SPRINT Academy

Cyber Security

סילבוס

1. Introduction & Computer Structure

- Course intro
- Black Hat
- Homework solution
- White Hat
- Malware Types
- Hardware (Power Supply and Motherboard)
- Hardware (CPU)
- Hardware (RAM)
- Hardware (Input Output)
- Storage (HHD, SSD)
- BIOS
- CMOS
- Computer Hardware (CPU-Z)
- Binary
- Sizes
- ASCII
- Binary to Dec
- Ascii to Binary1.19. Hexadecimal
- Hex to Decimal
- Theoretical Summary Exercise
- Practical Summary Exercise

2. Computer networks

- Network Fundamentals
- Network Addresses
- Network Addresses Practice
- Network Devices (Part 1)
- Network Devices (Part 2)
- OSI (Part 1)
- OSI (Part 2)
- OSI (Part 3) + TCP IP
- Encupsulation
- Network Flow
- Subnet Mask
- Subnetting
- Subnet Practice
- Network Diagram
- Wireshark Basics
- ICMP
- ARP
- NAT + IPv6
- NAT Theory
- VLAN
- TCP UDP (Part 1)
- TCP UDP (Part 2) 3 Way Handshake
- TCP UDP (Part 3) Advanced TCP
- TCP - Wireshark
- DNS
- DNS - Wireshark
- DHCP Theory
- DHCP Practical
- HTTP Protocol (Part 2)
- HTTP - Wireshark
- Remote Connection
- FTP
- Computer Networks Exam (Part 1)
- Computer Networks Exam (Part 2)
- Computer Networks Practical Exam

3. Operating Systems & Virtualization

- Resources
- VT types
- Network types
- VirtualBox / Vmware
- Boot process
- OS principles
- File systems
- GUI vs. CLI
- I/O commands
- Files commands
- Network commands
- Services commands
- Package management commands
- Text processing commands
- Important files
- Artifacts

4. Bash

- Logical thinking
- Pseudo Codes
- Flowcharts
- Input & Output commands
- Variables & Casting
- Flow control
- Loops
- Functions
- Arguments

5. Python

- Logical thinking
- Pseudo Codes
- Flowcharts
- Compilation process
- Input & Output commands
- Variables & Casting
- Advanced data types
- Strings
- Flow control
- Loops
- Functions
- Scopes
- Import libraries
- Relevant libraries (os, socket, requests, etc,)
- Working with APIs
- Networking
- Reverse & Bind shell

6. Forensics

- Reputation engines
- Sandboxes
- Static & Dynamic analysis
- Files forensics
- strings
- PEView, PEStudio
- CFF
- Network forensics
- Wireshark
- Network Miner
- TCPView
- Captipper
- File system forensics
- FolderChangesView
- Memory forensics
- Volatility
- OS forensics
- OSForensics
- Procmon
- Process forensics
- Process Explorer
- Event forensics
- Event viewer
- Sysmon
- Registry forensics
- RegMon
- RegView Explorer
- Mail forensics
- EMLView
- OLEView
- Macros
- Other tools
- Forensics advanced techniques & methodologies

7. Cryptography

- Symmetric vs. Asymmetric
- Hash vs. Coding vs. Encryption
- Modern techniques
- Traditional techniques
- RSA
- SSL and TLS
- Diffie Hellman

8. Penetration Testing

- MITRE / Kill Chain
- Exploit vs. Vulnerability vs. Payload
- Attack groups
- Reconnaissance
- nmap + NSE
- Spiderfoot
- Nessus
- Enumeration & Auxiliary
- Metasploit
- Searchsploit
- Exploit DB
- Shodan + GHDB (Google Dorks)
- Persistence techniques
- Local & Remote Privilege Escalation
- SAM file + lsass
- passwd + shadow
- psexec
- Wordlist generation
- brute force (John, Hydra, Sprays)
- Discover new assets
- Data collection using scripts
- C&C techniques
- Protocol tunneling
- Social Engineering & Phishing
- Wifi Hacking
- MITM
- Post Exploitation
- Reports

9. Active Directory

- Domain Environment
- Set up labs
- Objects
- Group vs. OU
- GPO
- Trusts
- Authentication vs. Authorization
- NTLM & Kerberos
- LLMNR
- Pass The Hash
- Pass The Ticket
- Silver Ticket
- Golden Ticket
- Kerberoasting
- BloodHound & GoFetch
- Responder
- Mimikatz

10. Web Security

- OWASP
- Burp / Fiddler
- SQLinjection
- XSS
- XXE
- RCE
- Insecure deserialation
- Directory Traversal
- LFI/RFI
- CSRF
- Command injection
- Broken authentication

11. Security products

- Firewalls in linux & windows
- WAF
- IDS / IPS concepts
- Snort rules
- EDR & AV
- YARA rules
- NAC
- sysmon
- Honeypots
- SIEM concepts & basics
- Event analysis

12. Security Management

- About the teams
- Vulnerability Assessment
- Asset analysis & management
- CIA & NIST
- Employees awareness
- Working with
- CERT

13. Advanced Topics

- Process vs. Thread vs. Service vs. Program
- Memory structure
- Stack structure
- Buffer Overflow
- DEP + ASLR + Canaries
- Hooking concepts
- AV Evasion techniques
- Anti debugging & Anti VT techniques
- Darket basics
- CTFs

14. Career Management

- Projects & Git
- CV workshop
- Interview questions & simulations
- LinkedIn

***נא לשים לב!**
תכני הסילבוס עלולים להשתנות

מסלול קורסי העשרה

- פתיחת עסק עצמאי
- דיני חוזים
- מכירות
- דיני עבודה
- פיתוח עסקי
- שפת גוף
- מחקרי שוק והתנהגות צרכנים
- כתיבת תוכן שיווקי
- אסטרטגיה למנהל דיגיטל
- מבוא לשיווק דיגיטלי


SA
SPRINT
Academy