CENTER OF ACADEMIC EXCELLENCE

Cyber Operations

CYBV474
Advanced Analytics for Security Operations

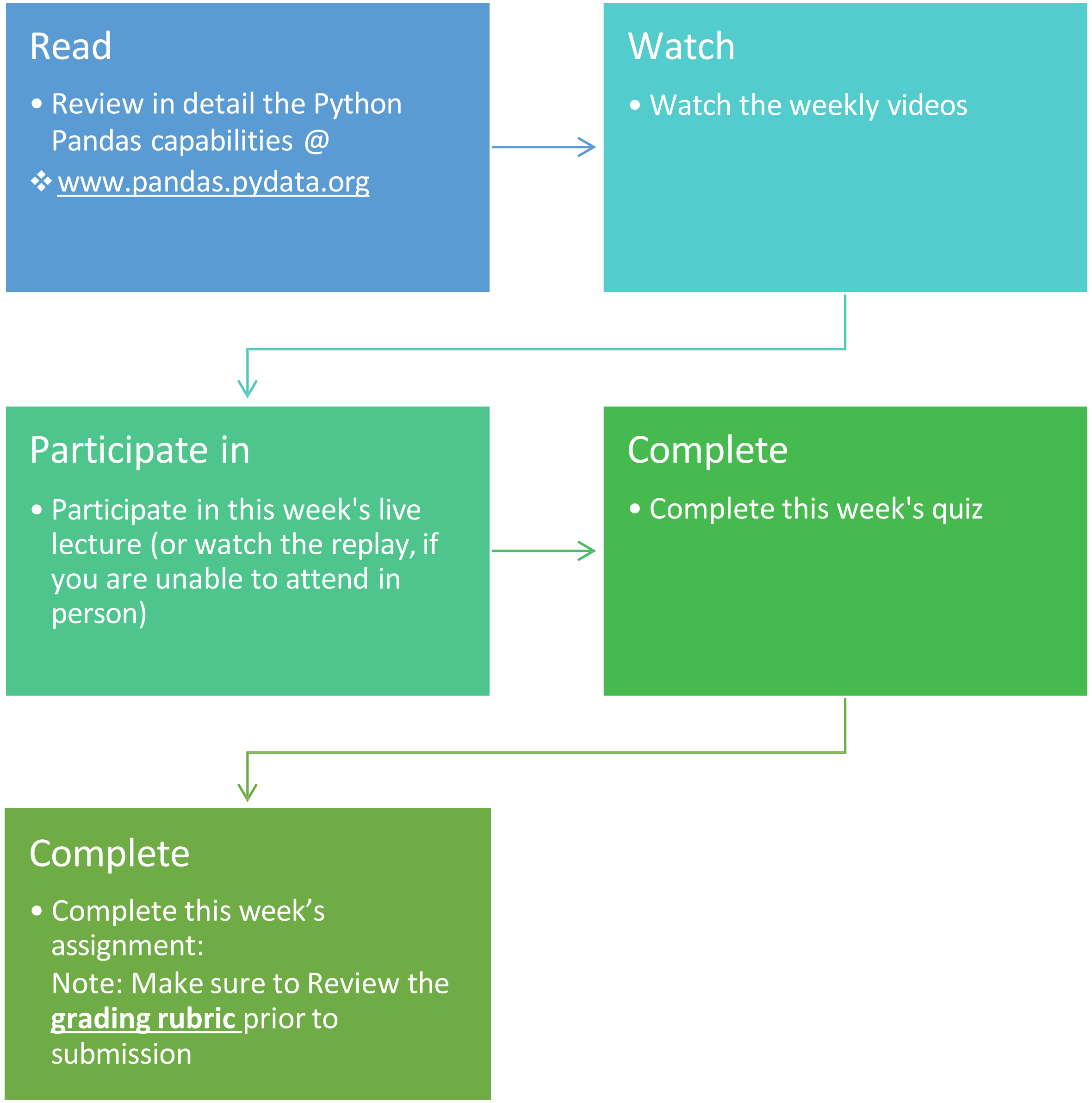
Week 2

Identify elements of cyber operations that can benefit from advanced Python Solutions (Part II)

Agenda

- Overview of the Cyber Kill Chain
- Overview of Active Cyber Defense
- Overview of Incident Response
- Extract, record and characterize network behavior characteristics
- Asset Mapping Considerations
- Brief introduction to Pandas

