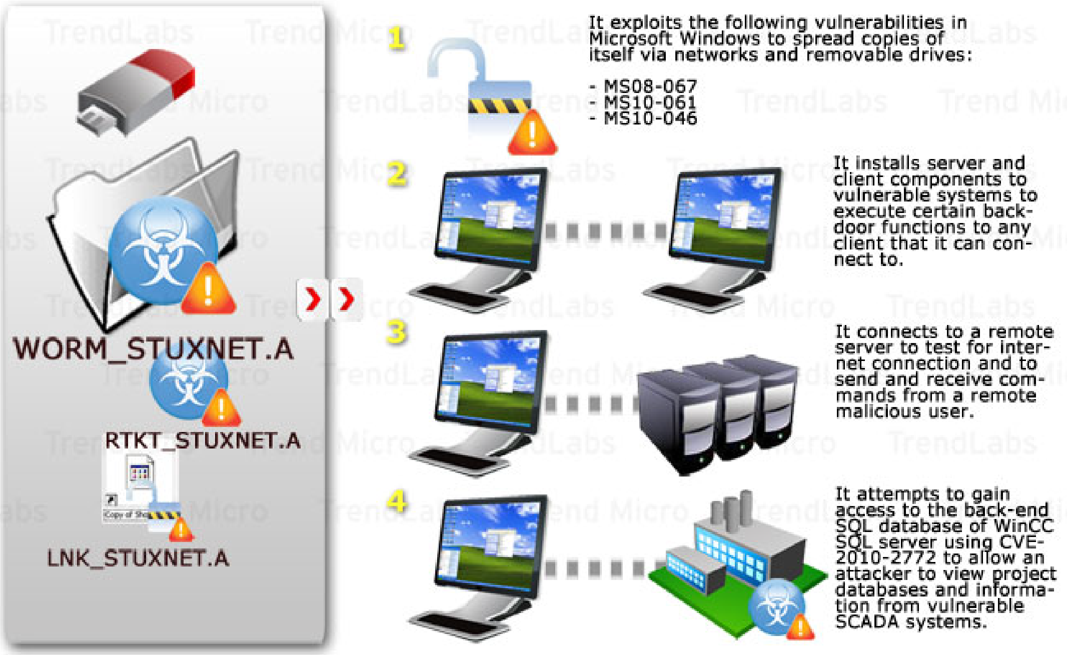
# ICS Malware Timeline

## Timeline of ICS Malware

- Stuxnet 2010 – Iranian Centrifuge Attack
  - Periodic Overspeed of Centrifuges (Lifetime Reduction)
  - Reported Normal Conditions to SCADA
- Havex 2013 (RAT) – Multiple Targets
  - Energy, Aviation, Pharmaceutical, Defense, and Petrochemical Sectors
- BlackEnergy 3 2015 – Ukraine Energy Grid (Mostly Manual)
  - DDoS, KillDisk, RAT
- Industroyer1\CrashOveride 2016 – Ukraine Energy Grid (Mostly Automated)
  - ICS protocols IEC101, IEC104, IEC61850, and OPC-DA
  - Open\Close Breaker Commands, Scanning\Mapping, DoS, KillDisk\Wiper
  - Limited Knowledge of Protocols Demonstrated
- TRISIS 2017 – One Middle East Victim Identified
  - Safety Systems Targeted
  - Not Highly Scalable
  - Deeper Understanding of Protocols
- Pipedream – 2022 No Known Victims
  - Evil Scholar, BadOmen, MouseHole, DustTunnel, LazyCargo
  - FINS, ModBus, CODESYS Libraries, OPC UA, Schneider Electric NetMange
  - Very Advanced Toolkit; Mitigation Began "Left of Bang"; Metasploit Analogs
  - Combines Aspects of CrashOverride and TRISIS

# Stuxnet Attack

- Advanced Malware Targeting Industrial Systems [4]
- Allowed Access to Discover Facility Architecture
- Specific System Function Calls Sent to Field Devices [5]
- Destroyed an Estimated 984 Nuclear Centrifuges [6]

