

ESERCIZI DI RIPASSO

MODULO 1

Sommario

Consegna Esercizi	2
1) Tipi di Hacker	3
White Hat	3
Black Hat.....	3
Grey Hat	3
2) Modello ISO-OSI: descrivi tutti i livelli.....	4
3) Modello TCP-IP: descrivi tutti i livelli.....	4
4) Spiega le differenze.....	5
5) Confronto sulle macchine virtuali	5
6) Confronto sugli esercizi di Cisco Packet Tracer.....	5
7) Configurazione schede di rete delle macchine virtuali	6
8) Ping di controllo.....	6
9) Ripasso Inetsim.....	6
10) Approfondimento Wireshark.....	7
11) Architettura Cisco Packet Tracer DMZ.....	8
12) Rendere Inetsim il DNS di meta collegando l'IP di Meta come DNS.....	9

Consegna Esercizi

- 1) Tipi di hacker: white hat ecc.
- 2) Modello ISO-OSI: descrivi tutti i livelli
- 3) Modello TCP-IP: descrivi i livelli
- 4) Spiega le differenze fra i modelli ISO-OSI e TCP-IP
- 5) Confronto sulle macchine virtuali (cosa è stato complicato)
- 6) Confronto sugli esercizi di Cisco Packet Tracer
- 7) Configurazione schede di rete macchine virtuali
- 8) Ping controllo se funziona e perché si fa
- 9) Ripasso Inetsim
- 10) Approfondimento Wireshark:
 - controllare se Kali Linux e Metasploitable2 comunichino tra loro con il comando del ping
 - avviare Wireshark
 - sniffare il ping tra Kali Linux e Metasploitable2 e tra Metasploitable2 e Kali Linux
- 11) Strutturare una rete sicura basata su una DMZ e una intranet dove un'utente utilizzando un app mobile di un vendor di terze parti può collegarsi al server nella DMZ che estrae i dati da dentro la intranet (schema su Cisco Packet Tracer)
- 12) Rendere Inetsim il DNS di Metasploitable2 collegando l'indirizzo IP di Metasploitable2 come DNS.

1) Tipi di Hacker

Ci sono principalmente 3 tipologie di hacker:

- white hat
- black hat
- grey hat

White Hat

Sono hacker etici e utilizzano le loro competenze per scopi legittimi e legali come aiutare le organizzazioni, le aziende e/o governi migliorando la loro sicurezza e rilevando le vulnerabilità.

Lavorano con il consenso del proprietario e non superano mai il confine legale, sono spesso tecnici e/o consulenti assunti dalle aziende per occuparsi nell'ambito della sicurezza informatica.

Black Hat

Sono hacker, chiamati anche cracker, che utilizzano le loro competenze per scopi malevoli e/o dannosi. Sfruttano le vulnerabilità e le falle di sicurezza per i loro scopi soprattutto attraverso l'utilizzo di minacce informatiche come le varie tipologie di virus informatici, attacchi informatici.

Un loro sottogruppo, i cracker, sono coloro che craccano software, inclusi i videogiochi, per rimuovere protezioni DRM o altre misure di sicurezza.

Un esempio potrebbero essere gruppi criminali che attaccano l'internet banking di una banca, sfruttando una falla di sicurezza, facendosi i bonifici a loro stessi oppure bloccare e criptare dati importanti di aziende chiedendo ingenti riscatti.

Grey Hat

Sono hacker operano in una zona intermedia tra i white hat e i black hat. Utilizzano le loro competenze di hacking anche senza autorizzazione e talvolta oltre i confini legali. Tuttavia, i loro obiettivi non sono maliziosi. Piuttosto, cercano di identificare vulnerabilità nei sistemi e spesso le segnalano ai proprietari affinché possano essere risolte. Sebbene le loro azioni possano essere considerate illegali, agiscono con l'intento di migliorare la sicurezza complessiva dei sistemi.

