

Lab HP Manual

Configurazione del Laboratorio

Per procedere alla configurazione del laboratorio:

1. Estrarre dagli imballaggi il firewall, i due switch, l'access point Wi-Fi e il server di virtualizzazione.
2. Accendere e collegare i dispositivi tra loro seguendo lo schema riportato nella sezione **Collegamenti**.
3. Facoltativamente, per abilitare la connettività Internet, collegare la porta WAN del firewall a una rete esterna dotata di accesso a Internet.
4. Collegarsi alla rete Wi-Fi **Lab** utilizzando la password indicata nella sezione **Credenziali**. In alternativa, collegarsi tramite cavo Ethernet alla porta 16 dello switch **SW1**.

Rete

Il laboratorio è stato preconfigurato per utilizzare le VLAN.

Sul collegamento trunk è configurata la **VLAN 31**, che identifica la rete LAN. Per modificare la configurazione o aggiungere ulteriori VLAN, consultare la [guida ufficiale di Opnsense](#) e dello [switch TP-Link](#) relative alla configurazione delle VLAN e all'assegnazione delle porte.

La rete LAN utilizza la sottorete: **192.168.1.0/24**

Il firewall è raggiungibile all'indirizzo: **192.168.1.1**

I servizi **Unbound DNS** e **Dnsmasq** sono configurati per fornire le funzionalità DNS e DHCP.

OPNsense

Il firewall viene fornito con una licenza **OPNsense Business Edition** valida per un anno.

Al termine della licenza, per continuare a ricevere gli aggiornamenti tramite la versione Community, effettuare le seguenti operazioni dall'interfaccia web:

1. Accedere a **System > Firmware > Settings**.
2. Impostare **Release Type** su **Community**.
3. Ripristinare il valore predefinito del campo **Mirror**.
4. Rimuovere la chiave di sottoscrizione.
5. Fare clic su **Save**.
6. Aprire la sezione **Updates** e verificare la disponibilità di aggiornamenti.

Proxmox VE

Proxmox VE è installato sul server ed è un hypervisor dotato di un'interfaccia grafica di gestione accessibile tramite browser.

L'indirizzo dell'interfaccia web e le credenziali di accesso sono riportati nella sezione **Credenziali**.

Nell'ambiente è già stata caricata e configurata una macchina virtuale **Kali Linux**, contenente strumenti utili per:

- analisi di file binari;
- reverse engineering;
- estrazione e analisi di firmware;
- attività SDR, Software-Defined Radio.

Per un'introduzione al sistema e per informazioni sulla configurazione e sulla manutenzione, consultare la documentazione ufficiale di Proxmox VE:

<https://pve.proxmox.com/pve-docs/pve-admin-guide.html>

Strumenti per l'analisi radio e wireless

Il laboratorio include un **HackRF One con PortaPack H2** e un **WiFi Pineapple Pager**. Questi dispositivi sono destinati ad attività formative, ricerca, analisi dello spettro radio e verifica della sicurezza delle reti wireless.

Devono essere utilizzati esclusivamente su reti, dispositivi e frequenze per cui si dispone di un'autorizzazione esplicita, nel rispetto della normativa vigente.

HackRF One con PortaPack H2

HackRF One è un dispositivo **Software-Defined Radio**, SDR, in grado di ricevere e trasmettere segnali radio nella gamma compresa tra **1 MHz e 6 GHz**. Il dispositivo opera in modalità half-duplex e può essere utilizzato come periferica USB oppure, tramite il PortaPack H2, come strumento portatile autonomo.

Il PortaPack H2 aggiunge uno schermo, controlli fisici e la possibilità di utilizzare applicazioni SDR senza collegare HackRF One a un computer. Il dispositivo è equipaggiato con il firmware **Mayhem**.

Prima dell'utilizzo:

1. Collegare un'antenna adatta alla banda di frequenza che si intende analizzare.
2. Per utilizzare HackRF One con un computer, collegarlo tramite un cavo USB dati.
3. Per utilizzarlo dalla macchina virtuale Kali Linux, assegnare il dispositivo USB alla macchina virtuale tramite la funzione di USB passthrough di Proxmox VE.

HackRF One può essere utilizzato con strumenti come **HackRF Tools** e GNU Radio (già configurati sulla VM Kali in dotazione) e altre applicazioni SDR compatibili.

Attenzione: non collegare direttamente all'ingresso RF segnali di potenza elevata. La documentazione di HackRF One indica una potenza massima d'ingresso di **-5 dBm**; il superamento di questo valore può danneggiare permanentemente il dispositivo.

