EECS 3482

Lab 3

Name : AKALPIT SHARMA

id : 212650628

Pre-lab Procedures: Environment Preparation

Kali-1 IPV4: 192.168.1.101
Kali-2 IPV4: 192.168.1.102

Default Gateway: 192.168.1.1

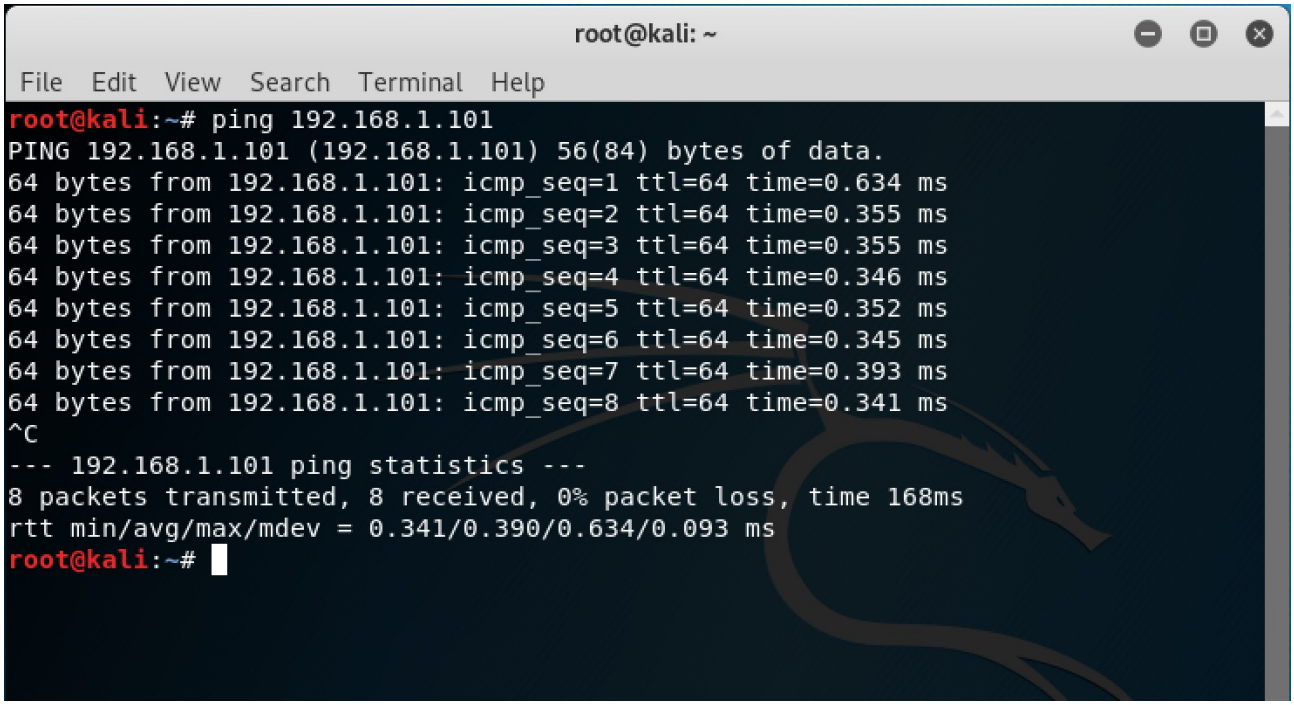
Metrics: This is used to make routing decisions. The value is 100 in both instances.

Ping output:

Kali-2 from Kali-1

```
root@kali:/# ping 192.168.1.102
PING 192.168.1.102 (192.168.1.102) 56(84) bytes of data.
64 bytes from 192.168.1.102: icmp_seq=1 ttl=64 time=0.349 ms
64 bytes from 192.168.1.102: icmp_seq=2 ttl=64 time=0.399 ms
64 bytes from 192.168.1.102: icmp_seq=3 ttl=64 time=2.84 ms
64 bytes from 192.168.1.102: icmp_seq=4 ttl=64 time=0.341 ms
64 bytes from 192.168.1.102: icmp_seq=5 ttl=64 time=0.361 ms
64 bytes from 192.168.1.102: icmp_seq=6 ttl=64 time=2.91 ms
64 bytes from 192.168.1.102: icmp_seq=7 ttl=64 time=1.25 ms
64 bytes from 192.168.1.102: icmp_seq=8 ttl=64 time=0.351 ms
64 bytes from 192.168.1.102: icmp_seq=9 ttl=64 time=0.312 ms
64 bytes from 192.168.1.102: icmp_seq=10 ttl=64 time=0.519 ms
64 bytes from 192.168.1.102: icmp_seq=11 ttl=64 time=0.750 ms
64 bytes from 192.168.1.102: icmp_seq=12 ttl=64 time=2.62 ms
^C
--- 192.168.1.102 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 169ms
rtt min/avg/max/mdev = 0.312/1.084/2.909/1.019 ms
```

Kali-1 from Kali-2



Gateway from Kali -1

```
ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.36 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=2.08 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.04 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.29 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.39 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=2.14 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=2.09 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=1.94 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=1.16 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=6.94 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=2.18 ms
^C
--- 192.168.1.1 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 21ms
rtt min/avg/max/mdev = 1.155/2.325/6.942/1.509 ms
```

Gateway from Kali-2

```
ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.36 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=2.08 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=2.04 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.29 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=1.39 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=2.14 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=2.09 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=1.94 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=1.16 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=6.94 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=2.18 ms
^C
--- 192.168.1.1 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 21ms
rtt min/avg/max/mdev = 1.155/2.325/6.942/1.509 ms
```

traceroute yorku.ca from Kali-1

```
root@kali:~# traceroute yorku.ca
traceroute to yorku.ca (130.63.236.137), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  1.975 ms  3.339 ms  3.330 ms
 2  192.168.0.1 (192.168.0.1)  4.599 ms  5.018 ms  4.838 ms
 3  192.168.10.1 (192.168.10.1)  4.724 ms  4.639 ms  4.614 ms
 4  142.168.150.1 (142.168.150.1)  63.431 ms  63.526 ms  63.302 ms
 5  173-33-166-226.rogers.com (173.33.166.226)  68.843 ms  69.033 ms  69.247 ms
 6  196.201.222.146 (196.201.222.146)  77.766 ms  117.832 ms  40.180 ms
 7  196.201.222.145 (196.201.222.145)  41.394 ms  44.297 ms  41.365 ms
 8  196.201.222.130 (196.201.222.130)  44.276 ms  41.263 ms  41.208 ms
 9  ix-ge-4-0-0.core1.n71-fujairah.as6453.net (195.219.174.42)  93.858 ms  94.066 ms  94.051 ms
10  if-xe-4-0-7-0.tcore1.wyn-marseille.as6453.net (195.219.174.129)  195.285 ms  196.229 ms  196.211 ms
11  if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  196.178 ms  196.967 ms  197.291 ms
12  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  183.797 ms  182.497 ms  182.429 ms
13  be6453.ccr31.par04.atlas.cogentco.com (130.117.15.69)  182.559 ms  182.548 ms  184.940 ms
14  be3184.ccr42.par01.atlas.cogentco.com (154.54.38.157)  185.588 ms be3183.ccr41.par01.atlas.cogentco.com
(154.54.38.65)  176.646 ms be3184.ccr42.par01.atlas.cogentco.com (154.54.38.157)  176.593 ms
15  be3684.ccr51.lhr01.atlas.cogentco.com (154.54.60.170)  190.758 ms be3685.ccr52.lhr01.atlas.cogentco.com
(154.54.60.174)  195.999 ms be3684.ccr51.lhr01.atlas.cogentco.com (154.54.60.170)  191.015 ms
16  be2391.ccr21.lpl01.atlas.cogentco.com (154.54.39.150)  201.688 ms  201.689 ms
be2491.ccr22.lpl01.atlas.cogentco.com (154.54.39.117)  201.676 ms
17  be3043.ccr22.ymq01.atlas.cogentco.com (154.54.44.166)  272.704 ms  272.602 ms
be3042.ccr21.ymq01.atlas.cogentco.com (154.54.44.162)  266.926 ms
18  be3259.ccr31.yyz02.atlas.cogentco.com (154.54.41.205)  279.517 ms  279.077 ms  279.498 ms
19  te0-0-2-0.rcr11.b011027-3.yyz02.atlas.cogentco.com (154.54.6.238)  279.487 ms  279.412 ms
te0-0-2-3.rcr11.b011027-3.yyz02.atlas.cogentco.com (154.54.6.242)  279.748 ms
20  38.104.251.82 (38.104.251.82)  281.018 ms  280.960 ms  287.491 ms
21  york-hub-ut-hub-if-re.gtanet.ca (205.211.94.18)  296.861 ms  295.096 ms  296.762 ms
22  yorku-york-hub-if-internet.gtanet.ca (205.211.95.134)  286.098 ms  286.099 ms  286.015 ms
23  core01-border.gw.yorku.ca (130.63.27.17)  296.432 ms  296.410 ms  296.384 ms
24  130.63.2.62 (130.63.2.62)  296.352 ms  296.335 ms  296.249 ms
25  * * *
26  * * *
```