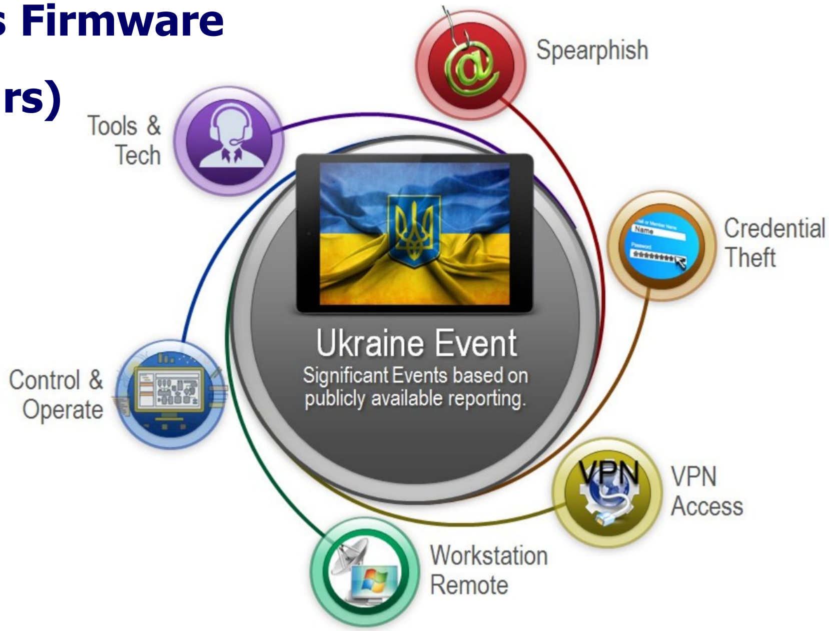


1. It exploits the following vulnerabilities in Microsoft Windows to spread copies of itself via networks and removable drives:
   - MS08-067
   - MS10-061
   - MS10-046
2. It installs server and client components to vulnerable systems to execute certain backdoor functions to any client that it can connect to.
3. It connects to a remote server to test for internet connection and to send and receive commands from a remote malicious user.
4. It attempts to gain access to the back-end SQL database of WinCC SQL server using CVE-2010-2772 to allow an attacker to view project databases and information from vulnerable SCADA systems.

**Stuxnet diagram.**
**Credit: Trendmicro [7]**

# 2015 Ukraine Attack

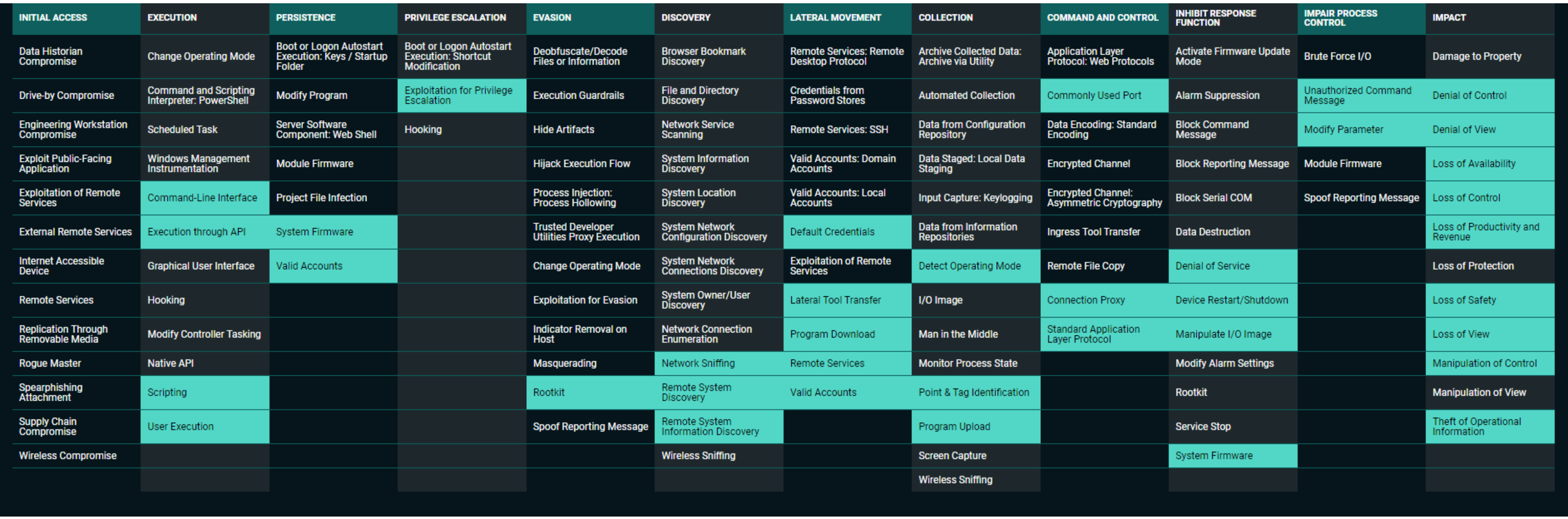
- **Utilized "Black Energy 3" Malware**
- **Gained Access to Industrial Control Systems (ICSs)**
- **Target Field Devices Using Custom Malicious Firmware**
- **225,000 Customers Without Power (1-6 hours)**
- **30 Substations Disabled**



