SCHEDA CORSO ETHICAL HACKER

Dati del corso

Voce	Dettaglio
Titolo	Ethical Hacker – Hacker Path
Erogato da	Fata Informatica S.r.l. – CybersecurityUP
Modalità	E-learning (percorso completo anche in formula Blended)
Struttura	10 moduli indipendenti, acquistabili singolarmente, in 3 pacchetti o come percorso completo
Durata video	65 ore 10 min complessive (24 h 54 min Fondamenti · 26 h 02 min Offensive · 14 h 13 min Extreme)
Lingua	Italiano
Piattaforma pratica	HackMeUP: 1 anno di accesso incluso nel percorso completo
Accesso	h24, per 12 mesi
Docenti	Docenti universitari ed esperti del settore
Attestati	Attestato di partecipazione al termine di ogni modulo
Certificazioni	CPEH o CTEH, solo con il percorso completo e in base al possesso dei requisiti di accesso all'esame

Presentazione e finalità

Il percorso Ethical Hacker (Hacker Path) forma professionisti della sicurezza informatica offensiva, partendo dalle nozioni fondamentali fino alle competenze avanzate.

I corsi sono tenuti da docenti universitari ed esperti del settore, per garantire un apprendimento pratico e altamente qualificato. Il percorso è pensato per offrire una preparazione completa per operare nell'Ethical Hacking: dai primi passi su reti e Linux alla ricognizione, al vulnerability assessment, agli attacchi a sistemi, reti e applicazioni web, fino a privilege escalation, evasione delle difese e tecniche d'attacco di frontiera.

La teoria si affianca alla pratica: ogni modulo prevede laboratori didattici e il percorso completo include HackMeUP, la cyber arena con scenari di attacco e difesa a difficoltà crescente.

Completando il percorso completo è possibile accedere all'esame per la certificazione professionale CPEH (Certified Professional Ethical Hacker) o, in assenza dei requisiti, CTEH (Certified Technician Ethical Hacker).

A chi è rivolto e requisiti per iscriversi

Il percorso è pensato per chi vuole entrare nel mondo della sicurezza informatica offensiva. Ethical Hacker e Penetration Tester sono professioni che permettono di lavorare su attività diverse: dal Vulnerability Assessment al Penetration Test,

fino alle campagne di Red Team. Il percorso è adatto sia a chi muove i primi passi nel settore, sia a chi vuole approfondire tecniche e strategie sempre più avanzate.

Moduli	Competenze richieste
Foundation, Systems, Recon, Exploit, Offensive	Nessuna competenza specifica, solo dimestichezza con PC e navigazione Internet.
Mastery, Intelligence, Exploitation	Preparazione già solida sui temi dei moduli precedenti (ricognizione, vulnerability assessment, enumerazione).
Extreme Privilege & Evasion, Extreme Attack Techniques	Conoscenza consolidata dell'intero percorso; per Extreme Attack Techniques utile familiarità di base con applicazioni Java e dispositivi Android.

I prerequisiti specifici di ciascun modulo sono indicati nel programma dettagliato. Fata Informatica non fornisce consulenza sulle esigenze formative del Cliente: la scelta dei moduli è responsabilità dell'acquirente.

Obiettivi formativi

Al termine del percorso completo il discente sarà in grado di:

- Comprendere cos'è un attacco informatico, le fasi della Kill Chain e il mindset dell'Ethical Hacker, e conoscere reti, protocolli e sistemi di protezione.
- Muoversi con sicurezza in ambiente Linux e Kali Linux: file system, shell, pipeline, scripting, bind e reverse shell.
- Condurre un penetration test con metodo, dalla ricognizione (OSINT, footprinting, scanning) al vulnerability assessment con strumenti manuali e automatici (nmap, Nikto, OpenVAS, Nessus, Burp Suite).
- Eseguire attacchi a sistemi, reti e applicazioni web: password cracking, buffer overflow, Metasploit e Meterpreter, ARP poisoning, XSS e SQL Injection.
- Svolgere network enumeration in ambienti Windows e Unix (Active Directory, SMB, NFS, SNMP) e attacchi a memoria.
- Applicare tecniche di privilege escalation su Windows e Linux, post-exploitation, esfiltrazione ed evasione di firewall e antivirus.
- Affrontare tecniche d'attacco avanzate: Log4Shell, Apache Commons Text RCE, attacchi ad Android tramite APK trojanizzati e hacking di sistemi fisici con Flipper Zero.
- Prepararsi all'esame per la certificazione professionale CPEH o CTEH.

Gli obiettivi specifici di ogni modulo sono riportati nel programma dettagliato.

Struttura del percorso: moduli e pacchetti

Il percorso è articolato in 10 moduli indipendenti, acquistabili singolarmente, in pacchetti consigliati o come percorso completo.

Cod.	Modulo	Pacchetto	Durata video
EH-FND	Foundation: reti e difesa	Fondamenti	08:21:19
EH-SYS	Systems: fondamenti Linux	Fondamenti	07:26:26
EH-RCN	Recon: metodologia e ricognizione	Fondamenti	05:55:32
EH-MST	Mastery: sistemi e rete avanzati	Fondamenti	03:11:22
EH-EXA	Exploit: vulnerabilità e sfruttamento	Offensive	06:29:57
EH-OFF	Offensive: attacchi di rete e web	Offensive	06:47:37
EH-INT	Intelligence: ricognizione e vulnerability assessment avanzati	Offensive	06:46:23
EH-EXN	Exploitation: network enumeration e sfruttamento avanzato	Offensive	05:58:28
EH-EPE	Extreme Privilege & Evasion	Extreme	06:10:13
EH-EAT	Extreme Attack Techniques	Extreme	08:03:34
	Totale		**65:10:51**

Pacchetti

Pacchetto	Codice	Moduli inclusi	Durata video
Fondamenti	EH-PKG-FND	Foundation, Systems, Recon, Mastery	24:54:39
Offensive	EH-PKG-OFF	Exploit, Offensive, Intelligence, Exploitation	26:02:25
Extreme	EH-PKG-EXT	Extreme Privilege & Evasion, Extreme Attack Techniques	14:13:47
Percorso completo	EH-FULL	Tutti i 10 moduli + piattaforma HackMeUP + voucher esame nominale	65:10:51

Fondamenti è il punto di partenza per chi entra nel mondo dell'Ethical Hacking. **Offensive** è il cuore operativo: dal vulnerability assessment ai primi attacchi, fino a Metasploit e Burp Suite. **Extreme** è il livello più avanzato, per chi vuole padroneggiare le tecniche offensive di frontiera. Il **Percorso completo** è l'unica opzione che dà accesso alla certificazione professionale.

