NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Providing A Hands-on Advanced Persistent Threat Learning Experience Through Ethical Hacking Labs

Yen-Hung (Frank) Hu, D.Sc.

Professor and CCI Fellow

Department of Computer Science

Norfolk State University

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Outline

- Introduction – Advanced Persistent Threat (APT)
- Research Methodology
- Conclusion

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Introduction – APT

- Advanced
  - Adopts a full spectrum of sophisticated cyberattack techniques which usually take advantage of zero-day vulnerabilities.
- Persistent
  - Expands from their original footholds to any reachable compromised devices to survive any disruptions while keeping silent and stealthy to avoid detection
- Threat
  - Is much more harmful than traditional cyberattacks since it involves many more human interactions

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Research Methodology

- Adopting a hands-on learning model
- Analyzing APT lifecycle
- Mapping APT KSAs to NICE framework
- Mapping APT lifecycle with KUs of NICE framework
- Adopting NDG ethical hacking lab series
- Applying NDG ethical hacking labs to APT lifecycle
- Integrating NDG ethical hacking labs with supplemental lectures to comply with NICE framework

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Adopting Hands-on Learning Model

- Kolb's experiential learning model
  - Practical experiences of a learner to a subject can enhance the individual to learn that subject
  - 4 stages, 4 behaviors, and 4 learning styles

	Active Experimentation (Doing)	Reflective Observation (Watching)
Concrete Experience (Felling)	**Accommodating (Feeling & Doing)**	Diverging (Watching & Feeling)
Abstract Conceptualization (Thinking)	Converging (Thinking & Doing)	Assimilating (Watching & Thinking)

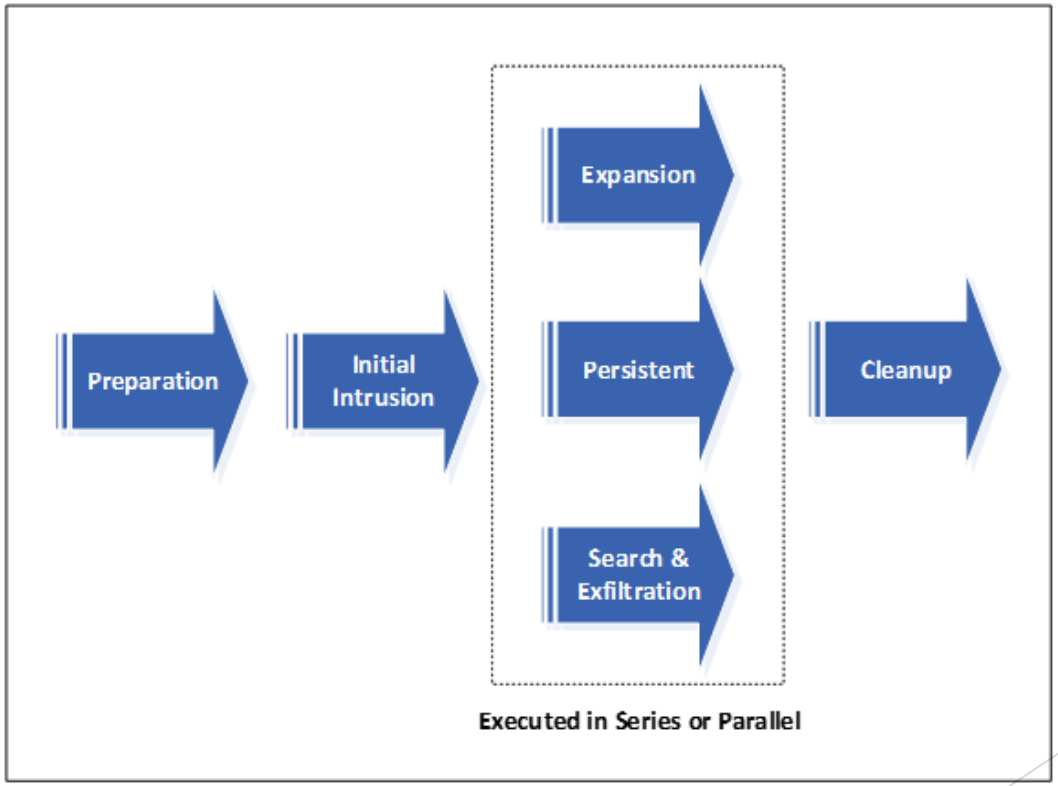
- Accommodating learning style focuses on hands-on (i.e., feeling and doing) and relies on intuition not logic.
  - A learner will use other people's experiences and conduct hands-on exercises following the instruction concluded and summarized from such experiences.

