External Penetration Test

Virginia Bankers Association
Glen Allen, Virginia

Performed:
February 2025

Prepared by:
SBS CyberSecurity's
Tony Tyndall

The information contained in this report was derived from proprietary data provided by:
Virginia Bankers Association - Glen Allen, Virginia

Table of Contents

External Penetration Test Risk Codes:

RISK CODE DEFINITIONS

High: Assets, data or reputation is at risk with minimum effort from rogue users, external vendors, or network hackers.

Medium: Assets, data or reputation is at risk with extensive effort, but very possible.

Low: Assets, data or reputation is at risk, but the risk is either small or the cost to fix the issue may not be commensurate with the loss possibility.

Overview

The external penetration test for Virginia Bankers Association (Client) was accomplished from February 24th through 28th, 2025. The below report includes an overview of the network mapping, vulnerability scanning, any exploitations, and reports of those subsequent areas.

Executive Summary

The Client's network is configured in a manner that minimizes the risk of an outside intrusion. Solid configurations of hardware and software devices protect the network in a manner that should allow early detection and remediation of outside attacks or problems. Listed below are our areas of management concern and our key recommendations.

#	Audit Agency	Action Items: Recommendations and comments *Management Comments (if applicable)*	Risk Code	Status Open / Closed	Target / Completion Date Action to Close
1.	SBS 2025 External Penetration Test	According to its version, the Microsoft IIS 7.5 remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. **RECOMMENDATION (High):** The client should remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.	*High*		
2.	SBS 2025 External Penetration Test	The following application does not have HTTP Strict Transport Security (HSTS) enforced: • https://remote.mdbankers.com:4433/ If an attacker can modify a user's network traffic, they could bypass the web application's use of SSL/TLS encryption. **RECOMMENDATION (Low):** The Client should consider enabling HTTP Strict Transport Security (HSTS). This will instruct web browsers to only access the application using the encrypted HTTPS protocol.	*Low*		

#	Audit Agency	Action Items: Recommendations and comments *Management Comments (if applicable)*	Risk Code	Status Open / Closed	Target / Completion Date Action to Close

3.	SBS 2025 External Penetration Test	Auditors performed a review of the Client's internet-facing web portals that rely on SSL/TLS for protection. SSL testing was performed to provide a deep analysis of the strengths and weaknesses of the current SSL configurations. The following devices or services were identified with less than ideal settings.
		
		• https://remote.mdbankers.com:4433/ (68.134.20.155)
		  ○ TLSv1.0 Supported
		  ○ TLSv1.1 Supported
		  ○ Weak Diffie-Hellman key exchange parameters
		
		RECOMMENDATION (Low): The Client should disable TLSv1.0, disable TLSv1.1, and use custom DH primes. This would help mitigate the risk of information disclosure and/or communications compromise associated with the use of these devices.
			Low		

About This Assessment

SBS CyberSecurity (SBS) is a premier cybersecurity consulting and audit firm. Since 2004, SBS has been dedicated to assisting organizations with the implementation of valuable risk management programs and to mitigating cybersecurity risks. The company has provided cybersecurity solutions to over 1,300 organizations across the United States and abroad, including financial institutions ranging in asset size from $12 million to over $20 billion. SBS delivers unique, turnkey solutions tailored to each client's needs, including cybersecurity risk management software, consulting services, network security, IT audit, and education. SBS CyberSecurity empowers customers to make more informed security decisions and trust the safety of their data.

SBS CyberSecurity believes that the findings discussed in this report are of the utmost importance. It is at the discretion of the organization to determine the relevance of these findings. The findings are not requirements, and the implementation of any recommendation is at the organization's discretion. Virginia Bankers Association may wish to contact vendors that manage hardware for the organization to discuss the findings.