Modalità di erogazione e metodologia didattica

E-learning

Il corso è fruibile 24 ore su 24 dalla piattaforma di formazione di Fata Informatica, con credenziali personali (username e password). Ogni modulo comprende:

- video lezioni registrate;

- test ed esercizi di valutazione;
- laboratori didattici;
- materiale scaricabile;
- e-mail di supporto per interagire con i docenti;
- Uppy, l'AI Tutor addestrato sui materiali ufficiali del corso, disponibile 24/7;
- attestato di partecipazione al termine del modulo.

Il percorso completo include inoltre l'accesso alla piattaforma HackMeUP e il voucher per l'esame nominale.

Blended

Il Blended è un unico percorso completo, che copre l'intero programma dalle fondamenta alle tecniche avanzate. Comprende un anno di accesso alla piattaforma HackMeUP, classi con date di partenza prestabilite e webinar settimanali con i docenti.

Uppy – il tutor AI

Uppy è incluso nel percorso formativo e risponde in modo istantaneo sui temi complessi, assiste durante le esercitazioni di laboratorio e aiuta nel ripasso mirato prima dei test, 24 ore su 24.

HackMeUP – la cyber arena

HackMeUP è la piattaforma pratica inclusa nel percorso completo (acquistabile anche singolarmente) per sviluppare capacità operative reali:

- scenari di attacco realistici, in ambienti di simulazione a difficoltà crescente;
- approccio offensivo strutturato, dalla ricognizione allo sfruttamento fino al mantenimento dell'accesso, secondo il flusso reale di un penetration test;
- Cyber Game: sfide pratiche su credential access, privilege escalation, lateral movement ed evasion;
- gli stessi strumenti professionali usati in ambito offensive security;
- laboratori aggiornati per riflettere nuove tecniche di attacco e nuove vulnerabilità.

CPEH Elite Club

Pacchetto opzionale, riservato a chi ha completato il percorso e ottenuto la certificazione CPEH. Assicura per cinque anni l'aggiornamento e il mantenimento delle competenze, con lezioni avanzate e corsi specialistici (Dynamic Malware Analysis, Reverse Engineering, Python for Pentester) e l'accesso a HackMeUP per cinque anni.

Verifiche, attestati e certificazioni

Ogni modulo prevede test di valutazione dell'apprendimento, composti da domande a risposta multipla e/o prove pratiche. Il superamento dei test è requisito necessario per completare il percorso.

Titolo	Chi lo ottiene	Come
Attestato di partecipazione	Chi acquista singoli moduli o pacchetti parziali	Al termine di ogni modulo, dopo aver completato i materiali e superato i test; rilasciato su richiesta

Titolo	Chi lo ottiene	Come
CPEH – Certified Professional Ethical Hacker	Chi completa il percorso completo e possiede i requisiti previsti	Esame finale: prova scritta, esame pratico con laboratori virtuali e prova orale, in lingua italiana
CTEH – Certified Technician Ethical Hacker	Chi completa il percorso completo ma non possiede ancora i requisiti per la CPEH	Esame finale, come sopra

L'accesso all'esame e alle certificazioni è riservato a chi acquista il percorso completo, che include il voucher per l'esame nominale. Il mancato superamento dell'esame non consente di conseguire la certificazione.

Certificazione CPEH

La CPEH è rilasciata da Fata Informatica, ente accreditato secondo ISO/IEC 17024:2012 e conforme alle norme UNI 11506:2021 e UNI 11621-4:2024. In linea con la Legge 4/2013, i professionisti certificati saranno inseriti nel registro Accredia dei Certified Professional Ethical Hacker.

Requisiti per la CPEH

- Istruzione: almeno il diploma di scuola secondaria di primo grado.
- Formazione: almeno 24 ore di aggiornamento nell'ultimo anno (corsi, webinar, convegni).
- Esercizio dell'attività di Ethical Hacker: 3 mesi per chi ha una laurea o corsi post-diploma, 5 mesi per chi ha completato la scuola superiore, 6 mesi per chi possiede il diploma di scuola media.

Mantenimento: Ogni anno il professionista trasmette a Fata Informatica l'evidenza di formazione continua, l'evidenza di continuità professionale (o di incremento della formazione, in caso di perdita di lavoro) e l'evidenza della registrazione e del trattamento di eventuali reclami ricevuti.

Rinnovo: Al quinto anno il professionista presenta l'assenza o la corretta gestione dei reclami, il continuo esercizio della professione, i crediti formativi acquisiti negli anni di mantenimento, supera l'esame di rinnovo e paga la relativa quota, come indicato nel tariffario ufficiale. In funzione degli esiti il certificato può essere rinnovato, sospeso o revocato.

Programma dettagliato

Ogni modulo include: e-learning, video lezioni registrate, accesso h24, test ed esercizi di valutazione, laboratori didattici, materiale scaricabile, attestato di partecipazione, e-mail di supporto per interagire con i docenti e Uppy, l'AI Tutor disponibile 24/7. Di seguito, per ciascun modulo, sono indicati i numeri specifici.

