Sicurezza dei sistemi e delle reti - Laboratorio

Matteo Celardo

Primo semestre A.A. 2023/2024

Indice

Capitolo 1

Squalo dei cavi

1.1 note utili

- premendo tasto destro su un pacchetto, è possibile selezionare la voce *segui* e vedere il flusso di pachetti che riguarda quello selezionato
- nei filtri di surf shark, è possibile scrivere *frame matches "str"* per vedere solo i frame che contengono la string *str* al loro interno

1.2 appello 13/7/23

1. (a) *domanda: quali sono i nodi coinvolti? quali sono i MAC dei dispositivi coinvolti?*
   cliccando su una riga, si vede in basso a sinistra IP e MAC di ogni host coinvolto (la seconda riga ha i MAC tra parentesi, mentre la terza ha gli IP)
   - 192.168.0.20 - MAC: 00:1f:3c:4f:30:1d
   - 91.203.99.45 - MAC: 00:18:4d:b0:d6:8c
   - 209.85.227.139 - MAC: 00:18:4d:b0:d6:8c
   - 86.59.84.66 - MAC: 00:18:4d:b0:d6:8c
   - 66.102.9.147 - MAC: 00:18:4d:b0:d6:8c
   - 209.85.229.154 - MAC: 00:18:4d:b0:d6:8c

   (b) *domanda: Quali sono le caratteristiche dei diversi nodi coinvolti?*
   supponiamo che voglia sapere cose come sistema operativo, browser, scheda di rete, inforazioni relative al MAC, chi è client e chi è server
   - *host 192.168.0.20*:
     - è un client
     - ha una scheda di rete intel → si ricava da un qualunque pacchetto in uscita vedendo il campo *ethernet II* (campo sorgente o destinazione in base a quello che si vuole vedere)
     - per le richieste http usa un browser opera (v 9.80) su sistema operativo windows (v 6.0) → si ricava prendendo una richiesta http e andando nella tendina *hyper text transer protocol* (campo *user-agent*)
   - *host 91.203.99.45*:
     - è un server
     - il router ha una shceda di rete netgear
     - il web server usa apache → sempre nella tendina dell'HTTP, campo *server*
   - *host 209.85.227.139*:
     - è un server
     - il router ha una shceda di rete netgear

  - server GFE
- ... (risposta analoga per gli altri server)

siccome tutti i server hanno lo stesso MAC address, si può ipotizzare che siano tutti gestiti dallo stesso ente

(c) *domanda: Quando è avvenuta la prima connessione TCP (giorno/mese e anno).*
supponendo che con connessione intenda il completamento di una connessione TCP (three way handshake), bisogna cercare il primo segmento che ha flag ACK settato.
nel nostro esercizio, questa condizione è soddisfatta dal segmento 9 (impostando il filtro sul TCP): 3/1/2010 CET, 2/1/2010 UTC

2. (a) *domanda: quali sono le pagine richieste al server.*
le richieste di pagine si possono osservare filtrando per protocollo HTTP e osservando il contenuto delle risposte. nel caso sia presente, come sottotendina di HTTP, una tendina contente HTML, verosimilmente quella è una pagina.

(b) *domanda: quali sono alcuni dei pacchetti che contengono le richieste HTTP e le relative risposte.*
supponendo che voglia sapere la risposta che corrisponde ad ogni richiesta di GET: basta cliccare su una qualunque riga HTTTP → su una appare una freccia verso destra (indica che quella riga è una richiesta HTTP) e sull'altra una freccia verso sinistra (indica che quella è la rispota)

- la risposta al segmento 15 è il segmento 22
- la risposta al segmento 16 è il segmento 21
- la risposta al segmento 17 è il segmento 24
- ...

(c) *domanda: nella funzione javascript debug(str), di che colore viene settato il background?*
per rispondere a questa domanda, bisogna basarsi sul fatto che js viene usato nelle pagine html → cerco solo segmenti che contengono http.
detto qeusto, si cerca nel campo info qualcosa che abbia a che vedere con js (nel nostro caso, segmento 45) e si trova il segmento che contiene la risposta.
nella tendina *line-based text data*, bisogna leggere quello che c'è scritto e trovare la funzione js richiesta.

nel nostro caso, la risposta è nel segmento 112 e il colore impostato è "yellow"

1.3 appello 29/05/2020

1. ...