Overlapping vulnerabilities and attacks related to Ukraine Event. Source: E-ISAC-TLP Report [8]

- **DoS Attack** Utilized bots to "flood" Call/Service centers
- **Malicious Firmware** Disabled and/or destroyed devices
- **Spearfishing** Resulted in employees providing credentials
- **Malware** Implemented DDoS and Trojan Botnet "Black Energy"

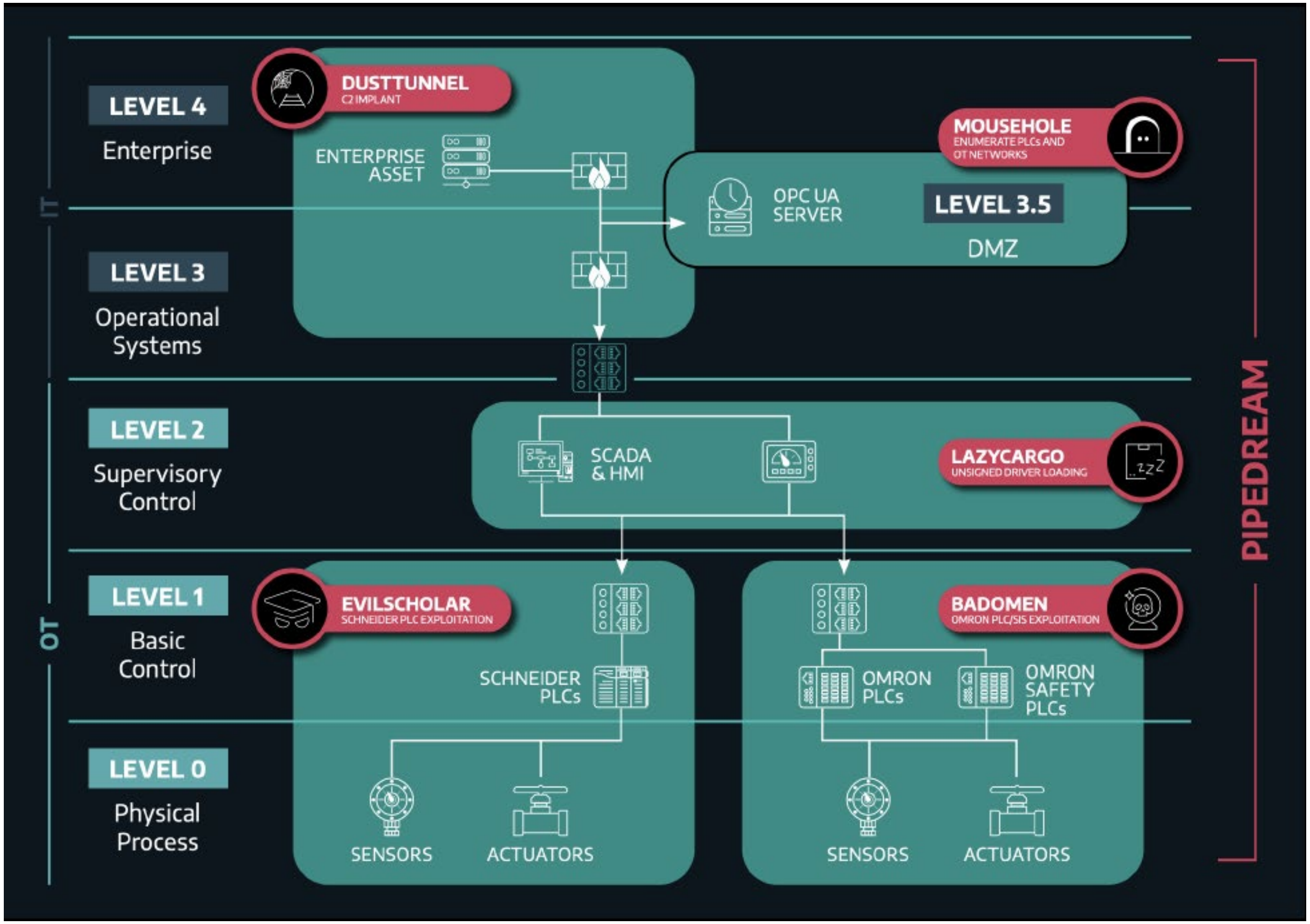
# PIPEDREAM: MITRE ATT&CK for ICS



| INITIAL ACCESS | EXECUTION | PERSISTENCE | PRIVILEGE ESCALATION | EVASION | DISCOVERY | LATERAL MOVEMENT | COLLECTION | COMMAND AND CONTROL | INHIBIT RESPONSE FUNCTION | IMPAIR PROCESS CONTROL | IMPACT |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Data Historian Compromise | Change Operating Mode | Boot or Logon Autostart Execution: Keys / Startup Folder | Boot or Logon Autostart Execution: Shortcut Modification | Deobfuscate/Decode Files or Information | Browser Bookmark Discovery | Remote Services: Remote Desktop Protocol | Archive Collected Data: Archive via Utility | Application Layer Protocol: Web Protocols | Activate Firmware Update Mode | Brute Force I/O | Damage to Property |
| Drive-by Compromise | Command and Scripting Interpreter: PowerShell | Modify Program | Exploitation for Privilege Escalation | Execution Guardrails | File and Directory Discovery | Credentials from Password Stores | Automated Collection | Commonly Used Port | Alarm Suppression | Unauthorized Command Message | Denial of Control |
| Engineering Workstation Compromise | Scheduled Task | Server Software Component: Web Shell | Hooking | Hide Artifacts | Network Service Scanning | Remote Services: SSH | Data from Configuration Repository | Data Encoding: Standard Encoding | Block Command Message | Modify Parameter | Denial of View |
| Exploit Public-Facing Application | Windows Management Instrumentation | Module Firmware | | Hijack Execution Flow | System Information Discovery | Valid Accounts: Domain Accounts | Data Staged: Local Data Staging | Encrypted Channel | Block Reporting Message | Module Firmware | Loss of Availability |