Le funzioni di trasmissione devono essere utilizzate esclusivamente all'interno delle bande e con i livelli di potenza consentiti dalla normativa applicabile. Quando possibile, effettuare le prove di trasmissione utilizzando attenuatori, carichi fittizi, cavi coassiali o ambienti schermati, evitando emissioni radio non necessarie.

WiFi Pineapple Pager

Il **WiFi Pineapple Pager** è un dispositivo portatile per l'analisi e la verifica della sicurezza delle reti Wi-Fi. Consente di eseguire attività di ricognizione wireless, acquisizione autorizzata del traffico, analisi degli access point e automazione di test tramite payload.

Il Pager utilizza, per le interfacce USB-C e Wi-Fi di management, la rete: **172.16.52.0/24**

L'indirizzo del dispositivo è: **172.16.52.1**

Verificare che questa sottorete non sia già utilizzata da altre interfacce, macchine virtuali, container o servizi presenti sul computer.

L'interfaccia web **Virtual Pager** consente di visualizzare da browser lo schermo del dispositivo, accedere a un terminale e scaricare i risultati delle attività eseguite. È raggiungibile tramite la connessione USB-C o la rete Wi-Fi di management. Per accedere usare le credenziali specificate nella sezione **Credenziali**.

Per impostazione predefinita, il firewall del Pager limita l'accesso alle interfacce amministrative SSH e Virtual Pager alle connessioni provenienti dall'interfaccia USB-C e dalla rete Wi-Fi di management. Si raccomanda di mantenere questa protezione attiva e di non esporre l'interfaccia amministrativa su reti non affidabili.

Norme di utilizzo

HackRF One e WiFi Pineapple Pager sono strumenti con funzionalità di trasmissione e analisi attiva. Il loro utilizzo deve essere limitato:

- alla rete e ai dispositivi del laboratorio;
- a sistemi di proprietà dell'utilizzatore;
- a sistemi per i quali è stata ottenuta un'autorizzazione scritta;
- a bande radio e livelli di potenza consentiti dalla normativa locale.

Non utilizzare i dispositivi per intercettare comunicazioni private, interferire con reti o servizi radio, disconnettere utenti, simulare reti di terzi o acquisire credenziali senza un'autorizzazione esplicita.

Kali Linux

Nell'ambiente Proxmox VE è già disponibile una macchina virtuale con **Kali Linux**, distribuzione GNU/Linux basata su Debian e progettata per attività di analisi della sicurezza informatica,

digital forensics, reverse engineering e verifica autorizzata di reti e sistemi.

L'indirizzo IP, il nome utente e la password della macchina virtuale sono riportati nella sezione **Credenziali**.

Avvio e accesso

Per avviare la macchina virtuale:

1. Accedere all'interfaccia web di Proxmox VE.
2. Selezionare la macchina virtuale Kali Linux dall'elenco.
3. Fare clic su **Start**.
4. Aprire la sezione **Console** per accedere all'interfaccia grafica o al terminale.

Se la macchina virtuale dispone di connettività di rete, è possibile accedervi anche tramite SSH, purché il servizio sia stato abilitato:

```
1 ssh kali@192.168.1.20
```

La macchina virtuale è collegata alla rete LAN del laboratorio tramite il bridge virtuale configurato in Proxmox VE. Verificare che riceva un indirizzo appartenente alla rete:

192.168.1.0/24

Per visualizzare la configurazione delle interfacce di rete:

```
1 ip address
```

Per verificare la raggiungibilità del firewall:

```
1 ping 192.168.1.1
```

Aggiornamento del sistema

Prima di utilizzare gli strumenti installati, si raccomanda di aggiornare l'elenco dei pacchetti e il sistema operativo:

```
1 sudo apt update
2 sudo apt full-upgrade
```

Al termine degli aggiornamenti, riavviare la macchina virtuale quando richiesto:

```
1 sudo reboot
```

Eseguire gli aggiornamenti con regolarità, soprattutto prima di attività di laboratorio che richiedono versioni recenti degli strumenti.

Strumenti preinstallati

La macchina virtuale include strumenti dedicati a diverse attività tecniche, tra cui:

- analisi di file eseguibili e binari;
- reverse engineering statico e dinamico;
- debugging;
- estrazione e analisi di firmware;
- analisi del traffico di rete;
- verifica della sicurezza di reti e applicazioni;
- digital forensics;
- utilizzo di dispositivi Software-Defined Radio;
- interazione con dispositivi USB collegati al server.