This assessment was developed and performed to assist Virginia Bankers Association in improving its security posture; however, it will not ensure absolute security. SBS CyberSecurity assures the accuracy of this report to the best of its ability. This document is property of SBS CyberSecurity. It is considered confidential and unauthorized copying or distribution is prohibited.

Methodology

SBS CyberSecurity has adopted the following methodology for conducting Penetration Tests to ensure thorough and consistent results. This methodology is based on guidance provided by the Penetration Testing Execution Standard (PTES, www.pentest-standard.org).

Pre-Engagement Interaction

The aim of this phase of the penetration test is to define overall scope of the assessment. During this phase, the client will need to answer several questions to properly estimate the engagement scope. These may include (for example): total number of IP addresses and Web applications to be tested, date/time for active portion of the penetration test (scanning, enumeration, and exploitation), etc. These details will be verified with the client during this initial phase of the penetration test.

Information Gathering
In the information gathering (reconnaissance) phase of the Penetration Test, publicly available databases and sources are searched for information about the organization. This information includes items such as IP addresses, email addresses, employee names, phone numbers, internal technologies, and contracted vendors. This information is used throughout the penetration testing process.

Vulnerability Analysis
Vulnerability analysis is the process of identifying, researching and verifying potential weaknesses and misconfigurations in the applications or services identified in the network enumeration process.

After an IP address is verified in the Pre-Engagement Interaction or information gathering phase, all accessible network ports and services are enumerated. Services are identified by port number and transportation layer protocol. Both TCP and UDP transportation layer protocols use a range of 65,535 ports.

Nessus, an industry-leading comprehensive automated vulnerability scanner, is used to identify network vulnerabilities. Supplemental tools are utilized to explore the vulnerabilities found with Nessus and to identify additional vulnerabilities.

Exploitation
The exploitation process attempts to take advantage of the vulnerabilities identified during the previous phases. Successful exploitation may result in unauthorized system access, privilege escalation, denial of service, malicious code execution, additional vulnerability discovery, and increased knowledge of the network environment.

Post Exploitation
The purpose of the Post-Exploitation phase is to determine the value of the machine or application compromised, and to maintain control of the victim for later use. The tester will try to identify the sensitivity of the data stored, as well as usefulness in further compromising the network. Various techniques to access the target machine at a later time may be utilized. This includes, but is not limited to: privilege escalation, malware drop, etc.

Reporting
The final phase of the penetration test will provide the client with details and analysis regarding the test results. The report will contain all the key components, including: executive summary, purpose of the test, scope of the test, identified vulnerabilities and their impact, and remediation suggestions.

Assessment Scope

Penetration testing was performed for Virginia Bankers Association using a variety of network and software analysis tools. Publicly accessible ports and services operating on the IP address(es) listed below were assessed. Ports and services not publicly accessible, or those that fall outside the domain of the authorization of SBS, were not assessed and are not included in this report. These findings may require interaction with vendors of these services to mitigate vulnerabilities. SBS is willing to provide additional information and feedback to aid in this interaction as needed for the institution. The scope of this assessment was discussed with Virginia Bankers Association before it was conducted. The address included in assessment scope was:

- 68.134.20.155
- 107.1.82.170

External Network Penetration Testing

The electronic footprint of Virginia Bankers Association has been evaluated and tested. This process includes, but is not limited to the following:

- Domain registration (WHOIS) information
- Circuit identification and ARIN lookups
- An evaluation of DNS configuration
- Mapping and enumeration
- Zone dump testing
- Identification of any externally accessible services

Virginia Bankers Association's domain registration information has been registered privately. Solid configurations of the DNS servers mitigate the risks associated with information leakage and address poisoning. Virginia Bankers Association's circuit names are not easily identifiable when searching the ARIN WHOIS database. Auditors were able to identify the following externally accessible services:

- Primary Website: https://www.vabankers.org/
- SonicWALL SSL VPN: https://remote.mdbankers.com:4433/

Virginia Bankers Association's external network was evaluated from the Internet with tools and techniques used by hackers to compromise networks. Multiple industry-leading tools were used to check the security of Virginia Bankers Association's internet-accessible network hardware and software devices. The tools that were used include:

- Qualys
- Nmap / NSE
- Kali
- Nessus
- Metasploit / Armitage

Auditors performed extensive port scanning and vulnerability testing against the devices configured on Virginia Bankers Association's external perimeter and the following exceptions were identified during the course of testing:

According to its version, the Microsoft IIS 7.5
remote web server is obsolete and no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor.

