TLS Audit Report

Server security audit

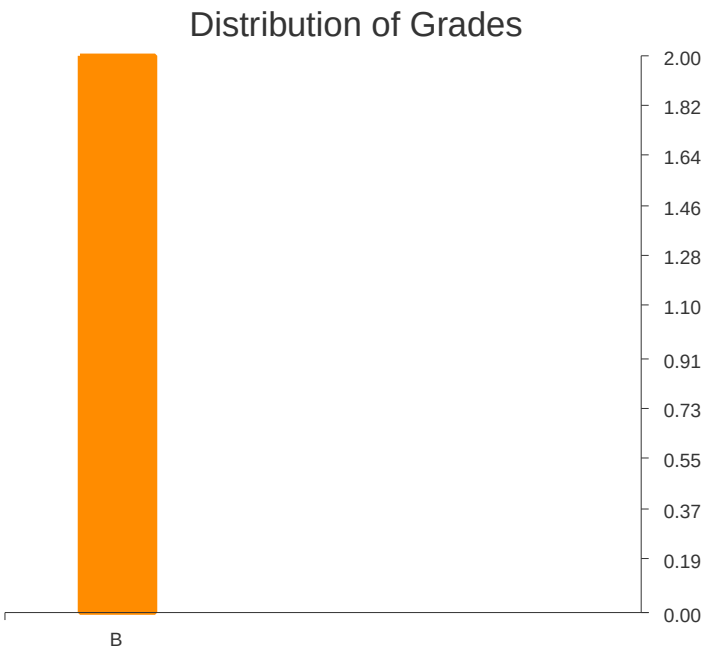
https://github.com/adedayo/tlsaudit v0.0.0

Mon, 13 Apr 2020 22:06:32 UTC

1. Executive Summary

This is a report of the security audit of your server(s) conducted on Mon, 13 Apr 2020 22:06:32 UTC

Worst Measured Grade



Interpretation of Worst Measured Grade

- Adequate security with modern clients, with older and potentially obsolete crypto used with older clients; potentially smaller configuration problems
- An example is a service running on Port 443 and IP Address 104.17.175.85 with hostname cloudflare.com

Table 1. Grade Legend and count of occurrence

Grade	Meaning	Number Found
B	Adequate security with modern clients, with older and potentially obsolete crypto used with older clients; potentially smaller configuration problems	2

2. Detailed Metrics

The following are some details and result metrics from the TLS Audit.

Table 2. TLS Audit Metrics

Worst Grade observed	B (on 104.17.175.85:443)
Best Grade observed	B (on 104.17.175.85:443)
Total Number of Hosts (IPs)	2
Total number of Ports (Unique IP:Port(s))	2
IP:Port(s) with grade B	104.17.175.85:443, 104.17.176.85:443
Grade range for 104.17.175.85	**Worst Grade**: B, **Best Grade**: B
Grade range for 104.17.176.85	**Worst Grade**: B, **Best Grade**: B

3. Details of Individual Scan Results

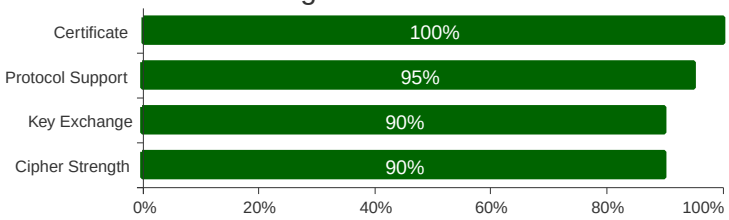
The following sections contain detailed description of results for each port that implements SSL/TLS

TLS Audit Report for 104.17.175.85 (cloudflare.com) on Port 443

Summary

Overall Grade

Rating Breakdown



Advisories

- Grade B : *Adequate security with modern clients, with older and potentially obsolete crypto used with older clients; potentially smaller configuration problems*
- Supports TLS v1.1 or TLS v1.0. Grade capped to or below B

Certificate number #1: ECDSA EC 256 bits (ECDSA-SHA256)

Server Key and Certificate #1

Subject	SERIALNUMBER=4710875,CN=cloudflare.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California,C=US
Subject Serial Number	4710875
Common Names	cloudflare.com
Alternative Names	cloudflare.com, www.cloudflare.com
Serial Number	a68bb984a507399f4716e809a44a7b0
Valid From	Tue, 30 Oct 2018 00:00:00 UTC
Valid Until	Tue, 03 Nov 2020 12:00:00 UTC
Key Algorithm	ECDSA
Key	EC 256 bits
Issuer	CN=DigiCert ECC Extended Validation Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US
Signature Algorithm	ECDSA-SHA256
Signature	306502301e1b3d10...a8bec3c098fa4a91
OCSP Must Staple	false
Certificate Version	3
Chain Length	2
	Chain 1 (CA: false): SERIALNUMBER=4710875,CN=cloudflare.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California,C=US. (Expires: Tue, 03 Nov 2020 12:00:00 UTC) Chain 0 (CA: true): CN=DigiCert ECC Extended Validation Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US. (Expires: Sat, 21 Jun 2031 12:54:27 UTC)