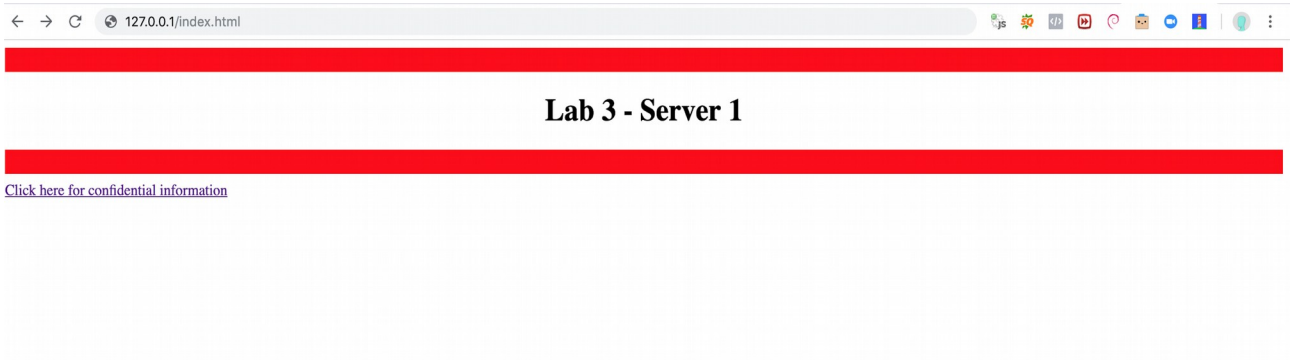
traceroute yorku.ca from Kali-2

```
root@kali:~# traceroute yorku.ca
traceroute to yorku.ca (130.63.236.137), 30 hops max, 60 byte packets
 1  _gateway (192.168.1.1)  2.989 ms  4.498 ms  5.641 ms
 2  192.168.0.1 (192.168.0.1)  5.633 ms  5.611 ms  5.483 ms
 3  192.168.10.1 (192.168.10.1)  5.331 ms  5.298 ms  5.276 ms
 4  142.168.150.1 (142.168.150.1)  31.695 ms  31.965 ms  31.784 ms
 5  173-33-166-226.rogers.com (173.33.166.226)  48.597 ms  48.549 ms  48.473 ms
 6  196.201.222.146 (196.201.222.146)  55.797 ms  76.651 ms  63.444 ms
 7  196.201.222.145 (196.201.222.145)  65.511 ms  65.438 ms  66.383 ms
 8  196.201.222.130 (196.201.222.130)  65.381 ms  66.344 ms  66.323 ms
 9  ix-ge-5-0-0.core1.n71-fujairah.as6453.net (195.219.174.44)  110.630 ms ix-ge-4-0-0.core1.n71-
fujairah.as6453.net (195.219.174.42)  111.814 ms ix-ge-5-0-0.core1.n71-fujairah.as6453.net
(195.219.174.44)  111.399 ms
10  if-xe-4-0-7-0.tcore1.wyn-marseille.as6453.net (195.219.174.129)  220.065 ms  219.945 ms
219.892 ms
11  if-ae-8-1600.tcore1.pye-paris.as6453.net (80.231.217.6)  218.048 ms  218.960 ms  219.698 ms
12  if-ae-11-2.tcore1.pvu-paris.as6453.net (80.231.153.49)  217.783 ms  252.145 ms  248.346 ms
13  be6453.ccr31.par04.atlas.cogentco.com (130.117.15.69)  248.950 ms  209.659 ms  209.556 ms
14  be3183.ccr41.par01.atlas.cogentco.com (154.54.38.65)  204.582 ms
be3184.ccr42.par01.atlas.cogentco.com (154.54.38.157)  209.933 ms
be3183.ccr41.par01.atlas.cogentco.com (154.54.38.65)  209.326 ms
15  be3684.ccr51.lhr01.atlas.cogentco.com (154.54.60.170)  225.330 ms  249.219 ms  249.139 ms
16  be2491.ccr22.lpl01.atlas.cogentco.com (154.54.39.117)  256.608 ms
be2391.ccr21.lpl01.atlas.cogentco.com (154.54.39.150)  256.173 ms
be2491.ccr22.lpl01.atlas.cogentco.com (154.54.39.117)  256.567 ms
17  be3042.ccr21.ymq01.atlas.cogentco.com (154.54.44.162)  333.123 ms
be3043.ccr22.ymq01.atlas.cogentco.com (154.54.44.166)  381.992 ms  316.035 ms
18  be3260.ccr32.yyz02.atlas.cogentco.com (154.54.42.89)  313.610 ms
be3259.ccr31.yyz02.atlas.cogentco.com (154.54.41.205)  315.944 ms
be3260.ccr32.yyz02.atlas.cogentco.com (154.54.42.89)  314.281 ms
19  te0-0-2-3.rcr11.b011027-3.yyz02.atlas.cogentco.com (154.54.6.242)  315.899 ms  315.905 ms
315.786 ms
20  38.104.251.82 (38.104.251.82)  315.716 ms  315.679 ms  362.386 ms
21  * york-hub-ut-hub-if-re.gtanet.ca (205.211.94.18)  377.857 ms  377.844 ms
22  yorku-york-hub-if-internet.gtanet.ca (205.211.95.134)  375.612 ms  375.535 ms  375.372 ms
23  core01-border.gw.yorku.ca (130.63.27.17)  285.149 ms  284.357 ms  284.923 ms
24  130.63.2.62 (130.63.2.62)  286.969 ms  285.068 ms  286.939 ms
```

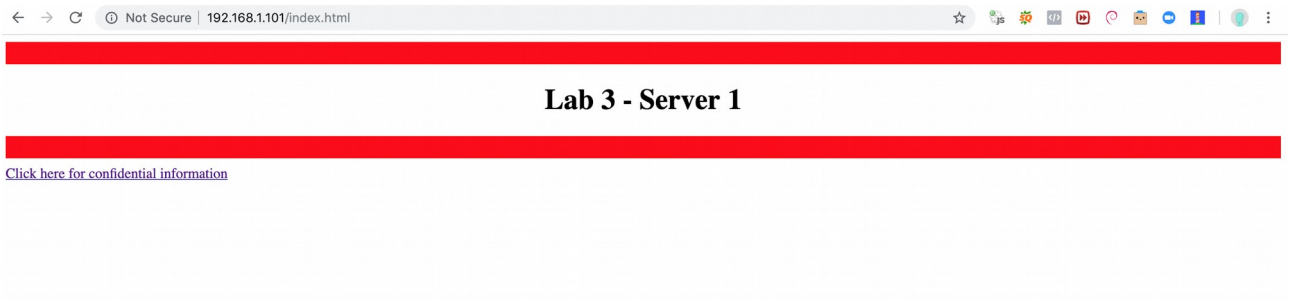
Lab 3 (P1): Apache Basic Authentication

Kali-1 Task

Access Kali-1 server using local-loop address : http://127.0.0.1/index.html



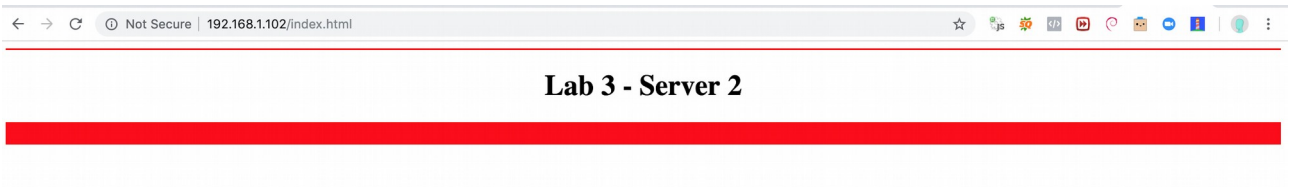
Access Kali-1 index.html from Kali-2 server using "kali-1-IPv4/index.html" : http://192.168.1.101/index.html



Kali 2 Task

Parse the page in the browser using the local-loop address: http://127.0.0.1/index.html

Parse the code on the browser of Kali-1 server using "kali-2-IPv4/index.html as the URL : http://192.168.1.102/index.html