2) Modello ISO-OSI: descrivi tutti i livelli

- 1) **Livello Fisico:** questo livello si occupa della trasmissione dei segnali fisici che rappresentano i dati. I protocolli in questo strato definiscono come i bit vengono inviati attraverso cavi o onde radio. Esempi di protocolli includono Ethernet, IEEE 802.3 (per cavi) e IEEE 802.11 (per wireless).
- 2) **Livello di Collegamento dei Dati:** questo livello organizza i dati in "frame" per il trasporto affidabile e gestisce gli errori di trasmissione. Un esempio di protocollo a questo livello è il MAC (Media Access Control) di Ethernet, che regola l'accesso al mezzo di trasmissione.
- 3) **Livello di Rete:** questo livello determina il percorso ottimale per inviare i dati attraverso la rete. Utilizza gli indirizzi IP per identificare i dispositivi. Un esempio di protocollo a questo livello è l'IP (Internet Protocol), che gestisce l'instradamento dei pacchetti dati in rete.
- 4) **Livello di Trasporto:** questo livello assicura che i dati siano trasmessi senza errori e in ordine. Suddivide i dati in pacchetti e si occupa del loro trasporto. Un esempio di protocollo a questo livello è il TCP (Transmission Control Protocol), che garantisce la consegna affidabile dei dati e il controllo del flusso.
- 5) **Livello di Sessione:** questo livello gestisce le sessioni di comunicazione tra i dispositivi, stabilendo, mantenendo e terminando le connessioni.
- 6) **Livello di Presentazione:** questo livello traduce i dati nel formato appropriato per le applicazioni. Si occupa anche della crittografia dei dati per la sicurezza e della compressione per ridurre la dimensione dei dati. Un esempio di protocollo a questo livello è SSL/TLS (Secure Sockets Layer/Transport Layer Security) per la crittografia dei dati.
- 7) **Livello Applicativo:** questo è il livello più alto del modello OSI, dove le applicazioni interagiscono direttamente con gli utenti. Fornisce servizi di rete come la navigazione web, il trasferimento di file e la posta elettronica. Esempi di protocolli a questo livello includono HTTP per il web, FTP (File Transfer Protocol) per il trasferimento di file e SMTP (Simple Mail Transfer Protocol) per la posta elettronica.

3) Modello TCP-IP: descrivi tutti i livelli

- 1) **Accesso alla rete:** si occupa di come i dispositivi fisici (come computer e dispositivi di rete) si collegano fisicamente alla rete. Include l'hardware e i protocolli necessari per trasmettere i dati attraverso il mezzo fisico, come cavi Ethernet o connessioni wireless. Esempi di protocolli a questo livello sono Ethernet e Wi-Fi (IEEE 802.11).
- 2) **Internet:** gestisce il routing dei pacchetti di dati attraverso la rete. Il protocollo principale utilizzato è l'IP (Internet Protocol), che assegna un indirizzo univoco a ciascun dispositivo connesso a Internet e decide il percorso ottimale per inviare i dati da un dispositivo all'altro tramite nodi intermedi (router). L'IP è responsabile dell'instradamento dei pacchetti da sorgente a destinazione.
- 3) **Trasporto:** fornisce un trasporto affidabile dei dati tra due dispositivi che comunicano tra loro. Due dei protocolli più comuni a questo livello sono TCP (Transmission Control Protocol) e UDP (User Datagram Protocol): TCP è affidabile e garantisce che i dati vengano ricevuti nell'ordine corretto senza errori. Gestisce anche la ritrasmissione dei pacchetti in caso di perdita. UDP è meno affidabile ma più veloce, ideale per applicazioni che richiedono una comunicazione rapida come lo streaming video o le chiamate VoIP.
- 4) **Applicazione:** è il livello più alto del modello TCP/IP, dove le applicazioni interagiscono direttamente con l'utente. Fornisce servizi specifici come il recupero delle pagine web (HTTP), il trasferimento di file (FTP), la posta elettronica (SMTP), la navigazione sicura (HTTPS), e molti altri. Questi protocolli permettono agli utenti di utilizzare le risorse di rete per scopi diversi in modo trasparente e affidabile.

4) Spiega le differenze

La principale distinzione tra i due modelli risiede nel fatto che nel modello TCP/IP, ciascuno dei suoi livelli combina le funzioni di più strati nel modello OSI/ISO. Ad esempio, il livello Applicazione del TCP/IP integra le funzioni di Applicazione, Presentazione e Sessione del modello OSI/ISO, mentre il livello Accesso alla Rete del TCP/IP gestisce le funzioni di Collegamento e Fisico del modello OSI/ISO. Questa integrazione rende il modello TCP/IP meno articolato e più pragmatico, facilitando l'implementazione e la gestione delle reti in ambienti reali.

Appunto il modello ISO-OSI è teorico standardizzato ISO, utilizzato per una migliore comprensione mentre TCP/IP è più pratico quindi ampiamente utilizzato.