2. (a) *domanda: Il cifrario proposto dal Server.*
la proposta la troviamo nel pacchetto contenente il *server hello*. bisogna guardare tendina TLS>tendina handshake protocol: server hello>contenuto del campo *cipher suite*.
in questo caso, il server propone *TLS_RSA_WITH_3DES_EDE_CBC_SHA* (o una frase che spieghi la stringa appena trovata. **chiedere al professore**)

(b) *domanda: Quali sono le caratteristiche e il contenuto del certificato?*
sempre nel pacchetto con il *server hello*, bisogna andare in tendina TLS >handshake protocol: certificate>certificates>certificate>cercare nelle voci (anche nelle tendine) il campo *signedCertificate* per sapere quale algoritmo è stato usato per la firma. sempre nello stesso percorso, cercare il campo *subject* per sapere a chi corrisponda quel certificato (aprire la tendina e andare nel campo che contiene l'espressione *id-at-organizationName=...*).
per quanto riguarda l'ente che verifica la firma, bisogna seguire il flusso TCP del pacchetto con il *server hello* e scorrere il testo nell'interfaccia che si apre. da qualche parte viene nominato il server CA che verifica la firma.

nel nostro caso:

- il server che autentica la firma è www.verisign.com/rpa
- il certificato è firmato con sha1 con crittografia RSA
- il certificato è di paypal

(c) *domanda: Quando finisce la fase di hasndshake e la connessione SSL (indicare numero del pacchetto).*
la comunicazione SSL termina col pacchetto 18 → è un alert con codice che inizia per due (errore fatale cha causa la chiusura della connessione. da TLS 1.3 tutti gli alert sono considerati fatali).
per quel che riguarda l'handshake, bisogna chiedere se intenda quello TCP o quello di TLS:

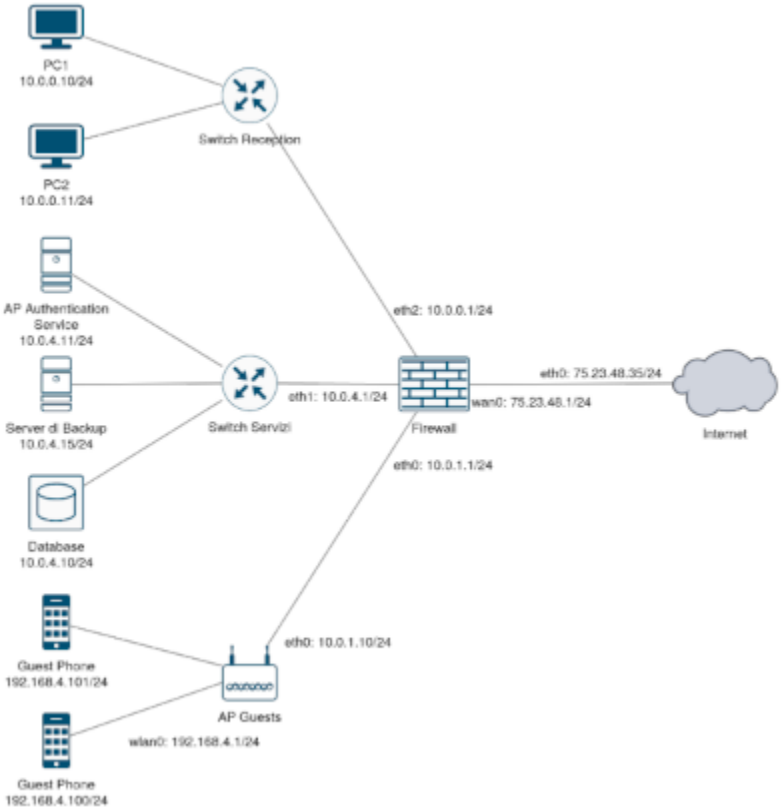
- *per TLS*: l'handshake termina con la decisione del protocollo di crittografia da usare e quindi col pacchetto 11 (ovvero la risposta del server al *change cipher spec* mandato dal client).
- *per TCP*: cercare il pacchetto ACK relativo alla connessione TLS → seguire il flusso TCP della connessione e trovarlo.
  in questo caso, è il numero 3

data la domanda, suppondo volesse l'handshake di SSL/TLS

Capitolo 2

muro di fuoco

2.1 appello 13/7/2023



traccia:

- *La sottorete della reception contiene i nodi PC1 e PC2*
- *La sottorete dei servizi contiene un server di backup (HTTPS e TCP 445), un servizio di autenticazione degli AP (HTTPS) e un database (TCP 5432)*

soluzione con iptables (supponendo che siano sul firewall):

```
1    // domanda: La sottorete reception puo' accedere al server di backup e al
     servizio di autenticazione
```

```
2
3 //permetto in ingresso le connessioni dalla reception al server di
    autenticazione e al server di backup (HTTPS)
4 iptables -t filter -A FORWARD -p tcp -s 10.0.0.0/24 --dport 443 -d 10.0.4.11,
    10.0.4.15 -m state --state NEW,ESTABLISHED -j ACCEPT
5 //permetto le risposte da parte del server di autenticazione e di backup (
    HTTPS)
6 iptables -t filter -A FORWARD -p tcp -s 10.0.4.11, 10.0.4.15 --sport 443 -d
    10.0.0.0/24 -m state --state ESTABLISHED -j ACCEPT
7
8 //permetto in ingresso le connessioni dalla reception al server di backup (TCP
     445)
9 iptables -t filter -A FORWARD -p tcp -s 10.0.0.0/24 --dport 445 -d 10.0.4.15 -
    m state --state NEW,ESTABLISHED -j ACCEPT
10 //permetto le risposte da parte del server di backup (TCP 445)
11 iptables -t filter -A FORWARD -p tcp -s 10.0.4.15 --sport 445 -d 10.0.0.0/24 -
    m state --state ESTABLISHED -j ACCEPT
12
13     //domanda: L'AP WiFi comunica con il servizio di autenticazione per
    registrare gli accessi
14
15 //permetto all'AP di comunicare con il server auth
16 iptables -t filter -A FORWARD -p tcp -s 10.0.1.10 -d 10.0.4.11 --dport 443 -m
    state --state NEW,ESTABLISHED -j ACCEPT
17 //permetto le risposte del server all'AP
18 iptables -t filter -A FORWARD -p tcp -s 10.0.4.11 -sport 443 -d 10.0.1.10 -m
    state --state ESTABLISHED -j ACCEPT
19
20
21     //scarto tutto il resto
22 iptables -t filter -P FORWARD DROP
```

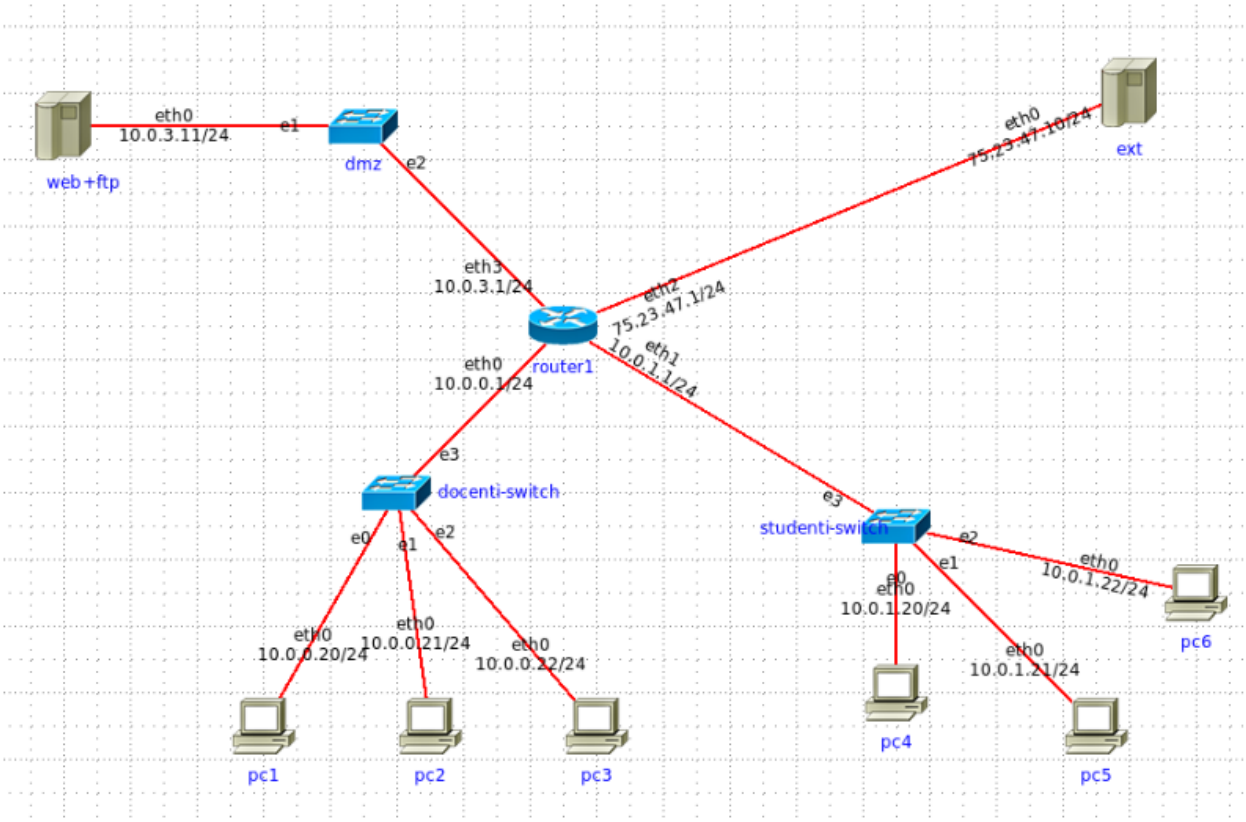
eventaulmente, domandare se con *AP wifi in modalità bridge* intende anche la possibilità di comunicare su internet.

