



# UNIVERSITA' DEGLI STUDI DELL'AQUILA

AFFARI GENERALI DI ATENEO  
AREA GESTIONE DELLE RISORSE UMANE  
SETTORE CONCORSI E SELEZIONI

## TRACCE DELLE PROVE SCRITTE - 27.09.2021

### **Blocco B, (Polo Universitario di Roio) Piazzale E. Pontieri Montelucio di Roio – 67100 – L'Aquila in Aula B+1.1**

Concorso pubblico, per esami, per n. 12 posti di categoria D, posizione Economica D1 – Area tecnica, tecnico-scientifica ed elaborazione dati con rapporto di lavoro subordinato a tempo pieno e indeterminato di cui n. 1 posto per il profilo 2 Allegato 5 – Area Tecnica, Tecnico-Scientifica ed Elaborazione Dati con competenze informatiche - Bandito con D.D.G. n. 714/2020 - prot. n. 124863 del 2.12.2020 - pubblicato sulla G.U. n. 99 del 22.12.2020 e rettificato con D.D.G n. 543/2021 – prot. n. 69241 del 21.6.2021.

### **TRACCE DELLA PRIMA PROVA SCRITTA del 27.09.2021 ore 9.00**

#### TRACCIA 1

Il candidato illustri gli strumenti ed i protocolli principali impiegati in attività di monitoraggio di asset tecnologici quali reti, servizi digitali, infrastrutture, desktop PC. Il candidato inoltre illustri in dettaglio i protocolli di accesso ad una rete aziendale quali VPN e desktop remoto, e il relativo uso.

#### TRACCIA 2

Il candidato illustri gli strumenti ed i protocolli principali impiegati in attività di monitoraggio di asset tecnologici quali reti, servizi digitali, infrastrutture, desktop PC. Il candidato inoltre illustri in dettaglio il protocollo SNMP, la relativa architettura e le applicazioni.

#### TRACCIA 3

Il candidato illustri gli strumenti ed i protocolli principali impiegati in attività di monitoraggio di asset tecnologici quali reti, servizi digitali, infrastrutture, desktop PC. Il candidato inoltre illustri in dettaglio la suite SSL/TLS, le applicazioni e gli impatti sul monitoraggio delle infrastrutture di rete.

#### TRACCIA ESTRATTA N.3



# UNIVERSITA' DEGLI STUDI DELL'AQUILA

AFFARI GENERALI DI ATENE  
AREA GESTIONE DELLE RISORSE UMANE  
SETTORE CONCORSI E SELEZIONI

TRACCE DELLA SECONDA PROVA SCRITTA del 27.09.2021 ore 15.30

TRACCIA 1

The screenshot displays a network traffic capture in Wireshark. The main pane shows a list of packets, with packet 112 selected. The packet list pane shows the following details for packet 112:

- Frame 112 (218 bytes on wire (218 bytes captured))
- Ethernet II, Src: IBM\_10:60:199 (00:09:6b:10:60:199), Dst: All-MSRP-routers\_00 (00:00:0c:07:ac:00)
- Internet Protocol, Src: 128.238.38.162 (128.238.38.162), Dst: 216.75.194.220 (216.75.194.220)
- Transmission Control Protocol, Src Port: 2271 (2271), Dst Port: https (443), Seq: 79, Ack: 2785, Len: 204
- Secure Socket Layer
- SSLv3 Record Layer: Handshake Protocol: Client Key Exchange
- Content Type: Handshake (22)
- Version: SSL 3.0 (0x0300)
- Length: 132
- Handshake Protocol: Client Key Exchange
- Handshake Type: Client Key Exchange (16)
- Length: 128
- SSLv3 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
- Content Type: Change Cipher Spec (20)
- Version: SSL 3.0 (0x0300)
- Length: 1
- Change Cipher Spec Message
- SSLv3 Record Layer: Handshake Protocol: Encrypted Handshake Message
- Content Type: Handshake (22)
- Version: SSL 3.0 (0x0300)
- Length: 56
- Handshake Protocol: Encrypted Handshake Message

The packet bytes pane shows the raw data of the selected packet, with a hex dump and ASCII representation. The hex dump shows the following bytes: 0030 f0 1f c2 d9 00 00 18 03 00 00 84 80 00 00 80 00 19 4b 41 29 88 23 90 41 01 00 29 03 8a e7 89 38 c5 70 14 af 08 04 7c 60 1e 61 71 01 00 fb f8 38 11 20 08 c9 10 03 9c ad 1e c8 25 99 09 e5 50 b9 0040 0b 40 38 c9 10 03 9c ad 1e c8 25 99 09 00 7b 95 0070 12 38 14 c9 10 03 9c ad 1e c8 25 99 09 00 9c ad 0080 04 0e 74 00 98 7e 11 ee b5 bc 02 c4 f3 63 70 a3 0090 04 28 72 c5 3a 04 18 79 40 98 1e c4 f3 63 70 a3 00a0 03 04 09 12 76 18 74 47 78 7f 02 18 64 30 14 00c0 03 00 00 01 01 18 03 00 00 28 49 49 0c 11 3a 74 00d0 7a 41 48 15 4f 30 4b e2 df 0c 00 5b c4 44 a8 e8 00e0 44 e5 12 b9 11 f6 b3 9a de b7 22 0d 3a 17 9a 83 00f0 77 1c de ab f2 41 e7 2e ad d5 1c 5b a2 0d ab e4