La disponibilità e la versione dei programmi possono variare in base agli aggiornamenti effettuati sul sistema.

Snapshot e ripristino

Prima di modificare configurazioni importanti, installare nuovi driver o eseguire attività che potrebbero compromettere la stabilità della macchina virtuale, creare uno snapshot tramite Proxmox VE.

Per creare uno snapshot:

1. Spegnerne o sospendere le attività in corso nella macchina virtuale.
2. Selezionare la macchina virtuale dall'interfaccia Proxmox VE.
3. Aprire la sezione **Snapshots**.
4. Fare clic su **Take Snapshot**.
5. Inserire un nome e una breve descrizione.
6. Confermare la creazione.

Gli snapshot consentono di riportare la macchina virtuale a uno stato precedente. Non devono tuttavia essere considerati un sostituto dei backup.

Collegamento dei dispositivi USB

I dispositivi USB, come HackRF One, adattatori Wi-Fi o supporti di memoria, possono essere assegnati alla macchina virtuale utilizzando la funzione di USB passthrough di Proxmox VE.

Prima di collegare un dispositivo:

1. Verificare che il dispositivo sia riconosciuto dal server Proxmox.
2. Spegnerne la macchina virtuale, quando richiesto dalla configurazione.
3. Aprire **Hardware** nelle impostazioni della macchina virtuale.
4. Selezionare **Add > USB Device**.
5. Scegliere il dispositivo corretto tramite identificativo USB o porta fisica.
6. Avviare la macchina virtuale.

All'interno di Kali Linux, verificare il riconoscimento del dispositivo con:

```
1 lsusb
```

Evitare di assegnare contemporaneamente lo stesso dispositivo USB al sistema Proxmox e a più macchine virtuali.

Accesso tramite Desktop remoto

Per semplificare la gestione e proiezione della macchina virtuale, è possibile abilitare l'accesso tramite **Remote Desktop Protocol**, RDP, installando il server `xrdp`.

Dalla console di Kali Linux eseguire:

```
1 sudo apt update
2 sudo apt install -y xorg xrdp xorgxrdp
3 sudo systemctl enable --now xrdp
```

Verificare che il servizio sia attivo con:

```
1 systemctl status xrdp
```

Individuare quindi l'indirizzo IP della macchina virtuale mediante il comando `ip address` e collegarsi utilizzando un client RDP, come **Connessione Desktop remoto** di Windows o RoyalTSX su MacOS.

Buone pratiche

Per preservare l'integrità dell'ambiente:

- utilizzare un account non amministrativo per le normali attività;
- ricorrere a `sudo` solo quando necessario;
- creare uno snapshot prima di modifiche rilevanti;
- conservare i file di analisi in directory dedicate;
- non installare pacchetti provenienti da repository non verificati;
- non disabilitare le protezioni di rete senza una motivazione documentata;
- non archiviare credenziali in chiaro all'interno della macchina virtuale;
- verificare sempre l'origine dei file analizzati.

Utilizzo autorizzato

Kali Linux deve essere utilizzato esclusivamente per attività didattiche, di ricerca e di verifica della sicurezza eseguite su sistemi appartenenti al laboratorio o per i quali è stata ottenuta un'autorizzazione esplicita.

Non utilizzare gli strumenti presenti nel sistema per accedere a reti, dispositivi, account o dati di terzi senza autorizzazione.

Con l'acquisto del laboratorio di cybersecurity viene fornito anche l'**EXPLIoT IoT Security Learning Kit**, un ambiente didattico progettato per lo studio pratico della sicurezza dei dispositivi Internet of Things, dei sistemi embedded e dei relativi protocolli di comunicazione.

Il kit comprende oltre 24 esercitazioni guidate dedicate all'analisi di interfacce hardware e protocolli quali **UART, I²C, SPI, JTAG, Zigbee e Bluetooth Low Energy**, BLE. Le attività sono descritte nel manuale di laboratorio fornito con il prodotto.

Contenuto del kit

In base alla configurazione fornita, il kit può includere:

- scheda **DIVA**, Damn Insecure and Vulnerable Application;
- dispositivo **EXPLIoT NANO**;
- **Zigbee Auditor**;
- scheda Arduino Nano;
- smartwatch Bluetooth Low Energy;
- analizzatore logico;
- adattatore per memorie flash SPI;
- multimetro portatile;
- breadboard;
- cavi USB;
- cavetti jumper maschio-maschio, maschio-femmina e femmina-femmina.

La composizione effettiva può variare in base alla versione e al lotto di fornitura. Prima dell'utilizzo, confrontare il materiale ricevuto con l'inventario incluso nella confezione.