5) Confronto sulle macchine virtuali

Personalmente non ci sono state difficoltà nella installazione e configurazione delle macchine virtuali. La più grande sfida è trovare il pacchetto di installazione corretto e/o aggiornato come nel caso di Windows 7 perché è sempre meglio cercarselo con cura, siccome il link consigliato era molto spesso poco disponibile, si è dovuto cercare altre vie per scaricare l'iso ufficiale. Inoltre Windows siccome è un sistema operativo proprietario ha è limitato a 30 giorni di prova se non si inserisce la product key. In questo caso si potrebbero usare metodi legali, siccome siamo hacker etici, come il reset del contatore per estendere il periodo di prova come suggerito dalle guide ufficiali.

6) Confronto sugli esercizi di Cisco Packet Tracer

Abbiamo eseguito vari esercizi:

- a) il primo è stato configurare e mettere in comunicazione due dispositivi di due reti diverse attraverso un router;
- b) al seconda un pochino più complessa è stato configurare le varie tipologie di server e farli funzionare correttamente (DHCP, DNS e HTTP);

Da questi esercizi, possiamo apprezzare l'importanza e il funzionamento della rete, con particolare attenzione al ruolo cruciale di Internet nel nostro quotidiano. Digitando semplicemente www.epicode.com nel nostro browser, il nostro dispositivo utilizza i diversi strati dei modelli TCP/IP e OSI/ISO per connettersi. Innanzitutto, si stabilisce una connessione con il server DHCP, che assegna un indirizzo IP al nostro dispositivo. Successivamente, il dispositivo si collega a un server DNS, che può essere locale, fornito dal provider di rete o personalizzato (come CloudFlare o Google), per tradurre il nome di dominio [epicode.com](http://www.epicode.com) nell'indirizzo IP 35.207.141.200 (IPv4). Attraverso il protocollo HTTP, il server invia al nostro dispositivo la memoria salvata del contenuto del sito in formato HTML, consentendoci di visualizzare l'interfaccia utente, ovvero la homepage del sito.

7) Configurazione schede di rete delle macchine virtuali

Per creare il laboratorio virtuale con i dispositivi sulla stessa rete, prima di avviare le macchine, si imposta la scheda di rete su VirtualBox su "rete interna"

Per configurare la scheda di rete in IP statico è abbastanza semplice per i tre O.S. che abbiamo affrontato.

Per quanto riguarda Kali Linux e Metasploitable2 sono entrambi sistemi Linux e quindi si configurano allo stesso modo:

- A. aprire il terminale (su Kali siamo già sul terminale) e avviare il comando per configurare l'interfaccia network "sudo nano /etc/network/interfaces"
- B. configurare in ip statico quindi, cancellare DHCP e scrivere static
- C. inserire address **192.168.50.100/24** e gateway **192.168.50.1** (dipende seconda della configurazione)
- D. salvare la configurazione con CTRL+O invio
- E. riavviare con "sudo reboot"
- F. verificare la configurazione con il comando "ifconfig" e pingare le altre macchine.

Per quanto riguarda Windows 7 è ancora più semplice, andando in pannello di controllo, reti e scheda di rete, sulla scheda di rete utilizzata su IPV4 aprendo c'è proprio la finestra per inserire tutti i dati opportuni della configurazione.

8) Ping di controllo

Il ping di controllo è necessario per verificare se ci sia o meno il collegamento tra il dispositivo sulla quale stiamo lanciando il comando e sul dispositivo ricevente.

Per avviarlo basta scrivere su terminale "PING" + indirizzo ip o dominio del ricevente e si otterranno varie informazioni fra cui la mancata connessione oppure in caso di successo il tempo di risposta, eventuali pacchetti persi ecc...

9) Ripasso Inetsim

InetSim è uno strumento progettato per simulare vari servizi di rete e protocolli su un sistema locale. Nel nostro caso abbiamo visto insieme come configurarlo per simulare una pagina web. Utilizzando i vari comandi come "sudo nano /etc/inetsim/inetsim.conf" per entrare nell'interfaccia di configurazione e per avviarlo, una volta terminato la configurazione "sudo inetsim".

10) Approfondimento Wireshark

- Controllare se Kali Linux e Metasploitable2 comunichino tra loro con il comando ping

```
kali@kali:~$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.845 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.57 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.717 ms
^C
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.717/1.050/1.567/0.324 ms
kali@kali:~$
```