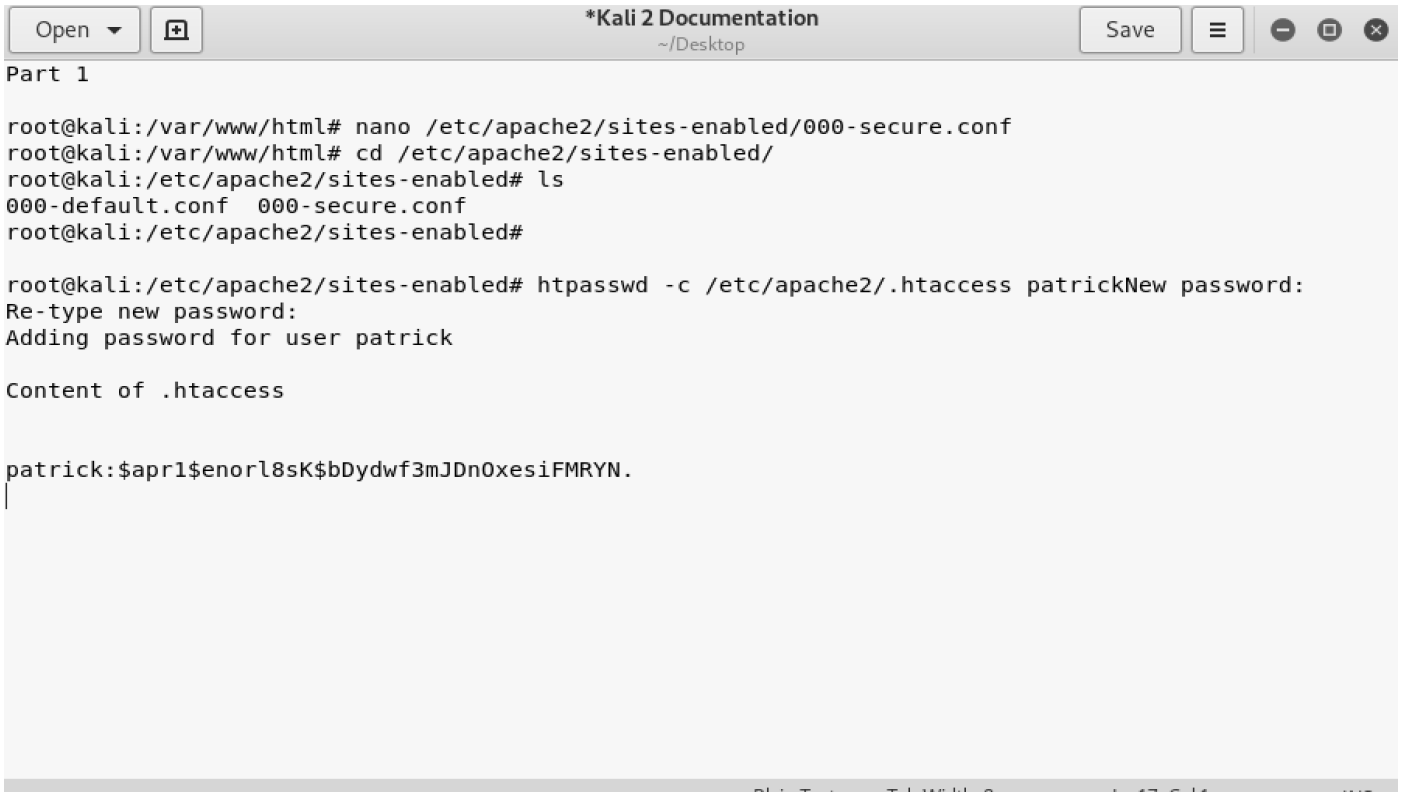


List the files stored in the directory /etc/apache2/sites-enabled

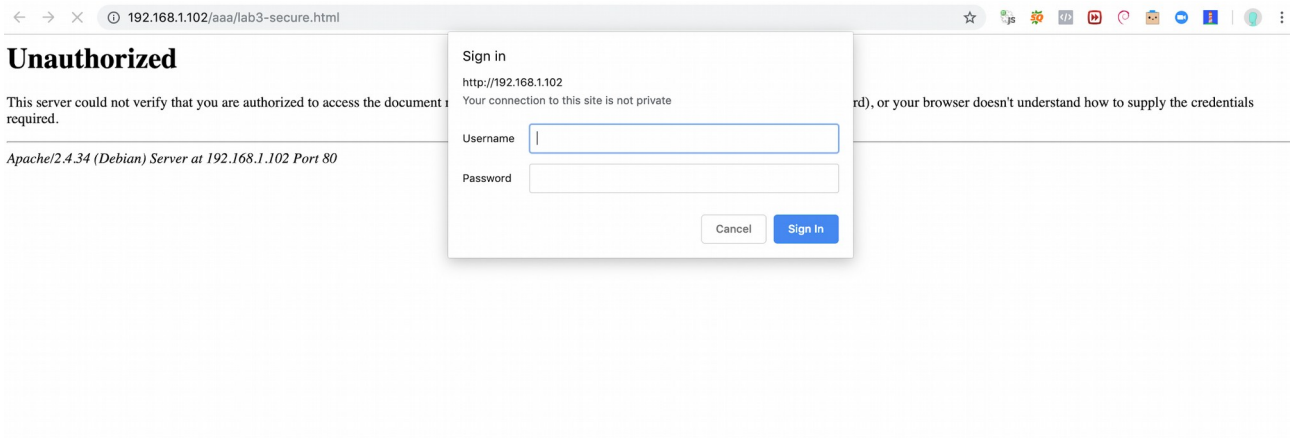
Run The command dir /etc/apache2 to list the files in the directory

```
root@kali:/etc/apache2/sites-enabled# ls
000-default.conf  001-secure.conf
root@kali:/etc/apache2/sites-enabled# htpasswd -c /etc/apache2/.htaccess patrick
New password:
Re-type new password:
Adding password for user patrick
root@kali:/etc/apache2/sites-enabled# dir /etc/apache2/
apache2.conf    conf-enabled  magic           mods-enabled  sites-available
conf-available  envvars       mods-available  ports.conf    sites-enabled
root@kali:/etc/apache2/sites-enabled#
```

Document the contents of the .htaccess file



Access server-2-IP-Address/aaa/lab3- secure.html from Kali-1: http://192.168.1.102/aaa/lab3-secure.html



Lab 3 (P2): HTTPS

openssl s_client -connect localhost:443

root@prof:/etc/apache2/sites-enabled# openssl s_client -connect localhost:443
CONNECTED(00000003)
depth=0 C = CA, ST = Ontario, L = Quebec, O = Patrick Assignments, OU = IT, CN = localhost, emailAddress = patrick@gmail.com
verify error:num=18:self signed certificate
verify return:1
depth=0 C = CA, ST = Ontario, L = Quebec, O = Patrick Assignments, OU = IT, CN = localhost, emailAddress = patrick@gmail.com
verify return:1

Certificate chain
 0 s:/C=CA/ST=Ontario/L=Quebec/O=Patrick Assignments/OU=IT/CN=localhost/emailAddress=patrick@gmail.com
   i:/C=CA/ST=Ontario/L=Quebec/O=Patrick Assignments/OU=IT/CN=localhost/emailAddress=patrick@gmail.com
---
Server certificate
-----BEGIN CERTIFICATE-----
MIID+jCCAuKgAwIBAgIJAK5hpJRoIiWDMA0GCSqGSIb3DQEBCwUAMIGRMQswCQYD
VQQGEwJDQTEQMA4GA1UECAwHT250YXJpbzEPMA0GA1UEBwwGUXVlYmVjMRwwGgYD
VQQKDBNQYXRyaWNrIEFzc2lnbm1lbnRzMQswCQYDVQQLDAJJVDESMBAGA1UEAwwJ

bG9jYWxob3N0MSAwHgYJKoZIhvcNAQkBFhFwYXRyaWNrQGdtYWlsLmNvbTAeFw0x
OTAyMjUwNzIwMjJaFw0yMDAyMjUwNzIwMjJaMIGRMQswCQYDVQQGEwJDQTEQMA4
G
A1UECAwHT250YXJpbzEPMA0GA1UEBwwGUXVlYmVjMRwwGgYDVQQKDBNQYXRya
WNr
IEFzc2lnbm1lbnRzMQswCQYDVQQLDAJJVDESMBAGA1UEAwwJbG9jYWxob3N0MSAw
HgYJKoZIhvcNAQkBFhFwYXRyaWNrQGdtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBAMc1aU7AaWpxxRiBzVCbs432h91I/SNh8XlALAhfsrhi
n736Qr6C6vyq13RCbepL/rlAdqn0bfSolUx7HQdqv/n59YFY8Z0Nnxc5uhwoAiCm
huMHKC9kALCdmkAWPodrqCnZYmiXh3dXf9WlR1Dm5TQbfur2Da+dh3dgXiviber3
2U4k1J733fnMzsPzo+WHMomxgDlvLkliD3d7x+Bino/Aa7zbJLIZCKaY+LtUE8h1
aWrsVkmNGC/4V5B0c9GJsF5Ld09WCLFts8i2xJaStTTqDPFxAaCkGfD9Ghi/Lc0m
aLwB8RQnG6MOvJ57FGxNGuzVlJ76uMdpEl57J+dm6WUCAwEAAaNTMFEwHQYDVR0O
BBYEFMNVvD22BJQhzF9gzZSVvPGrXiPIMB8GA1UdIwQYMBaAFMNVvD22BJQhzF9g
zZSVvPGrXiPIMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEBAA0d
6kb8/g/w/nAjw7I3Hnj3q8kit9xfFp3PnvS+1dmi+8JVGpA0JM0oSYurXdjIc60S
wiFDKJPGkcfdsVhxoyywoRDsKXUCpNtEwF5d32gj0B3MLbGBAawvRmyT7+rS4/HE
WgW/KMI9lwAAAu3jyarEfMoTv9MX/5ODQxbiq05qn0FK+/NlRwypqho+aGKkL1n9
pAe5B5Q/6gAIStmF+UYUzhZWONw5JQjBGvMEHoSaaXjac01phFtY6ddedgnPPHLK
q8esMJFzOm2+Ea4OIqLRzcTe+SQD586IoJ8ewM/FilfFV3vhviMVHGWulygu1GNw
G4BD1mvDPv0f4m+dpd8=
-----END CERTIFICATE-----
subject=/C=CA/ST=Ontario/L=Quebec/O=Patrick Assignments/OU=IT/CN=localhost/emailAddress=patrick@gmail.com
issuer=/C=CA/ST=Ontario/L=Quebec/O=Patrick Assignments/OU=IT/CN=localhost/emailAddress=patrick@gmail.com
---
No client certificate CA names sent
Peer signing digest: SHA256
Server Temp Key: X25519, 253 bits

SSL handshake has read 1679 bytes and written 386 bytes
Verification error: self signed certificate

New, TLSv1.2, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol : TLSv1.2
    Cipher   : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID:
3105844A4FEFD7ECA005E96E3751FD16793DA67D29AF7AB555CA647F5921775A
    Session-ID-ctx:
    Master-Key:
4194B786AE3CB281C8B714D784ED06B0171B207AEEAF6BF32C3D856748002CBA4ED9CF8
7F0E0FEEECC868C5640600E0E
    PSK identity: None
    PSK identity hint: None
    SRP username: None

TLS session ticket lifetime hint: 300 (seconds)
TLS session ticket:
0000 - 40 95 7f b3 c7 88 b1 a6-c8 73 fb f7 15 d2 d1 ae @.....s.....
0010 - 15 e9 83 ac d4 e5 ad 48-a9 10 35 6f 16 a2 85 c4 .....H..5o....
0020 - e8 15 44 8c 66 46 47 71-b4 df 90 58 a5 ad b6 75 ..D.fFGq...X...u
0030 - 54 d4 91 45 b3 51 74 50-1d 13 ed 58 a8 23 07 60 T..E.QtP...X.#.`
0040 - b1 44 64 47 bb 73 ff c8-09 b2 4f 64 62 dd 8f 30 .DdG.s....Odb..0
0050 - 0f 48 74 a2 c3 b6 06 c8-db 05 9b 7f f9 ba 4f f2 .Ht.....O.
0060 - ec 8e dd a9 b5 89 d2 29-a0 03 a7 61 9f d4 f0 f2 .....)...a....
0070 - 53 4d 1e ff 87 24 ab ba-2c 75 bc 18 2b 13 2e 99 SM...$..,u..+...
0080 - 16 24 29 08 ed c4 74 b2-dc bf 18 9d 0c dc 83 6e .$)...t.....n
0090 - 54 5d c3 e4 28 d2 5c 79-8c af a8 e1 af 1d 69 d9 T]..(.\y.....i.
00a0 - 49 f1 28 32 4c a4 0c 05-d8 7c fd d2 03 4d 0d 43 I.(2L....|...M.C
00b0 - f7 76 4d 12 57 33 da c0-01 fb c5 1b 4a d7 f4 f5 .vM.W3.....J...