Week Two Assignments



Read

- Review in detail the Python Pandas capabilities @

❖ www.pandas.pydata.org

Watch

- Watch the weekly videos

Participate in

- Participate in this week's live lecture (or watch the replay, if you are unable to attend in person)

Complete

- Complete this week's quiz

Complete

- Complete this week’s assignment:

  Note: Make sure to Review the **grading rubric** prior to submission

Cyber Kill Chain

Cyber Attack Process

How Hacking Occurs

Cyber Kill Chain

- Basic Steps
  1. Reconnaissance
  2. Weaponization
  3. Delivery
  4. Exploitation
  5. Installation
  6. Command and Control
  7. Action

Cyber Kill Chain

- Reconnaissance
  - Analogous to driving by potential targets in the physical world.
  - Specific Methods Include:
    - IP Scanning
    - Port Scanning
      - Obtaining software and OS versions
      - Identify possible attack vectors
  - Typically performed by Botnets or other automated methods

Cyber Kill Chain

- Weaponization
  - Based on the recon, assess potential vulnerabilities and then select an exploit.
  - In some cases configuration or modification of known exploitation methods is required.

Cyber Kill Chain

- Delivery
  - Multiple methods are possible:
    - Internet attack against a known vulnerability
    - Tricking a user to insert an infected flash drive
    - Social engineering of a user a phishing attack for example
    - Or compromising an insider of the organization to assist an attacker

Cyber Kill Chain

- Exploitation
  - Unauthorized use of a credential
  - Cracking of weak passwords
  - Malware attachment to e-mail
  - Targeting vulnerable operating systems and services

Cyber Kill Chain

- Installation
  - The payload is installed on the disk of the server or workstation. In some cases just in memory as a running process.
  - More sophisticated installation will involve modification to the system itself, allowing the payload to re-launch upon reboot.

Cyber Kill Chain

- Command and Control
  - The infected system will typically contact a command and control server to register and receive command.
  - Then information can be leaked through this covert channel of communication.
  - In addition, other systems may be infected.

Cyber Kill Chain

- Action
  - Finally, information can be leaked through this covert channel of communication.
    - Steal Information
    - Encrypted a system for ransom
    - Destroy or disrupt operations
    - Deface the organization
  - In addition, other vulnerable systems may be infected through local connections.

