Title	Evasion & Defense Analysis
Long Title	Evasion & Defense Analysis
Credits	**10**
NFQ Level	Expert
Module Author	Dr George D O'Mahony

Module Description:

Today's adversaries and attackers are no longer focused simply on doing the maximum possible damage; they're looking to remain undetected as long as possible. This module will utilize purple teaming to develop evasion and detection skills to maximize the cyber capabilities of the learner. The module's red team approach will provide the learner with defense evasion skills that consists of techniques that adversaries use to avoid detection throughout their compromise. This module's blue team approach will use data collected from a variety of cyber defense tools to analyze, detect, and prevent modern-day techniques that are deployed to bypass security tools and professionals. On successful competition, the learner will have the skills and knowledge required to conduct penetration testing in highly secured networks and identify these evasion approaches through data analysis. This module was developed under the CyberSkills HCI Pillar 3 Project. Please refer to the consortium agreement for ownership.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1	Assess and evaluate attack frameworks and appraise intelligence-driven defense.
LO2	Identify evasion techniques and critically appraise how the techniques are used to bypass defense and detection strategies and other security mechanisms.
LO3	Assess and employ the exploitation tools required to perform defense evasion.
LO4	Identify data from a variety of cyber defense resources that can detect and analyze a security incident involving evasion techniques.
LO5	Critically employ monitoring and anlaysis solutions to identify evasion techniques used by attackers and apply mitigation.

Indicative Content

Attack frameworks

What is the Cyber Kill Chain® framework. What Intelligence Driven Defense. How do they apply to the identification and prevention of cyber intrusions activity. What must adversaries complete in order to achieve their objective. How the framework enhances visibility into an attack and enriches an analyst's understanding of an adversary's tactics, techniques and procedures. The seven steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control and Actions on Objectives.

Defense Evasion

Security Systems: How many endpoint security tools work. How a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes. How to identify the attack surface. Windows and Linux Operating System Concepts and programming theory. Commonly used network IPS evasion techniques - Examples: Encryption and Tunneling, Timing Attacks, Resource Exhaustion, Traffic Fragmentation, Protocol-level Misinterpretation, Traffic Substitution and Insertion, polymorphic code, uninstalling/disabling security software, obfuscating/encrypting data and scripts, leveraging and exploiting trusted processes to hide and masquerade attack. Associated Tools for implementation - Nmap, Nessus, Metasploit, fragroute, encryption protocol. Bypassing Antivirus with Metasploit - Metasploit Encoders and Metasploit Encryptors. Application whitelisting theory and setup - basic bypasses. Lateral movements.

Defense Evasion Tools

How to customize the Meterpreter tooling to be stealthy (stay under the radar) and evade defensive security systems. Explore Metasploit's Meterpreter payloads in detail. Discover how to slip past signature-based detections on disk and in memory. Defeat emulators and heuristic analysis engines as well as network-based security tools. Conduct security assessments successfully in highly secured networks. Windows AV bypass with Veil-evasion.

Atack Data

Collect data from various cyber defense sources - Packet Capture, Intrusion Detection and Prevention Systems, logs HIDS, Netflows, security devices, memory, forensics artifacts. Packet Capture analysis using Wireshark and tcpdump for common protocols such as DHCP, SMB, SMTP, DNS. Packet Crafting, Log Analysis, SIEM, patching, user awareness, physical security, backup, passwords, sniffing in a switched environment, Tunnelling, data loss prevention

Monitoring and Analysis Tools

Extensive use of tools such as tcpdump, wireshark, tshark, hping, scapy, iptables, nfdump, splunk, snort, Metasploit. Kali, BlackArch and Security Onion will be used as platforms. Respond to attacks using these tools and platforms using incident handling methodologies and by applying knowledge of developing and deploying signatures and reading and interpreting packet analysis and attack signatures.

Mitigation - Security Hardening

System administration, network, and operating system hardening techniques. Countermeasure design for identified security risks. Implement monitoring solutions for attack evasion activity. Anti-evasion techniques and mitigation strategies.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	The learner will use the tools, techniques and data (information sources) used for intelligence-driven defense. This will be assessed through a project consisting of locating and utilizing available data to detect and analyze a security incident.	1,4,5	40.0	Week 7
Project	The learner will use defense evasion techniques to bypass detection and other security strategies. This will be assessed through a project consisting of an advanced pentest using evasion techniques and enhancing the detection strategies of the target.	2,3,5	60.0	Sem End

No End of Module Formal Examination

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework

This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes	2.0	Every Week	2.0
Tutorial	Tutorial to support student learning	1.0	Every Week	1.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	9.0	Every Week	9.0
		Total Hours		14
		Total Weekly Learner Workload		14
		Total Weekly Contact Hours		5

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lectures covering the theoretical concepts underpinning the learning outcomes.	2.0	Every Week	2.0
Tutorial	Tutorial to support student learning	1.0	Every Week	1.0
Lab	Lab to support the learning outcomes.	2.0	Every Week	2.0
Independent & Directed Learning (Non-contact)	Independent learning by the student.	9.0	Every Week	9.0
		Total Hours		14
		Total Weekly Learner Workload		14
		Total Weekly Contact Hours		5

Recommended Book Resources

- **Gus Khawaja 2021, *Kali Linux Penetration Testing Bible*, Wiley [ISBN: 9781119719083]**

Supplementary Book Resources

- **Daniel W. Dieterle 2018, Basic Security Testing with Kali Linux 3, Third Ed., CreateSpace Independent Publishing Platform [ISBN: 9781725031982]**
- **Abhinav Singh, Nipun Jaswal, Monika Agarwal, Daniel Teixeira 2018, Metasploit Penetration Testing Cookbook, Third Ed., Packt Publishing Ltd [ISBN: 9781788629713]**
- **Peter Kim 2018, The Hacker Playbook 3: Practical Guide To Penetration Testing, Secure Planet LLC [ISBN: 9781980901754]**
- **Dafydd Stuttard, Marcus Pinto 2011, The Web Application Hacker's Handbook, Wiley [ISBN: 1118026470]**
- **Bill Nelson 2015, Guide to Computer Forensics and Investigations, 5th Ed., Course Technology [ISBN: 1285060032]**
- **Sagar Rahalkar, Nipun Jaswal 2019, The Complete Metasploit Guide, Packt [ISBN: 9781838822477]**