Il candidato descriva lo strumento mostrato in figura discutendo in particolare:

- Gli scenari di utilizzo tipici dello strumento
- I dati riportati in generale e nel caso presentato in figura

Nello specifico il candidato risponda alle seguenti domande:

- Quale protocollo di trasporto viene utilizzato?
- Quale protocollo di sicurezza viene utilizzato?
- Il pacchetto 112 è spedito dal client o dal server?
- Quale è l'indirizzo IP e il numero di porta del server?
- Quale è l'indirizzo MAC del server?
- Assumendo che non ci sia perdita o trasmissione di messaggi, quale sarà il sequence number del prossimo segmento TCP spedito dal client?
- Quale è il significato dei messaggi di client e server Hello?
- Quanti SSL records contiene il pacchetto 112?
- Il pacchetto 112 contiene un Master Secret or un Encrypted Master Secret o nessuno dei due?



# UNIVERSITA' DEGLI STUDI DELL'AQUILA

AFFARI GENERALI DI ATENEO  
AREA GESTIONE DELLE RISORSE UMANE  
SETTORE CONCORSI E SELEZIONI

TRACCIA 2

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.31.19.54	172.31.19.73	SNMP	82	get-request 1.3.6.1.2.1.1.2.0
2	0.000673	172.31.19.73	172.31.19.54	SNMP	100	get-response 1.3.6.1.2.1.1.2.0
3	0.003623	172.31.19.54	172.31.19.73	SNMP	96	get-request 1.3.6.1.2.1.1.5.0 1.3.6.1.2.1.1.6.0
4	0.009495	172.31.19.73	172.31.19.54	SNMP	115	get-response 1.3.6.1.2.1.1.5.0 1.3.6.1.2.1.1.6.0
5	0.012212	172.31.19.54	172.31.19.73	SNMP	84	get-request 1.3.6.1.2.1.2.1.6.1
6	0.012960	172.31.19.73	172.31.19.54	SNMP	98	get-response 1.3.6.1.2.1.2.1.6.1
7	0.016247	172.31.19.54	172.31.19.73	SNMP	148	get-request 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104
8	0.022827	172.31.19.73	172.31.19.54	SNMP	165	get-response 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104
9	0.025662	172.31.19.54	172.31.19.73	SNMP	86	get-request 1.3.6.1.2.1.43.14.1.1.6.1.5
10	0.026580	172.31.19.73	172.31.19.54	SNMP	87	get-response 1.3.6.1.2.1.43.14.1.1.6.1.5

Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0  
Ethernet II, Src: Dell\_4a:33:d2 (08:12:3f:4a:33:d2), Dst: Fujixero\_15:e6:bc (08:00:37:15:e6:bc)  
Internet Protocol Version 4, Src: 172.31.19.54, Dst: 172.31.19.73  
User Datagram Protocol, Src Port: 15916, Dst Port: 161  
Source Port: 15916  
Destination Port: 161  
Length: 48  
Checksum: 0x0ca5 [unverified]  
[Checksum Status: Unverified]  
[Stream Index: 0]  
Simple Network Management Protocol  
version: version-1 (0)  
community: public  
data: get-request (0)  
get-request  
request-id: 3B  
error-status: noError (0)  
error-index: 0  
variable-bindings: 1 item  
1.3.6.1.2.1.1.2.0: Value (Null)  
Object Name: 1.3.6.1.2.1.1.2.0 (iso.3.6.1.2.1.1.2.0)  
Value (Null)

Il candidato descriva lo strumento mostrato in figura discutendo in particolare:

- Gli scenari di utilizzo tipici dello strumento
- I dati riportati in generale e nel caso presentato in figura

Nello specifico il candidato risponda alle seguenti domande:

- Quale protocollo di network management viene utilizzato?
- Cosa rappresentano i dispositivi identificati dagli indirizzi IP 172.31.19.54 e 172.31.19.73 rispetto ad un tipico sistema di network management basato sul protocollo utilizzato in figura?
- Qual è la semantica del messaggio evidenziato e identificato dal numero 1?
- Quale protocollo di trasporto viene utilizzato?
- Su quale numero di porta è in ascolto l'agente del protocollo di management?
- In generale cosa rappresenta il codice numerico (es. 1.3.6.1.2.1.1.2.0) impiegato nei messaggi get-request e come viene interpretato?