Finalità didattiche

Il kit consente di acquisire familiarità con le principali fasi di valutazione della sicurezza di un dispositivo IoT:

- riconoscimento dei componenti elettronici;
- individuazione delle interfacce di debug e comunicazione;
- analisi dei segnali digitali;
- comunicazione tramite interfacce seriali;
- acquisizione e analisi del contenuto delle memorie;
- analisi del firmware;
- osservazione dei protocolli radio IoT;
- identificazione delle configurazioni non sicure;
- verifica e documentazione delle vulnerabilità;
- studio delle possibili misure di mitigazione.

Le schede vulnerabili presenti nel kit sono state progettate appositamente per attività formative e per consentire lo svolgimento di esercitazioni controllate.

Preparazione dell'ambiente

Prima di iniziare un'esercitazione:

1. Preparare un'area di lavoro pulita, asciutta e priva di materiali conduttivi.
2. Verificare il contenuto del kit e identificare i componenti necessari per il laboratorio.
3. Consultare il manuale EXPLIoT e seguire l'ordine delle esercitazioni indicato.
4. Spegner e scollegare i dispositivi prima di modificare i collegamenti.
5. Controllare attentamente tensione, polarità e disposizione dei pin.
6. Collegare alla macchina virtuale Kali Linux soltanto gli adattatori USB richiesti dall'attività.
7. Creare, quando opportuno, uno snapshot della macchina virtuale prima di installare driver o modificare la configurazione del sistema.

Si raccomanda di fotografare o annotare i collegamenti prima di alimentare il circuito, soprattutto durante le esercitazioni che utilizzano breadboard e cavetti jumper.

Utilizzo con Kali Linux

La macchina virtuale Kali Linux può essere utilizzata come postazione di analisi per le attività previste dal kit.

Gli adattatori USB devono essere assegnati alla macchina virtuale tramite la funzione di USB passthrough di Proxmox VE. Dopo il collegamento, verificare che siano stati rilevati correttamente:

```
1 lsusb
```

Per visualizzare le eventuali interfacce seriali disponibili:

```
1 ls -l /dev/ttyUSB* /dev/ttyACM* 2>/dev/null
```

I nomi dei dispositivi possono cambiare dopo un riavvio o dopo averli scollegati e ricollegati. Prima di avviare un'attività, verificare sempre quale interfaccia corrisponde allo strumento utilizzato.

Analisi delle interfacce hardware

Le attività sulle interfacce UART, I²C, SPI e JTAG devono essere eseguite seguendo gli schemi e le indicazioni del manuale.

Prima di collegare un adattatore:

- individuare correttamente il pin di massa, GND;
- misurare la tensione di funzionamento;
- non assumere che tutti i dispositivi utilizzino una logica a 3,3 V;

- evitare di applicare tensione ai pin di segnale;
- non cortocircuitare pin adiacenti;
- non collegare contemporaneamente più alimentazioni;
- non modificare i collegamenti mentre il circuito è alimentato.

L'analizzatore logico deve essere utilizzato principalmente per osservare i segnali. Il multimetro deve essere impiegato per verificare massa, continuità e livelli di tensione prima di effettuare ulteriori connessioni.

Analisi delle memorie e del firmware

Il kit permette di svolgere esercitazioni relative all'identificazione e all'analisi delle memorie utilizzate dai dispositivi embedded.

Prima di effettuare operazioni di lettura o scrittura:

1. Identificare con precisione il componente.
2. Consultare il relativo datasheet.
3. Verificare tensione, piedinatura e protocollo.
4. Creare una copia completa del contenuto originale.
5. Calcolare e conservare l'hash del file acquisito.
6. Lavorare su una copia del dump, mantenendo inalterato l'originale.
7. Documentare strumenti, collegamenti e parametri utilizzati.

La scrittura sulle memorie deve essere effettuata soltanto quando espressamente prevista dall'esercitazione, poiché una configurazione errata può rendere inutilizzabile la scheda.

Zigbee e Bluetooth Low Energy

Il kit include strumenti ed esercitazioni per lo studio delle comunicazioni Zigbee e BLE. Queste attività permettono di osservare il funzionamento dei protocolli IoT, analizzare dispositivi didattici e comprendere i rischi associati a configurazioni, autenticazione e protezione dei dati non adeguate.

Le analisi radio devono essere limitate ai dispositivi forniti nel kit o a sistemi per i quali è stata ottenuta un'autorizzazione esplicita. Evitare l'acquisizione, la manipolazione o l'interferenza con comunicazioni appartenenti a dispositivi esterni al laboratorio.

