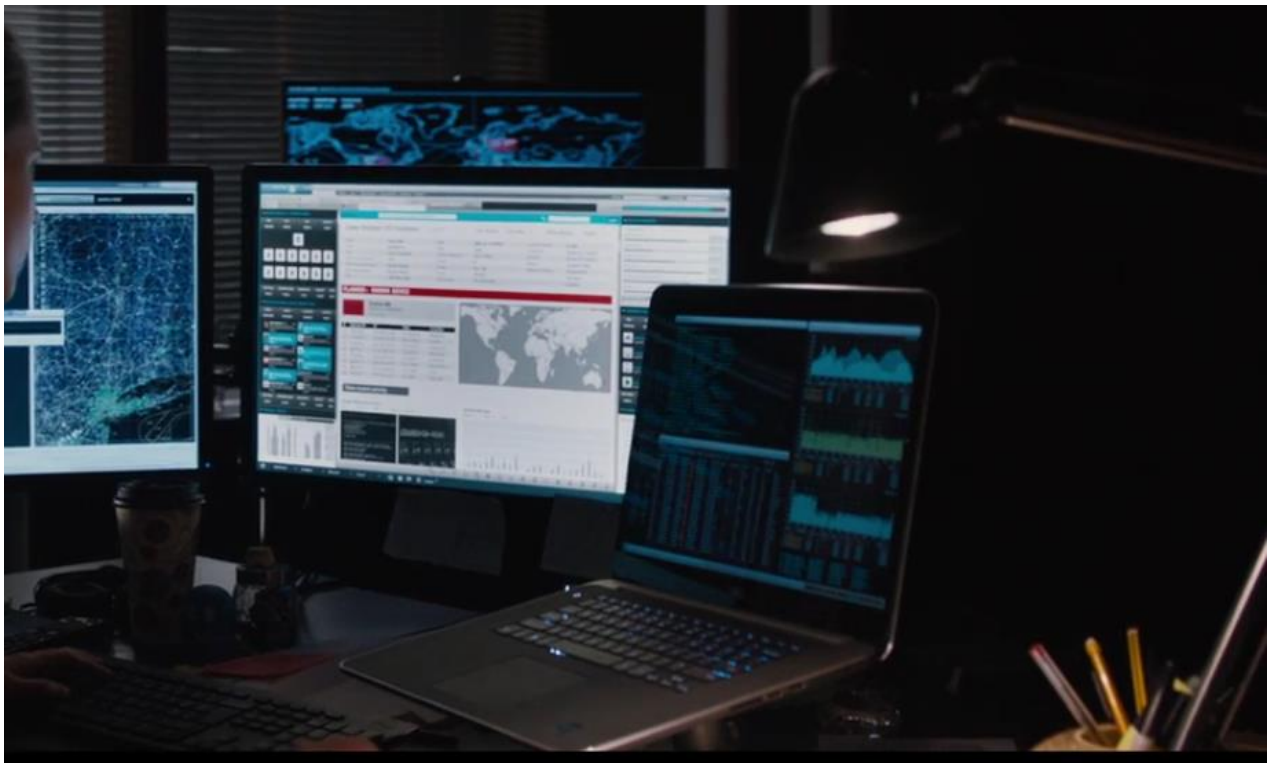
Active Défense for Adversary Pursuit



October 15th, 2019

OnNet

#For advanced cyber methods

ACTIVE DEFENSE for Adversary Pursuit COURSE NO: 105

STATEMENT OF DOCUMENT CONFIDENTIALITY

The content of this document is OPEN.

EXECUTIVE SUMMARY

Kenya like any other country in the world, is experiencing the rapid effects of digital modernization and information age which is fast dawning, requiring Law Enforcement Agencies, Intelligence Services and Military Services to transform their responses with adaptive capabilities. The local cyber threats and East African threats groups have grown and evolved with ease of circumventing typical security hygiene and defenders lacking Local Cyber Threat Intelligence feeds for countering these cyber gangs, the threat continues to spread. The enemy is well resourced than the defenders especially in our local financial sector and the defenders are forced to man hundreds to thousands points of entry whereas the Advanced Financial Threats just needs one for penetration. In this regard, the defenders will need to evolve and shift to the threat landscape and start focusing on the threat groups, their tactics, techniques and procedures to monitor and stop their activities. This course creates exposure to the student for adversary interpretation and understanding the subject behind the computer.

