OmniSOC

Honeypot Demo

Connect to the demo wireless network:

- SSID: **RSOCDEMO**
- Password: **This is awesome!**
- Make sure you are getting an IP address between:
  - **192.168.123.150**
  - **192.168,123,200**

Interact with the two honeypots:

- 192.168.123.100
- 192.168.123.101

Where we’re going

Topics:

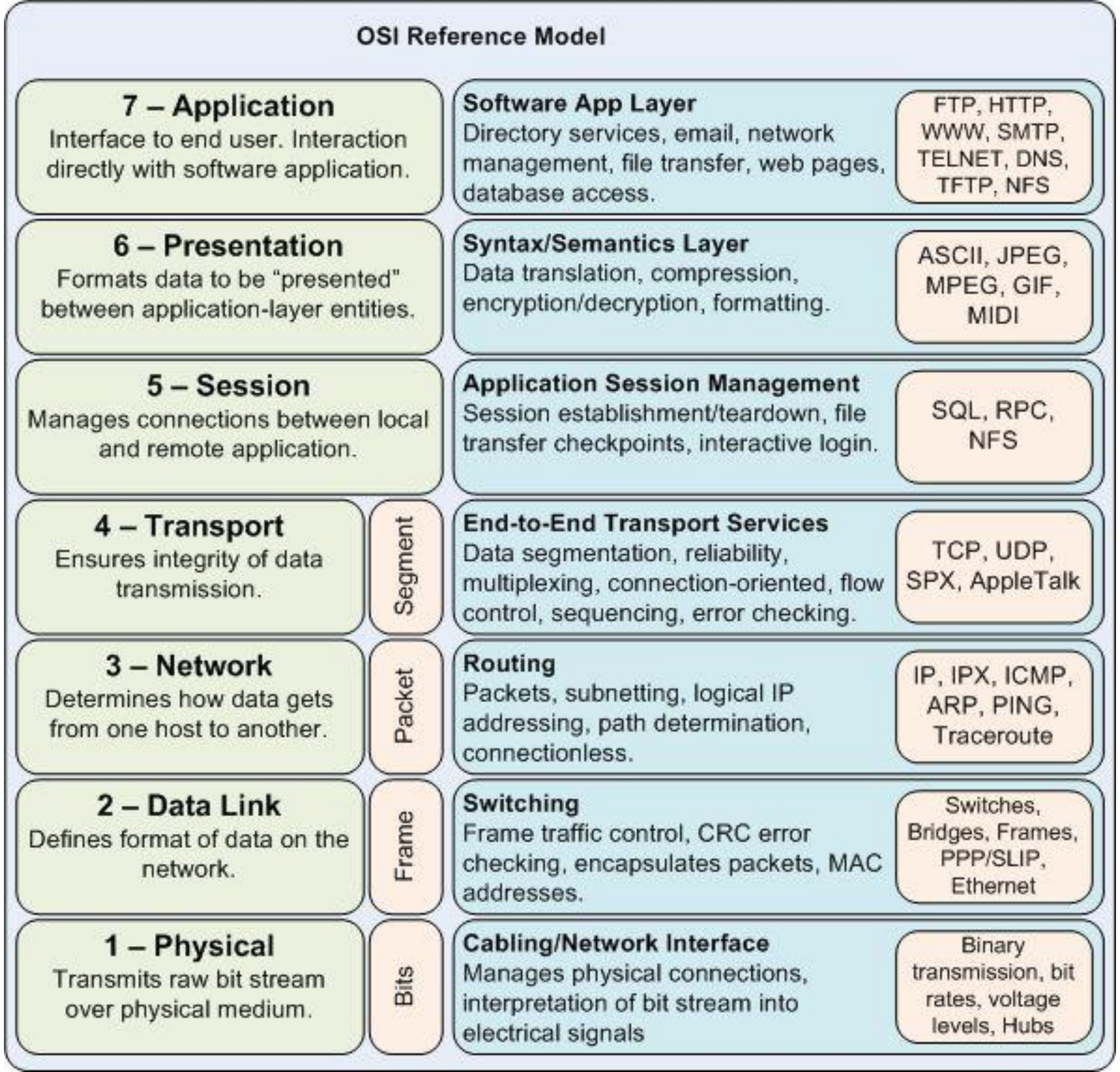
1. Fundamentals
2. Jargon
3. The OSI Model
4. Core protocols

Tools:

1. pcaps/tcpdump/wireshark
2. traceroute/tracert/mtr
3. nmap
4. Honeypots

Jargon disambiguation!