soluzione con ACL: (ipotizziamo di usare un'acl per il traffico in entrata sui server e una per il traffico in uscita dai server)

```
1     // domanda: La sottorete reception puo' accedere al server di backup e al
    servizio di autenticazione
2
3 //permetto in ingresso le connessioni dalla reception al server di
    autenticazione e al server di backup
4 access-list 110 permit tcp 10.0.0.0 0.0.0.255 host 10.0.4.11 eq 443 //https
5 access-list 110 permit tcp 10.0.0.0 0.0.0.255 host 10.0.4.15 eq 443 //https
6 access-list 110 permit tcp 10.0.0.0 0.0.0.255 host 10.0.4.15 eq 445 //tcp 445
7
8 //permetto le risposte da parte del server di autenticazione e di backup
9 access-list 111 permit tcp host 10.0.4.11 eq 443 10.0.0.0 0.0.0.255
    established //https
10 access-list 111 permit tcp host 10.0.4.15 eq 443 10.0.0.0 0.0.0.255
    established //https
11 access-list 111 permit tcp host 10.0.4.15 eq 445 10.0.0.0 0.0.0.255
    established //tcp 445
12
```

```
13      //domanda: L'AP WiFi comunica con il servizio di autenticazione per
        registrare gli accessi
14
15 //permetto all'AP di comunicare con il server auth
16 access-list 112 permit tcp host 10.0.1.10 host 10.0.4.11 eq 443
17 //permetto le risposte del server all'AP
18 access-list 113 permit tcp host 10.0.4.11 eq 443 host 10.0.1.10 established
19
20      //scarto tutto quanto il resto
21 access-list 110 deny tcp any any
22 access-list 111 deny tcp any any
23 access-list 112 deny tcp any any
24 access-list 113 deny tcp any any
25
26      //nel caso in cui vada anche impostata l'ACL nell'interfaccia del firewall
        :
27 //impostiamo la rete con AP
28 interface eth0
29 ip access-group 112 out
30 ip access-group 113 in
31
32 //impostiamo la rete con server
33 interface eth1
34 ip access-group 111 out
35 ip access-group 113 out
36 ip access-group 110 in
37 ip access-group 112 in
38
39 //impostiamo la rete della reception
40 interface eth2
41 ip access-group 110 out
42 ip access-group 111 in
```

2.2 appello 23/6/23



traccia:

- *il router fornisce connettività a internet*
- *è presente una DMZ con server web e mail*
  - *il portale interno studenti è attivo su porta 8000*
  - *il sito web pubblico è attivo solo su https*
- abbiamo poi una rete docenti e una studenti

```
1     //domanda: Solo i docenti possono inviare e ricevere email (definire quali
      protocolli di posta si usano)
2     //(si suppongano usati POP3 per la ricezione e SMTP per l'invio)
3
4 //permetto ai docenti di inviare richieste al server mail (SMTP (25) e POP3
      (110))
5 iptables -t filter -A FORWARD -p tcp -s 10.0.0.0/24 -d 10.0.3.11 -m multiport
      --dports 25,110 -m state --state NEW,ESTABLISHED -j ACCEPT
6 //permetto al server mail di rispondere alle richeiste dei docenti
7 iptables -t filter -A FORWARD -p tcp -s 10.0.3.11 -m multiport --sports 25,110
      -d 10.0.0.0/24 -m state --state ESTABLISHED -j ACCEPT
8
9
```

```
10      //domanda: Gli studenti possono navigare all'esterno solo su siti che
        supportano https
11
12 //permetto agli studenti di raggiungere l'esterno su https (443)
13 iptables -t filter -A FORWARD -p tcp -s 10.0.1.0/24 -d 75.23.47.10 --dport 443
       -m state --state NEW,ESTABLISHED -j ACCEPT
14 //permetto alle risposte di tornare indietro
15 iptables -t filter -A FORWARD -p tcp -s 75.23.47.10 --sport 443 -d 10.0.1.0/24
       -m state --state ESTABLISHED -j ACCEPT
16
17      //domanda: Le reti docenti e studenti non possono scambiarsi comunicazioni
18 //impedisco comunicazioni dai docenti agli studenti (omettere -p vuol dire
        ogni protocollo)
19 iptables -t filter -A FORWARD -s 10.0.0.0/24 -d 10.0.1.0/24 -j DROP
20 //impedisco comunicazioni dagli studenti ai docenti
21 iptables -t filter -A FORWARD -s 10.0.1.0/24 -d 10.0.0.0/24 -j DROP
22
23      //domanda: Solo il pc3 della rete docenti puo' connettersi in telnet alle
        macchine della dmz
24 //permetto messaggi di andata
25 iptables -t filter -A FORWARD -p tcp -s 10.0.0.22 -d 10.0.3.0/24 --dport 23 -m
       state --state NEW,ESTABLISHED -j ACCEPT
26 //permetto risposte dal server telnet
27 iptables -t filter -A FORWARD -p tcp -s 10.0.3.0/24 --sport 23 -d 10.0.0.22 -m
       state --state ESTABLISHED -j ACCEPT
28
29 //NB: ho usato l'intera rete 10.0.3.0/24 siccome la domanda parla di "macchine
        ". chiedere al professore se usare solo l'IP del server, nel caso
30
31
32      //vietiamo il resto del traffico
33 iptables -t filter -P FORWARD DROP
```

2.3 considerazioni

- domandare se, in iptables, alla richiesta *il restate traffico deve essere vietato* e simili bisogna rispondere impostando il drop come politica di base solo nelle catene usate nell'esercizio o in tutte
- porte tcp usate dai protocolli noti generalmente chiesti:
  - SMTP: porta 25
  - POP3: porta 110
  - IMAP: porta 143
  - FTP:
    - porta 21 per connessione di controllo
    - porta 20 per connessione dati nel caso di FTP attivo: il server contatta il client per sapere su che porta instaurare la connessione con lui (la porta usata dal server nella comunicazione è la 20)
    - porta >1023 per connessione dati nel caso di FTP passivo: è il client che chiede sulla connessione di controllo su quale porta debba contattare il server per la connessione dati (il server risponderà con una porta che, verosimilmente è maggiore di 1023) → si ricorda che il numero di porte è $2^{16} = 65536$, quindi *maggiore di 1023* si traduce in un range che va da 1023 a

un valore massimo di 65535 (non è necessario mettere tutto quanto il range per intero, anzi, verosimilmente è sconsigliabile aprire così tante porte).
per sintassi range di porte, vedere più avanti nell'elenco puntato

  - telnet: porta 23
  - HTTP: porta 80
  - HTTPS: porta 443

- quando in iptables si specifica *-m multiport* e si vuole mettere un **range di porte contigue**, la sintassi è *portaIniziale:portaFinale*. la separazione con le virgole usata negli esercizi sopra significa che vengono prese **solo le singole porte scritte**