| Exploitation of Remote Services | Command-Line Interface | Project File Infection | | Process Injection: Process Hollowing | System Location Discovery | Valid Accounts: Local Accounts | Input Capture: Keylogging | Encrypted Channel: Asymmetric Cryptography | Block Serial COM | Spoof Reporting Message | Loss of Control |
| External Remote Services | Execution through API | System Firmware | | Trusted Developer Utilities Proxy Execution | System Network Configuration Discovery | Default Credentials | Data from Information Repositories | Ingress Tool Transfer | Data Destruction | | Loss of Productivity and Revenue |
| Internet Accessible Device | Graphical User Interface | Valid Accounts | | Change Operating Mode | System Network Connections Discovery | Exploitation of Remote Services | Detect Operating Mode | Remote File Copy | Denial of Service | | Loss of Protection |
| Remote Services | Hooking | | | Exploitation for Evasion | System Owner/User Discovery | Lateral Tool Transfer | I/O Image | Connection Proxy | Device Restart/Shutdown | | Loss of Safety |
| Replication Through Removable Media | Modify Controller Tasking | | | Indicator Removal on Host | Network Connection Enumeration | Program Download | Man in the Middle | Standard Application Layer Protocol | Manipulate I/O Image | | Loss of View |
| Rogue Master | Native API | | | Masquerading | Network Sniffing | Remote Services | Monitor Process State | | Modify Alarm Settings | | Manipulation of Control |
| Spearphishing Attachment | Scripting | | | Rootkit | Remote System Discovery | Valid Accounts | Point & Tag Identification | | Rootkit | | Manipulation of View |
| Supply Chain Compromise | User Execution | | | Spoof Reporting Message | Remote System Information Discovery | | Program Upload | | Service Stop | | Theft of Operational Information |
| Wireless Compromise | | | | | Wireless Sniffing | | Screen Capture | | System Firmware | | |
| | | | | | | | Wireless Sniffing | | | | |