- Protocols are standards for different networking functionality
- Packets are the individual messages sent by nodes on a network.
- Encapsulation is the process of building a network packet
- Ports are used to tell computers what software should get the data
- IP addresses identify nodes on an IP network
- Domain Names are human readable names that are translated into IP addresses.



OSI Reference Model

7 – Application Interface to end user. Interaction directly with software application.		**Software App Layer** Directory services, email, network management, file transfer, web pages, database access.	FTP, HTTP, WWW, SMTP, TELNET, DNS, TFTP, NFS
6 – Presentation Formats data to be "presented" between application-layer entities.		**Syntax/Semantics Layer** Data translation, compression, encryption/decryption, formatting.	ASCII, JPEG, MPEG, GIF, MIDI
5 – Session Manages connections between local and remote application.		**Application Session Management** Session establishment/teardown, file transfer checkpoints, interactive login.	SQL, RPC, NFS
4 – Transport Ensures integrity of data transmission.	Segment	**End-to-End Transport Services** Data segmentation, reliability, multiplexing, connection-oriented, flow control, sequencing, error checking.	TCP, UDP, SPX, AppleTalk
3 – Network Determines how data gets from one host to another.	Packet	**Routing** Packets, subnetting, logical IP addressing, path determination, connectionless.	IP, IPX, ICMP, ARP, PING, Traceroute
2 – Data Link Defines format of data on the network.	Frame	**Switching** Frame traffic control, CRC error checking, encapsulates packets, MAC addresses.	Switches, Bridges, Frames, PPP/SLIP, Ethernet
1 – Physical Transmits raw bit stream over physical medium.	Bits	**Cabling/Network Interface** Manages physical connections, interpretation of bit stream into electrical signals	Binary transmission, bit rates, voltage levels, Hubs

Internet Protocol (IP)

Get packets from a source to a destination.

Internet Protocol (IP): IPv4 addressing

00000001.00000001.00000001.00000001 = 1.1.1.1

11111111.11111111.11111111.11111111 = 255.255.255.255

For the subnet 192.168.123.0/24 the default broadcast address is:

192.168.123.255

Internet Protocol (IP): IPv4 Subnets

192.168.0.0/24: 24 bits address range, 8 bits for subnet = 256 possible addresses in range.

Practically speaking, this is 192.168.0.2 - 192.168.0.254

- 192.168.0.0 - defines the subnet
- 192.168.0.1 - Often the gateway address, if linked to other networks.
  - Really can be any of the IP addresses except the first and last. Could be more than one!

Internet Protocol (IP): IPv4 Reserved Ranges

Reserved range examples:

1. 10.0.0.0/8 - Private network range
2. 172.16.0.0/12 - Private network range
3. 192.168.0.0/16 - Private network range
4. 127.0.0.0/8 - Loopback address range
5. 100.64.0.0/10 - Carrier grade NAT

Full list, IPv4:
https://www.iana.org/assignments/iana-ipv4-special-registry/iana-ipv4-special-registry.xhtml

TCP

“Do you want a glass of water?”
“Yes, I’d like a glass of water.”
“Ok, here’s a glass of water.”
“Thanks for the glass of water”
“Was that glass of water good?”
“Yeah, that glass of water was good. Please give me another”

UDP

“Here, have this glass of water”