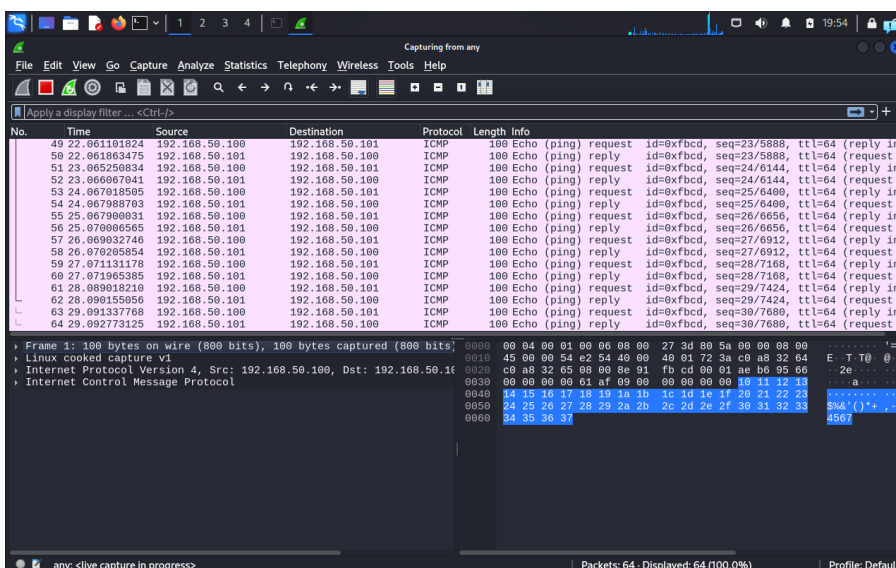
```
Last login: Mon Jul 15 14:34:03 EDT 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

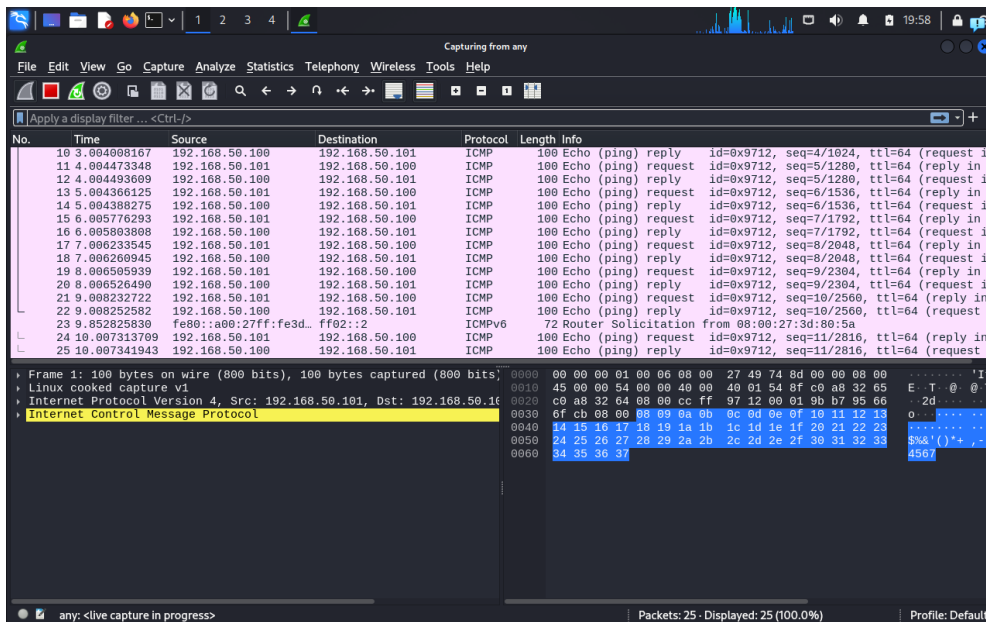
The programs included with the Ubuntu system are free software:
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=4.24 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.924 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.841 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.00 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.954 ms
--- 192.168.50.100 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.841/1.593/4.240/1.324 ms
msfadmin@metasploitable:~$
```

- Avviare Wireshark
- Sniffare il Ping tra Kali Linux e Metasploitable2 e tra Metasploitable2 e Kali Linux