Source : DRAGOS.com

# PIPEDREAM: Example Deployment



**Source : DRAGOS.com**

# Cyber Kill Chain

e, and MiTM Attacks

**Stage 1: Planning, Preparation, Cyber Intrusion, Management and Enablement (Explore/Exploit), Deployment and Entrenchment (Execute Malware)**

**Stage 2: Attack Development, Validation, ICS Attack**

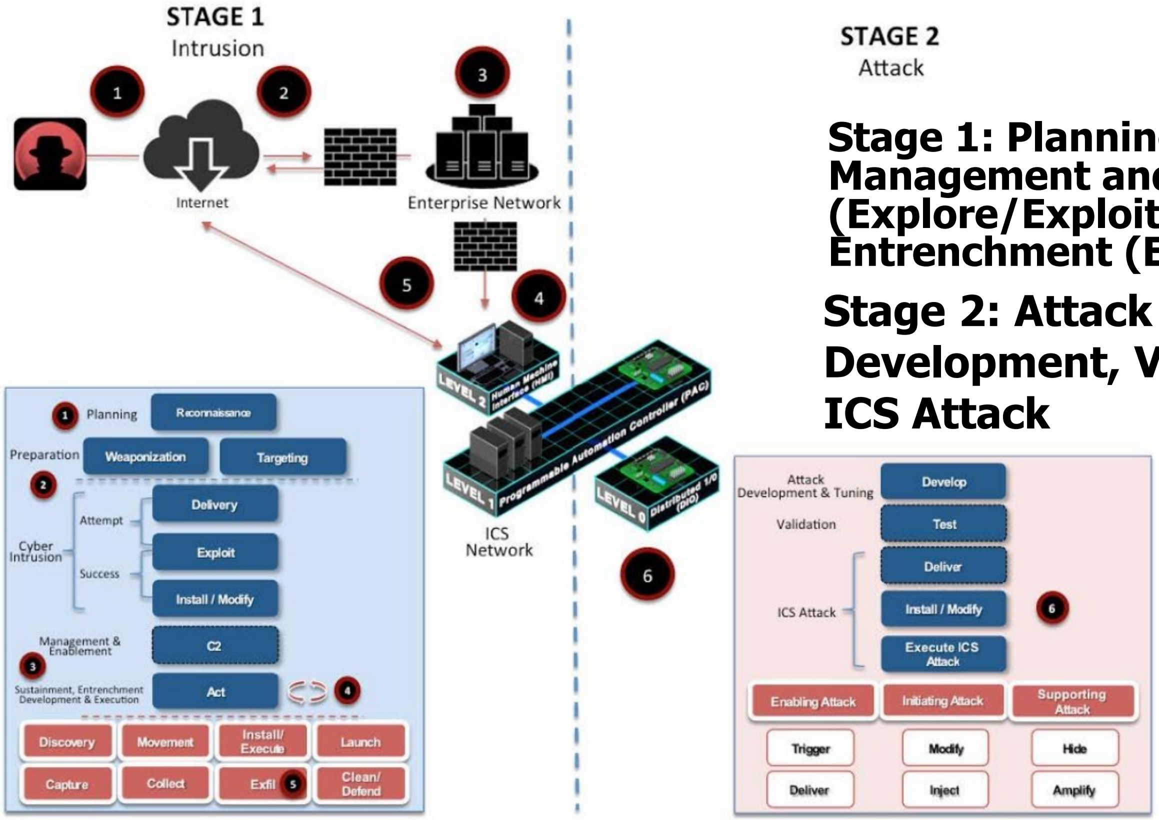


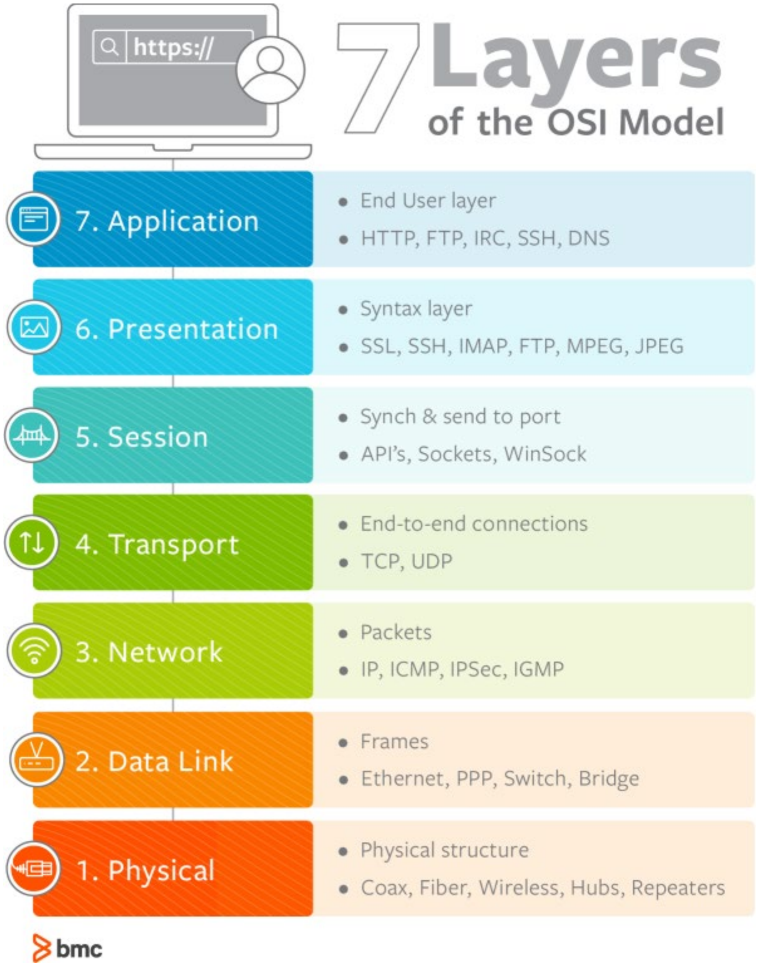
**Diagram of stages of ICS Cyber Kill Chain. Source: Idaho National Labs Aug 2016 "INL/EXT-16-40692" [9]**

# Additional Attacks/Notes

- Florida’s Oldsmar Water Treatment System
  - Sodium hydroxide, or lye, to more than 100 times normal
  - TeamViewer, Potential of shared passwords for remote access
- Aurora Generator Test
  - 27-Ton Generator vs less than 30 lines of code
  - Kinetic Attacks
- Bingham County Ransomware
  - Brute-Force Attack on Open Port
  - Paid Ransom to restore two servers
- Coffee Machine Ransomware
  - Unencrypted WiFi
  - No code signing for firmware updates
- SolarWinds
  - Software Supply Chain and Firmware Attacks
  - Compromised update to SolarWinds' Orion software
  - Currently believed March 2020 Campaign Start Date
  - Backdoor access to allow credential harvesting and pivoting

# OSI 7-Layer Network Model

- Open Systems Interconnection (OSI) model
- The OSI model is a reference framework that explains the process of transmitting data between computers.
- Please Do Not Throw Sausage Pizza Away