Start Time: 1551082297
Timeout : 7200 (sec)
Verify return code: 18 (self signed certificate)
Extended master secret: yes
---
closed

2.2.6.a Display Cipher List

root@prof:/var/www/html/www.amazon.ca/ap# openssl ciphers
TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES256-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:DHE-RSA-AES128-SHA:RSA-PSK-AES256-GCM-SHA384:DHE-PSK-AES256-GCM-SHA384:RSA-PSK-CHACHA20-POLY1305:DHE-PSK-CHACHA20-POLY1305:ECDHE-PSK-CHACHA20-POLY1305:AES256-GCM-SHA384:PSK-AES256-GCM-SHA384:PSK-CHACHA20-POLY1305:RSA-PSK-AES128-GCM-SHA256:DHE-PSK-AES128-GCM-SHA256:AES128-GCM-SHA256:PSK-AES128-GCM-SHA256:AES256-SHA256:AES128-SHA256:ECDHE-PSK-AES256-CBC-SHA384:ECDHE-PSK-AES256-CBC-SHA:SRP-RSA-AES-256-CBC-SHA:SRP-AES-256-CBC-SHA:RSA-PSK-AES256-CBC-SHA384:DHE-PSK-AES256-CBC-SHA384:RSA-PSK-AES256-CBC-SHA:DHE-PSK-AES256-CBC-SHA:AES256-SHA:PSK-AES256-CBC-SHA384:PSK-AES256-CBC-SHA:ECDHE-PSK-AES128-CBC-SHA256:ECDHE-PSK-AES128-CBC-SHA:SRP-RSA-AES-128-CBC-SHA:SRP-AES-128-CBC-SHA:RSA-PSK-AES128-CBC-SHA256:DHE-PSK-AES128-CBC-SHA256:RSA-PSK-AES128-CBC-SHA:DHE-PSK-AES128-CBC-SHA:AES128-SHA:PSK-AES128-CBC-SHA256:PSK-AES128-CBC-SHA

2.2.6 b

DEFAULT CALLBACK BEHAVIOUR

If an application doesn't set its own security callback the default callback is used. It is intended to provide sane defaults. The meaning of each level is described below.

Level 0

Everything is permitted. This retains compatibility with previous versions of OpenSSL.

Level 1

The security level corresponds to a minimum of 80 bits of security. Any parameters offering below 80 bits of security are excluded. As a result RSA, DSA and DH keys shorter than 1024 bits and ECC keys shorter than 160 bits are prohibited. All export ciphersuites are prohibited since they all offer less than 80 bits of security. SSL version 2 is prohibited. Any ciphersuite using MD5 for the MAC is also prohibited.

Level 2

Security level set to 112 bits of security. As a result RSA, DSA and DH keys shorter than 2048 bits and ECC keys shorter than 224 bits are prohibited. In addition to the level 1 exclusions any ciphersuite using RC4 is also prohibited. SSL version 3 is also not allowed. Compression is disabled.

Level 3

Security level set to 128 bits of security. As a result RSA, DSA and DH keys shorter than 3072 bits and ECC keys shorter than 256 bits are prohibited. In addition to the level 2 exclusions ciphersuites not offering forward secrecy are prohibited. TLS versions below 1.1 are not permitted. Session tickets are disabled.

Level 4

Security level set to 192 bits of security. As a result RSA, DSA and DH keys shorter than 7680 bits and ECC keys shorter than 384 bits are prohibited. Ciphersuites using SHA1 for the MAC are prohibited. TLS versions below 1.2 are not permitted.

Level 5

Security level set to 256 bits of security. As a result RSA, DSA and DH keys shorter than 15360 bits and ECC keys shorter than 512 bits are prohibited.

SET Level 2

root@prof:/var/www/html/www.amazon.ca/ap# openssl ciphers -s -v 'ALL:@SECLEVEL=2'
TLS_AES_256_GCM_SHA384 TLSv1.3 Kx=any Au=any Enc=AESGCM(256) Mac=AEAD
TLS_CHACHA20_POLY1305_SHA256 TLSv1.3 Kx=any Au=any
Enc=CHACHA20/POLY1305(256) Mac=AEAD
TLS_AES_128_GCM_SHA256 TLSv1.3 Kx=any Au=any Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA
Enc=AESGCM(256) Mac=AEAD
ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(256)
Mac=AEAD

DHE-DSS-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(256) Mac=AEAD
DHE-RSA-AES256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(256) Mac=AEAD
ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=ECDSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=ECDH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
DHE-RSA-CHACHA20-POLY1305 TLSv1.2 Kx=DH Au=RSA Enc=CHACHA20/POLY1305(256) Mac=AEAD
ECDHE-ECDSA-AES256-CCM8 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM8(256) Mac=AEAD
ECDHE-ECDSA-AES256-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(256) Mac=AEAD
DHE-RSA-AES256-CCM8 TLSv1.2 Kx=DH Au=RSA Enc=AESCCM8(256) Mac=AEAD
DHE-RSA-AES256-CCM TLSv1.2 Kx=DH Au=RSA Enc=AESCCM(256) Mac=AEAD
ECDHE-ECDSA-ARIA256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=ARIAGCM(256) Mac=AEAD
ECDHE-ARIA256-GCM-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=ARIAGCM(256) Mac=AEAD
DHE-DSS-ARIA256-GCM-SHA384 TLSv1.2 Kx=DH Au=DSS Enc=ARIAGCM(256) Mac=AEAD
DHE-RSA-ARIA256-GCM-SHA384 TLSv1.2 Kx=DH Au=RSA Enc=ARIAGCM(256) Mac=AEAD
ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESGCM(128) Mac=AEAD
ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AESGCM(128) Mac=AEAD
DHE-DSS-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AESGCM(128) Mac=AEAD
DHE-RSA-AES128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AESGCM(128) Mac=AEAD
ECDHE-ECDSA-AES128-CCM8 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM8(128) Mac=AEAD
ECDHE-ECDSA-AES128-CCM TLSv1.2 Kx=ECDH Au=ECDSA Enc=AESCCM(128) Mac=AEAD
DHE-RSA-AES128-CCM8 TLSv1.2 Kx=DH Au=RSA Enc=AESCCM8(128) Mac=AEAD
DHE-RSA-AES128-CCM TLSv1.2 Kx=DH Au=RSA Enc=AESCCM(128) Mac=AEAD
ECDHE-ECDSA-ARIA128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=ARIAGCM(128) Mac=AEAD
ECDHE-ARIA128-GCM-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=ARIAGCM(128) Mac=AEAD
DHE-DSS-ARIA128-GCM-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=ARIAGCM(128) Mac=AEAD
DHE-RSA-ARIA128-GCM-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=ARIAGCM(128) Mac=AEAD
ECDHE-ECDSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA384
ECDHE-RSA-AES256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA384
DHE-RSA-AES256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(256) Mac=SHA256
DHE-DSS-AES256-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(256) Mac=SHA256
ECDHE-ECDSA-CAMELLIA256-SHA384 TLSv1.2 Kx=ECDH Au=ECDSA

Enc=Camellia(256) Mac=SHA384
ECDHE-RSA-CAMELLIA256-SHA384 TLSv1.2 Kx=ECDH Au=RSA Enc=Camellia(256) Mac=SHA384
DHE-RSA-CAMELLIA256-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA256
DHE-DSS-CAMELLIA256-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA256
ECDHE-ECDSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA256
ECDHE-RSA-AES128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA256
DHE-RSA-AES128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=AES(128) Mac=SHA256
DHE-DSS-AES128-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=AES(128) Mac=SHA256
ECDHE-ECDSA-CAMELLIA128-SHA256 TLSv1.2 Kx=ECDH Au=ECDSA Enc=Camellia(128) Mac=SHA256
ECDHE-RSA-CAMELLIA128-SHA256 TLSv1.2 Kx=ECDH Au=RSA Enc=Camellia(128) Mac=SHA256
DHE-RSA-CAMELLIA128-SHA256 TLSv1.2 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA256
DHE-DSS-CAMELLIA128-SHA256 TLSv1.2 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA256
ECDHE-ECDSA-AES256-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(256) Mac=SHA1
ECDHE-RSA-AES256-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(256) Mac=SHA1
DHE-RSA-AES256-SHA SSLv3 Kx=DH Au=RSA Enc=AES(256) Mac=SHA1
DHE-DSS-AES256-SHA SSLv3 Kx=DH Au=DSS Enc=AES(256) Mac=SHA1
DHE-RSA-CAMELLIA256-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(256) Mac=SHA1
DHE-DSS-CAMELLIA256-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(256) Mac=SHA1
ECDHE-ECDSA-AES128-SHA TLSv1 Kx=ECDH Au=ECDSA Enc=AES(128) Mac=SHA1
ECDHE-RSA-AES128-SHA TLSv1 Kx=ECDH Au=RSA Enc=AES(128) Mac=SHA1
DHE-RSA-AES128-SHA SSLv3 Kx=DH Au=RSA Enc=AES(128) Mac=SHA1
DHE-DSS-AES128-SHA SSLv3 Kx=DH Au=DSS Enc=AES(128) Mac=SHA1
DHE-RSA-SEED-SHA SSLv3 Kx=DH Au=RSA Enc=SEED(128) Mac=SHA1
DHE-DSS-SEED-SHA SSLv3 Kx=DH Au=DSS Enc=SEED(128) Mac=SHA1
DHE-RSA-CAMELLIA128-SHA SSLv3 Kx=DH Au=RSA Enc=Camellia(128) Mac=SHA1
DHE-DSS-CAMELLIA128-SHA SSLv3 Kx=DH Au=DSS Enc=Camellia(128) Mac=SHA1
AES256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(256) Mac=AEAD
AES256-CCM8 TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM8(256) Mac=AEAD
AES256-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(256) Mac=AEAD
ARIA256-GCM-SHA384 TLSv1.2 Kx=RSA Au=RSA Enc=ARIAGCM(256) Mac=AEAD
AES128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AESGCM(128) Mac=AEAD
AES128-CCM8 TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM8(128) Mac=AEAD
AES128-CCM TLSv1.2 Kx=RSA Au=RSA Enc=AESCCM(128) Mac=AEAD
ARIA128-GCM-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=ARIAGCM(128) Mac=AEAD
AES256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA256
CAMELLIA256-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA256
AES128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA256
CAMELLIA128-SHA256 TLSv1.2 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA256
AES256-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(256) Mac=SHA1
CAMELLIA256-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(256) Mac=SHA1
AES128-SHA SSLv3 Kx=RSA Au=RSA Enc=AES(128) Mac=SHA1
SEED-SHA SSLv3 Kx=RSA Au=RSA Enc=SEED(128) Mac=SHA1
CAMELLIA128-SHA SSLv3 Kx=RSA Au=RSA Enc=Camellia(128) Mac=SHA1

