
Intrusion Operations
@FortyNorthSec

Introduction

- Welcome to FortyNorth Security's Intrusion Operations training class
- This is designed to be a comprehensive red team training class
- The class will cover:
  - The overall red team assessment methodology
  - Techniques and tricks
  - Stories from past lives
- We're here for the next few days to talk shop, ask questions!

FORTYNORTH SECURITY

whoami

- Previous Systems Administrator
- Co-Owner and Red Team Lead of FortyNorth Security
- BlackHat Instructor
- Open Source Developer
  - Veil
  - EyeWitness
  - WMImplant
  - Just-Metadata

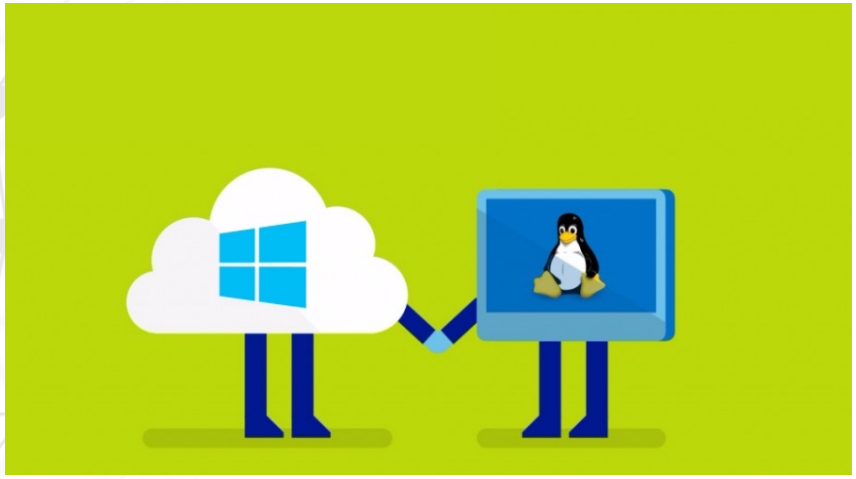
FORTYNORTH SECURITY

whoami

- Senior Offensive Security Engineer @ FortyNorth
- Open Source Python/C# Dev
  - EyeWitness
  - MiddleOut
  - Phishing-Phramework
- Avid Hiker and Backcountry Camper

FORTYNORTH SECURITY

Class Options



- You can use multiple VMs
  - Kali Linux
    - Run this locally if you want, not a requirement at all
    - Really any platform you want to choose is ok
  - Windows 10
    - This VM is for everything in the lab environment
    - This is provided to you once you have accessed the lab

FORTYNORTH SECURITY

Class Requirements

- We will be using Slack to talk during the course
  - Come up with a cool nickname
  - Connect in to the class Slack
  - Join the room for the whole class
    - Questions can also be asked here
  - Join a room for your team
    - This is for internal team communications
    - An instructor will also be in the room for private questions

FORTYNORTH SECURITY

What is a Red Team?

- Before we start, might be good to define this right?
- "If your primary customer is a dev/sysadmin, then you're delivering a pentest. You're only doing #redteam if your primary customer is SOC/IR" - @malcomvetter
- If your goal and report targets patch levels on in-scope systems, you're not performing a red team assessment

FORTYNORTH SECURITY

https://static1.squarespace.com/static/511d8f3ae4b02acb17b5ced9/t/59fd8fae8e7b0f1f9f716c18/1509789663441/ep001.png

What is a Red Team

- A red team is designed to emulate a threat, and you should expect active defenders
- The blue team you are facing should be following their defensive procedures if they detect any of your actions
  - Beyond emulating a threat, a red team also allows a blue team to find deficiencies in their investigative and remediation techniques

https://vignette.wikia.nocookie.net/rvb/images/7/7c/Red_vs_Blue_Logo.jpg/revision/latest?cb=20170405182912

FORTYNORTH SECURITY

What is a Red Team

- A red team assessment is a goal driven test – **ALWAYS**
- This isn't just hacking for the lulz
- You're doing work to demonstrate impact – this gets and keeps buy-in from non-technical executives
- If you can show you can access their client list, that's impact
- Getting DA – isn't

http://qmediasolutions.com/wp-content/uploads/2016/10/keep-calm-the-red-team-is-here.png

FORTYNORTH SECURITY

Steps of a Red Team

- We're going to be covering the different steps of a red team in this course
  - OSINT
  - Active Reconnaissance
  - Phishing
  - Initial Access and Reconnaissance
  - Persistence
  - Privilege Escalation
  - Lateral Movement
  - Attacking Cloud Infrastructure
  - Targeting Red Team Objectives

FORTYNORTH SECURITY

Final Notes

- You are not going to be running "Hail Mary" to gain access, or spread internally
- While you may run sweeps, they are targeted in nature
- Try to blend in to the norm
- … or be where you aren't expected

FORTYNORTH SECURITY