Certificate number #2: RSA 2048 bits (e 65537) (SHA256-RSA)

Server Key and Certificate #2

Subject	SERIALNUMBER=4710875,CN=cloudflare.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California,C=US
Subject Serial Number	4710875
Common Names	cloudflare.com
Alternative Names	cloudflare.com, www.cloudflare.com
Serial Number	37de406f9402b2433c595bc1cba8f88

Server Key and Certificate #2

Valid From	Tue, 30 Oct 2018 00:00:00 UTC
Valid Until	Tue, 03 Nov 2020 12:00:00 UTC
Key Algorithm	RSA
Key	2048 bits (e 65537)
Issuer	CN=DigiCert SHA2 Extended Validation Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US
Signature Algorithm	SHA256-RSA
Signature	88dd9beb4e84b62d...b86ec9472f41c626
OCSP Must Staple	true
Certificate Version	3
Chain Length	2 Chain 1 (CA: false): SERIALNUMBER=4710875,CN=cloudflare.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California,C=US. (Expires: Tue, 03 Nov 2020 12:00:00 UTC) Chain 0 (CA: true): CN=DigiCert SHA2 Extended Validation Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US. (Expires: Sun, 22 Oct 2028 12:00:00 UTC)

Configuration

Supported Protocols

TLS v1.3
TLS v1.2
TLS v1.1
TLS v1.0

Cipher Suites

TLS v1.3 (server has no suites order preference)

	Supports secure renegotiation: false
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: false

Cipher	Bits	Grade

TLS_CHACHA20_POLY1305_SHA256 (0x1303) (Supported Group: x25519) FS	256	A
TLS_AES_256_GCM_SHA384 (0x1302) (Supported Group: x25519) FS	256	A
TLS_AES_128_GCM_SHA256 (0x1301) (Supported Group: x25519) FS	128	A

TLS v1.2 (server has no suites order preference)

	Supports secure renegotiation: true
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: false

Cipher	Bits	Grade
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) (Supported Group: x25519) FS	256	A
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) (Supported Group: x25519) FS	256	A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) (Supported Group: x25519) FS	256	A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) (Supported Group: x25519) FS	128	A
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) (Supported Group: x25519) FS	256	A
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) (Supported Group: x25519) FS	128	A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) (Supported Group: x25519) FS Weak	256	A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) (Supported Group: x25519) FS Weak	128	A
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) (Supported Group: x25519) FS Weak	256	A
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) (Supported Group: x25519) FS Weak	128	A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) (Supported Group: x25519) FS Weak	256	A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) (Supported Group: x25519) FS Weak	128	A
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) Weak	256	E
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) Weak	128	E
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) Weak	256	E
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) Weak	128	E
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) Weak	256	E
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) Weak	128	E

TLS v1.1 (suites in server-preferred order)

	Supports secure renegotiation: true
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: true

Cipher	Bits	Grade
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) (Supported Group: x25519) FS Weak	128	A
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) Weak	128	C
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) (Supported Group: x25519) FS Weak	256	A
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) Weak	256	B

TLS v1.0 (suites in server-preferred order)

	Supports secure renegotiation: true
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: true

Cipher	Bits	Grade
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) (Supported Group: x25519) FS Weak	128	A
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) Weak	128	C

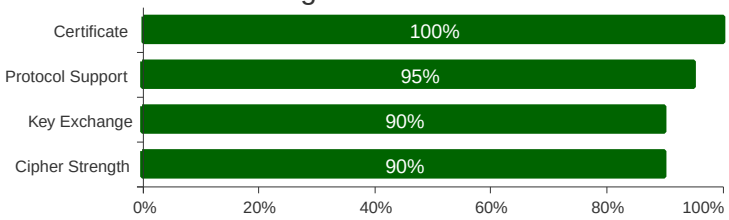
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) (Supported Group: x25519) FS Weak	256	A
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) Weak	256	B
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) Weak	112	C

TLS Audit Report for 104.17.176.85 (cloudflare.com) on Port 443

Summary

Overall Grade

Rating Breakdown



Advisories

- Grade B : *Adequate security with modern clients, with older and potentially obsolete crypto used with older clients; potentially smaller configuration problems*
- Supports TLS v1.1 or TLS v1.0. Grade capped to or below B

Certificate number #1: ECDSA EC 256 bits (ECDSA-SHA256)