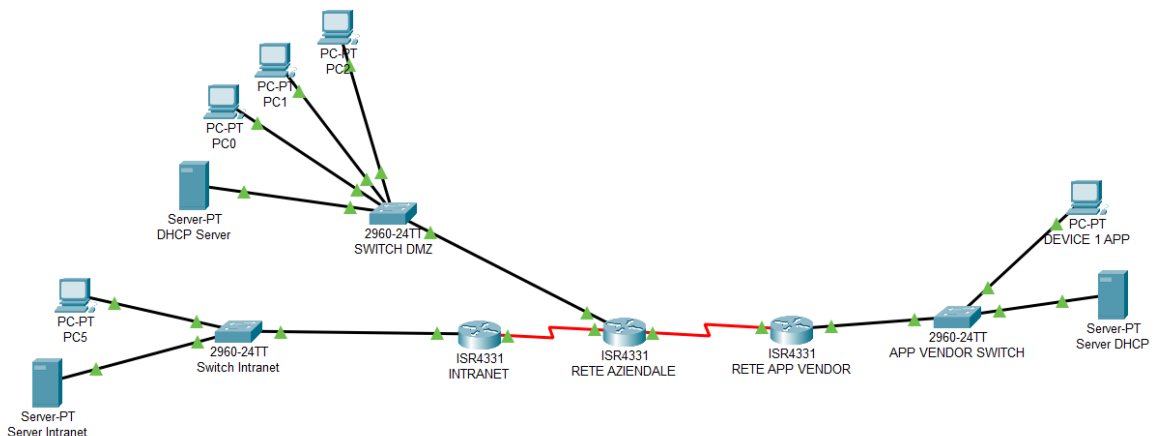




Da Meta a Kali

11) Architettura Cisco Packet Tracer DMZ

Strutturare una rete sicura basata su una DMZ e una intranet dove un'utente utilizzando un app mobile di un Vendor di terze parti può collegarsi al server nella DMZ che estrae i dati da dentro la intranet.



Questa configurazione ha Intranet che non comunica con la rete dell'app Vendor, ma solo con la rete aziendale sulla quale è collegata la DMZ. Infatti se l'App Vendor manda una richiesta passa prima per la rete aziendale DMZ e poi questa preleverà le risorse dall'intranet.

12) Rendere Inetsim il DNS di meta collegando l'IP di Meta come DNS

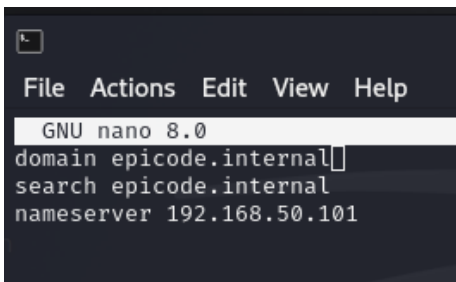
Interpretazione della consegna:

Configura Inetsim come server DNS: Assicurati che Inetsim sia configurato correttamente per agire come un server DNS. Inetsim è uno strumento che può emulare vari servizi di rete, inclusi DNS.

Collega l'IP di Meta come DNS su Kali: Modifica la configurazione di rete di Kali (192.168.50.100) per utilizzare l'indirizzo IP di Meta (192.168.50.101) come server DNS predefinito. Questo significa che quando Kali ha bisogno di risolvere nomi di dominio in indirizzi IP (per esempio quando esegui ping `www.example.com`), utilizzerà Inetsim (configurato per risolvere i nomi dei domini) attraverso l'indirizzo IP di Meta.

Impostiamo 192.168.50.101 come server DNS predefinito su Kali

`"sudo nano /etc/resolv.conf"` nameserver 192.168.50.101 CTRL+O + Invio



```
File Actions Edit View Help
GNU nano 8.0
domain epicode.internal
search epicode.internal
nameserver 192.168.50.101
```

Configuriamo inetsim con `"sudo nano /etc/inetsim/inetsim.conf"` attiviamo o immettiamo i seguenti comandi:

Default: none

`start_service dns+http+https`

`service_bind_address 192.168.50.100`

`service_dns yes`

`dns_default_ip 192.168.50.100`

CTRL+O invio e CTRL+X

`"sudo inetsim"` per avviare.

```
└─$ sudo nano /etc/inetsim/inetsim.conf
(kali@kali)~$ sudo inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Using log directory:      /var/log/inetsim/
Using data directory:    /var/lib/inetsim/
Using report directory:  /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Warning: Unknown option 'Default:' in configuration file '/etc/inetsim/inetsim.conf' line 19
Warning: Unknown option 'service_dns' in configuration file '/etc/inetsim/inetsim.conf' line 196
Configuration file parsed successfully.
== INetSim main process started (PID 14242) ==
Session ID:      14242
Listening on:    192.168.50.100
Real Date/Time:  2024-07-18 04:17:02
Fake Date/Time:  2024-07-18 04:17:02 (Delta: 0 seconds)
Forking services...
  * dns_53_tcp_udp - started (PID 14244)
deprecatd method; prefer start_server() at /usr/share/perl5/INetSim/DNS.pm line 69.
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/perl5/INetSim/DNS.pm line 69.
  * http_80_tcp - started (PID 14245)
  * https_443_tcp - started (PID 14246)
done.
Simulation running.
```

Apriamo la pagina web di inetsim a <http://192.168.50.100> e ricarichiamo la pagina verificandolo con Wireshark