Incident Response

Understanding

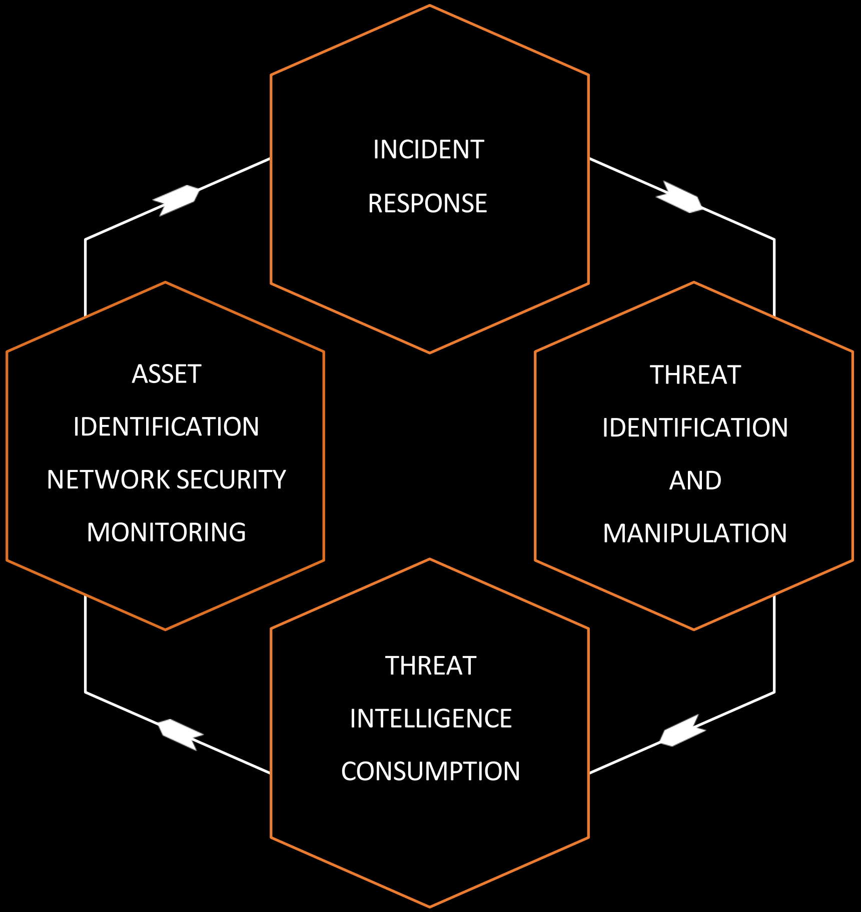
A new model for cyber defence

Active Cyber Defense (ACD)

OVERVIEW

WHAT IS ACD

- ACD is a new concept developed by DARPA and the US Air Force that is now being adapted within critical infrastructures and traditional public and private businesses.
- The core concept is the *anticipation* of an attack against cyber assets and proactively preparing and responding.



INCIDENT RESPONSE

THREAT IDENTIFICATION AND MANIPULATION

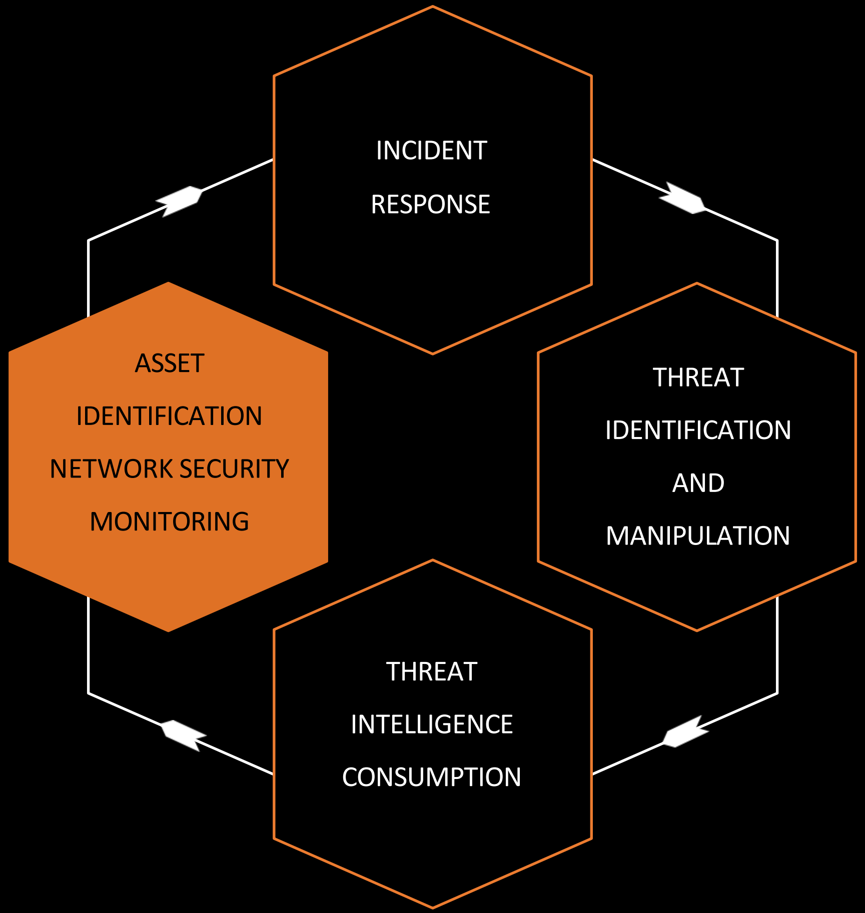
THREAT INTELLIGENCE CONSUMPTION

ASSET IDENTIFICATION NETWORK SECURITY MONITORING

Active Cyber Defense (Asset Mapping)