EH-FND – Foundation: reti e difesa

Introduzione. Costruisce le fondamenta dell'intero percorso. Si parte dal capire cos'è un attacco informatico e come ragiona chi lo conduce, si riconoscono le fasi di una Kill Chain e si padroneggia il funzionamento di reti e protocolli. Si allarga poi lo sguardo ai sistemi di protezione della rete, al framework OWASP Top 10, alle principali categorie di attacchi e di malware e alle tecniche di social engineering.

Obiettivi

- Comprendere cos'è un attacco informatico, chi sono gli attori in gioco e quali tecniche e vettori privilegiano.
- Conoscere il processo di Incident Response e i principi della Triade CIA.
- Padroneggiare le fasi della Kill Chain e riconoscerle in scenari reali.

- Acquisire solide basi di reti e protocolli: dai modelli ISO/OSI e TCP/IP a routing, DNS, DHCP, protocolli applicativi e web.
- Conoscere i sistemi di protezione della rete (firewall, proxy, IDS/IPS, VPN, DLP, Honeypot) e il framework OWASP Top 10.
- Riconoscere le principali categorie di attacchi, di malware e le tecniche di social engineering.
- Sviluppare il mindset dell'Ethical Hacker: comprendere le tecniche di attacco per rafforzare la difesa.

A chi è rivolto. A chi si affaccia per la prima volta alla cybersecurity offensiva.

Competenze richieste. Nessuna competenza specifica, solo dimestichezza di base con PC e navigazione Internet.

Programma del corso

1. **Introduzione.** Cos'è un attacco informatico · Il processo di Incident Response · La Triade CIA · Le tipologie di Hacker · Cyber Theft Ring · Quanto valgono i nostri dati sul Dark Web · I principali attori, attacchi, tecniche e vettori preferiti.
2. **Kill Chain.** Le fasi: Targeting, Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, Action · L'attacco a Target.
3. **Reti e protocolli.** I pacchetti: modello ISO/OSI, modello TCP/IP, livelli, incapsulamento · Gli header: TCP, IP, Ethernet · Il protocollo IP: indirizzi, classi di indirizzamento, netmask, IPv6 · Il routing IP: tabelle di routing, Autonomous System, protocolli IGP/EGP, Distance Vector, RIP, Link State, Path Vector · Il livello Data Link: indirizzi MAC, MAC Table, switch, protocollo ARP · TCP e UDP: porte, header, comando Netstat, three way handshake · DNS: struttura, risoluzione · Il protocollo DHCP: fasi, discover, offer, request, hack, rinnovo · Altri protocolli: SNMP, ICMP, FTP, SMTP, IMAP, POP3 · Le applicazioni web: protocollo HTTP, request, response, HTTPS, cookies, sessioni HTTP.
4. **Sistemi per proteggere la rete.** I proxy · I firewall · Gli Honeypot · VPN · IDS/IPS · I sistemi DLP.
5. **Top 10 OWASP.** Chi è OWASP · Come si compone un'applicazione web · La Top Ten OWASP: Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities, Broken Access Control, Security Misconfiguration, Cross Site Scripting, Insecure Deserialization, Using Components with Known Vulnerabilities, Insufficient Logging and Monitoring.
6. **Gli attacchi.** Cos'è uno Zero Day · DoS, DDoS e DRDoS (Smurf, Xmas Scan Attack) · Man in the Middle · Man in the Browser · Buffer Overflow · Privilege Escalation · ARP Poisoning · DNS Poisoning · Domain Hijacking · ClickJacking · Session Hijacking · Spoofing: MAC, Email, Phone · Downgrade Attack · Attacchi a WiFi: protocolli Wi-Fi, Reply Attack, Rogue AP, Evil Twin, attacchi a WPS · Attacchi a Bluetooth: Bluejacking, Bluesnarfing, Bluebugging · Attacchi crittografici · Funzioni Hash · Pass the Hash · Attacco alle password: tabelle arcobaleno, sale, attacchi a dizionario, ibridi, online, Brute Force, attacco al compleanno.
7. **Il malware.** Il formato PE · Le DLL · Kernel Mode vs User Mode · I Protection Ring · Le API · Come si viene infettati · Le firme · Obfuscation & mutation · Malware polimorfico e metamorfico · Mutation engines · La persistenza: registri di sistema, DLL Hijacking, DLL Load Order Hijacking, Trojanized System Binaries · Le tipologie di malware: virus, backdoor, adware, spyware, keylogger, trojan, RAT, criptojacking · Macrovirus · Scareware · Fileless Malware · I rootkit: user mode, kernel mode, IAT Hooking, bootkit · I malware ibridi (Conficker) · I Ransomware: fasi di un attacco, WannaCry, come comportarsi · Gli Exploit Kit: Angler, Zeus Builder · Crime as a Service (GrandCrab).
8. **Social engineering.** Cos'è il social engineering · Scenari · Phishing, spear phishing, lateral phishing, truffe BEC, smishing, vishing · Tailgating, impersonation, dumpster diving, shoulder surfing, watering hole · I principi base del social engineering · Un esempio di attacco · Social Engineering Attack Framework.

EH-SYS – Systems: fondamenti Linux

Introduzione. Porta nel sistema operativo che è di casa nella sicurezza offensiva: Linux. Dalla filosofia e struttura del sistema fino alla riga di comando, si impara a muoversi con sicurezza tra file system, processi, redirezioni e primi script di shell. Senza padronanza dell'ambiente Linux, gli strumenti dell'Ethical Hacker restano scatole chiuse.

Obiettivi

- Conoscere origini, filosofia e struttura di Linux: kernel, shell, comandi e processi.
- Muoversi con sicurezza nel file system, gestendo file, directory, permessi e protezioni.
- Padroneggiare la redirezione di input, output ed errore.
- Usare filtri e pipeline per elaborare dati dalla riga di comando (grep, sort, sed, awk e altri).
- Gestire processi, job, variabili d'ambiente e segnali.
- Acquisire i primi rudimenti di programmazione shell: quoting, metacaratteri, globbing e composizione di comandi.