RECOMMENDATION (High): The client should remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

The following application does not have HTTP Strict Transport Security (HSTS) enforced:

- https://remote.mdbankers.com:4433/

If an attacker can modify a user's network traffic, they could bypass the web application's use of SSL/TLS encryption.

RECOMMENDATION (Low): The Client should consider enabling HTTP Strict Transport Security (HSTS). This will instruct web browsers to only access the application using the encrypted HTTPS protocol.

Auditors performed a review of the Client's internet-facing web portals that rely on SSL/TLS for protection. SSL testing was performed to provide a deep analysis of the strengths and weaknesses of the current SSL configurations. The following devices or services were identified with less than ideal settings.

- https://remote.mdbankers.com:4433/ (68.134.20.155)
  - TLSv1.0 Supported
  - TLSv1.1 Supported
  - Weak Diffie-Hellman key exchange parameters

RECOMMENDATION (Low): The Client should disable TLSv1.0, disable TLSv1.1, and use custom DH primes. This would help mitigate the risk of information disclosure and/or communications compromise associated with the use of these devices.

DISCOVERIES AND LOGS

Information Gathering:

WHOIS:

ICANN WHOIS

Domain Information

Name: vabankers.org

Internationalized Domain Name: vabankers.org

Registry Domain ID: 724fc16aa23b4420b1e43a2a1c640478-LROR

Domain Status:
clientTransferProhibited

Nameservers:
art.ns.cloudflare.com
lia.ns.cloudflare.com

Dates

Registry Expiration: 2026-12-01 05:00:00 UTC

Updated: 2021-10-25 19:40:44 UTC

Created: 1997-12-02 05:00:00 UTC

Contact Information

Registrant:

Name: Virginia Bankers Association

Organization: Virginia Bankers Association

Email: dnsadmin@vabankers.org

Whois Server: whois.networksolutions.com

Phone: +1.8048194742

Fax: +1.8046436308

Mailing Address: 4490 COX RD, GLEN ALLEN, VA, 23060-3325, US

Technical:

Name: Hancock, Todd

Organization: Virginia Bankers Association

Email: thancock@vabankers.org

Whois Server: whois.networksolutions.com

Phone: 804-819-4742

Mailing Address: 4490 Cox Road, Glen Allen, VA, 23060, US

Administrative:

Name: Hancock, Todd

Organization: Virginia Bankers Association

Email: thancock@vabankers.org

Whois Server: whois.networksolutions.com

Phone: 804-819-4742

Mailing Address: 4490 Cox Road, Glen Allen, VA, 23060, US

ARIN:

"68.134.20.155"

Network: NET-68-128-0-0-1

Source Registry	ARIN
Net Range	68.128.0.0 - 68.141.255.255
CIDR	68.128.0.0/13 68.136.0.0/14 68.140.0.0/15
Name	NETBLK-UUNET97DU-3BLK
Handle	NET-68-128-0-0-1
Parent	NET-68-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	*not provided*
Registration	Mon, 13 May 2002 04:00:00 GMT (Sun May 12 2002 local time)
Last Changed	Tue, 31 May 2022 18:00:56 GMT (Tue May 31 2022 local time)
Self	https://rdap.arin.net/registry/ip/68.128.0.0
Alternate	https://whois.arin.net/rest/net/NET-68-128-0-0-1
Port 43 Whois	whois.arin.net