Server Key and Certificate #1

Subject	SERIALNUMBER=4710875,CN=cloudflare.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California,C=US
Subject Serial Number	4710875
Common Names	cloudflare.com
Alternative Names	cloudflare.com, www.cloudflare.com
Serial Number	a68bb984a507399f4716e809a44a7b0
Valid From	Tue, 30 Oct 2018 00:00:00 UTC
Valid Until	Tue, 03 Nov 2020 12:00:00 UTC
Key Algorithm	ECDSA
Key	EC 256 bits
Issuer	CN=DigiCert ECC Extended Validation Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US
Signature Algorithm	ECDSA-SHA256
Signature	306502301e1b3d10...a8bec3c098fa4a91
OCSP Must Staple	true
Certificate Version	3
Chain Length	2

Chain 1 (CA: false): SERIALNUMBER=4710875,CN=cloudflare.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California,C=US. (Expires: Tue, 03 Nov 2020 12:00:00 UTC)

Chain 0 (CA: true): CN=DigiCert ECC Extended Validation Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US. (Expires: Sat, 21 Jun 2031 12:54:27 UTC)

Certificate number #2: RSA 2048 bits (e 65537) (SHA256-RSA)

Server Key and Certificate #2

Subject	SERIALNUMBER=4710875,CN=cloudflare.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California,C=US
Subject Serial Number	4710875
Common Names	cloudflare.com
Alternative Names	cloudflare.com, www.cloudflare.com
Serial Number	37de406f9402b2433c595bc1cba8f88

Server Key and Certificate #2

Valid From	Tue, 30 Oct 2018 00:00:00 UTC
Valid Until	Tue, 03 Nov 2020 12:00:00 UTC
Key Algorithm	RSA
Key	2048 bits (e 65537)
Issuer	CN=DigiCert SHA2 Extended Validation Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US
Signature Algorithm	SHA256-RSA
Signature	88dd9beb4e84b62d...b86ec9472f41c626
OCSP Must Staple	true
Certificate Version	3
Chain Length	2 Chain 1 (CA: false): SERIALNUMBER=4710875,CN=cloudflare.com,O=Cloudflare\, Inc.,L=San Francisco,ST=California,C=US. (Expires: Tue, 03 Nov 2020 12:00:00 UTC) Chain 0 (CA: true): CN=DigiCert SHA2 Extended Validation Server CA,OU=www.digicert.com,O=DigiCert Inc,C=US. (Expires: Sun, 22 Oct 2028 12:00:00 UTC)

Configuration

Supported Protocols

TLS v1.3
TLS v1.2
TLS v1.1
TLS v1.0

Cipher Suites

TLS v1.3 (server has no suites order preference)

	Supports secure renegotiation: false
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: false

Cipher	Bits	Grade

TLS_CHACHA20_POLY1305_SHA256 (0x1303) (Supported Group: x25519) FS	256	A
TLS_AES_256_GCM_SHA384 (0x1302) (Supported Group: x25519) FS	256	A
TLS_AES_128_GCM_SHA256 (0x1301) (Supported Group: x25519) FS	128	A

TLS v1.2 (server has no suites order preference)

	Supports secure renegotiation: true
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: false

Cipher	Bits	Grade
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) (Supported Group: x25519) FS	256	A
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) (Supported Group: x25519) FS	256	A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) (Supported Group: x25519) FS	256	A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) (Supported Group: x25519) FS	128	A
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) (Supported Group: x25519) FS	256	A
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) (Supported Group: x25519) FS	128	A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) (Supported Group: x25519) FS Weak	256	A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) (Supported Group: x25519) FS Weak	128	A
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) (Supported Group: x25519) FS Weak	256	A
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) (Supported Group: x25519) FS Weak	128	A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) (Supported Group: x25519) FS Weak	256	A

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) (Supported Group: x25519) FS Weak	128	A
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) Weak	256	E
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) Weak	128	E
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) Weak	256	E
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) Weak	128	E
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) Weak	256	E
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) Weak	128	E

TLS v1.1 (suites in server-preferred order)

	Supports secure renegotiation: true
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: true

Cipher	Bits	Grade
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) (Supported Group: x25519) FS Weak	128	A
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) Weak	128	C
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) (Supported Group: x25519) FS Weak	256	A
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) Weak	256	B

TLS v1.0 (suites in server-preferred order)

	Supports secure renegotiation: true
	Application Layer Protocol Negotiation: http/1.1
	Has a cipher preference order: true

Cipher	Bits	Grade
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) (Supported Group: x25519) FS Weak	128	A
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) Weak	128	C

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) (Supported Group: x25519) FS Weak	256	A
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) Weak	256	B
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa) Weak	112	C