A chi è rivolto. A chi vuole acquisire familiarità con l'ambiente Linux, base operativa per tutti i moduli successivi.

Competenze richieste. Nessuna competenza specifica; può essere seguito in parallelo o subito dopo Foundation.

Programma del corso

1. **Introduzione a Linux.** Cenni storici, la filosofia, distribuzioni · Il Kernel, la shell, i comandi, i processi.
2. **Il File System.** File e Directory, la struttura del File System · Permessi e protezioni, comandi per file e directory.
3. **Redirezione.** Stdin, Stdout e Stderr · La redirezione dell'input, dell'output, dell'errore.
4. **Filtri e pipeline.** Le pipes · I principali filtri: grep, sort, uniq, nl, tr, head, tail, wc, sed, awk.
5. **La gestione dei processi.** Le variabili ambientali · I job · Gli stati dei processi · I segnali.
6. **Rudimenti di programmazione shell.** Quoting · Metacaratteri e globbing · Semplici esempi di sostituzione · Composizione di comandi · Il primo programma.

EH-RCN – Recon: metodologia e ricognizione

Introduzione. Introduce la prima fase operativa di ogni penetration test: la ricognizione. Si impara come si struttura un penetration test dall'ingaggio alla presentazione dei risultati e come raccogliere informazioni sul bersaglio sfruttando fonti aperte (OSINT), tecniche attive e passive e i primi strumenti di scanning.

Obiettivi

- Comprendere motivazioni, fasi e modalità di ingaggio di un penetration test, fino alla presentazione dei risultati.
- Padroneggiare le tecniche di information gathering e Open Source Intelligence (OSINT).
- Distinguere ricerca attiva e passiva e applicare i diversi livelli di profondità.
- Eseguire System Identification con strumenti come whois, ping, traceroute, nslookup, dig e trasferimenti di zona DNS.
- Condurre footprinting e scanning con Google dorks, banner grabbing e scanning automatico via nmap e dmitry.

A chi è rivolto. A chi vuole muovere i primi passi nel penetration testing vero e proprio, imparando a raccogliere informazioni su un bersaglio.

Competenze richieste. Conoscenze di reti e protocolli equivalenti a quelle fornite dal modulo Foundation.

Programma del corso

1. **Introduzione al processo di Penetration Test.** Le motivazioni e l'ingaggio · Le fasi · Presentare i risultati.

2. **Information Gathering.** Intelligence gathering · Open Source Intelligence gathering (OSINT) · Ricerca attiva vs passiva, i tre livelli di profondità · Servizi di informazione online · System Identification: le basi (Netcraft, whois, ping, traceroute, nslookup vs host vs dig) · System Identification e DNS: zone transfer · System Identification e servizi di rete: port scanning, nc, banner grabbing, introduzione a nmap.
3. **Footprinting & Scanning.** Le fasi del footprinting · Definire il raggio di azione · Strumenti del footprinting · Hack Google: query Google, operatori avanzati, Google dorks · Hack DNS: spremere un DNS · Ancora banner grabbing · Mappare le reti remote · Port Scanning automatico: nmap · System Identification automatico: nmap, dmitry.

EH-EXA – Exploit: vulnerabilità e sfruttamento

Introduzione. Porta nel cuore del vulnerability assessment: il processo con cui si individuano, classificano e valutano le vulnerabilità di un sistema. Si impara a definire il perimetro di analisi, a distinguere vulnerabilità ed effettiva sfruttabilità, a orientarsi tra standard e basi dati di riferimento (CVSS, MITRE, NIST) e a usare strumenti manuali e automatici. Si passa poi alle prime fasi offensive: l'enumerazione di sistemi e servizi in ambiente Windows e Linux e gli attacchi a sistema tramite password cracking e buffer overflow. È il ponte tra la ricognizione e le tecniche offensive vere e proprie.

Obiettivi

- Comprendere il processo di vulnerability assessment e le sue fasi.
- Definire correttamente il perimetro di analisi, distinguendo contesti Inside e Internet Facing.
- Interpretare le evidenze rilevate e comprenderne i limiti.
- Distinguere il concetto di vulnerabilità da quello di sfruttabilità (exploitability).
- Impostare un processo di assessment continuo.
- Orientarsi tra gli standard e le basi dati di riferimento: FIRST CVSS, MITRE, NIST.
- Utilizzare strumenti manuali e automatici: nmap, Nikto, OpenVAS, Nessus.
- Eseguire l'enumerazione di sistemi e servizi di rete in ambiente Windows e Linux.
- Condurre attacchi a sistema tramite password cracking (tecniche online/offline, attive/passive) e buffer overflow, con strumenti come John e le Rainbow tables.

A chi è rivolto. A chi vuole imparare a valutare le vulnerabilità di un sistema e muovere i primi passi nelle tecniche di attacco.

Competenze richieste. Contenuti dei moduli Foundation e Recon (reti, protocolli, metodologia di ricognizione).

Programma del corso

1. **Vulnerability Assessment.** Introduzione · Il processo di VA · Definizione del perimetro · Inside vs Internet Facing · Le evidenze rilevate dal processo di VA · Limiti della VA: il concetto di vulnerabilità, il concetto di exploitability · Costruzione di un processo continuo · Gli standard e le basi dati di riferimento: FIRST CVSS, MITRE, NIST · Strumenti manuali vs automatici: nmap, Nikto, OpenVAS, Nessus.
2. **Fondamenti ed enumerazione.** La fase di exploit · Classificazione degli exploit · Enumerazione dei sistemi · Enumerazione dei servizi di rete · Enumerazione in ambiente Windows · Enumerazione in ambiente Linux.
3. **Attacchi a sistema.** Password cracking: tecniche online e offline, tecniche attive e passive, i metodi · Strumenti: John, Rainbow tables · Buffer overflow.