Related Entities ▾ 2 Entities

Source Registry	ARIN
Kind	Org
Full Name	Verizon Business
Handle	MCICS
Address	22001 Loudoun County Pkwy Ashburn VA 20147 United States

"107.1.82.170"

Network: NET-107-0-0-0-1

Source Registry	ARIN
Net Range	107.0.0.0 - 107.5.255.255
CIDR	107.0.0.0/14 107.4.0.0/15
Name	JUMPSTART-5
Handle	NET-107-0-0-0-1
Parent	NET-107-0-0-0-0
Net Type	DIRECT ALLOCATION
Origin AS	AS7922
Registration	Tue, 29 Jun 2010 16:36:51 GMT (Tue Jun 29 2010 local time)
Last Changed	Mon, 25 Jan 2021 21:53:21 GMT (Mon Jan 25 2021 local time)
Self	https://rdap.arin.net/registry/ip/107.0.0.0
Alternate	https://whois.arin.net/rest/net/NET-107-0-0-0-1
Port 43 Whois	whois.arin.net

Related Entities ▾ 1 Entity

Source Registry	ARIN
Kind	Org
Full Name	Comcast Cable Communications, LLC
Handle	CCCS
Address	1800 Bishops Gate Blvd Mt Laurel NJ 08054 United States

DNS Report:

Parent Nameserver Tests

STATUS	TEST CASE	INFORMATION
INFO	NS records listed at parent servers	Nameserver records returned by the parent servers are: art.ns.cloudflare.com. [NO GLUE] [TTL=3600] lia.ns.cloudflare.com. [NO GLUE] [TTL=3600] This information was kindly provided by a0.org.afilias-nst.info.
OK	Domain listed at parent servers	Good! The parent servers have information on your domain. Some other domains (like .co.us) do not have a DNS zone at the parent servers.
OK	NS records listed at parent servers	Good! The parent servers have your NS records listed. If they didn't, people wouldn't be able to find your domain!
INFO	Parent servers return glue	OK. The TLD of your domain (org) differs from that of your nameservers (com). As such, the parent servers are not required to send glue.
INFO	A record for each NS at parent	OK. The parent servers don't need to have A records for your nameservers since the TLD of your domain (org) differs from that of your nameservers (com).

Local Nameserver Tests

STATUS	TEST CASE	INFORMATION
INFO	NS records at your local servers	NS records retrieved from your local nameservers were: art.ns.cloudflare.com. [NO GLUE] [TTL=86400] lia.ns.cloudflare.com. [NO GLUE] [TTL=86400]
WARNING	Glue at local nameservers	Oops! Your local nameservers don't return IP addresses (glue) along with your NS records! This isn't a fatal error but means an extra lookup needs to be performed increasing the load time to your site. You can fix this by adding A records for each of the nameservers listed above.
INFO	Same glue at local and parent servers	OK. Since the GTLD for your domain (org) differs from that of your nameservers (com), the result of this test is irrelevant since the parent servers aren't even required to hold the A records for your nameservers.
OK	Same NS records at each local nameserver	Good! All your local nameservers have identical NS records for your domain.
OK	Check that all nameservers respond	Good! All of your nameservers listed at the parent servers responded.
OK	Check all nameservers are valid	Good! All of your nameservers appear to be valid (e.g. are not IP addresses or partial domain names).
OK	Number of nameservers	Good! You have at least 2 nameservers. Whilst RFC218 section 2.5 specifies a minimum of 3, as long as you have 2 or more, you should be ok!