2.2.6 e: Commands

openssl list -cipher-algorithms

root@prof:/var/www/html/www.amazon.ca/ap# openssl list -cipher-algorithms
AES-128-CBC
AES-128-CBC-HMAC-SHA1
AES-128-CBC-HMAC-SHA256
id-aes128-CCM
AES-128-CFB
AES-128-CFB1
AES-128-CFB8
AES-128-CTR
AES-128-ECB
id-aes128-GCM
AES-128-OCB
AES-128-OFB
AES-128-XTS
AES-192-CBC
id-aes192-CCM
AES-192-CFB
AES-192-CFB1
AES-192-CFB8
AES-192-CTR
AES-192-ECB
id-aes192-GCM
AES-192-OCB
AES-192-OFB
AES-256-CBC
AES-256-CBC-HMAC-SHA1
AES-256-CBC-HMAC-SHA256
id-aes256-CCM
AES-256-CFB
AES-256-CFB1
AES-256-CFB8
AES-256-CTR
AES-256-ECB
id-aes256-GCM
AES-256-OCB
AES-256-OFB
AES-256-XTS
aes128 => AES-128-CBC
aes128-wrap => id-aes128-wrap
aes192 => AES-192-CBC
aes192-wrap => id-aes192-wrap
aes256 => AES-256-CBC
aes256-wrap => id-aes256-wrap
ARIA-128-CBC
ARIA-128-CCM
ARIA-128-CFB
ARIA-128-CFB1
ARIA-128-CFB8

ARIA-128-CTR
ARIA-128-ECB
ARIA-128-GCM
ARIA-128-OFB
ARIA-192-CBC
ARIA-192-CCM
ARIA-192-CFB
ARIA-192-CFB1
ARIA-192-CFB8
ARIA-192-CTR
ARIA-192-ECB
ARIA-192-GCM
ARIA-192-OFB
ARIA-256-CBC
ARIA-256-CCM
ARIA-256-CFB
ARIA-256-CFB1
ARIA-256-CFB8
ARIA-256-CTR
ARIA-256-ECB
ARIA-256-GCM
ARIA-256-OFB
aria128 => ARIA-128-CBC
aria192 => ARIA-192-CBC
aria256 => ARIA-256-CBC
bf => BF-CBC
BF-CBC
BF-CFB
BF-ECB
BF-OFB
blowfish => BF-CBC
CAMELLIA-128-CBC
CAMELLIA-128-CFB
CAMELLIA-128-CFB1
CAMELLIA-128-CFB8
CAMELLIA-128-CTR
CAMELLIA-128-ECB
CAMELLIA-128-OFB
CAMELLIA-192-CBC
CAMELLIA-192-CFB
CAMELLIA-192-CFB1
CAMELLIA-192-CFB8
CAMELLIA-192-CTR
CAMELLIA-192-ECB
CAMELLIA-192-OFB
CAMELLIA-256-CBC
CAMELLIA-256-CFB
CAMELLIA-256-CFB1
CAMELLIA-256-CFB8
CAMELLIA-256-CTR
CAMELLIA-256-ECB
CAMELLIA-256-OFB

camellia128 => CAMELLIA-128-CBC
camellia192 => CAMELLIA-192-CBC
camellia256 => CAMELLIA-256-CBC
cast => CAST5-CBC
cast-cbc => CAST5-CBC
CAST5-CBC
CAST5-CFB
CAST5-ECB
CAST5-OFB
ChaCha20
ChaCha20-Poly1305
des => DES-CBC
DES-CBC
DES-CFB
DES-CFB1
DES-CFB8
DES-ECB
DES-EDE
DES-EDE-CBC
DES-EDE-CFB
des-ede-ecb => DES-EDE
DES-EDE-OFB
DES-EDE3
DES-EDE3-CBC
DES-EDE3-CFB
DES-EDE3-CFB1
DES-EDE3-CFB8
des-ede3-ecb => DES-EDE3
DES-EDE3-OFB
DES-OFB
des3 => DES-EDE3-CBC
des3-wrap => id-smime-alg-CMS3DESwrap
desx => DESX-CBC
DESX-CBC
id-aes128-CCM
id-aes128-GCM
id-aes128-wrap
id-aes128-wrap-pad
id-aes192-CCM
id-aes192-GCM
id-aes192-wrap
id-aes192-wrap-pad
id-aes256-CCM
id-aes256-GCM
id-aes256-wrap
id-aes256-wrap-pad
id-smime-alg-CMS3DESwrap
rc2 => RC2-CBC
rc2-128 => RC2-CBC
rc2-40 => RC2-40-CBC
RC2-40-CBC
rc2-64 => RC2-64-CBC

RC2-64-CBC
RC2-CBC
RC2-CFB
RC2-ECB
RC2-OFB
RC4
RC4-40
RC4-HMAC-MD5
seed => SEED-CBC
SEED-CBC
SEED-CFB
SEED-ECB
SEED-OFB
sm4 => SM4-CBC
SM4-CBC
SM4-CFB
SM4-CTR
SM4-ECB
SM4-OFB

openssl list -public-key-algorithms

root@prof:/var/www/html/www.amazon.ca/ap# openssl list -public-key-algorithms
Name: OpenSSL RSA method
    Type: Builtin Algorithm
    OID: rsaEncryption
    PEM string: RSA
Name: rsa
    Alias for: rsaEncryption
Name: OpenSSL PKCS#3 DH method
    Type: Builtin Algorithm
    OID: dhKeyAgreement
    PEM string: DH
Name: dsaWithSHA
    Alias for: dsaEncryption
Name: dsaEncryption-old
    Alias for: dsaEncryption
Name: dsaWithSHA1-old
    Alias for: dsaEncryption
Name: dsaWithSHA1
    Alias for: dsaEncryption
Name: OpenSSL DSA method
    Type: Builtin Algorithm
    OID: dsaEncryption
    PEM string: DSA
Name: OpenSSL EC algorithm
    Type: Builtin Algorithm
    OID: id-ecPublicKey
    PEM string: EC
Name: OpenSSL HMAC method
    Type: Builtin Algorithm

OID: hmac
PEM string: HMAC
Name: OpenSSL CMAC method
Type: Builtin Algorithm
OID: cmac
PEM string: CMAC
Name: OpenSSL RSA-PSS method
Type: Builtin Algorithm
OID: rsassaPss
PEM string: RSA-PSS
Name: OpenSSL X9.42 DH method
Type: Builtin Algorithm
OID: X9.42 DH
PEM string: X9.42 DH
Name: OpenSSL X25519 algorithm
Type: Builtin Algorithm
OID: X25519
PEM string: X25519
Name: OpenSSL X448 algorithm
Type: Builtin Algorithm
OID: X448
PEM string: X448
Name: OpenSSL POLY1305 method
Type: Builtin Algorithm
OID: poly1305
PEM string: POLY1305
Name: OpenSSL SIPHASH method
Type: Builtin Algorithm
OID: siphash
PEM string: SIPHASH
Name: OpenSSL ED25519 algorithm
Type: Builtin Algorithm
OID: ED25519
PEM string: ED25519
Name: OpenSSL ED448 algorithm
Type: Builtin Algorithm
OID: ED448
PEM string: ED448
Name: sm2
Alias for: id-ecPublicKey

openssl list -message-digest-commands ===> Returned an error, so I used the following command (openssl list -digest-commands):