EH-OFF – Offensive: attacchi di rete e web

Introduzione. Segna il passaggio dalla teoria all'attacco vero e proprio. Si mettono in pratica le tecniche per compromettere sistemi, reti e applicazioni web: dagli attacchi di rete con authentication cracking, sfruttamento delle

share Windows e ARP poisoning, all'uso del framework Metasploit e Meterpreter, fino alle vulnerabilità web come XSS e SQL Injection. Gli strumenti professionali dell'offensive security entrano in gioco in ambienti di laboratorio controllati.

Obiettivi

- Eseguire attacchi di rete: authentication cracking con Hydra, sfruttamento di share Windows e null session, ARP poisoning e man-in-the-middle.
- Padroneggiare il framework Metasploit e Meterpreter: payload, sessioni, information gathering.
- Attaccare applicazioni web: fingerprinting ed enumerazione di web server, verbi HTTP, file e directory.
- Sfruttare le principali vulnerabilità web: Cross Site Scripting (Reflected e Persistent) e SQL Injection con strumenti come SQLmap.

A chi è rivolto. A chi vuole mettere in pratica attacchi reali su reti, sistemi e applicazioni web.

Competenze richieste. Contenuti del modulo Exploit (vulnerability assessment, prime tecniche di enumerazione e attacco a sistema).

Programma del corso

1. **Network Attacks.** Authentication Cracking: vulnerabilità, tool Hydra · Share di Windows: Universal Naming Convention paths (UNC), share amministrativi e nascosti · Null session: vulnerability, tool Enum · ARP poisoning: protocollo ARP, ARP Table, man-in-the-middle (MITM) · Metasploit: framework, console, comandi, payload · Meterpreter: connessione (bind, reverse), session, information gathering (sysinfo, route, getuid).
2. **Attacchi Applicazioni Web.** Introduzione: fingerprinting web server, test della scatola nera, Httprint, exploitation manuale di server · Protocollo HTTP: metodi GET, POST, HEAD, PUT, DELETE, OPTION · Enumerazione: verbi HTTP, file e directory, motori di ricerca, OWASP DirBuster · Cross Site Scripting: contromisure, tipologie, Reflected (non-persistent), Persistent · SQL Injection (SQLi): punto di iniezione, anatomia di un attacco, SQLmap.

EH-MST – Mastery: sistemi e rete avanzati

Introduzione. Fa salire di livello nella padronanza degli ambienti operativi. Al centro ci sono Kali Linux e l'arte di dominare la riga di comando in modo avanzato: amministrazione, gestione di servizi e processi, tecniche di "shell kung-fu" e networking sia in ambiente Linux che Windows. Si impara a creare bind shell e reverse shell su entrambe le piattaforme, competenza operativa fondamentale per muoversi dentro i sistemi compromessi con agilità e controllo.

Obiettivi

- Amministrare Kali Linux: gestione pacchetti (APT, dpkg) e gestione servizi (systemctl).
- Padroneggiare tecniche avanzate di shell: gestione processi e job, automazione, analisi dei dati.
- Applicare bash hack, history hack, SSH hack e l'uso di Zsh.
- Gestire il networking in Linux con strumenti come nc e socat.
- Creare bind shell e reverse shell in ambiente Linux.
- Gestire il networking in Windows con PowerShell e creare bind/reverse shell con Powercat.

A chi è rivolto. A chi vuole approfondire l'uso avanzato di Kali Linux, della shell e del networking operativo.

Competenze richieste. Contenuti del modulo Systems (fondamenti Linux: file system, processi, shell scripting).

Programma del corso

1. **Kali e dintorni.** Amministrazione e servizi: gestione pacchetti (Advanced Package Tool e dpkg), gestione dei servizi (systemctl) · Shell Kung-fu: gestione processi, gestione job, azioni ripetute, analisi dei dati, comandi e sinonimi, bash hack, history hack, matematica ma non troppo, SSH hack, Zsh · Networking essential: networking in Linux, nc,

socat, bind shell e reverse shell in ambiente Linux, networking in Windows con PowerShell, bind shell e reverse shell in ambiente Windows, Powercat.

EH-INT – Intelligence: ricognizione e vulnerability assessment avanzati

Introduzione. Porta ricognizione e vulnerability assessment a un livello professionale. Partendo dalla figura del penetration tester in azienda, si approfondiscono le tecniche avanzate di information gathering, passivo e attivo, con strumenti come Maltego, Shodan, masscan e Wireshark, e si impara a condurre audit di sicurezza strutturati secondo framework come PCI-DSS e le linee guida NIST. È il modulo che trasforma la ricognizione da attività tecnica a vera e propria intelligence, con uno sguardo maturo sulla superficie di attacco e sulla valutazione del rischio.

Obiettivi

- Conoscere la professione del penetration tester: ruolo in azienda, attività e competenze necessarie.
- Padroneggiare l'information gathering avanzato basato su Kill Chain e MITRE ATT&CK.
- Condurre ricognizione passiva con fonti aperte, Web Mirroring, Maltego, Shodan e posizionamenti Man-in-the-Middle.
- Eseguire ricognizione attiva con nmap, hping3, netcat, masscan e strumenti di enumerazione DNS/SNMP/web.
- Condurre audit di sicurezza secondo framework e standard (PCI-DSS, SCAP, MSCT, NIST) con Nessus Professional.
- Applicare il vulnerability assessment alle applicazioni web con strumenti come Burp Suite.

A chi è rivolto. A chi vuole portare ricognizione e vulnerability assessment a un livello professionale, con strumenti e framework avanzati.

Competenze richieste. Contenuti dei moduli Recon ed Exploit.