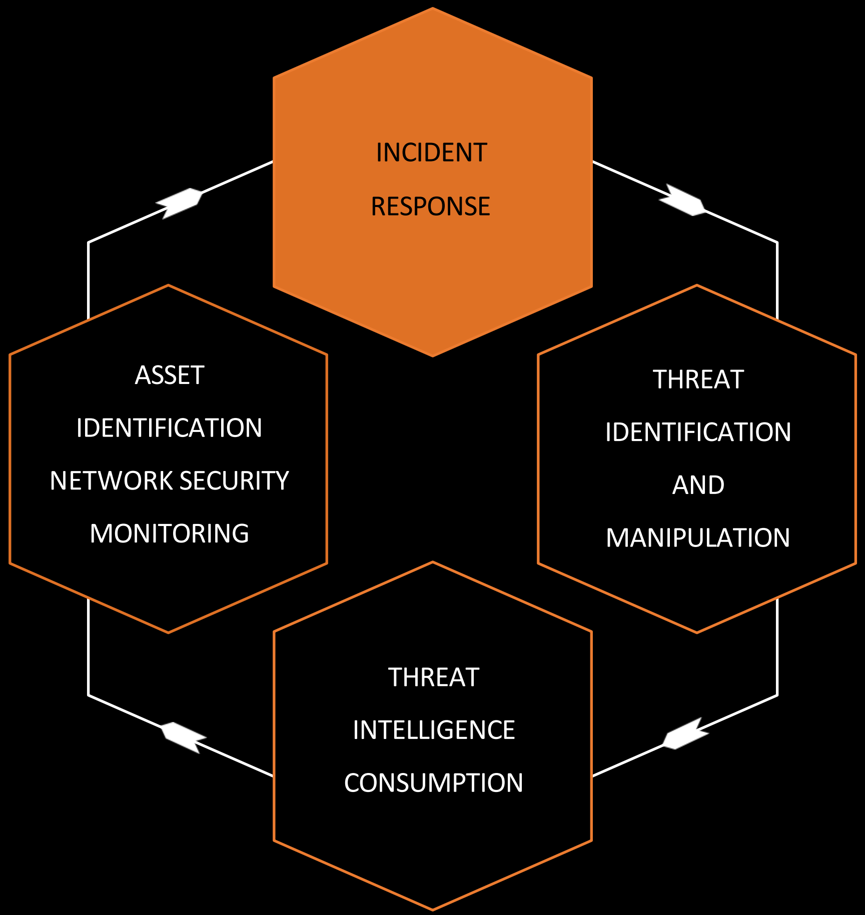
ASSET MAPPING
Detailed Active and Passive mapping of systems, networks and their “normal behavior” prior to an attack).

Detection of aberrant behavior (known signatures, heuristics, unusual changes or activity).


INCIDENT RESPONSE
THREAT IDENTIFICATION AND MANIPULATION
THREAT INTELLIGENCE CONSUMPTION
ASSET IDENTIFICATION NETWORK SECURITY MONITORING

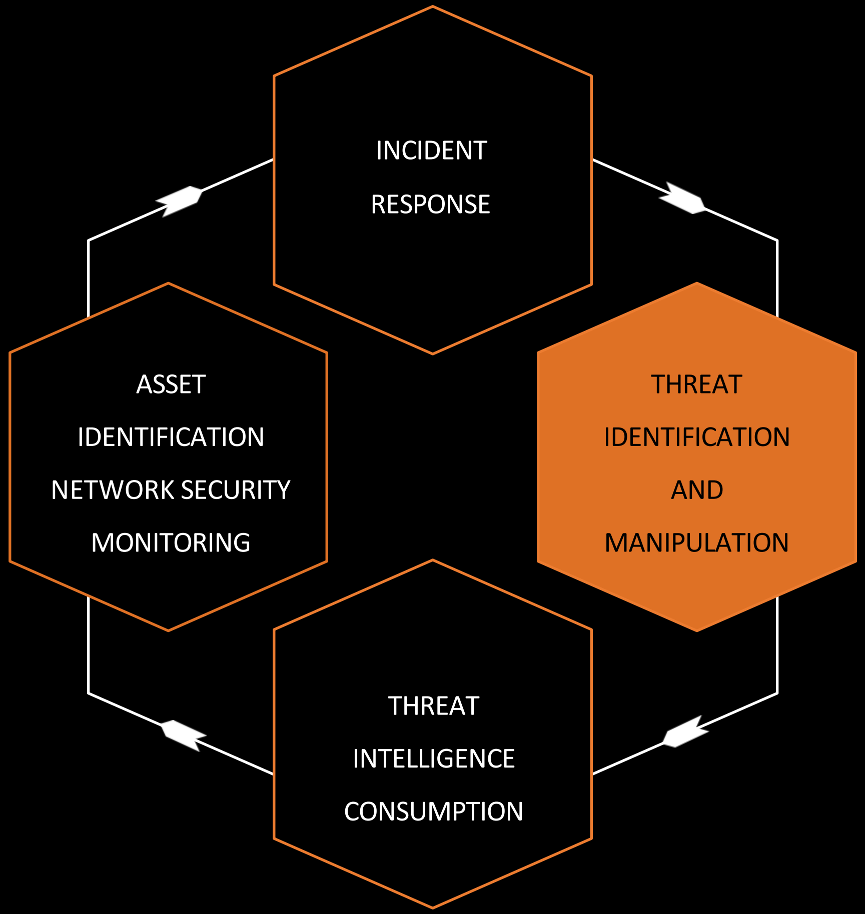
Active Cyber Defense (Incident Response)

