Title	Scripting for Cybersecurity
Long Title	Scripting for Cybersecurity
Credits	**5**
NFQ Level	**9**

Module Description:

In this module students will learn how to write programs and scripts to perform cyber security functions such as packet manipulation and network scanning techniques. In addition, they will learn ethical hacking techniques to program a range of network, web and malware attacks with the aim of evaluating and identifying vulnerabilities in systems and networks.

Learning Outcomes

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

LO1 Evaluate the principles and techniques of ethical hackers to help businesses protect their infrastructure and information.

LO2 Applying programming concepts to evaluate the security and identify vulnerabilities in systems, networks or system infrastructure in an ethical manner.

LO3 Utilise programming libraries and its associated functionality to preform network packet manipulation.

LO4 Leverage programming libraries to implement a range of network based attacks.

LO5 Communicate with websites and web APIs for the purpose of utilising third-party services and identifying web application vulnerabilities.

Indicative Content

Ethical Hacking

Legal side of hacking. Hacking environment. Virtual Box - Kali linux. Linux basics. Python and ethical hacking. Python environment.

Python Scripting

Data structures, looping and conditionals, formatted printing, regular expressions, environment variables, functions, modules, command line arguments, file I/O, error handling, reading config files, logging, parsing and formatting dates and times. Regular expressions. Functions. Classes. String method. Containers. Using APIs.

Network packet manipulation

Scapy library. MAC address. Changing a MAC address using Python. Address Resolution Protocol (ARP). Scanning, sniffing and fuzzing. Packet design. Building packets. Stacking layers. Reading PCAP files. Port scanning. Domain Specific Language (DSL). Decoding packets. Graphical dumps. Generating sets of packets. Sending packets. Send and Receive. SYN Scans. TCP Traceroute. Super Sockets. Sniffing. Importing and exporting data. Frame injection.

Classical Network Attacks

Password interception. Malformed packets. Ping of Death. Nestea attack. Land Attack. ARP Cache Poisoning. DNS spoofer. Bypassing HTTPs. Sniffing login credentials. Rouge DHCP Server Detector. OS fingerprinting.

Malware

Writing malware basics. Execute Systems command payloads. Sending emails. Stealing wifi passwords. Stealing passwords on remote computers. File systems manipulation. Writing a keylogger. Write a backdoor - sending and receiving data over TCP. Implementing skeleton for client/server communication. Serialisation. Reading, writing and uploading files. Converting to binary executable. Running executable. Trojan. Anti virus programs.

Web Attacks

Sending GET requests. Website subdomains. Hidden paths and discovery. Reading response content. POST requests. Login information. Brute force attack. DoS attack. Vulnerability scanner. Posting forms. Sessions. XSS Vulnerabilities and discovery. OWASP Top 10

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Project	Students will develop and submit assigned scripts which will demonstrate their command of the language and its libraries to execute Red/Blue Team operations.	1,2,3	50	Week 8
Project	The student for example, will design and develop scripts/program that will launch a network based attack and design a solution that prevents the exploitation of the vulnerability that lead to the attack.	2,3,4,5	50	Sem End
No End of Module Formal Exam				

Assessment Breakdown	**%**
Coursework	100

Re-Assessment Requirement

Coursework Only

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	Lecture delivering theory underpinning learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent learning.	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2	Every Week	2.00
Lab	Lab to support learning outcomes.	2	Every Week	2.00
Independent & Directed Learning (Non-contact)	Independent Study.	3	Every Week	3.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		4.00

Recommended Book Resources

Mark Lutz. (2013), Learning Python, O'Reilly Media, [ISBN: 9781449355739].

Justin Sietz. (2014), Black Hat Python: Python Programming for Hackers and Pentesters, No Starch Press, [ISBN: 9781593275907].