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Analyzing APT Lifecycle

- Adopt 6-stage APT lifecycle
  - Preparation
  - Initial Intrusion
  - Expansion
  - Persistent
  - Search & Exfiltration
  - Cleanup



NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Mapping APT KSA to NICE Framework

- NICE Cybersecurity workforce framework
  - 7 categories, 33 specialty areas, 52 work roles, 1007 tasks, 630 knowledge units, 374 skills, and 176 abilities
- APT actor is not a work role in the existing NICE framework
  - 10 tasks and required 63 knowledge units, 37 skills and 9 abilities

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Mapping APT Lifecycle With KUs Of NICE Workforce

- Preparation – 11 KUs
- Initial Intrusion – 15 KUs
- Expansion – 25 KUs
- Persistent – 6 KUs
- Search and Exfiltration – 5 KUs
- Cleanup – 1 KUs

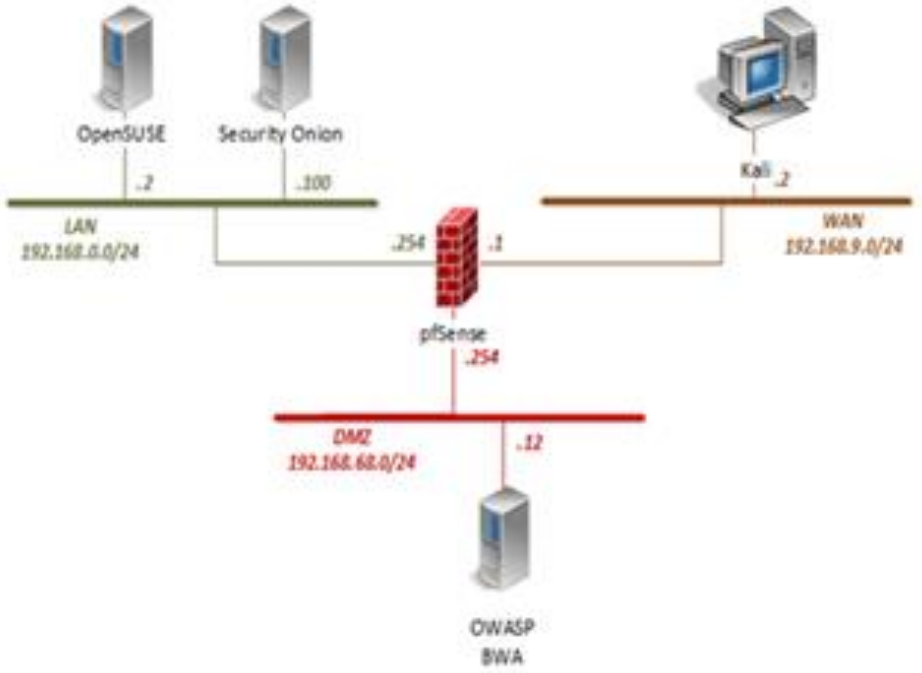
APT Lifecycle	NICE Cybersecurity Workforce Framework Knowledge Units
Preparation	K0111, K0144, K0162, K0177, K0302, K0447, K0474, K0535, K0538, K0548, K0604
Initial Intrusion	K0001, K0004, K0060, K0113, K0131, K0151, K0161, K0206, K0224, K0234, K0310, K0362, K0408, K0436, K0603
Expansion	K0005, K0006, K0007, K0009, K0049, K0059, K0061, K0062, K0070, K0106, K0110, K0119, K0129, K0147, K0160, K0174, K0221, K0272, K0301, K0318, K0332, K0336, K0397, K0471, K0475
Persistent	K0002, K0013, K0259, K0298, K0367, K0523
Search and Exfiltration	K0116, K0117, K0132, K0308, K0536
Cleanup	K0003

