

Cybersecurity con sistemi GNU/Linux

Programma del corso

Andrea Fazzi



1 Presentazione

Il corso ha lo scopo di fornire una comprensione approfondita di Arch Linux, configurandolo opportunamente per utilizzarlo nel campo della sicurezza informatica e del penetration testing. Il corso copre una vasta gamma di argomenti, tra cui l'installazione di Arch Linux, l'analisi delle informazioni pubbliche e lo scanning di reti, le tecniche e le problematiche di sniffing, la sicurezza dei servizi come posta, DNS, web e SSH, l'hardening di Arch Linux, la prevenzione da tecniche di hacking comuni, e infine l'uso del bash scripting per la cybersecurity. Attraverso una combinazione di lezioni teoriche e pratiche, gli studenti avranno l'opportunità di acquisire competenze pratiche nel campo della sicurezza informatica.

2 Obiettivi

- Fornire una comprensione delle caratteristiche e dei vantaggi di Arch Linux.
- Insegnare le tecniche di raccolta di informazioni e di scanning di reti.
- Spiegare le tecniche e le problematiche di sniffing e come proteggersi.
- Fornire una comprensione della sicurezza dei servizi di posta, DNS, web e SSH.
- Insegnare come rafforzare un sistema Arch Linux attraverso l'hardening.
- Fornire una comprensione delle tecniche di hacking comuni e come prevenirle.
- Insegnare l'uso del bash scripting per automatizzare le attività di sicurezza e migliorare la cybersecurity.

3 Metodologie

Le lezioni saranno dialogiche e partecipate. Gli studenti verranno condotti verso la costruzione delle conoscenze e competenze attraverso esempi, compiti di realtà, attività di problem solving.

4 Mezzi e strumenti

Ciascuno studente avrà a disposizione un'installazione di Arch Linux GNU/Linux predisposta all'interno di una macchina virtuale.

5 Articolazione dei contenuti (40 ore)

5.1 Installazione di Arch Linux

- Caratteristiche della distribuzione: Arch Linux è una distribuzione Linux basata su Debian che è stata progettata specificamente per il penetration testing e la sicurezza informatica. Include numerose utility preinstallate per l'hacking etico, come Wireshark, Nmap, Metasploit e altre.
- Installazione su macchina laptop: l'installazione di Arch Linux su un laptop comporta il download dell'immagine ISO dal sito ufficiale, la creazione di una chiavetta USB avviabile, il boot da questa chiavetta e infine la configurazione dell'installazione. Durante l'installazione, è possibile selezionare le utility specifiche che si desidera installare.

5.2 Analisi delle Informazioni pubbliche e network scanning

- Tecniche di raccolta di informazioni: utilizzo di strumenti come Whois, Nslookup e Dig per ottenere informazioni su un dominio o un indirizzo IP.
- Utilizzo di scanner di rete: utilizzo di strumenti come Nmap per identificare i dispositivi sulla rete e le porte aperte su questi dispositivi.
- Analisi delle vulnerabilità: utilizzo di strumenti come Nessus o OpenVAS per identificare le vulnerabilità nei dispositivi e nei servizi di rete.
- Metodi di mitigazione: implementazione di patch e aggiornamenti, configurazione di firewall e IDS, utilizzo di VPN e crittografia.

5.3 Tecniche e problematiche di sniffing

- Cos'è lo sniffing e come funziona: lo sniffing è una tecnica utilizzata per intercettare e leggere il traffico di rete. Può essere fatto utilizzando strumenti come Wireshark o Tcpdump.
- Tecniche di sniffing: sniffing passivo, sniffing attivo, sniffing diretto, sniffing indiretto.
- Protezione da sniffing: utilizzo di protocolli crittografati come HTTPS e SSH, configurazione di VPN, utilizzo di firewall e IDS.

5.4 Sicurezza dei servizi: posta, dns, web, ssh

- Sicurezza del servizio di posta elettronica: configurazione di protocolli sicuri come SMTPS, POP3S e IMAPS, implementazione di SPF, DKIM e DMARC.
- Sicurezza del servizio DNS: implementazione di DNSSEC, configurazione di firewall per limitare le query DNS, monitoraggio del traffico DNS per rilevare attività sospette.

- Sicurezza del servizio web: configurazione di HTTPS, implementazione di HSTS, utilizzo di WAF, attuazione di politiche di sicurezza del contenuto.
- Sicurezza del servizio SSH: disabilitazione dell'accesso root, limitazione degli utenti che possono utilizzare SSH, configurazione di chiavi SSH, utilizzo di Fail2ban.

5.5 Hardening di Arch Linux

- Cosa significa hardening: l'hardening è il processo di rafforzamento di un sistema informatico per ridurre la sua superficie di attacco.
- Passaggi per l'hardening di un sistema Arch Linux: aggiornamento del sistema, rimozione di servizi non necessari, configurazione di firewall e IDS, implementazione di politiche di sicurezza avanzate.
- Strumenti e tecniche per l'hardening: utilizzo di strumenti come Lynis per l'hardening automatizzato, implementazione di SELinux o AppArmor, configurazione di auditd.

5.6 Prevenzione da tecniche di hacking comuni

- Tipi comuni di attacchi hacking: attacchi brute force, attacchi DDoS, phishing, SQL injection, cross-site scripting.
- Tecniche di prevenzione: utilizzo di password complesse, limitazione del numero di tentativi di login, configurazione di firewall e IDS, aggiornamento e patching del sistema e delle applicazioni, formazione degli utenti.
- Strumenti di monitoraggio e rilevamento degli attacchi: utilizzo di strumenti come Snort, Wireshark, Syslog, ELK Stack.

5.7 Bash Scripting e Cybersecurity

- Introduzione al bash scripting: cos'è lo scripting bash, perché è utile, come scrivere script bash di base.
- Utilizzo di script bash per automatizzare le attività di sicurezza: creazione di script per l'automazione di attività come il monitoraggio del sistema, la scansione di rete, l'hardening del sistema.
- Esempi di script bash utili per la cybersecurity: script per l'analisi dei log, script per l'automazione di Nmap o Wireshark, script per la generazione di report di sicurezza.
- Best practices per la scrittura di script bash sicuri: utilizzo di variabili non modificabili, controllo degli input, gestione degli errori, limitazione dei privilegi.

6 Verifiche e valutazione

Le verifiche saranno somministrate nella forma di test strutturati a risposta chiusa (4 risposte di cui solo una corretta). All'inizio del corso verrà proposto agli studenti un test per verificare le loro competenze iniziali. Al termine del corso verrà proposta una simulazione di test utile alla preparazione dell'esame conclusivo.