



SIMULATING THE ADVANCED PERSISTENT THREAT WITH PENETRATION TESTING

MARCH 16, 2016

Dr. Wesley McGrew

Director of Cyber Operations

HORNE CYBER

wesley.mcgrew@ornecyber.com

The Role of Penetration Testing



Team

- Background
- Skill set
- Training
- Improvement

- Terminology
- Presentation
- Types of Engagements
 - Internal
 - External
 - Wireless/Physical/Social
- Meetings needed, emergency contacts

Open Source Intelligence Gathering

Enumerating the Attack Surface

Vulnerability Identification

Public vs. Private

Research

Automation

- When do we pull the trigger?
- Validating and testing 3rd party code
- Best practices

Network-Connected Devices

Extending into the network

Traditional post-exploitation

Combining first-phase results

Exfiltration

Operational Security

Reporting and Post-Mortem



**QUESTIONS &
DISCUSSION**