Information and intelligence dominance in this context are a precursor to overall success over the adversaries and is an investment in the future.

Adversaries make mistakes, even Nation State operators do, during counter cyber as defenders, we rely on those mistakes. Intelligence services across the world that activate Offensive Cyber Operations (OCO), aren't a one size fits of all things, even from states with abundant resources and active top tier intelligence services, dangerous mistakes are made.

As do Nation States, small Financial groups do the same and with this course, the students are shown how to observe, collect and attribute during Active Defense.

Table of Contents

0.0 OBJECTIVES

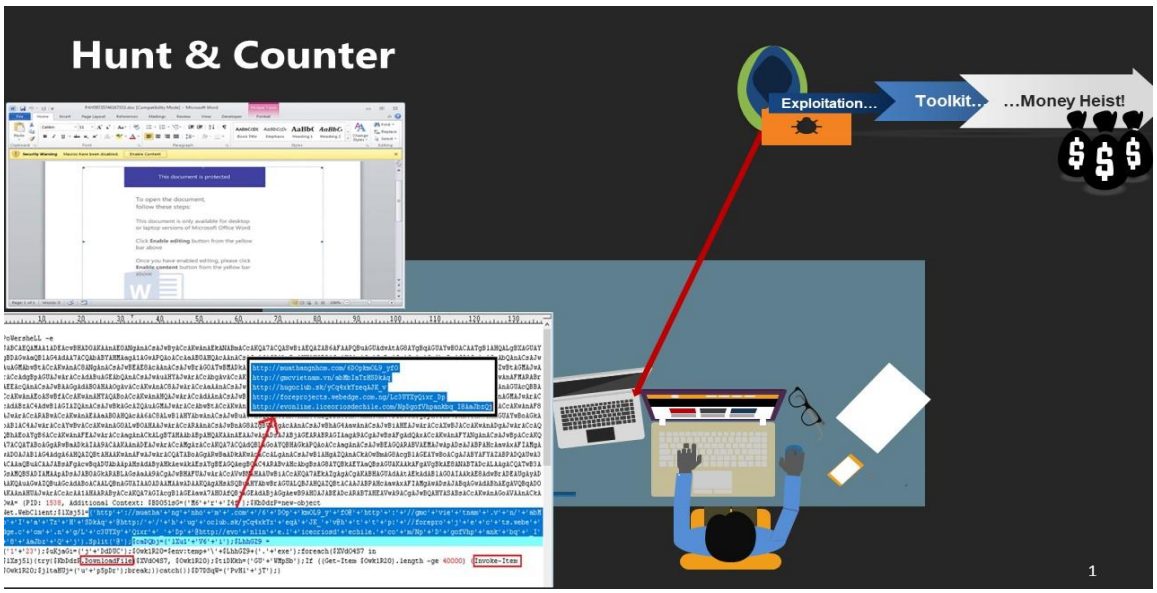
The Active Défense operations are part of CNO, in a pillar known as Computer Network Défense (CND) and the following are the objectives for this course:

a/ Understand the local cyber threats.
b/ Threat hunting.
c/ Reversing intrusion code.
d/ Collecting data to attain attribution.
e/ CNE operations against adversaries.

1.0 TRAINING SCOPE

The CNO training will include:

a/ Collection Activities.
b/ Enabling Activities.
c/ Defensive Activities.