root@prof:/var/www/html/www.amazon.ca/ap# openssl list -digest-commands

blake2b512 blake2s256 gost md4
md5 rmd160 sha1 sha224
sha256 sha384 sha512

openssl speed

root@prof:/var/www/html/www.amazon.ca/ap# openssl speed

Doing md4 for 3s on 16 size blocks: 956616 md4's in 3.00s
Doing md4 for 3s on 64 size blocks: 678853 md4's in 3.00s
Doing md4 for 3s on 256 size blocks: 399749 md4's in 3.00s
Doing md4 for 3s on 1024 size blocks: 154780 md4's in 3.00s
Doing md4 for 3s on 8192 size blocks: 22744 md4's in 3.00s
Doing md4 for 3s on 16384 size blocks: 11478 md4's in 3.00s
Doing md5 for 3s on 16 size blocks: 1303662 md5's in 3.00s
Doing md5 for 3s on 64 size blocks: 750936 md5's in 3.00s
Doing md5 for 3s on 256 size blocks: 338295 md5's in 3.00s
Doing md5 for 3s on 1024 size blocks: 104041 md5's in 3.00s
Doing md5 for 3s on 8192 size blocks: 14061 md5's in 3.00s
Doing md5 for 3s on 16384 size blocks: 7141 md5's in 3.00s
Doing hmac(md5) for 3s on 16 size blocks: 569400 hmac(md5)'s in 3.00s
Doing hmac(md5) for 3s on 64 size blocks: 408231 hmac(md5)'s in 3.00s
Doing hmac(md5) for 3s on 256 size blocks: 3259466 hmac(md5)'s in 3.00s
Doing hmac(md5) for 3s on 1024 size blocks: 1479099 hmac(md5)'s in 3.00s
Doing hmac(md5) for 3s on 8192 size blocks: 226346 hmac(md5)'s in 3.00s
Doing hmac(md5) for 3s on 16384 size blocks: 115041 hmac(md5)'s in 3.00s
Doing sha1 for 3s on 16 size blocks: 17028136 sha1's in 3.00s
Doing sha1 for 3s on 64 size blocks: 10561110 sha1's in 3.00s
Doing sha1 for 3s on 256 size blocks: 5501816 sha1's in 3.00s
Doing sha1 for 3s on 1024 size blocks: 1877355 sha1's in 3.00s
Doing sha1 for 3s on 8192 size blocks: 262642 sha1's in 3.00s
Doing sha1 for 3s on 16384 size blocks: 132324 sha1's in 3.00s
Doing sha256 for 3s on 16 size blocks: 9639663 sha256's in 3.00s
Doing sha256 for 3s on 64 size blocks: 5486108 sha256's in 3.00s
Doing sha256 for 3s on 256 size blocks: 2718467 sha256's in 3.00s
Doing sha256 for 3s on 1024 size blocks: 878524 sha256's in 3.00s
Doing sha256 for 3s on 8192 size blocks: 119516 sha256's in 3.00s
Doing sha256 for 3s on 16384 size blocks: 60268 sha256's in 3.00s
Doing sha512 for 3s on 16 size blocks: 6549838 sha512's in 3.00s
Doing sha512 for 3s on 64 size blocks: 6495490 sha512's in 3.00s
Doing sha512 for 3s on 256 size blocks: 3343852 sha512's in 3.00s
Doing sha512 for 3s on 1024 size blocks: 1441325 sha512's in 3.00s
Doing sha512 for 3s on 8192 size blocks: 215192 sha512's in 3.00s
Doing sha512 for 3s on 16384 size blocks: 109146 sha512's in 3.00s
Doing whirlpool for 3s on 16 size blocks: 5758213 whirlpool's in 3.00s
Doing whirlpool for 3s on 64 size blocks: 3073649 whirlpool's in 3.00s
Doing whirlpool for 3s on 256 size blocks: 1273909 whirlpool's in 3.00s
Doing whirlpool for 3s on 1024 size blocks: 380948 whirlpool's in 3.00s
Doing whirlpool for 3s on 8192 size blocks: 50758 whirlpool's in 3.00s
Doing whirlpool for 3s on 16384 size blocks: 25500 whirlpool's in 3.00s
Doing rmd160 for 3s on 16 size blocks: 7514246 rmd160's in 3.00s
Doing rmd160 for 3s on 64 size blocks: 4596490 rmd160's in 3.00s
Doing rmd160 for 3s on 256 size blocks: 2138477 rmd160's in 3.00s
Doing rmd160 for 3s on 1024 size blocks: 677536 rmd160's in 3.00s
Doing rmd160 for 3s on 8192 size blocks: 91896 rmd160's in 3.00s
Doing rmd160 for 3s on 16384 size blocks: 46202 rmd160's in 3.00s
Doing rc4 for 3s on 16 size blocks: 68741878 rc4's in 3.00s

Doing rc4 for 3s on 64 size blocks: 30165828 rc4's in 3.00s
Doing rc4 for 3s on 256 size blocks: 8913629 rc4's in 3.00s
Doing rc4 for 3s on 1024 size blocks: 2236070 rc4's in 3.00s
Doing rc4 for 3s on 8192 size blocks: 290164 rc4's in 3.00s
Doing rc4 for 3s on 16384 size blocks: 144373 rc4's in 3.00s
Doing des cbc for 3s on 16 size blocks: 12561578 des cbc's in 3.00s
Doing des cbc for 3s on 64 size blocks: 3235157 des cbc's in 3.00s
Doing des cbc for 3s on 256 size blocks: 815304 des cbc's in 3.00s
Doing des cbc for 3s on 1024 size blocks: 203946 des cbc's in 3.00s
Doing des cbc for 3s on 8192 size blocks: 25489 des cbc's in 3.00s
Doing des cbc for 3s on 16384 size blocks: 12757 des cbc's in 3.00s
Doing des ede3 for 3s on 16 size blocks: 4790715 des ede3's in 3.00s
Doing des ede3 for 3s on 64 size blocks: 1210953 des ede3's in 3.00s
Doing des ede3 for 3s on 256 size blocks: 303600 des ede3's in 3.00s
Doing des ede3 for 3s on 1024 size blocks: 75806 des ede3's in 3.00s
Doing des ede3 for 3s on 8192 size blocks: 9494 des ede3's in 3.00s
Doing des ede3 for 3s on 16384 size blocks: 4747 des ede3's in 3.00s
Doing aes-128 cbc for 3s on 16 size blocks: 23310115 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 64 size blocks: 6413869 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 256 size blocks: 1638047 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 1024 size blocks: 412772 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 8192 size blocks: 51773 aes-128 cbc's in 3.00s
Doing aes-128 cbc for 3s on 16384 size blocks: 25908 aes-128 cbc's in 3.00s
Doing aes-192 cbc for 3s on 16 size blocks: 19764919 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 64 size blocks: 5353815 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 256 size blocks: 1363300 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 1024 size blocks: 342963 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 8192 size blocks: 42993 aes-192 cbc's in 3.00s
Doing aes-192 cbc for 3s on 16384 size blocks: 21494 aes-192 cbc's in 3.00s
Doing aes-256 cbc for 3s on 16 size blocks: 17199511 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 64 size blocks: 4593576 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 256 size blocks: 1163350 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 1024 size blocks: 292303 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 8192 size blocks: 36729 aes-256 cbc's in 3.00s
Doing aes-256 cbc for 3s on 16384 size blocks: 18363 aes-256 cbc's in 3.00s
Doing aes-128 ige for 3s on 16 size blocks: 23789990 aes-128 ige's in 3.00s
Doing aes-128 ige for 3s on 64 size blocks: 6264405 aes-128 ige's in 3.00s
Doing aes-128 ige for 3s on 256 size blocks: 1581850 aes-128 ige's in 3.00s
Doing aes-128 ige for 3s on 1024 size blocks: 397455 aes-128 ige's in 3.00s
Doing aes-128 ige for 3s on 8192 size blocks: 49669 aes-128 ige's in 3.00s
Doing aes-128 ige for 3s on 16384 size blocks: 24833 aes-128 ige's in 3.00s
Doing aes-192 ige for 3s on 16 size blocks: 20221688 aes-192 ige's in 3.00s
Doing aes-192 ige for 3s on 64 size blocks: 5254825 aes-192 ige's in 3.00s
Doing aes-192 ige for 3s on 256 size blocks: 1313691 aes-192 ige's in 3.00s
Doing aes-192 ige for 3s on 1024 size blocks: 331730 aes-192 ige's in 3.00s
Doing aes-192 ige for 3s on 8192 size blocks: 41240 aes-192 ige's in 3.00s
Doing aes-192 ige for 3s on 16384 size blocks: 20584 aes-192 ige's in 3.00s
Doing aes-256 ige for 3s on 16 size blocks: 17513870 aes-256 ige's in 3.00s
Doing aes-256 ige for 3s on 64 size blocks: 4519444 aes-256 ige's in 3.00s
Doing aes-256 ige for 3s on 256 size blocks: 1136743 aes-256 ige's in 3.00s
Doing aes-256 ige for 3s on 1024 size blocks: 285047 aes-256 ige's in 3.00s
Doing aes-256 ige for 3s on 8192 size blocks: 35475 aes-256 ige's in 3.00s