Programma del corso

1. **La professione del pen-tester.** Introduzione · La figura dell'ethical hacker in azienda · Le attività svolte dal penetration tester · Le competenze necessarie.
2. **Mastering Information Gathering.** Introduzione: le motivazioni, gli schemi di attacco, la superficie di attacco, analisi della difesa · Come realizzare una ricognizione: Kill Chain, MITRE ATT&CK, cosa cercare, strumenti di ricognizione nel tempo, tipologie di ricognizione · La ricognizione passiva: cosa e dove cercare, fonti aperte, Google e exploit-db, Web Mirroring, Maltego, Shodan, posizionamenti MiM per il gathering (Wireshark) · La ricognizione attiva: port scanning con nmap, hping3, netcat, masscan; post-exploitation recon (ARP Scan); DNS Enumeration; SNMP Scanning (onesixtyone); Web App Recon (wappalyzer).
3. **Mastering Vulnerability Assessment.** Oltre la scansione: audit di sicurezza e framework, PCI-DSS, SCAP, MSCT, esecuzione audit mediante Nessus Professional, valutazione del rischio, guida NIST al Risk Assessment · Oltre Nessus: un nuovo punto di vista (LHF), alla ricerca di alternative, generazione di dizionari · Vulnerability Assessment e Applicazioni Web: strumenti rapidi, Burp Suite.

EH-EXN – Exploitation: network enumeration e sfruttamento avanzato

Introduzione. Entra nel vivo dello sfruttamento avanzato. Si parte dalla network enumeration in ambienti Unix e Windows, inclusa l'enumerazione di Active Directory e SNMP, per poi affrontare l'exploitation vera e propria: dagli scenari e vettori di attacco fino agli attacchi a memoria, con laboratori pratici su Buffer Overflow e Windows Memory Exploitation. È il modulo in cui teoria e pratica offensiva si fondono nei loro aspetti più tecnici e profondi.

Obiettivi

- Condurre network enumeration in ambienti Unix (NFS) e Windows (RPC, Active Directory, attacco spray).

- Eseguire l'enumerazione SNMP e sfruttarne le vulnerabilità in laboratorio (violazione di SNMPv3).
- Comprendere scenari, vettori di attacco e l'uso responsabile degli exploit pubblici.
- Padroneggiare gli attacchi a memoria: architetture, stack, meccanismo di ritorno funzione, rudimenti di assembly.
- Analizzare e sfruttare un Buffer Overflow tramite laboratori pratici (BOF, Windows Memory Exploitation).
- Comprendere le tecniche di mantenimento dell'accesso, inclusa la costruzione di un macrovirus in laboratorio.

A chi è rivolto. A chi vuole affrontare l'enumerazione avanzata di reti Windows/Unix e le tecniche di sfruttamento a livello di memoria.

Competenze richieste. Contenuti dei moduli Exploit e Offensive, con buona familiarità di reti Windows e Linux.

Programma del corso

1. **Network enumeration.** Generalità e primi passi: introduzione, ancora sull'enumerazione SMB · Enumerazione in ambito Unix: protocollo NFS, enumerazione NFS · Enumerazione in ambito Windows: enumerazione RPC e domini Microsoft, informazioni da Active Directory, dall'enumerazione all'attacco (attacco spray), considerazioni sulla disponibilità degli attacchi · Enumerazione in SNMP: introduzione, versioni del protocollo e sicurezza, forme di enumerazione possibili, Lab: violazione della sicurezza SNMPv3 e ottenimento di un accesso non autorizzato.
2. **Exploitation.** Introduzione: scenari di attacco ed exploitation, vettori di attacco, altri metodi di violazione, exploit pubblici (rischi e benefici), ricerca di un exploit, risorse online e offline · Gli attacchi a memoria: introduzione, architetture, memoria e indirizzi virtuali, memoria per un programma, lo stack, meccanismo di ritorno funzione, CPU Internals, rudimenti di assembly, strumenti, Lab: Analisi di un BOF (Buffer Overflow), Lab: analisi allo sfruttamento, Lab: Windows Memory Exploitation · Mantenimento dell'accesso e altre forme di exploit: i macrovirus, Lab: costruire un macrovirus.

EH-EPE – Extreme Privilege & Evasion

Introduzione. Porta nelle tecniche più sofisticate della sicurezza offensiva: la privilege escalation e l'evasione dalle difese. Si impara a scalare i privilegi su Windows e Linux con approcci metodici e strumenti automatizzati, e a superare i sistemi di protezione tramite tecniche avanzate di esfiltrazione, offuscamento ed evasione da firewall e antivirus. È il modulo in cui si affrontano le sfide che distinguono un professionista esperto: mantenere l'accesso e restare invisibili.

Obiettivi

- Applicare un approccio metodico alla ricerca di privilege escalation.
- Condurre privilege escalation su Windows e Linux: privilegi, rete, servizi, programmi, DLL, casi d'uso concreti.
- Utilizzare strumenti di ricerca automatizzata come linPEAS e winPEAS.
- Padroneggiare tecniche di post-exploitation ed esfiltrazione dei dati.
- Applicare tecniche di codifica e offuscamento (Base64, URI/URL Obfuscation, Unicode, omoglifi).
- Superare i sistemi di protezione: evasione da firewall e antivirus, ondisk/in-memory/network evasion, pivoting e tunneling.

A chi è rivolto. A chi vuole padroneggiare le tecniche più sofisticate di post-exploitation: scalare privilegi e restare invisibili ai sistemi di difesa.

Competenze richieste. Solida preparazione offensiva, equivalente al completamento del pacchetto Offensive.

Programma del corso

1. **Privilege escalation.** Alla ricerca del privilegio: un approccio per la ricerca di una privilege escalation · Privilege Escalation per Windows: idee, privilegi, rete, servizi, programmi, DLL, casi d'uso concreti · Privilege Escalation per

Linux: idee, privilegi, rete, servizi, programmi, DLL, casi d'uso concreti · Ricerca automatizzata: linPEAS (Linux/mac), winPEAS (Windows).

