Kiauna Newman Week 6 Project 3 12/17/18

1.)

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > maryville.edu

SSL Report: maryville.edu

Assessed on: Fri, 14 Dec 2018 19:53:49 UTC | Hide | Clear cache

Scan Another >>

	Server	Test time	Grade
1	23.185.0.1 Ready	Fri, 14 Dec 2018 19:49:10 UTC Duration: 76.290 sec	A
2	2620:12a:8001:0:0:0:0:1 Ready	Fri, 14 Dec 2018 19:50:26 UTC Duration: 117.132 sec	A
3	2620:12a:8000:0:0:0:0:1 Ready	Fri, 14 Dec 2018 19:52:23 UTC Duration: 85.660 sec	A

SSL Report v1.32.13

https://www.ssllabs.com/ssltest/analyze.html?d=alpinesecurity.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > alpinesecurity.com

SSL Report: alpinesecurity.com

Assessed on: Fri, 14 Dec 2018 20:01:59 UTC | Hide | Clear cache

Scan Another >>

	Server	Test time	Grade
1	198.49.23.145 Ready	Fri, 14 Dec 2018 19:56:19 UTC Duration: 85.397 sec	A
2	198.49.23.144 Ready	Fri, 14 Dec 2018 19:57:44 UTC Duration: 84.634 sec	A
3	198.185.159.145 Ready	Fri, 14 Dec 2018 19:59:09 UTC Duration: 85.378 sec	A
4	198.185.159.144 Ready	Fri, 14 Dec 2018 20:00:34 UTC Duration: 85.14 sec	A

SSL Report v1.32.13

https://www.ssllabs.com/ssltest/analyze.html?d=facebook.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > facebook.com

SSL Report: facebook.com

Assessed on: Fri, 14 Dec 2018 20:12:33 UTC | Hide | Clear cache

Scan Another >>

	Server	Test time	Grade
1	157.240.11.35 edge-star-mini-shv-02-lax3.facebook.com Ready	Fri, 14 Dec 2018 20:09:11 UTC Duration: 102.456 sec	B
2	2a03:2880:f131:83:face:b00c:0:25de edge-star-mini6-shv-01-sjc3.facebook.com Ready	Fri, 14 Dec 2018 20:10:54 UTC Duration: 99.584 sec	B

SSL Report v1.32.13

https://www.ssllabs.com/ssltest/analyze.html?d=kittenwar.com

Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > kittenwar.com

SSL Report: kittenwar.com (208.97.137.184)

Assessed on: Fri, 14 Dec 2018 20:17:38 UTC | Hide | Clear cache

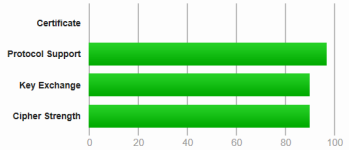
Scan Another »

Summary

Overall Rating

T

If trust issues are ignored: A



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server's certificate is not trusted, see below for details.

Certificate #1: RSA 2048 bits (SHA256withRSA)

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	sni.dreamhost.com Fingerprint SHA256: 5badf35a63f614bfb52ec86eab7fecf64bf5b3b1330652985e5b5801825084ec Pin SHA256: siOWG9sj7RDWPFWYb38fkhDr6JvEUR+WMwkCAxR749g=
Common names	sni.dreamhost.com
Alternative names	- INVALID
Serial Number	0badc0ffee
Valid from	Tue, 11 Aug 2015 18:24:23 UTC
Valid until	Fri, 08 Aug 2025 18:24:23 UTC (expires in 6 years and 7 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	sni.dreamhost.com Self-signed
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	No
OCSP Must Staple	No
Revocation information	None
DNS CAA	No (more info)
Trusted	No NOT TRUSTED (Why?) Mozilla Apple Android Java Windows

Additional Certificates (if supplied)

Certificates provided	1 (823 bytes)

Additional Certificates (if supplied)

Certificates provided	1 (823 bytes)
Chain issues	None

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	No
SSL 3	No
SSL 2	No

For TLS 1.3 tests, we only support RFC 8446.