TCP

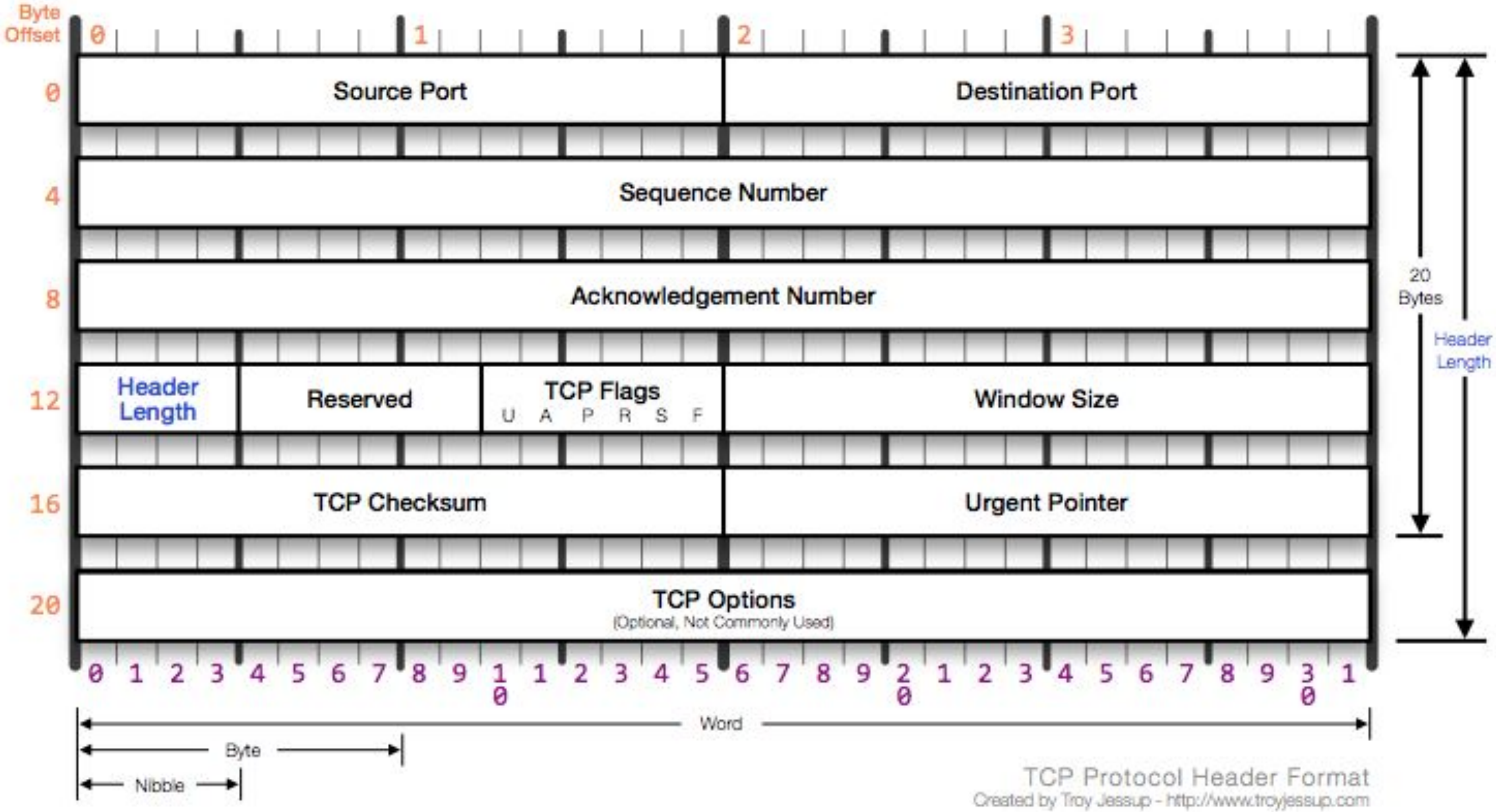
- Recipient can guarantee that data is error free and in the correct order,
- Establishes and maintains organized “sessions”
- Common examples: Email, web browsing, FTP, SSH

UDP

- Guarantees integrity of each individual packet, but not all the data sent.
- Doesn’t guarantee order of data or that it will all arrive
- “Just send it”
- Common examples: audio/video streaming, computer games, some network protocols that handle integrity checking separately

TCP Header

RFC 793 Outlines the TCP Protocol



Source Port

Destination Port

Sequence Number

Acknowledgement Number

Header Length

Reserved

TCP Flags

U A P R S F

Window Size

TCP Checksum

Urgent Pointer

TCP Options

(Optional, Not Commonly Used)

TCP Protocol Header Format

Created by Troy Jessup - http://www.troyjessup.com

Trace Route

- Time To Live (TTL) field in the IP packet
  - Meant to prevent loops in routes from causing infinite problems.
  - Each time a packet arrives at a router the TTL is decreased by one. If it reaches zero, the router sends a ICMP TTL EXCEEDED message back to the sender.
- Trace Route takes advantage of TTL to get the IP address of router interfaces in the path.
- Some routers are configured not to send these messages.
- tracert - Windows
- traceroute - Linux and Mac OS
- mtr - One of the fancier traceroute applications.