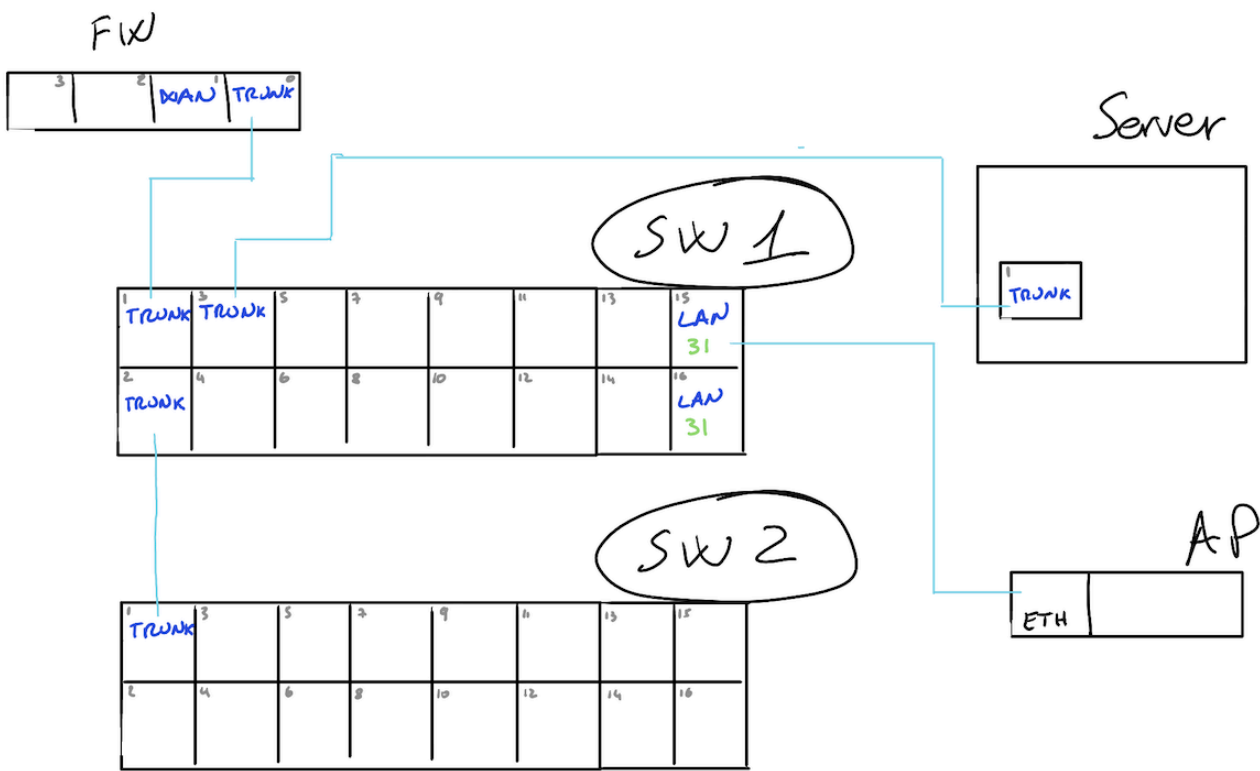
Conservazione del materiale

Al termine delle attività:

1. Spegner e scollegare tutti i dispositivi.
2. Rimuovere con cautela i cavetti dalla breadboard e dai connettori.
3. Riporre separatamente schede, adattatori e accessori.
4. Utilizzare, quando disponibili, buste o contenitori antistatici.
5. Verificare che i pin non siano piegati o danneggiati.

- 6. Aggiornare l'inventario del laboratorio.
- 7. Conservare i dump di memoria, gli screenshot e le note nelle cartelle assegnate all'esercitazione.

Collegamenti



Credenziali

Dispositivo	Modello	URL o IP	Credenziali	PIN
FW	Opnsense DEC677	https://192.168.1.1	root:LabHP2026	
SW1	TP-Link TL-SG1016PE	http://192.168.1.2	admin:LabHP2026	
SW2	TP-Link TL-SG1016PE	http://192.168.1.3	admin:LabHP2026	
AP	TP-Link TL-WA1801	http://192.168.1.4	admin:LabHP2026	
SERVER pve	HPE G11 E-2434	https://192.168.1.10:8006	root:LabHP2026	
KALI		192.168.1.20	admin:LabHP2026	
Pineapple Pager		http://172.16.52.1:1471	LabHP2026	1234

Lab WiFi

29267033