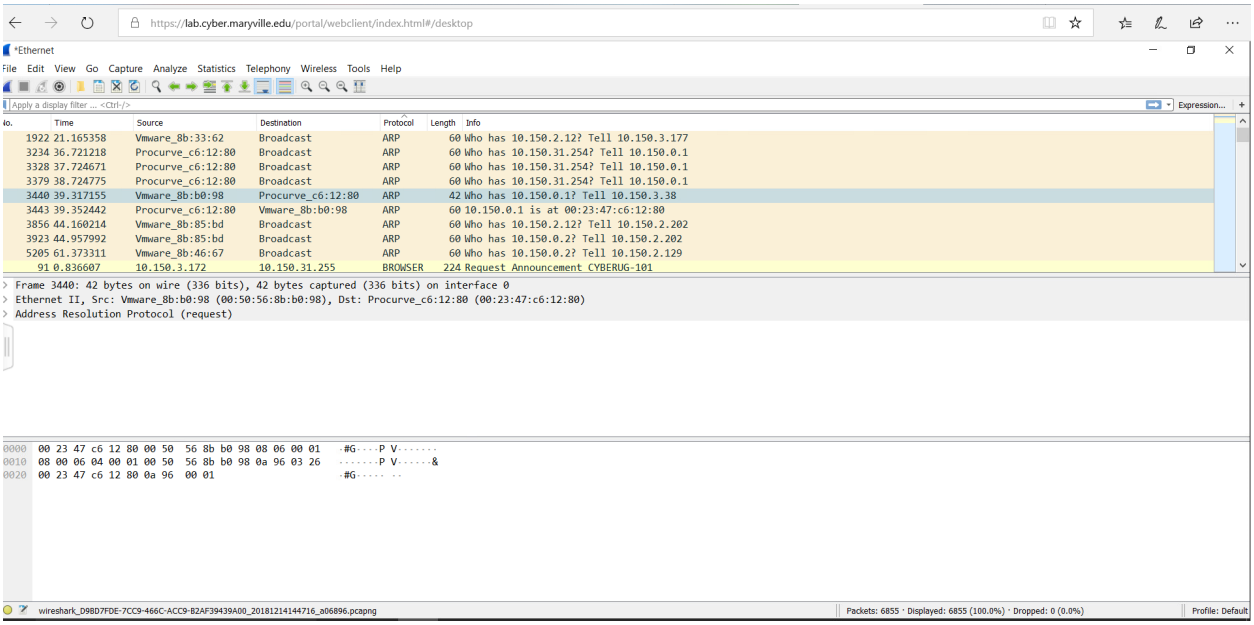
Cipher Suites

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS	256

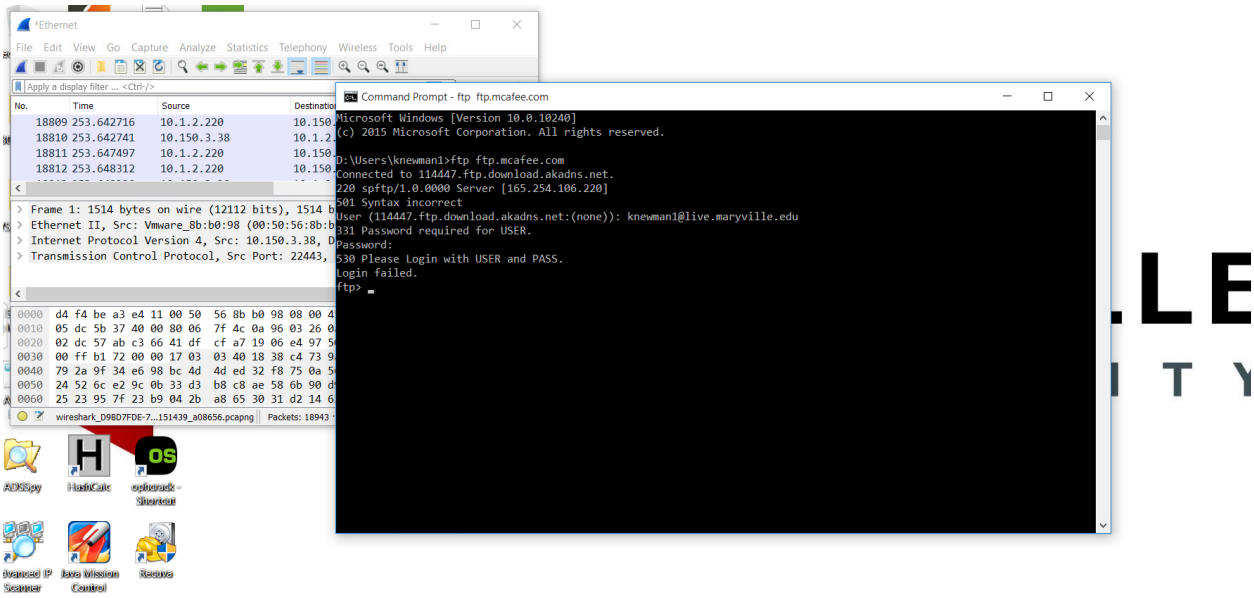
What is the significance of the SSL rating?
Its important because its shows whether or not a website is encrypted with an SSL certificate.
What are some of the concerns visiting a website with a low rating?
Information may be intercepted by a hacker and purchases and transactions are not secure.