2. **Superamento delle difese.** Post-exploitation ed esfiltrazione: il problema dell'esfiltrazione · Tecniche di codifica dei dati: Base64 Encoding, URI Obfuscation, URL Hostname Obfuscation, offuscamento del codice, Unicode e UTF, Omoglifi · Protocolli per l'esfiltrazione: TCP, FTP/SSH/SCP/SFTP, HTTP POST, ICMP, DNS, Weaponization con DNS · Vincoli di traffico: evasione dai firewall (port forward, tunnel SSH, pivoting, proxychain) · Superamento dei sistemi di protezione: forme di protezione, evasione dagli antivirus, Ondisk evasion: Packer, Obfuscator, Crypters · In memory evasion: PE Injection · Network evasion: caso d'uso debole (base64), caso d'uso forte (AES) · Application Whitelisting/Blacklisting: AppLocker.

EH-EAT – Extreme Attack Techniques

Introduzione. Mette alla prova con alcune delle tecniche di attacco più avanzate e attuali del panorama offensivo. Si affrontano vulnerabilità critiche note come Log4Shell, l'attacco a dispositivi Android tramite APK trojanizzati e persino l'hacking di sistemi fisici con strumenti come il Flipper Zero. È il culmine del percorso: porta le competenze sul terreno delle sfide reali che i professionisti affrontano oggi, tra vulnerabilità zero-day, mobile security e attacchi al mondo fisico.

Obiettivi

- Comprendere e sfruttare vulnerabilità Java critiche: Log4Shell (CVE-2021-44228) e Apache Commons Text RCE (CVE-2022-42889).
- Condurre attacchi ad Android tramite APK trojanizzati: weaponization, distribuzione e sfruttamento.
- Estrarre informazioni e file da dispositivi mobili compromessi.
- Comprendere le basi della comunicazione fisica: segnali e spettro elettromagnetico.
- Utilizzare il Flipper Zero per attaccare sistemi via Infrarossi, Wi-Fi, Bluetooth, Sub-GHz, NFC/RFID e Bad USB.

A chi è rivolto. A chi vuole affrontare le tecniche di attacco più avanzate e attuali del panorama offensivo, dalle vulnerabilità Java al mobile fino ai sistemi fisici.

Competenze richieste. Solida preparazione offensiva generale; utile familiarità di base con applicazioni Java e dispositivi Android.

Programma del corso

1. **Attacco a Java.** Attaccare la CVE-2021-44228 – Log4Shell: cos'è, Log4J e i lookup, ruolo dei DNS malevoli, come funziona, ruolo dei LDAP server malevoli, strumenti di base (URL LDAP, server LDAP custom), esempi di payload, superare i WAF, un PoC completo · Attaccare la CVE-2022-42889 – Apache Commons Text RCE: string substitutions, rischi di un input non sicuro, livelli del rischio, cosa non funziona in Commons Text, casi d'uso ed esempi.
2. **Attacco ad Android.** Attacco via APK: l'ambiente Android, il sistema APK, la weaponization: tecnica di distribuzione (drive-by-download), selezione e costruzione del payload, costruzione del pacchetto APK, Trojanized-APK · L'attacco: strumenti a disposizione, navigare nel dispositivo, estrarre informazioni e file · Altre forme di sfruttamento: la clipboard di Android.
3. **Attacco ai sistemi fisici.** Introduzione alla comunicazione fisica: segnali e spettro elettromagnetico · Dispositivi di attacco e Flipper Zero: architettura, interfaccia utente · Sistemi violabili con il Flipper Zero: Infrarossi, Wi-Fi, Bluetooth, Sub-GHz (cancelli, automobili, garage), NFC e RFID, Bad USB.

Requisiti hardware e software

Per accedere al corso il Cliente deve disporre dei requisiti seguenti. La verifica è a carico del Cliente (Condizioni di Vendita, art. 4 e art. 11).

Componente	Requisito
Personal computer	Per le sessioni di teoria e pratica sono necessari PC desktop o notebook, mentre per la fruizione dei contenuti teorici è possibile utilizzare dispositivi mobile. In particolare nelle sessioni pratiche è suggerito l'uso di PC con processori 64 bit, almeno quad-core, con supporto Intel VT-x / AMD-V o tecnologia equivalente per compatibilità con ambienti di virtualizzazione locali, con minimo 8 GB di RAM (consigliati almeno 16 GB) e almeno 80 GB di spazio libero su disco per l'installazione e l'esecuzione delle macchine virtuali. Monitor con risoluzione minima consigliata di 1280 × 720 pixel. Scheda audio e cuffie o altoparlanti. Webcam e microfono qualora siano previste attività formative in modalità blended.
Software di virtualizzazione	La postazione dedicata alle sessioni pratiche dovrà consentire l'installazione e l'utilizzo di un software di virtualizzazione compatibile con le macchine virtuali messe a disposizione per le esercitazioni, o comunque suggerite nell'ambito dei laboratori quale strumento per la costruzione di un proprio insieme di strumenti. Le VM saranno distribuite in formato OVA. Per la realizzazione di VM al fine della costruzione di un proprio laboratorio è consigliato seguire l'esempio d'uso di ciascun corso al fine di rendere speculare l'esperienza nelle videolezioni con la pratica. In ambito aziendale/corporate è del tutto evidente che l'utente dovrà disporre dei permessi necessari per installare, configurare ed eseguire software e macchine virtuali sulla propria postazione o avere soddisfatti in modo alternativo i requisiti. Per garantire la piena fruibilità delle attività formative e dei laboratori, è pertanto raccomandato l'utilizzo di un PC personale sul quale l'utente disponga di privilegi amministrativi.
Browser	È necessario utilizzare una versione aggiornata e supportata di uno dei principali browser web, quali: • Google Chrome • Mozilla Firefox • Microsoft Edge • Apple Safari Il browser dovrà consentire l'esecuzione di JavaScript, l'utilizzo dei cookie, il download di file e la riproduzione di contenuti multimediali.
Connettività	Connessione Internet ad alta velocità e stabile, necessaria per lo streaming dei video e per accesso ai laboratori