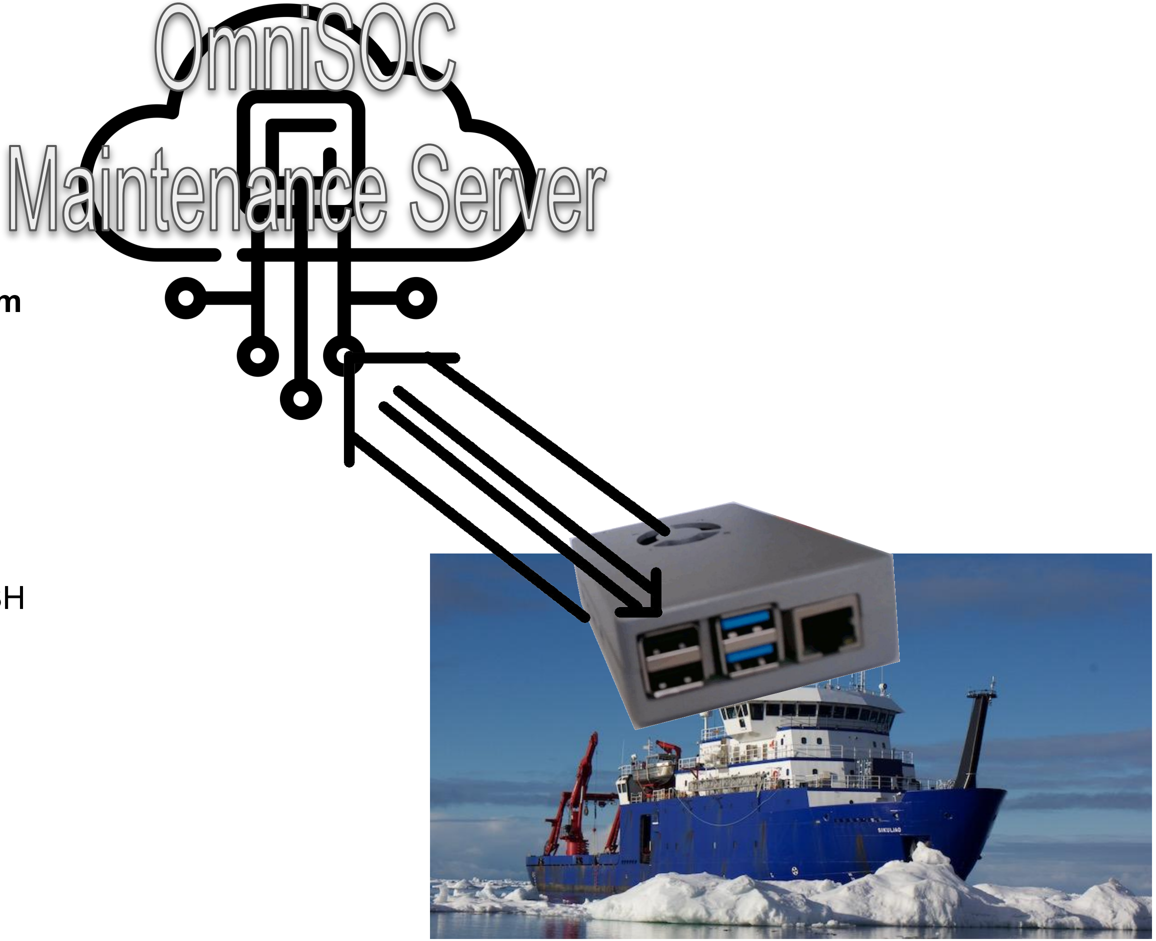
Network Mapper - nmap

- Great for discovering and getting information about devices on a network.
- Basic scan:
    - nmap -sT -p 0-65535 192.168.123.0/24
        - nmap - the command itself
        - -sT - scan for TCP ports using a full handshake
        - -p 0-65535 - scan all the ports
        - 192.168.123.0/24 - the subnet of IP addresses to scan
- https://nmap.org/

Light-touch

Once deployed OmniSOC VCS team performs all OS and software maintenance.