- Preparation
- Detection / Analysis
- Containment
- Eradication
- Recovery
- Post Response


INCIDENT RESPONSE
ASSET IDENTIFICATION NETWORK SECURITY MONITORING
THREAT IDENTIFICATION AND MANIPULATION
THREAT INTELLIGENCE CONSUMPTION

Active Cyber Defense (Threat Identification and Manipulation)

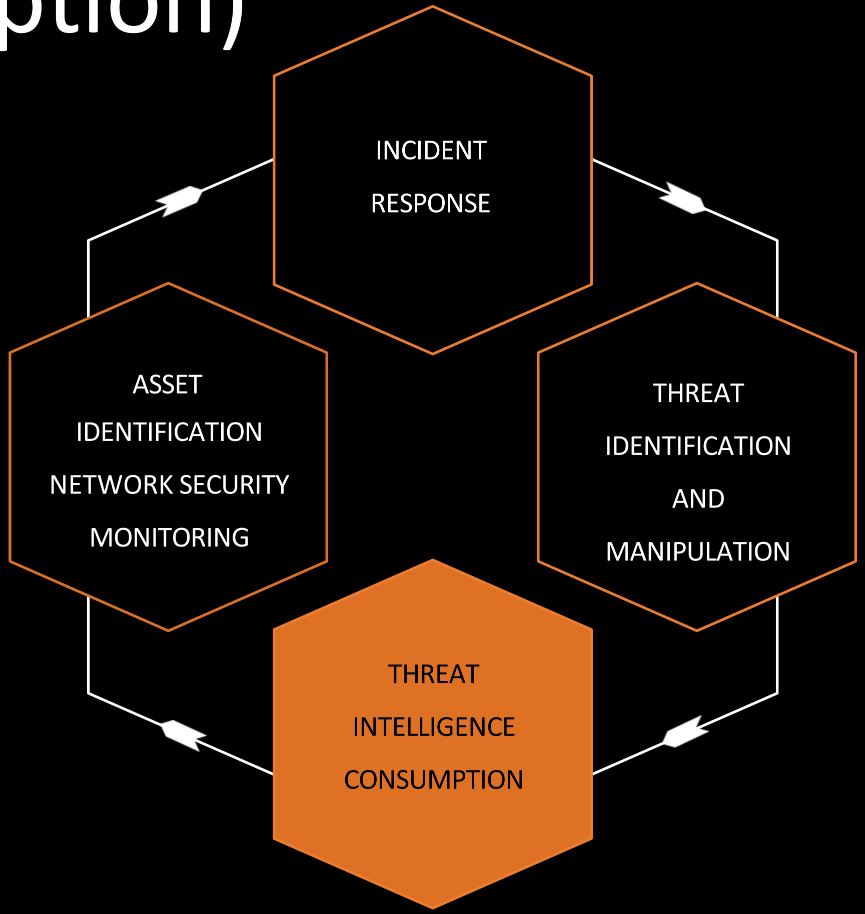
- Examining Attack Methods
- Identifying Objectives
- Gaming the Adversary
- Identifying key Characteristics
- Assessing the sophistication of the attack and attacker
- Determining location of the attacker(s)


INCIDENT RESPONSE
THREAT IDENTIFICATION AND MANIPULATION
THREAT INTELLIGENCE CONSUMPTION
ASSET IDENTIFICATION NETWORK SECURITY MONITORING

Active Cyber Defense
(Threat Intelligence Consumption)

Interpret the Threat Information and ask critical questions.

- Does the threat impact our environment?
- If yes, how?
- What changes to our security posture should we consider now or in the future?