Con riferimento invece al secondo messaggio esploso nella figura che segue:



# UNIVERSITA' DEGLI STUDI DELL'AQUILA

AFFARI GENERALI DI ATENEUM  
AREA GESTIONE DELLE RISORSE UMANE  
SETTORE CONCORSI E SELEZIONI

The screenshot shows a network traffic analysis tool interface. The top part displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 2 is highlighted in blue. Below the list, a detailed view of packet 2 is shown, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Network Management Protocol (SNMP) details.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.31.19.54	172.31.19.73	SNMP	82	get-request 1.3.6.1.2.1.1.2.0
2	0.000073	172.31.19.73	172.31.19.54	SNMP	180	get-response 1.3.6.1.2.1.1.2.0
3	0.003623	172.31.19.54	172.31.19.73	SNMP	96	get-request 1.3.6.1.2.1.1.5.0 1.3.6.1.2.1.1.6.0
4	0.009495	172.31.19.73	172.31.19.54	SNMP	115	get-response 1.3.6.1.2.1.1.5.0 1.3.6.1.2.1.1.6.0
5	0.012212	172.31.19.54	172.31.19.73	SNMP	84	get-request 1.3.6.1.2.1.2.2.1.6.1
6	0.012966	172.31.19.73	172.31.19.54	SNMP	98	get-response 1.3.6.1.2.1.2.2.1.6.1
7	0.016247	172.31.19.54	172.31.19.73	SNMP	148	get-request 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104
8	0.022827	172.31.19.73	172.31.19.54	SNMP	165	get-response 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104 1.3.6.1.4.1.253.8.64.4.2.1.7.10.14130104
9	0.025662	172.31.19.54	172.31.19.73	SNMP	86	get-request 1.3.6.1.2.1.43.14.1.1.6.1.5
10	0.026500	172.31.19.73	172.31.19.54	SNMP	87	get-response 1.3.6.1.2.1.43.14.1.1.6.1.5

Frame 2: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface  
Ethernet II, Src: Fujixero\_15:e6:b3c (08:00:37:15:e6:b3c), Dst: Dell\_4a:33:d2 (00:12:3f:4a:33:d2)  
Internet Protocol Version 4, Src: 172.31.19.73, Dst: 172.31.19.54  
0100 .... = Version: 4  
.... 0101 = Header Length: 20 bytes (5)  
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
Total Length: 80  
Identification: 0x1a1b (6683)  
Flags: 0x00  
Fragment offset: 0  
Time to live: 64  
Protocol: UDP (17)  
Header checksum: 0xe1be [validation disabled]  
[Header checksum status: Unverified]  
Source: 172.31.19.73  
Destination: 172.31.19.54  
[Source GeoIP: Unknown]  
[Destination GeoIP: Unknown]  
User Datagram Protocol, Src Port: 161, Dst Port: 15916  
Simple Network Management Protocol  
version: version-1 (0)  
community: public  
data: get-response (2)  
get-response  
request-id: 38  
error-status: noError (0)  
error-index: 0  
variable-bindings: 1 item  
1.3.6.1.2.1.1.2.0: 1.3.6.1.4.1.2001.1.1.1.297.93.1.27.2.2.1 (iso.3.6.1.4.1.2001.1.1.1.297.93.1.27.2.2.1)  
Object Name: 1.3.6.1.2.1.1.2.0 (iso.3.6.1.2.1.1.2.0)  
Value (OID): 1.3.6.1.4.1.2001.1.1.1.297.93.1.27.2.2.1 (iso.3.6.1.4.1.2001.1.1.1.297.93.1.27.2.2.1)

- g) Qual è la semantica del messaggio identificato dal numero 2?
- h) Qual è il significato del campo TTL del datagram IP che trasporta il messaggio evidenziato (n.2)?
- i) Cosa indica il campo request-id: 38 del messaggio get-response evidenziato?



# UNIVERSITA' DEGLI STUDI DELL'AQUILA

AFFARI GENERALI DI ATENEO  
AREA GESTIONE DELLE RISORSE UMANE  
SETTORE CONCORSI E SELEZIONI

## TRACCIA 3

Il candidato descriva lo strumento mostrato in figura discutendo in particolare:

- Gli scenari di utilizzo tipici dello strumento
- I dati riportati in generale e nel caso presentato in Figura 1

The screenshot shows a network traffic capture in Wireshark. The main pane displays a list of 15 packets. Packet 1 is an AS-REQ message from 10.1.12.2 to 10.5.3.1, which is marked as an error. Packet 3 is an AS-REQ message from 10.1.12.2 to 10.5.3.1, which is successful. The detailed view pane shows the structure of the first packet (AS-REQ):

Field	Value
Source Port	1059
Destination Port	88
Length	299
Checksum	0xb108 [unverified]

The hex dump shows the raw data of the packet, and the ASCII dump shows the corresponding characters.