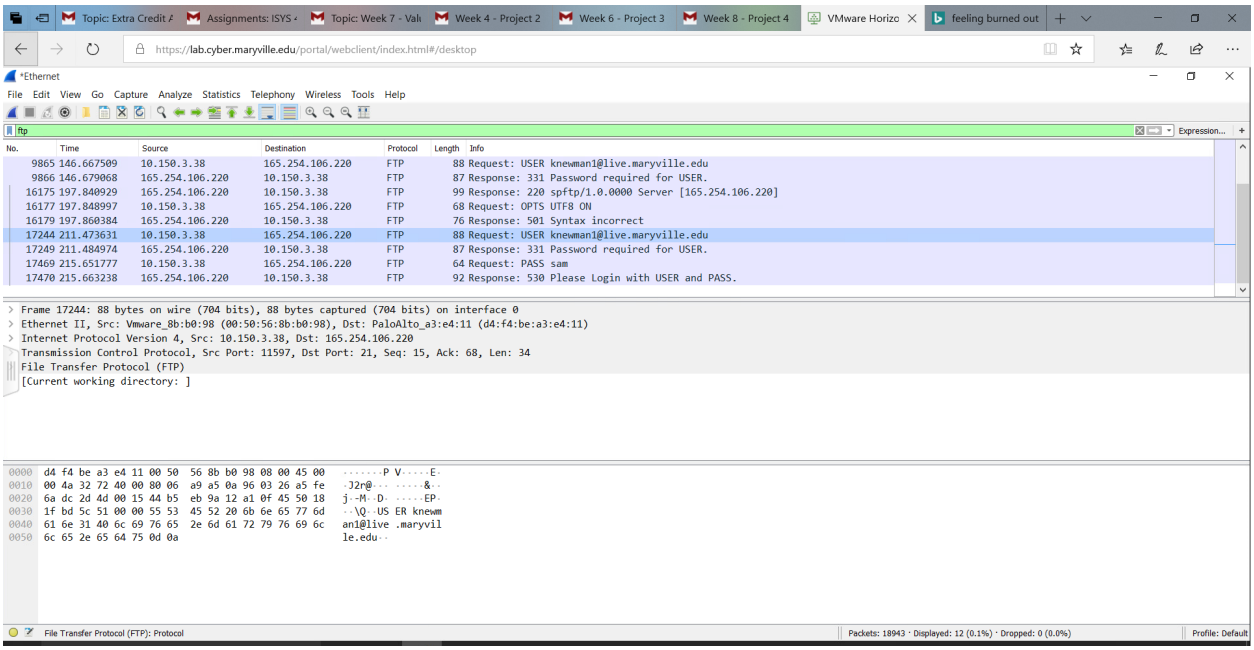
2.)



What type of ARP traffic do you see?
Broadcasts packets asking if any machine knows who has an ip address.
Why is the ARP traffic occurring?
ARP is an address resolution Protocol and its job is to map an Internet protcol address to a physical machine.

Is ARP secure?
No, it is vulnerable to ARP poisoning, session hijacking, denial of service, and man in the middle attacks.