INCIDENT RESPONSE
THREAT IDENTIFICATION AND MANIPULATION
THREAT INTELLIGENCE CONSUMPTION
ASSET IDENTIFICATION NETWORK SECURITY MONITORING

Why is Asset Mapping Vital?

1 Without it the incident response is hampered by the lack of knowledge of the environment.

2 Our ability to understand our adversary’s methods or objectives would be imprecise and lethargic.

3 Our ability to employ deceptive techniques (traps, decoys etc.) in order to game the adversary would be quite difficult.

4 Our ability to asses and consume threat intelligence reports and determine if/how the report applies to our environment would be difficult.

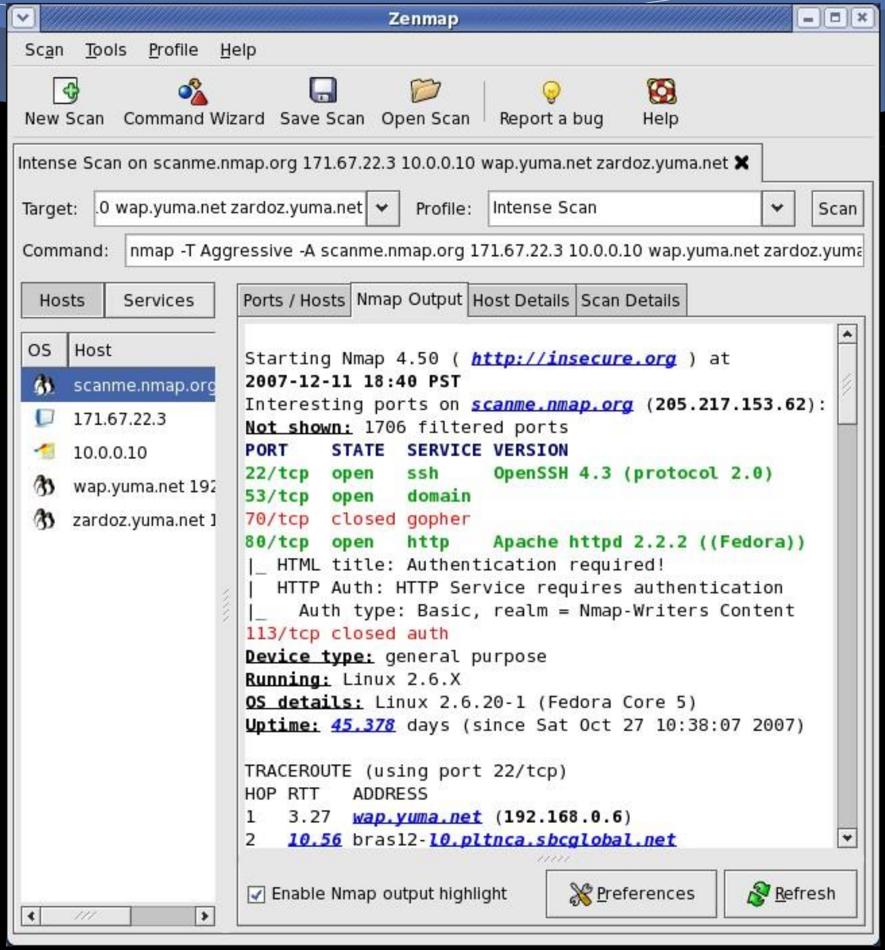
Extracting, recording and characterizing network behavior

Active Scanning?

Detailed mapping of systems, networks under a current state condition.

The mapping occurs by actively probing the network with tools like NMAP.

The probing activity can be "noisy" and may cause security appliances to detect unusual activity and generate alerts or worse.



Intense Scan on scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma.net

Target: .0 wap.yuma.net zardoz.yuma.net

Profile: Intense Scan

Command: nmap -T Aggressive -A scanme.nmap.org 171.67.22.3 10.0.0.10 wap.yuma.net zardoz.yuma