2.0 PREREQUISITES

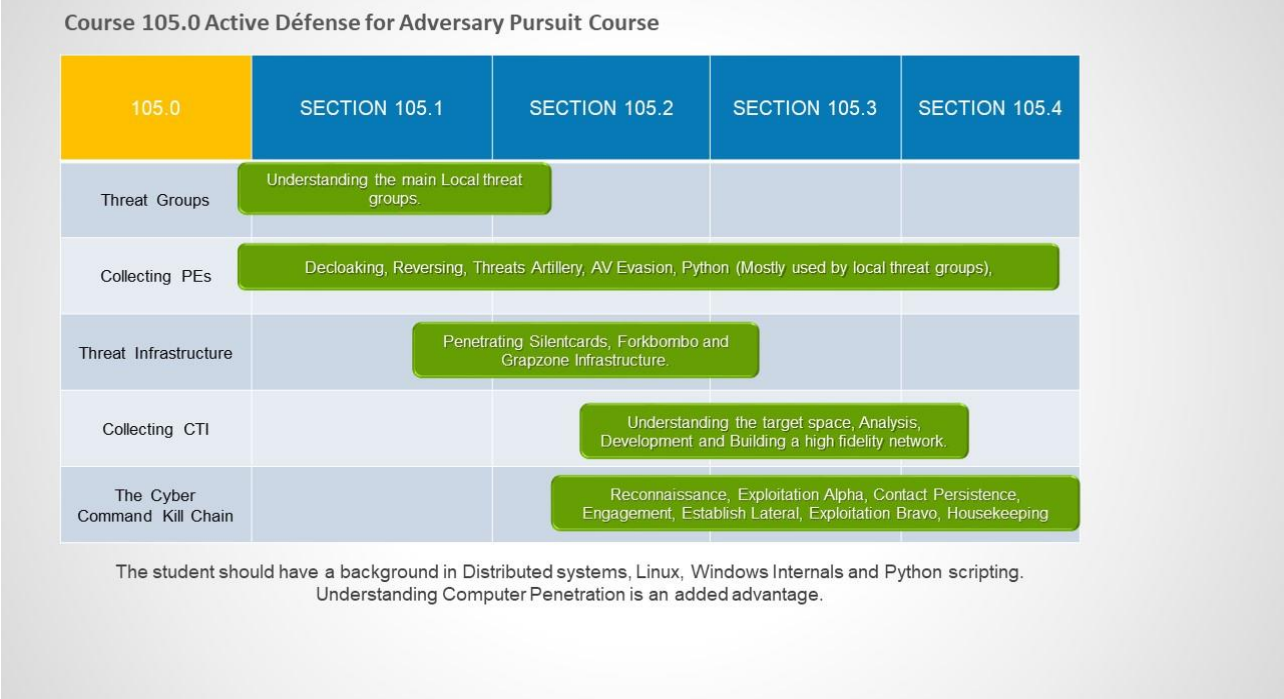
All the students should understand Windows and Linux Command line. With that, additional understanding of TCP/IP and some programming background is equally essential.

To get the most value out of this course, students are required to bring their own laptops to connect directly to the internet and assess real life attackers' infrastructure. It is the student's responsibility that the laptop is running Linux and is properly configured with all the drivers necessary to connect both Ethernet and Wireless.

3.0 FOCUS

The Active Défense training helps the blue teams to develop tools for counter cyber operations against threats and tracking them online, therefore attributing these efforts to clustered adversary groups and misinforming them during operations. Focusing on these threats and collecting Cyber Threat Intelligence reduces the impact before and after penetration.

4.0 COURSE TIMETABLE



5.0 ABOUT THE TRAINER

When I left [redacted] joined Cyber Command at [redacted], I never had thought, the experience I had gained in Europe and Middle East would come into much needed action in Government of Kenya ICT infrastructure. The first incidence I responded to was Chinese Advanced Persistent Threat actor inside and hooked into Ministry of [redacted] exfiltrating documentations needed [redacted] t industry. During the later ensuing operations, cybercom had to create its own capability not only to counter cyber operations from nation states, but to combat domestic Advanced Financial Threats. During this duration cybercom kill chain was developed and a team I headed called [redacted] against adversaries either for CNE operations or CNA takedown and disruption operations. During this duration, I served with men and women who countered the biggest Cyber Cartel the country has ever encountered. [redacted] that runs CNO operations against Financial Threats in East Africa and supported several Cyber Missions in Europe group office.