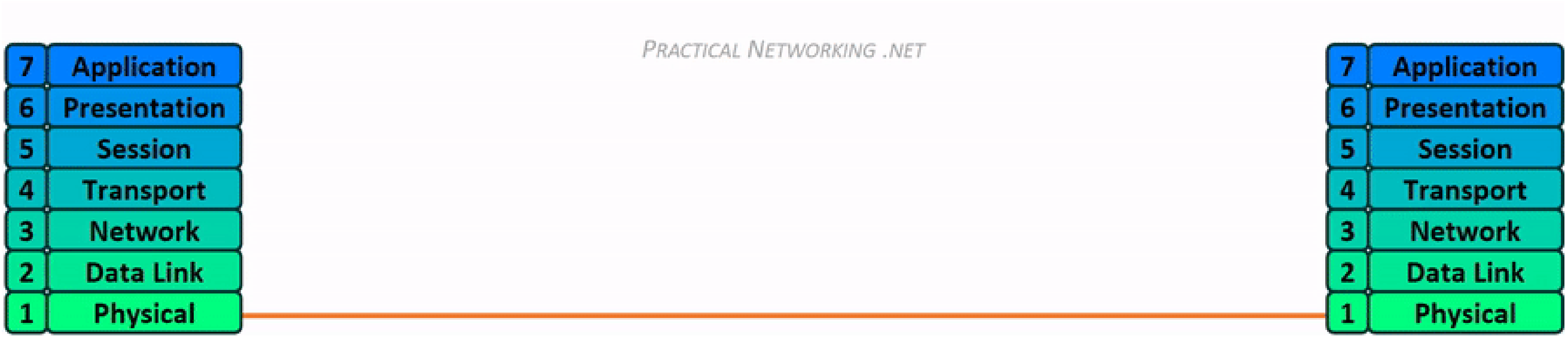


| Layer | |
|---|---|
| 7. Application | End User layer<br>HTTP, FTP, IRC, SSH, DNS |
| 6. Presentation | Syntax layer<br>SSL, SSH, IMAP, FTP, MPEG, JPEG |
| 5. Session | Synch & send to port<br>API's, Sockets, WinSock |
| 4. Transport | End-to-end connections<br>TCP, UDP |
| 3. Network | Packets<br>IP, ICMP, IPSec, IGMP |
| 2. Data Link | Frames<br>Ethernet, PPP, Switch, Bridge |
| 1. Physical | Physical structure<br>Coax, Fiber, Wireless, Hubs, Repeaters |

