Cybersecurity Bootcamp	
Session 1: Computer Fundamentals	Brief History of Computing
	The Von Neumann Architecture
	Digital Electronics (Binary Operations)
	Modern Computers
	Registers and the Register File
	Execution Flow
	Memory Management
	Data Representation
	Data Structures
	Instruction Encoding
	Fetch-Execute Cycle
	Bus/PCI
	UART
	Device Interrupts
	Intro to x86 asm

Session 2: Programming 101	What is a program/Algorithms
	Type of Programming Languages
	Variables and Data Types
	Control Structures
	Repetition Structures
	Functions and Modules
	Strings
	Lists
	File Input and Output
	Dictionaries
	Python for cybersec
	Pwntools
	Wrap-up
	How C/C++ is different, stack and heap, common security issues, system calls

Session 3: Unix Basics	The UNIX philosophy & history
	Introduction to Unix Shell
	Basic Shell Commands
	The Unix File System
	File system command
	Tree walking
	Text Editors (ed, vi(m), emacs, nano)
	Filters: cat, head, tail, sort, uniq
	UNIX Processes
	Pipes
	Signals
	Process Utilities (ps, kill, wait, sleep)

Session 4: Unix Management	User Management in Unix
	Directory Structure
	Disk Organization
	File System Management
	The init system
	Service Management
	Welcome to Make
	BSD Ports
	Linux Package Management overview
	Package management demonstration
	Disk Partition Table

	BIOS
	UEFI
	Bootcode / Bootloader
	File Systems
	Volume Management
	ext2/3/4, LVM2, ZFS
	ZFS
	Secure Shell (SSH)

Session 5: Computer Networks	Introduction
	Network Architectures
	Physical Layer
	Link Layer I
	Link Layer II
	Multi-access Link
	Switching Technologies
	Bridges and ATM
	Internetworking
	IP forwarding
	DHCP and Dynamic Routing
	Transport Protocols
	TCP
	DNS and content distribution networks
	Content Distribution
	Networked Applications
	Network Security
	Spam and Botnets
	Denial of Service and Prefix Hijacking Attacks

Session 6: Introduction to Information Security	What is Information Security?
	Examples of Information Security Incidents
	What is Information Security Management
	concepts of Information Security
	Basic terminologies
	Human Aspect
	Social Engineering
	Attacks to Server Systems connected to the Internet and counter measures
	Attacks to Web Servers and counter measure
	Denial of Service Attack
	Attacks to Network Systems
	Attacks for Personal Devices and counter measure
	malicious software
	Identifying Information Assets
	Identifying Security Risk and evaluation
	Risk Treatment
	Security Incident response
	Computer Security Incident response team
	Incident response exercise

Session 7: Introduction to Cryptography	What is Cryptography?
	Classic Cryptography
	Modern Cryptography
	Common Key Cryptography algorithms
	Applied Cryptography on Unix systems
	Problems of Key distribution for Common Key Cryptography
	What is Public Key Cryptography?
	Integrity of Data
	Hash Function
	Digital Signature
	Hash functions and Digital Signature on Unix Systems
	Key Certificate: Digital Signature of Public Key
	Public key Infrastructure (PKI) and Certificate Authority
	Exercise on PKI with PGP

Session 8: Red Team (Penetration Testing)	Netcat
	Socat
	PowerShell and Powercat basics
	Wireshark
	tcpdump
	Website Recon
	Whois Enumeration
	Google Hacking
	Recon-ng
	Shodan
	Security Headers Scanner
	SSL Server Test
	Pastebin
	User Information Gathering
	Email Harvesting
	Password Dumps
	Social Media Tools
	Site-Specific Tools
	OSINT Framework
	Maltego
	DNS and Subdomain Enumeration
	Port Scanning
	Network Scanning (masscan)
	SMB Enumeration
	NFS Enumeration
	SMTP Enumeration
	SNMP Enumeration
	Information Gathering and Enumeration
	Vulnerability Scanning
	Manual vs. Automated Scanning
	Internet Scanning vs Internal Scanning
	Authenticated vs Unauthenticated Scanning
	Vulnerability Scanning with Nessus
	Vulnerability Scanning with Nmap
	Web Application Enumeration
	Web Application Assessment Tools
	Scanning
	Exploiting Admin Consoles
	Cross-Site Scripting (XSS)
	Directory Traversal Vulnerabilities
	File Inclusion Vulnerabilities
	SQL Injection
	Introduction to Buffer Overflows
	Windows Buffer Overflows
	Linux Buffer Overflows
	Client-Side Attacks
	OWASP Top 10 vulnerabilities and exploitation
	Exploiting Microsoft Office
	Locating Public Exploits
	Searching for Exploits
	Antivirus Evasion
	Methods of Detecting Malicious Code
	Bypassing Antivirus Detection
	Windows Privilege Escalation Examples
	Linux Privilege Escalation Examples
	Race Condition Vulnerabilities Examples
	Password Attacks
	Common Network Service Attack Methods
	Leveraging Password Hashes
	Port Forwarding
	SSH Tunneling
	PLINK and NETSH
	HTTPTunnel-ing Through Deep Packet Inspection
	Active Directory Attacks
	The Metasploit Framework
	Post-Exploitation with Metasploit

	Building Our Own MSF Module
	Wifi Attacks (aircrack suite, reaver)
	Man in the Middle Attacks (MITM)
	Defences Against Wifi Attacks
	Defences Against MITM Attacks
	WAF/IDS Detection, Evasion and Spoofing
	Attacks Against Wireless Devices using SDR (jamming, sniffing)
	Cracking Attacks (Hashcat, John)
	Directory Discovery (ffuf, dirbuster)
	Docker Auditing
	Wrapping Up

Session 9: Blue Team (Defence)	Firewalls
	Anitiviruses
	File integrity monitors
	Monitoring
	SIEM
	Threat Intelligence, MITRE ATT&CK
	IDS
	DLP
	Patch managment
	Server security topics
	Endpoint security topics
	Network security topics
	Basics of incident investigationa and forensics
	Main InfoSec standarts main points
	OWASP, WAF

Session 10: Windows Overview	History of Windows, versions, licensing
	Windows Architecture
	Windows Services
	Windows Registry
	Win APIs
	File systems of Windows
	User managment, permissions
	Device managment, Drivers
	Control Panel, MS Config
	Networking in Windows
	Command Line and basic commands
	Batch file & PowerShell basics
	UAC
	Backup and Recovery
	SysInternals
	Remote Control
	Antiviruses and firewalls
	Entry level virtualization/sandboxing: VirtualBox, Hyper-V, Windows Sandbox and co
	Best practices for configuring average user PCs
	Windows in corp networks
	AD/Domain basics (Objects, Leaf Nodes, Containers, DNT, PDNT, Data Tables, Link Tables etc)

Session 11: Reverse Engineering	Intro to RE, essential idea of assembly
	Overview of GHIDRA (mainly) and IDA (briefly)
	Instruction set architectures
	Common file formats
	file-level reverse engineering tools
	Recognizing high-level constructs
	GHIDRA disassembly manipulation,datatypes, and data structures
	Control flow and data flow analysis
	Calling conventions
	Function recognition
	Introduction to decompilation techniques
	Challenges of disassembly techniques
	Common anti-disassembly techniques
	Basic dynamic analysis techniques

	Limitations of static analysis techniques
	Dynamic instrumentation
	Anti-debugging techniques
	Common software vulnerabilities and exploits
	Vulnerability analysis
	Cross-channel vulnerability
	Malware detection techniques
	Anti-signature techniques: Obfuscation and packing