Doing aes-256 ige for 3s on 16384 size blocks: 17806 aes-256 ige's in 3.00s
Doing ghash for 3s on 16 size blocks: 213385593 ghash's in 3.00s
Doing ghash for 3s on 64 size blocks: 192365081 ghash's in 3.00s
Doing ghash for 3s on 256 size blocks: 72934197 ghash's in 3.00s
Doing ghash for 3s on 1024 size blocks: 21475977 ghash's in 3.00s
Doing ghash for 3s on 8192 size blocks: 2845429 ghash's in 3.00s
Doing ghash for 3s on 16384 size blocks: 1426897 ghash's in 3.00s
Doing camellia-128 cbc for 3s on 16 size blocks: 17871118 camellia-128 cbc's in 3.00s
Doing camellia-128 cbc for 3s on 64 size blocks: 6875415 camellia-128 cbc's in 3.00s
Doing camellia-128 cbc for 3s on 256 size blocks: 1959687 camellia-128 cbc's in 3.00s
Doing camellia-128 cbc for 3s on 1024 size blocks: 509331 camellia-128 cbc's in 3.00s
Doing camellia-128 cbc for 3s on 8192 size blocks: 64529 camellia-128 cbc's in 3.00s
Doing camellia-128 cbc for 3s on 16384 size blocks: 32264 camellia-128 cbc's in 3.00s
Doing camellia-192 cbc for 3s on 16 size blocks: 15415912 camellia-192 cbc's in 3.00s
Doing camellia-192 cbc for 3s on 64 size blocks: 5379182 camellia-192 cbc's in 3.00s
Doing camellia-192 cbc for 3s on 256 size blocks: 1488679 camellia-192 cbc's in 3.00s
Doing camellia-192 cbc for 3s on 1024 size blocks: 383197 camellia-192 cbc's in 3.00s
Doing camellia-192 cbc for 3s on 8192 size blocks: 48379 camellia-192 cbc's in 3.00s
Doing camellia-192 cbc for 3s on 16384 size blocks: 24198 camellia-192 cbc's in 3.00s
Doing camellia-256 cbc for 3s on 16 size blocks: 15385357 camellia-256 cbc's in 3.00s
Doing camellia-256 cbc for 3s on 64 size blocks: 5380874 camellia-256 cbc's in 3.00s
Doing camellia-256 cbc for 3s on 256 size blocks: 1488625 camellia-256 cbc's in 3.00s
Doing camellia-256 cbc for 3s on 1024 size blocks: 383337 camellia-256 cbc's in 3.00s
Doing camellia-256 cbc for 3s on 8192 size blocks: 48385 camellia-256 cbc's in 3.00s
Doing camellia-256 cbc for 3s on 16384 size blocks: 24165 camellia-256 cbc's in 3.00s
Doing seed cbc for 3s on 16 size blocks: 15229209 seed cbc's in 3.00s
Doing seed cbc for 3s on 64 size blocks: 3963378 seed cbc's in 3.00s
Doing seed cbc for 3s on 256 size blocks: 1002647 seed cbc's in 3.00s
Doing seed cbc for 3s on 1024 size blocks: 251386 seed cbc's in 3.00s
Doing seed cbc for 3s on 8192 size blocks: 31453 seed cbc's in 3.00s
Doing seed cbc for 3s on 16384 size blocks: 15733 seed cbc's in 3.00s
Doing rc2 cbc for 3s on 16 size blocks: 8825592 rc2 cbc's in 3.00s
Doing rc2 cbc for 3s on 64 size blocks: 2269447 rc2 cbc's in 3.00s
Doing rc2 cbc for 3s on 256 size blocks: 571615 rc2 cbc's in 3.00s
Doing rc2 cbc for 3s on 1024 size blocks: 143224 rc2 cbc's in 3.00s
Doing rc2 cbc for 3s on 8192 size blocks: 17907 rc2 cbc's in 3.00s
Doing rc2 cbc for 3s on 16384 size blocks: 8949 rc2 cbc's in 3.00s
Doing blowfish cbc for 3s on 16 size blocks: 21111152 blowfish cbc's in 3.01s
Doing blowfish cbc for 3s on 64 size blocks: 5538734 blowfish cbc's in 3.00s
Doing blowfish cbc for 3s on 256 size blocks: 1416515 blowfish cbc's in 3.00s
Doing blowfish cbc for 3s on 1024 size blocks: 356111 blowfish cbc's in 3.00s
Doing blowfish cbc for 3s on 8192 size blocks: 44529 blowfish cbc's in 3.00s
Doing blowfish cbc for 3s on 16384 size blocks: 22234 blowfish cbc's in 3.00s
Doing cast cbc for 3s on 16 size blocks: 19165615 cast cbc's in 3.00s
Doing cast cbc for 3s on 64 size blocks: 5057974 cast cbc's in 3.00s
Doing cast cbc for 3s on 256 size blocks: 1293101 cast cbc's in 3.00s
Doing cast cbc for 3s on 1024 size blocks: 325637 cast cbc's in 3.00s
Doing cast cbc for 3s on 8192 size blocks: 40765 cast cbc's in 3.00s
Doing cast cbc for 3s on 16384 size blocks: 20401 cast cbc's in 3.00s
Doing 512 bit private rsa's for 10s: 203231 512 bit private RSA's in 10.00s
Doing 512 bit public rsa's for 10s: 2885244 512 bit public RSA's in 10.00s
Doing 1024 bit private rsa's for 10s: 72473 1024 bit private RSA's in 10.00s

Doing 1024 bit public rsa's for 10s: 1134767 1024 bit public RSA's in 10.00s
Doing 2048 bit private rsa's for 10s: 15011 2048 bit private RSA's in 10.00s
Doing 2048 bit public rsa's for 10s: 343094 2048 bit public RSA's in 10.00s
Doing 3072 bit private rsa's for 10s: 3249 3072 bit private RSA's in 10.00s
Doing 3072 bit public rsa's for 10s: 163125 3072 bit public RSA's in 10.00s
Doing 4096 bit private rsa's for 10s: 1438 4096 bit private RSA's in 10.00s
Doing 4096 bit public rsa's for 10s: 94022 4096 bit public RSA's in 10.00s
Doing 7680 bit private rsa's for 10s: 172 7680 bit private RSA's in 10.03s
Doing 7680 bit public rsa's for 10s: 27451 7680 bit public RSA's in 10.00s
Doing 15360 bit private rsa's for 10s: 30 15360 bit private RSA's in 10.08s
Doing 15360 bit public rsa's for 10s: 7047 15360 bit public RSA's in 10.00s
Doing 512 bit sign dsa's for 10s: 123544 512 bit DSA signs in 10.00s
Doing 512 bit verify dsa's for 10s: 214304 512 bit DSA verify in 10.00s
Doing 1024 bit sign dsa's for 10s: 66485 1024 bit DSA signs in 10.00s
Doing 1024 bit verify dsa's for 10s: 85366 1024 bit DSA verify in 10.00s
Doing 2048 bit sign dsa's for 10s: 24015 2048 bit DSA signs in 10.00s
Doing 2048 bit verify dsa's for 10s: 27324 2048 bit DSA verify in 10.00s
Doing 160 bit sign ecdsa's for 10s: 40383 160 bit ECDSA signs in 10.00s
Doing 160 bit verify ecdsa's for 10s: 44564 160 bit ECDSA verify in 10.00s
Doing 192 bit sign ecdsa's for 10s: 32902 192 bit ECDSA signs in 10.00s
Doing 192 bit verify ecdsa's for 10s: 36824 192 bit ECDSA verify in 9.94s
Doing 224 bit sign ecdsa's for 10s: 151060 224 bit ECDSA signs in 10.00s
Doing 224 bit verify ecdsa's for 10s: 64558 224 bit ECDSA verify in 10.00s
Doing 256 bit sign ecdsa's for 10s: 334068 256 bit ECDSA signs in 10.00s
Doing 256 bit verify ecdsa's for 10s: 103045 256 bit ECDSA verify in 10.00s
Doing 384 bit sign ecdsa's for 10s: 9096 384 bit ECDSA signs in 10.00s
Doing 384 bit verify ecdsa's for 10s: 12175 384 bit ECDSA verify in 10.00s
Doing 521 bit sign ecdsa's for 10s: 27043 521 bit ECDSA signs in 10.00s
Doing 521 bit verify ecdsa's for 10s: 13293 521 bit ECDSA verify in 10.00s
Doing 163 bit sign ecdsa's for 10s: 37655 163 bit ECDSA signs in 10.00s
Doing 163 bit verify ecdsa's for 10s: 19005 163 bit ECDSA verify in 10.00s
Doing 233 bit sign ecdsa's for 10s: 27197 233 bit ECDSA signs in 10.00s
Doing 233 bit verify ecdsa's for 10s: 13935 233 bit ECDSA verify in 10.00s
Doing 283 bit sign ecdsa's for 10s: 15869 283 bit ECDSA signs in 10.00s
Doing 283 bit verify ecdsa's for 10s: 8010 283 bit ECDSA verify in 10.00s
Doing 409 bit sign ecdsa's for 10s: 7769 409 bit ECDSA signs in 10.01s
Doing 409 bit verify ecdsa's for 10s: 313 409 bit ECDSA verify in 10.04s
Doing 571 bit sign ecdsa's for 10s: 247 571 bit ECDSA signs in 10.03s
Doing 571 bit verify ecdsa's for 10s: 125 571 bit ECDSA verify in 10.06s
Doing 163 bit sign ecdsa's for 10s: 2186 163 bit ECDSA signs in 10.01s
Doing 163 bit verify ecdsa's for 10s: 9989 163 bit ECDSA verify in 10.00s
Doing 233 bit sign ecdsa's for 10s: 26078 233 bit ECDSA signs in 10.00s
Doing 233 bit verify ecdsa's for 10s: 13313 233 bit ECDSA verify in 10.01s
Doing 283 bit sign ecdsa's for 10s: 15139 283 bit ECDSA signs in 10.00s
Doing 283 bit verify ecdsa's for 10s: 7702 283 bit ECDSA verify in 10.00s
Doing 409 bit sign ecdsa's for 10s: 8790 409 bit ECDSA signs in 10.00s
Doing 409 bit verify ecdsa's for 10s: 4479 409 bit ECDSA verify in 10.00s
Doing 571 bit sign ecdsa's for 10s: 3954 571 bit ECDSA signs in 10.00s
Doing 571 bit verify ecdsa's for 10s: 2026 571 bit ECDSA verify in 10.00s
Doing 160 bit ecdh's for 10s: 42250 160-bit ECDH ops in 10.00s
Doing 192 bit ecdh's for 10s: 34387 192-bit ECDH ops in 10.01s
Doing 224 bit ecdh's for 10s: 94786 224-bit ECDH ops in 10.00s

