The curriculum provided is an extensive and comprehensive course on information security, covering a broad range of topics essential for understanding, detecting, and defending against various cyber threats. Here's an overview of each module:

1: INTRODUCTION TO INFORMATION SECURITY

-security elements
-cyber kill chain
-mitre att&ck framework
-ethical hacking
-information assurance
-risk management
-incident management
-laws and standards

2: FOOTPRINTING AND RECONNAISSANCE

-concepts
-osint + osr framework
-theharvester
-api keys
-foca + advanced google search + google hacking + whois footprinting + whois research + dns footprinting + query dns with nslookup + website footprinting + webserver fingerprint + id serve + httrack + email footprinting + email tracing + network footprinting + social network footprinting + countermeasures

3: SCANNING NETWORKS

-concepts
-discovery scans
-icmp echo
-arp pings
-host discovery
-angry ip scanner
-port scans
-angry ip scanner
-hping3 packet crafting
-zenmap
-nmap
-host discovery with nmap
-nmap version detection
-idle (zombie) scan
-ftp bounce scan
-nmap scripts
-firewall and ids evasion
-nmap advanced scans
-proxies

4: ENUMERATION

-smb netbios enumeration
-hyena
-file transfer enumeration
-wmi enumeration
-snmp enumeration
-softperfect
-ldap enumeration
-dns enumeration
-smtp enumeration
-remote connection enumeration
-website enumeration
-dirbuster

5: VULNERABILITY ANALYSIS

-cveq
-serianu
-vpat
-vulnerability scanning
-openvas
-vulnerability assessment
-risk profiling
-african trends

6: SYSTEM HACKING

concepts
-common os exploits
-buffer overflows
-tools and frameworks
-linux targets
-metasploit
-meterpreter
-keylogging and spyware
-netcat
- hacking windows
-eternal blue
-hacking linux
-password attacks
-pass the hash
-password spraying
-cracking tools
-windows password crack
-hiding data
-least significant bit steganography
-covering tracks

-clearing tracks in windows
-auditpol

7: MALWARE

-malware
-viruses
-trojans
-deploying a rat
-rootkits
-advanced persistent threat
-malware dropper and handler
-detection
-malware analysis
-static code review
-solarwinds orion hack

8: SNIFFING

-network sniffing
-niffing tools
-sniffing http with wireshark
-capturing files from smb
-arp and mac attacks
-mitm attack with ettercap
-name resolution attacks
-spoofing responses with responder
-layer 2 attacks

9: SOCIAL ENGINEERING

concepts
-techniques
-baited usb stick
-o.mg lightning cable
-phishing for credentials
-social media
-identity theft
-insider threats

10: DENIAL-OF-SERVICE

dos-ddos concepts
-volumetric attacks
-fragmentation attacks
-state exhaustion
-application layer attacks

-loic attack
-hoic attack
-slowloris attack

11: SESSION HIJACKING

12: IDS, FIREWALLS, AND HONEYPOTS

13: WEB SERVERS

14: WEB APPLICATIONS

15: SQL INJECTION

16: WIRELESS NETWORKS

17: MOBILE AND IOT

18: CLOUD COMPUTING

19: CRYPTOGRAPHY

20: SOC AND INCIDENT RESPONSE