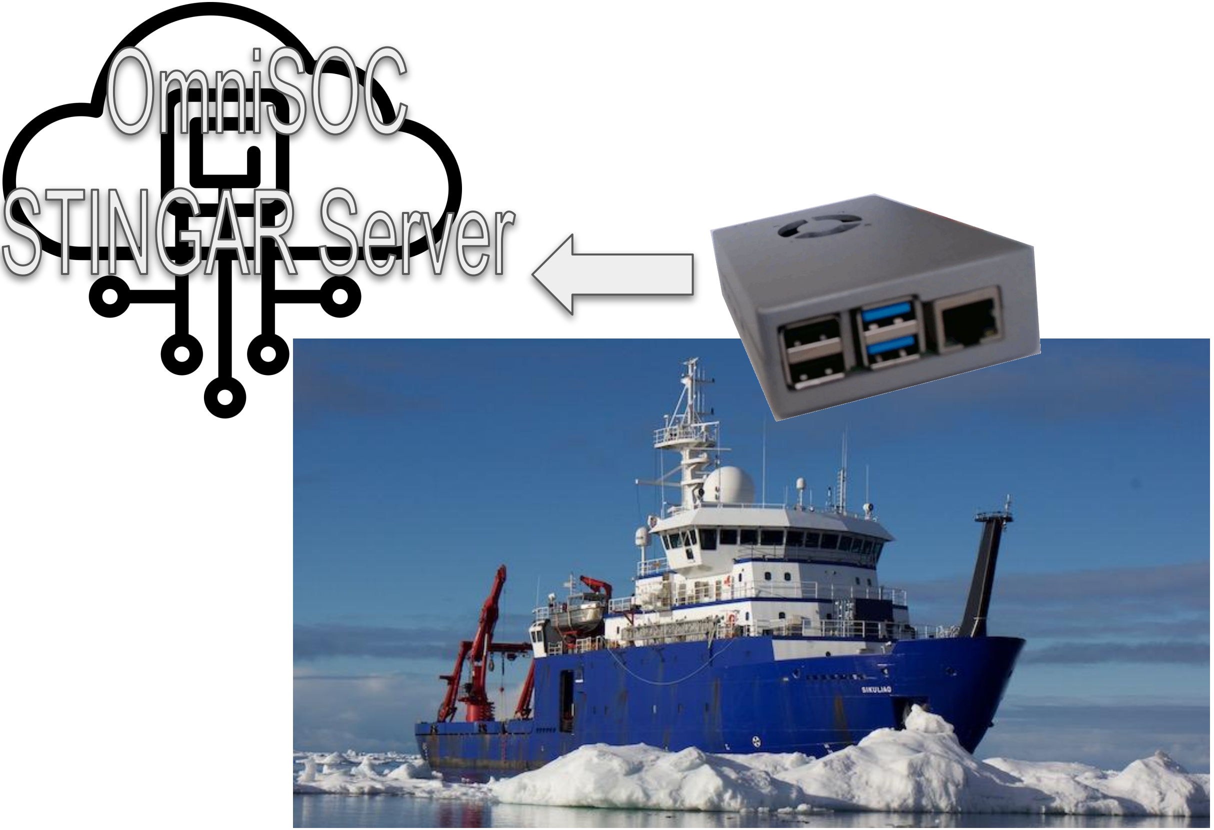
- **AutoSSH maintains an SSH tunnel to OmniSOC Maintenance Server**
  - VCS Team then can SSH into Honeypot
- **Hardened SSH servers on both ends.**
- **Authentication between honeypots and servers are not dependent on outside sources.**



Light-touch

Honeypot data is sent to OmniSOC's STINGARv2 Server using FluentBit.

- **Data is secure in transit.**
- **Honeypot data is cached on the honeypot if not able to report to STINGARv2 server.**
- **OmniSOC monitors honeypot data.**
- **Alerts if action is required.**



OmniSOC
STINGAR Server

Reliable

OmniSOC Maintenance & STINGAR Server

Designed to be reliable:

- **AutoSSH maintains an SSH tunnel to OmniSOC Maintenance Server**
- **FlunentBit will automatically reconnect to STINGARv2 server if the connection is lost.**
- **Honeypot data is stored on the honeypot until transmitted to STINGARv2 server.**
- **Honeypots maintains services automatically.**

Durable & Replaceable

OmniSOC Maintenance & STINGAR Server

- **Honeypots**
  - **Components are all docker containers; something goes wrong blow it away and deploy again.**
  - **Deployed VMs and Raspberry Pi are docker hosts, can easily be re-deployed.**

© VISIONS 11 UNIVERSITY OF WASHINGTON
PHOTO BY ALLISON FUNDIS

Cowrie

SSH/Telnet

- **Listenings on:**
  - **Telnet standard port: TCP 23**
  - **SSH standard port: TCP 22**
- **Records:**
  - **Credentials used**
  - **Commands attempted**
- **Detection:**
  - **Usernames and Passwords being used**
  - **Attackers infrastructure**

©VISIONS 11 UNIVERSITY OF WASHINGTON
PHOTO BY ALLISON FUNDIS

Conpot

Industrial Control System Services

- **Listenings on:**
  - **FTP: TCP 21**
  - **Trivial FTP (TFTP): TCP 69**
  - **HTTP: TCP 80**
  - **Simple Network Management Protocol (SNMP): TCP 161**
  - **Modbus Protocol: TCP 502**
  - **IPMI: TCP 623**
  - **EtherNet/IP explicit messaging: TCP 44818**
  - **BACnet Building Automation and Control Networks: TCP 47808**
- **Records various details depending on the service emulation.**