Figura 1

Nello specifico il candidato risponda alle seguenti domande:

- Qual è l'indirizzo IP del client ed il suo indirizzo MAC?
- Che tipo di protocollo di trasporto viene utilizzato?
- Qual è la porta locale che il client usa per interagire con il server?
- Qual è l'indirizzo MAC del server e l'indirizzo IP del server?
- A cosa serve il messaggio AS-REQ? La Figura 2 mostra i dettagli del messaggio AS-REQ quale è l'uso dei campi till e nonce?
- Perché il client riceve un errore quando invia la richiesta di tipo AS-REQ (messaggio 1, Figura 2) mentre la richiesta AS-REQ (messaggio 3, Figura 3) ha successo?



# UNIVERSITA' DEGLI STUDI DELL'AQUILA

AFFARI GENERALI DI ATENEO  
AREA GESTIONE DELLE RISORSE UMANE  
SETTORE CONCORSI E SELEZIONI

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.1.12.2	10.5.3.1	KRB5	333	AS-REQ
2	0.000011	10.5.3.1	10.1.12.2	KRB5	195	KRB Error: KRB5KDC_ERR_ETYPE_NOSUPP
3	0.027969	10.1.12.2	10.5.3.1	KRB5	328	AS-REQ
4	0.027977	10.5.3.1	10.1.12.2	KRB5	1298	AS-REP
5	0.036011	10.1.12.2	10.5.3.1	KRB5	1253	TGS-REQ
6	0.036018	10.5.3.1	10.1.12.2	KRB5	1231	TGS-REP
7	0.653001	10.1.12.2	10.5.3.1	KRB5	1265	TGS-REQ

```
- as-req
  pvno: 5
  msg-type: krb-as-req (10)
  - padata: 2 items
    - PA-DATA pA-ENC-TIMESTAMP
      - padata-type: pA-ENC-TIMESTAMP (2)
        - padata-value: 303da003020117a236043409a2244893aff5f384f79c37883f154a32d396a914a4d0a78e...
          etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
        > cipher: 09a2244893aff5f384f79c37883f154a32d396a914a4d0a78e979ba75d4ff53c1db72941...
      > PA-DATA pA-PAC-REQUEST
    - req-body
      Padding: 0
      > kdc-options: 40810010
      > cname
      > realm: DENYDC
      > sname
      > till: 2037-09-13 02:48:05 (UTC)
      > rtime: 2037-09-13 02:48:05 (UTC)
      > nonce: 197451134
      > etype: 7 items
```

Figura 2

Time	Source	Destination	Protocol	Length	Info	
1	0.000000	10.1.12.2	10.5.3.1	KRB5	333	AS-REQ
2	0.000011	10.5.3.1	10.1.12.2	KRB5	195	KRB Error: KRB5KDC_ERR_ETYPE_NOSUPP
3	0.027969	10.1.12.2	10.5.3.1	KRB5	328	AS-REQ
4	0.027977	10.5.3.1	10.1.12.2	KRB5	1298	AS-REP
5	0.036011	10.1.12.2	10.5.3.1	KRB5	1253	TGS-REQ
6	0.036018	10.5.3.1	10.1.12.2	KRB5	1231	TGS-REP
7	0.653001	10.1.12.2	10.5.3.1	KRB5	1265	TGS-REQ
8	0.653004	10.5.3.1	10.1.12.2	KRB5	1234	TGS-REP
9	0.729674	10.1.12.2	10.5.3.1	KRB5	1261	TGS-REQ
10	0.750863	10.5.3.1	10.1.12.2	KRB5	1247	TGS-REP

```
> Internet Protocol Version 4, Src: 10.1.12.2, Dst: 10.5.3.1
> User Datagram Protocol, Src Port: 1060, Dst Port: 88
Kerberos
  - as-req
    pvno: 5
    msg-type: krb-as-req (10)
    - padata: 2 items
      - PA-DATA pA-ENC-TIMESTAMP
        - padata-type: pA-ENC-TIMESTAMP (2)
          - padata-value: 3049a003020103a106020400a2f790a23a0438233b4272aa93727221facfdbd9a0...
            etype: eTYPE-DES-CBC-MD5 (3)
            kvno: 10680208
          > cipher: 233b4272aa93727221facfdbd9a0c43a2798c810600310c0daf48fb969c26cb47d...
        > PA-DATA pA-PAC-REQUEST
      - req-body
        Padding: 0
        > kdc-options: 40810010
        > cname
```

Figura 3