*Source: https://www.bmc.com/blogs/osi-model-7-layers/

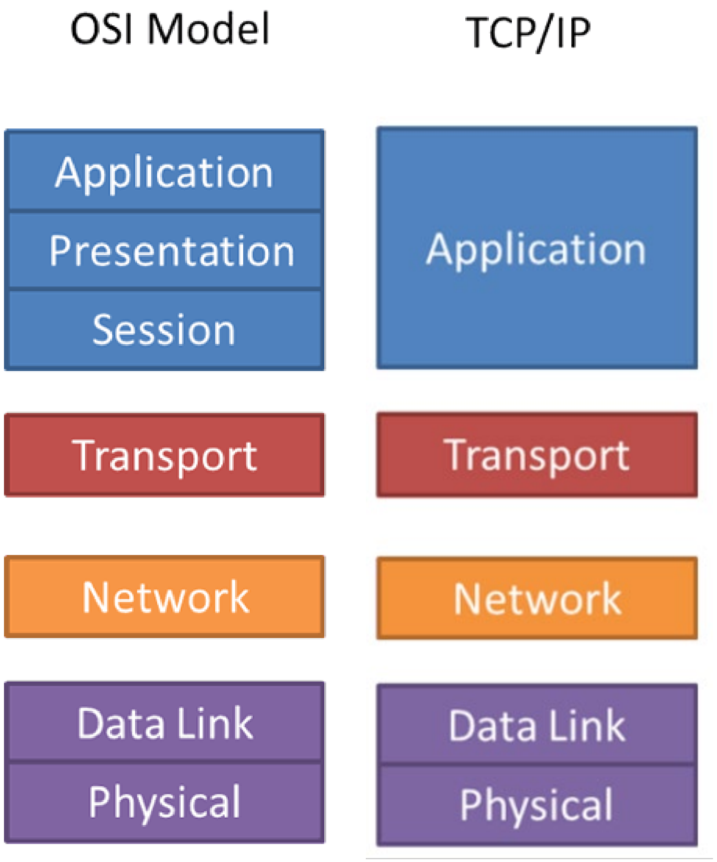
# OSI 7-Layer Network Model

- How does data move through the layers?
- As the data is handed from layer to layer, each layer adds the information it requires to accomplish its goal before the complete datagram is converted to 1s and 0s and sent across the wire.



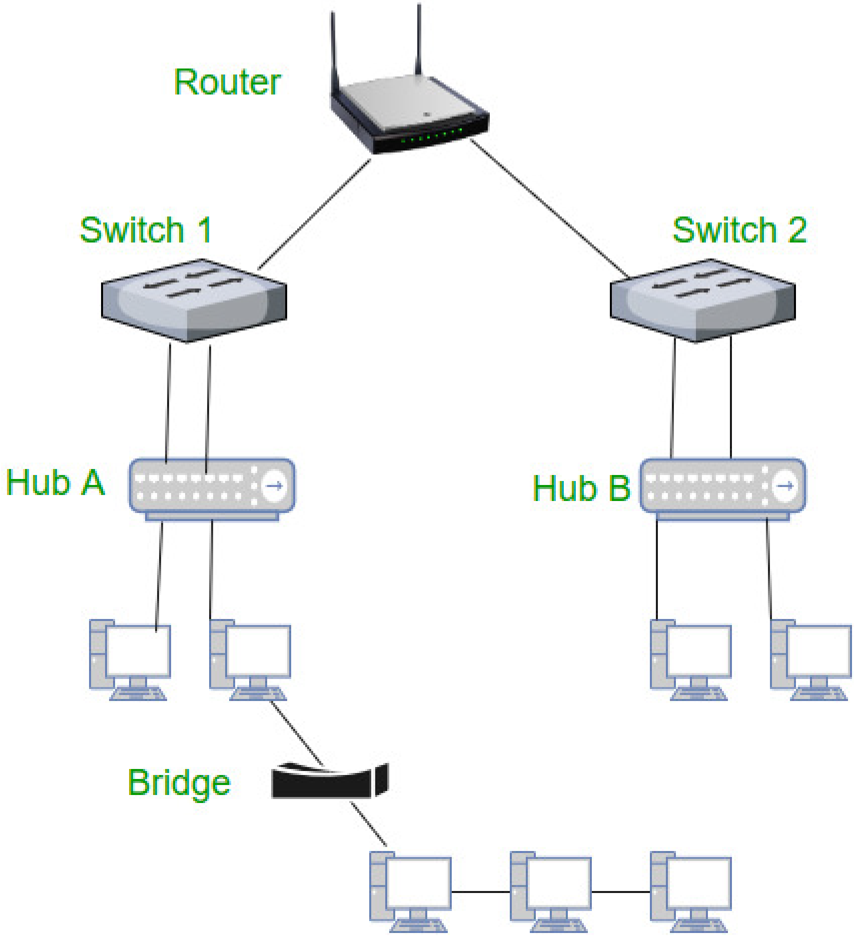
*Source: https://www.practicalnetworking.net/series/packet-traveling/osi-model/

# OSI vs TCP/IP


OSI Model
TCP/IP
Application
Presentation
Session
Application
Transport
Transport
Network
Network
Data Link
Physical
Data Link
Physical

# Networking Devices

- **Computer/Client**
  - **User Interface**
- **Servers**
  - **DHCP,DNS, Active Directory**
- **Ethernet Cables**
  - **Physical Media**
  - **Layer 1**
- **Hubs**
  - **Multiport repeaters**
  - **Layer 1 Devices (Media)**
- **Switches**
  - **DHCP,DNS, Active Directory**
  - **Layer 2 Devices (MAC)**
- **Routers**
  - **Connect Different Networks**
  - **Layer 3 Devices (IP)**



***Source:** https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/