scanme.nmap.org
171.67.22.3
10.0.0.10
wap.yuma.net 192
zardoz.yuma.net 1

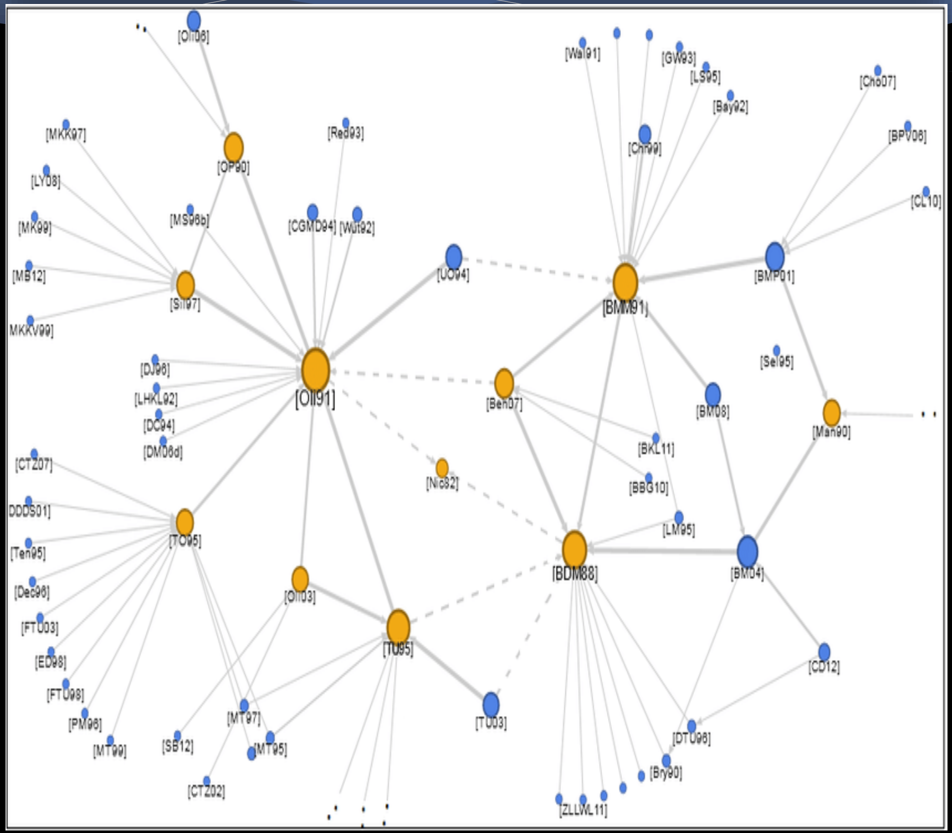
```
Starting Nmap 4.50 ( http://insecure.org ) at
2007-12-11 18:40 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
Not shown: 1706 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
|  HTTP Auth: HTTP Service requires authentication
|_   Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days (since Sat Oct 27 10:38:07 2007)

TRACEROUTE (using port 22/tcp)
HOP RTT   ADDRESS
1   3.27  wap.yuma.net (192.168.0.6)
2   10.56 bras12-10.pltnca.sbcglobal.net
```

☑ Enable Nmap output highlight

Passive Monitoring?

Detailed mapping of systems, networks and their “normal behavior” prior to an attack, under what would be consider “normal operating conditions”

The monitoring occurs without probing of networks or systems. Rather a sniffer is employed to capture Ethernet, IPv4, IPv6 or other network layers “normal behavior”



MACHINE LEARNING LIBRARIES OF THE WEEK

- NumPy
- Scipy
- matplotlib
- Pandas
- Scikit-learn
- Pytorch
- TensorFlow

PANDAS

What are Pandas? (short for panel data)

A Python library that provides key tools for creating and processing spreadsheet “like” objects.

The library provides many capabilities such as:

- Data alignment
- Data reshaping
- Data slicing
- Data subsetting

Why Pandas?

When preparing data for use in the training of machine learning pandas provide methods for creating data structures, evaluating, and cleaning data.

In addition, the ability to visualize the data provides insights and new ways of representing the data.

Learn more about Pandas

https://pandas.pydata.org

PANDAS AND PYTHON

Key Capabilities:

- ✓Provides Python with the ability to work with tables or spreadsheet type data.
- ✓Provides two new datatypes, Series and DataFrame. We will primarily be working with DataFrames, as they represent the complete spreadsheet. In addition, DataFrames are basically a dictionary or collection of Series objects.

SIMPLE DATAFRAME CREATION AND MANIPULATOINS

LIVE DEMO

Questions?

Coming Up Next Week:

Part III

Identify elements of cyber operations that can benefit from advanced Python Solutions (Part III)