Can you locate the user-name and password you used to connect to ftp.mcafee.com?
Yes
Why were you able to easily glean these using Wireshark?
Wireshark is a network sniffing program that captures package data transmitted over a network. FTP is a protocol that is vulnerable to network sniffing and the login credentials were sent in a FTP protocol.

What is a secure alternative to FTP?
SFTP (Secure Shell File Transfer Protocol)

3.)

VyprVPN: largest bank of IP addresses 70 locaions, offers its own high perofmance chameleon conncetion protocol.

Express VPN; 1700 servers in 145 locations. Uses SSTP. Privacy is a stadnout feature

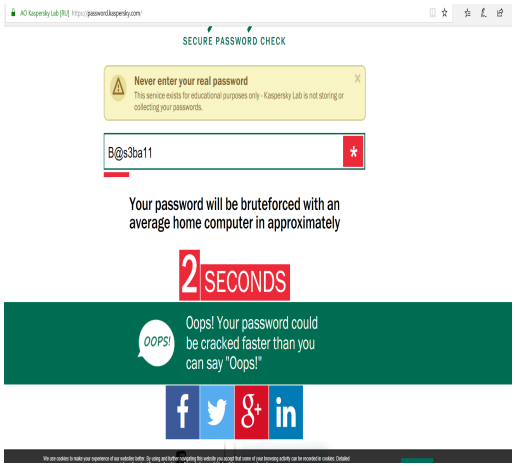
Tunnel Bear: Free; 450 servers in 20 locations, IPSed, IKEv2

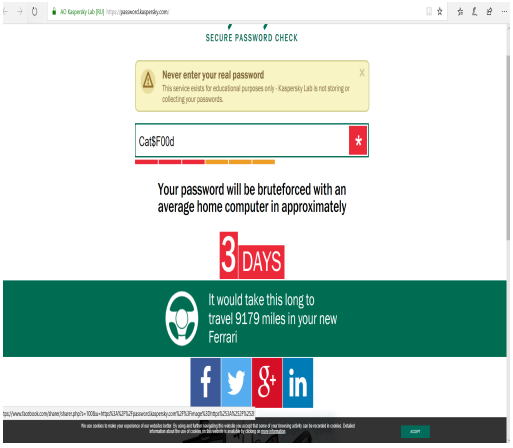
Similar: Each offer a wide range of protocols, a connection kill switch feature, unlimited data usage, and an open vpn. Express and Tunnel Bear offer Bitcoin as a form of payment and they both also use IPSec. VyprVpn and ExpressVpn both offer a 30 day money back guarantee and both use PPTP and L2TP.

4.)

Many organizations blindly make policy without ever checking effectiveness. As an example, many organizations still have a password policy where the password has to be eight (8) characters with at least one (1) of each: uppercase, lowercase, special character, and number. The policy will further state that passwords should be changed every 90 days.

Do you think this is an effective password policy? Explain your rationale.
I disagree with amount of characters. I think passwords should be required to be longer than 8 characters. They should be between 10 to 12 characters. I think longer passwords with a mixture of characters are harder to crack. The process takes longer.





How long did it take to crack these passwords? Show the screen captures.
It took 2 seconds to crack the password B@s3ba11 and it will take 3 days to crack the password Cat$F00d.

How does this relate to the policy above?
Each password is 8 characters withone of each character being a uppercase and lowercase letter, special charcter and number.

What do you recommend be changed?
I think the amount of characters should be increased to 10-12.

How does this relate to the change passwords every 90 days portion of the policy?

If the amount of characters required is increased the 90 days portion of the policy doesnt have to change because it would be harder for an intruder to crack the password.

5.)

```
Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

D:\Users\knewman1>nmap-h
'nmap-h' is not recognized as an internal or external command,
operable program or batch file.

D:\Users\knewman1>nmap -h
Nmap 7.70 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
```

```
Command Prompt
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES

D:\Users\knewman1>nmap www.maryville.edu
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-14 15:58 Central Standard Time
Nmap scan report for www.maryville.edu (23.185.0.1)
Host is up (0.0064s latency).
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.36 seconds

D:\Users\knewman1>
```

what ports are open on this site?

80 TCP and 443 TCP