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Adopting NDG Ethical Hacking Labs

- Prepare students for the EC-Council Certified Ethical Hacking (CEH) certification, Offensive Security Penetration Testing with Kali Linux (PWK) certification, and GIAC Penetration Tester (GPEN) certification
- 5 virtual machines:
  - Kali Linux, pfSense Firewall, OWASP Broken Web App, OpenSUSE, and Security Onion



Applying NDG Ethical Hacking Labs To APT Lifecycle

Lab Topic
Lab 1: Reconnaissance with Nmap & Amap
Lab 2: Social Engineering Attacks with Social Engineering Toolkit
Lab 3: Metasploit Framework Fundamentals
Lab 4: Web Pentesting with Nikto & OWSP Zap
Lab 5: Password Cracking with John the Ripper and Hashcat
Lab 6: Creating and Installing SSL Certificates
Lab 7: Vulnerability Scanning with OpenVAS
Lab 8: Enumerating SMB with enum4linux
Lab 9: Backdooring with Netcat
Lab 10: Packet Crafting with Scapy
Lab 11: Network Analysis
Lab 12: Client Side Exploitations
Lab 13: Testing Firewall Rules with Firewalking
Lab 14: Understanding SQL Commands & Injections
Lab 15: Understanding Buffer Overflows
Lab 16: Evading IDS
Lab 17: Packet Crafting with Hping
Lab 18: VNC as a Backdoor
Lab 19: Auditing Linux Systems
Lab 20: Anti-Virus Evasion

APT Lifecycle	NDG Ethical Hacking Labs
Preparation	Lab 1, Lab 2, Lab 3, Lab 4, Lab 6, Lab 7, Lab 12, Lab 13, Lab 19
Initial Intrusion	Lab 3, Lab 4, Lab 5, Lab 8, Lab 9, Lab 10, Lab 12, Lab 14, Lab 15, Lab 16, Lab 17, Lab 18, Lab 20
Expansion	Lab 3, Lab 4, Lab 5, Lab 8, Lab 9, Lab 10, Lab 12, Lab 14, Lab 15, Lab 16, Lab 17, Lab 18, Lab 20
Persistent	Lab 3, Lab 9, Lab 16, Lab 18, Lab 20
Search and Exfiltration	Lab 3, Lab 9, Lab 18
Cleanup	Lab 3, Lab 9, Lab 18

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Integrating The NDG Ethical Hacking Labs With Supplemental Lectures To Comply With NICE Framework

- Supplemental Lectures
  - APT Labs with NDG Ethical Hacking Labs
  - Introduction to Advanced Persistent Threat
  - Introduction to Stuxnet
  - Introduction to Poison Ivy
  - Introduction to GhostNet
  - Duqu: The APT Reconnaissance Worm
  - Autopsy Forensics Browser User Guide I
  - PTK Forensics WiKi
- Spring 2021, Fall 2021 CYS-765-90 Advanced Topics in Cybersecurity – overall 24 Students
- Summer 2021 DoD HRAP Summer Camp – 4 High School Students

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Conclusion

- Proposed a hands-on learning model for adopting the NDG ethical hacking lab series into APT learning
- Explained the procedures (methodology) to conduct this project
- Discussed preliminary research results which indicates the proposed hands-on learning model achieves the objectives of this research

NORFOLK STATE UNIVERSITY

Commonwealth Cyber Initiative

Questions and Comments