Doing 256 bit ecdh's for 10s: 134155 256-bit ECDH ops in 10.00s
Doing 384 bit ecdh's for 10s: 9485 384-bit ECDH ops in 10.00s
Doing 521 bit ecdh's for 10s: 20854 521-bit ECDH ops in 10.00s
Doing 163 bit ecdh's for 10s: 38957 163-bit ECDH ops in 10.00s
Doing 233 bit ecdh's for 10s: 28973 233-bit ECDH ops in 10.00s
Doing 283 bit ecdh's for 10s: 16580 283-bit ECDH ops in 10.00s
Doing 409 bit ecdh's for 10s: 10012 409-bit ECDH ops in 10.00s
Doing 571 bit ecdh's for 10s: 4386 571-bit ECDH ops in 10.00s
Doing 163 bit ecdh's for 10s: 37135 163-bit ECDH ops in 10.00s
Doing 233 bit ecdh's for 10s: 27229 233-bit ECDH ops in 10.00s
Doing 283 bit ecdh's for 10s: 15709 283-bit ECDH ops in 10.00s
Doing 409 bit ecdh's for 10s: 9276 409-bit ECDH ops in 10.00s
Doing 571 bit ecdh's for 10s: 4161 571-bit ECDH ops in 10.00s
ECDH failure.
139838251664448:error:100AE081:elliptic curve
routines:EC_GROUP_new_by_curve_name:unknown group:../crypto/ec/ec_curve.c:3132:
139838251664448:error:100AE081:elliptic curve
routines:EC_GROUP_new_by_curve_name:unknown group:../crypto/ec/ec_curve.c:3132:
OpenSSL 1.1.1a 20 Nov 2018
built on: Thu Nov 22 18:40:54 2018 UTC
options:bn(64,64) rc4(16x,int) des(int) aes(partial) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -Wa,--noexecstack -g -O2 -fdebug-prefix-map=/build/openssl-9jbgLq/openssl-1.1.1a=. -fstack-protector-strong -Wformat -Werror=format-security -DOPENSSL_USE_NODELETE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_ASM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA512_ASM -DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DGHASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPADLOCK_ASM -DPOLY1305_ASM -DNDEBUG -Wdate-time -D_FORTIFY_SOURCE=2
The 'numbers' are in 1000s of bytes per second processed.

type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes	16384 bytes
md2	0.00	0.00	0.00	0.00	0.00	0.00
mdc2	0.00	0.00	0.00	0.00	0.00	0.00
md4	5101.95k	14482.20k	34111.91k	52831.57k	62106.28k	62685.18k
md5	6952.86k	16019.97k	28867.84k	35512.66k	38395.90k	38999.38k
hmac(md5)	3036.80k	8708.93k	278141.10k	504865.79k	618075.48k	628277.25k
sha1	90816.73k	225303.68k	469488.30k	640803.84k	717187.75k	722665.47k
rmd160	40075.98k	98058.45k	182483.37k	231265.62k	250937.34k	252324.52k
rc4	366623.35k	643537.66k	760629.67k	763245.23k	792341.16k	788469.08k
des cbc	66995.08k	69016.68k	69572.61k	69613.57k	69601.96k	69670.23k
des ede3	25550.48k	25833.66k	25907.20k	25875.11k	25924.95k	25924.95k
idea cbc	0.00	0.00	0.00	0.00	0.00	0.00
seed cbc	81222.45k	84552.06k	85559.21k	85806.42k	85887.66k	85923.16k
rc2 cbc	47069.82k	48414.87k	48777.81k	48887.13k	48898.05k	48873.47k
rc5-32/12 cbc	0.00	0.00	0.00	0.00	0.00	0.00
blowfish cbc	112218.75k	118159.66k	120875.95k	121552.55k	121593.86k	121427.29k
cast cbc	102216.61k	107903.45k	110344.62k	111150.76k	111315.63k	111416.66k
aes-128 cbc	124320.61k	136829.21k	139780.01k	140892.84k	141374.81k	141492.22k
aes-192 cbc	105412.90k	114214.72k	116334.93k	117064.70k	117399.55k	117385.90k
aes-256 cbc	91730.73k	97996.29k	99272.53k	99772.76k	100294.66k	100286.46k
camellia-128 cbc	95312.63k	146675.52k	167226.62k	173851.65k	176207.19k	176204.46k

```
camellia-192 cbc    82218.20k   114755.88k   127033.94k   130797.91k   132106.92k   132153.34k
camellia-256 cbc    82055.24k   114791.98k   127029.33k   130845.70k   132123.31k   131973.12k
sha256          51411.54k   117036.97k   231975.85k   299869.53k   326358.36k   329143.64k
sha512          34932.47k   138570.45k   285342.04k   491972.27k   587617.62k   596082.69k
whirlpool       30710.47k    65571.18k   108706.90k   130030.25k   138603.18k   139264.00k
aes-128 ige     126879.95k   133640.64k   134984.53k   135664.64k   135629.48k   135621.29k
aes-192 ige     107849.00k   112102.93k   112101.63k   113230.51k   112612.69k   112416.09k
aes-256 ige      93407.31k    96414.81k    97002.07k    97296.04k    96870.40k    97244.50k
ghash         1138056.50k  4103788.39k  6223718.14k  7330466.82k  7769918.12k  7792760.15k
                  sign    verify    sign/s verify/s
rsa  512 bits 0.000049s 0.000003s  20323.1 288524.4
rsa 1024 bits 0.000138s 0.000009s   7247.3 113476.7
rsa 2048 bits 0.000666s 0.000029s   1501.1  34309.4
rsa 3072 bits 0.003078s 0.000061s    324.9  16312.5
rsa 4096 bits 0.006954s 0.000106s    143.8   9402.2
rsa 7680 bits 0.058314s 0.000364s     17.1   2745.1
rsa 15360 bits 0.336000s 0.001419s      3.0    704.7
                  sign    verify    sign/s verify/s
dsa  512 bits 0.000081s 0.000047s  12354.4  21430.4
dsa 1024 bits 0.000150s 0.000117s   6648.5   8536.6
dsa 2048 bits 0.000416s 0.000366s   2401.5   2732.4
                             sign    verify    sign/s verify/s
 160 bit ecdsa (secp160r1)   0.0002s   0.0002s   4038.3   4456.4
 192 bit ecdsa (nistp192)    0.0003s   0.0003s   3290.2   3704.6
 224 bit ecdsa (nistp224)    0.0001s   0.0002s  15106.0   6455.8
 256 bit ecdsa (nistp256)    0.0000s   0.0001s  33406.8  10304.5
 384 bit ecdsa (nistp384)    0.0011s   0.0008s    909.6   1217.5
 521 bit ecdsa (nistp521)    0.0004s   0.0008s   2704.3   1329.3
 163 bit ecdsa (nistk163)    0.0003s   0.0005s   3765.5   1900.5
 233 bit ecdsa (nistk233)    0.0004s   0.0007s   2719.7   1393.5
 283 bit ecdsa (nistk283)    0.0006s   0.0012s   1586.9    801.0
 409 bit ecdsa (nistk409)    0.0013s   0.0321s    776.1     31.2
 571 bit ecdsa (nistk571)    0.0406s   0.0805s     24.6     12.4
 163 bit ecdsa (nistb163)    0.0046s   0.0010s    218.4    998.9
 233 bit ecdsa (nistb233)    0.0004s   0.0008s   2607.8   1330.0
 283 bit ecdsa (nistb283)    0.0007s   0.0013s   1513.9    770.2
 409 bit ecdsa (nistb409)    0.0011s   0.0022s    879.0    447.9
 571 bit ecdsa (nistb571)    0.0025s   0.0049s    395.4    202.6
                             op      op/s
 160 bit ecdh (secp160r1)    0.0002s   4225.0
 192 bit ecdh (nistp192)     0.0003s   3435.3
 224 bit ecdh (nistp224)     0.0001s   9478.6
 256 bit ecdh (nistp256)     0.0001s  13415.5
 384 bit ecdh (nistp384)     0.0011s    948.5
 521 bit ecdh (nistp521)     0.0005s   2085.4
 163 bit ecdh (nistk163)     0.0003s   3895.7
 233 bit ecdh (nistk233)     0.0003s   2897.3
 283 bit ecdh (nistk283)     0.0006s   1658.0
 409 bit ecdh (nistk409)     0.0010s   1001.2
 571 bit ecdh (nistk571)     0.0023s    438.6
 163 bit ecdh (nistb163)     0.0003s   3713.5
 233 bit ecdh (nistb233)     0.0004s   2722.9
```

283 bit ecdh (nistb283) 0.0006s 1570.9
409 bit ecdh (nistb409) 0.0011s 927.6
571 bit ecdh (nistb571) 0.0024s 416.1
253 bit ecdh (X25519) 0.0000s inf

openssl enc -base64 -in h.txt -out h.base64

SEVMTE8K

openssl enc -aes256 -base64 -in h.txt -out Encrypted.txt

Password used in both cases: **1234**

U2FsdGVkX1/pMCcf+QR8gr4aiw3xryrBwlEmSDmBBzI=

Determine how to decrypt step 6.

openssl enc -d -aes256 -base64 -in Encrypted.txt -out decrypted.txt

after entering the aes-256-cbc decryption password (1234), the file decrypted.txt will be created.

The Slammer worm is classified as Denial of Service Attack; what resources are being compromised and affected by the attack?

SQL Server Resolution Service
User Datagram Protocol (UDP)

How does the network propagates through the Internet?

Once the worm infect a computer, it generates random IP addresses that now become the new target. Each successful infection become a new point of replication.

How does the Worm determine the IP addresses of the victim hosts and subnets?

The worm randomly generates ip addresses from the GetTickCount api function in an infected computer.

What are the functional requirements that ought to exist in order for the worm to function and deliver its intended goal.

1. Internet connectivity
2. Vulnerable SQL Server
3.Weak / No Firewall

How does the worm communicate remotely?

The worm uses Distributed Computing Environment / Remote Procedure Calls to communicate. From the slammer.pcap, the protocol used is DCWRPC with packet type being ping. With this

protocol the worm can communicate with other computers over the internet despite the underlying infrastructure.

Part 4: Teardrop Attack

Packet 8, and 9 consists of invalid fragments that are overlapping with oversized payloads from 10.1.1.1 targeting 129.111.30.27