Componente	Requisito
Requisiti di rete e sicurezza	La postazione e la connessione utilizzate devono consentire l'accesso ai servizi Internet necessari alla fruizione della piattaforma e allo svolgimento delle esercitazioni. Eventuali firewall, proxy, VPN, sistemi di filtraggio, DNS filtering, endpoint security o altre policy di sicurezza applicate da reti aziendali/corporate non devono impedire o limitare: • L'accesso alla piattaforma di erogazione e agli eventuali servizi esterni integrati; • Il download dei materiali didattici e delle immagini delle macchine virtuali • La riproduzione di contenuti audio/video • L'utilizzo di cookie, JavaScript e degli altri servizi web richiesti • Eventuali connessioni necessarie allo svolgimento dei laboratori pratici (VPN via UDP in porta non standard) Qualora venga utilizzata una postazione o una rete aziendale soggetta a restrizioni, l'utente dovrà verificare preventivamente la disponibilità dei permessi di installazione, virtualizzazione e accesso alla rete necessari. Per garantire la piena fruibilità delle attività formative e dei laboratori, è pertanto raccomandato l'utilizzo di un PC personale sul quale l'utente disponga di una connessione Internet non soggetta a restrizioni corporate incompatibili con le attività previste.
Lettura documenti	Software di lettura di file in formato .pdf
Audio e video	Software e dispositivi per la riproduzione di file audio e video (casse o cuffie)
Laboratori	I laboratori potranno essere fruibili attraverso: • Materiale scaricabile da sottoporre a strumenti locali (la cui installazione è a carico dell'utente), quali simulatori, analizzatori, ecc. Questi strumenti potranno essere collocati su proprio PC o in apposita VM sperimentale • Connessione Web diretta a piattaforma di simulazione/esercitazione • Connessione VPN (tramite differenti porte) ad infrastrutture virtuali remote. Gli strumenti di indagine devono essere predisposti dall'utente nel proprio PC o all'interno di VM predisposte all'esercitazione. In alcun caso viene fornito un ambiente di analisi o strumentazione di attacco attraverso le piattaforme. **ATTENZIONE**! In alcuni casi è possibile che il laboratorio trattino materiale pericoloso quale exploit o malware. È fondamentale trattare questi casi in VM isolate e protette in modo da evitare contaminazioni o incidenti alle infrastrutture estranee ai laboratori.

Il Cliente si impegna ad adeguare i propri sistemi hardware e software in caso di aggiornamenti o mutamenti della piattaforma. Fata Informatica non risponde dei difetti di fruizione dovuti al mancato possesso dei requisiti minimi di sistema.

Le tecniche mostrate nel corso vanno applicate solo in ambienti di laboratorio o su sistemi per cui si ha autorizzazione scritta.

Durata dell'iscrizione, accesso e assistenza

Voce	Dettaglio
Validità dell'iscrizione – singolo modulo	12 mesi dalla data di iscrizione
Scadenza	Terminato il periodo, l'iscrizione viene disattivata automaticamente: lezioni e test vanno completati entro la scadenza (salvo indicazioni specifiche sull'utilizzo del voucher di certificazione)
Accesso ai materiali	h24, con username e password personali, non cedibili
Area personale	Elenco dei corsi frequentati e dei materiali correlati
Credenziali	Generate automaticamente e inviate dal tutor didattico dopo l'iscrizione e il pagamento
Assistenza didattica	Sistema di ticket per domande ai docenti e allo staff, attivo per tutta la durata dell'iscrizione; e-mail di supporto supportodidattico@fatainformatica.it ; tutor AI Uppy 24/7
Reclami	Per iscritto a Fata Informatica, Via Tiburtina 912, 00156 Roma; esito comunicato entro 20 giorni lavorativi
Accesso HackMeUP	Incluso nel percorso completo; formula Blended: 1 anno dalla data di iscrizione;

Il Cliente deve svolgere personalmente le lezioni e i test. Eventuali ulteriori informazioni aggiornate sono comunicate dalla parte tecnica il primo giorno di lezione.

Prezzi e modalità di pagamento

I prezzi sono espressi in euro, IVA inclusa. Ogni opzione è acquistabile in un'unica soluzione oppure, dove indicato, a rate.

Il pagamento avviene online tramite il servizio Stripe. Fata Informatica non gestisce né memorizza i dati degli strumenti di pagamento. Eseguito il pagamento, viene emessa la fattura. Il pagamento a rate è disponibile solo ove espressamente indicato. Completata l'iscrizione e saldato il prezzo, il Cliente riceve le credenziali di accesso. Il pagamento a rate comporta una maggiorazione del 5%.

Recesso e condizioni di vendita

L'acquisto è regolato dalle Condizioni di Vendita dell'e-commerce di Fata Informatica S.r.l. (Rev. 03 del 07.10.2026), che il Cliente accetta con modalità point and click prima dell'acquisto. Il Cliente dichiara di aver letto questa Scheda del Corso prima di acquistare.

- **Recesso (consumatori).** 14 giorni dalla data di acquisto, senza motivazione e senza costi (art. 52 Codice del Consumo).
- **Perdita del recesso.** Il diritto non è più esercitabile dopo l'invio delle credenziali che danno accesso immediato alla piattaforma. Chi vuole recedere deve attendere i 14 giorni prima di ricevere le credenziali.
- **Fruizione immediata.** Il Cliente può chiedere, durante l'ordine, di accedere subito al corso, accettando di perdere il diritto di recesso (art. 59, comma 1, lett. o). Riceve conferma del contratto e ricevuta via e-mail.
- **Rimborso.** In caso di recesso valido, entro 60 giorni dall'esercizio, con riaccredito sullo stesso strumento di pagamento.
- **Diritto d'autore.** Videolezioni, slide e materiali sono di proprietà di Fata Informatica: è vietato copiarli, distribuirli o cederli. Le credenziali sono personali e non cedibili.
- Il testo completo delle Condizioni di Vendita prevale su quanto qui sintetizzato.