STATUS	TEST CASE	INFORMATION
OK	Local nameservers answer authoritatively	Good! All your nameservers answer authoritatively for your domain.
OK	Missing NS records at parent servers	Good! The parent servers have all the nameservers listed for your domain as your local nameservers!
OK	Missing NS records at local servers	Good! Your local servers have all the nameservers listed for your domain that are listed at the parent servers!
OK	No CNAME records for domain	Good! No CNAME records are present for 'vabankers.org'. RFC1912 section 2.4 and RFC2181 section 10.3 state that there should be no CNAME records if any other records are present for a given domain.
OK	No CNAME records for nameservers	Good! No CNAME records are present for your nameservers. RFC1912 section 2.4 and RFC2181 section 10.3 state that there should be no CNAME records if any other records (e.g. an A record) are present for a nameserver.
OK	Nameservers are on different IP subnets	Good! All your nameservers are in separate class C (/24) subnets.
OK	Nameservers have public IP's	Good! All your NS records have public IP addresses.
OK	Nameservers allow TCP connections	Good! We can establish a TCP connection with each of your nameservers on port 53. Whilst UDP is most commonly used for the DNS protocol, TCP connections are occasionally used.

Start of Authority (SOA) Tests

STATUS	TEST CASE	INFORMATION
INFO	SOA Record	Your Start of Authority (SOA) record is: Primary nameserver: art.ns.cloudflare.com. Hostmaster E-mail address: dns.cloudflare.com. Serial number: 2364788112 Refresh: 10000 Retry: 2400 Expire: 604800 Minimum TTL: 1800
OK	All nameservers have same SOA serial number	Good! All your nameservers agree that your SOA serial number is 2364788112
OK	SOA primary nameserver listed at parent	Good! The primary nameserver listed in your SOA record (art.ns.cloudflare.com.) is listed at the parent servers!
WARNING	SOA serial number format	Oops! Your SOA serial number (2364788112) doesn't seem to be in the recommended format (YYYYMMDDnn - where nn is the revision number). This is still OK, however, as long as you are keeping track of your SOA version details.
OK	SOA Refresh value	Good! Your SOA Refresh value (10000) is within the recommended range of 1 hour (3600) to 1 day (86400).
OK	SOA Retry value	Good! Your SOA Retry value (2400) is within the recommended range of 5 minutes (300) to 4 hours (14400).

STATUS	TEST CASE	INFORMATION
OK	SOA Expire value	Good! Your SOA Expire value (604800) is within the recommended range of 1 week (604800) to 4 weeks (2419200).
OK	SOA Minimum TTL value	Good! Your SOA Minimum TTL value (1800) is within the recommended range of less than 3 days (259200).

Mail eXchanger (MX) Tests

STATUS	TEST CASE	INFORMATION
INFO	MX Records	Your Mail eXchanger (MX) records are: 0 vabankers-org.mail.protection.outlook.com. [TTL=300]
OK	All nameservers have same MX records	Good! All of your nameservers have the same MX records.
OK	All MX records contain valid hostnames	Good! All of your MX entries have valid hostnames (e.g. are not IPs or invalid domain names).
OK	All MX records use public IP addresses	Good! All of your MX entries have public IP addresses.
OK	MX record is not a CNAME/alias	Good! When querying for your MX records we did not receive a CNAME record as a result.
OK	MX A records are not CNAME's	Good! No CNAME records are present for your MX A records.
WARNING	Number of MX records	Oops! You only have one MX record! In the event that this mail server is down, you could potentially lose mail! It is recommended to have two or more MX records (and hence mail servers) if you want uninterrupted mail functionality.
OK	Duplicate MX A records	Good! No two MX records resolve to the same IP address.
OK	Differing MX A records	Good! You have no different IPs for your MX A records than the DNS server that is authoritative for that hostname.
OK	MX records have reverse DNS entries	Good! All your MX IP addresses have reverse DNS entries. The reverse entries returned were: 16.42.101.52.in-addr.arpa <--> mail-co1pr05cu00300.inbound.protection.outlook.com.

WWW Record Tests

STATUS	TEST CASE	INFORMATION
INFO	WWW record	www.vabankers.org A records are: www.vabankers.org. A 23.185.0.3 [TTL=300]
OK	WWW A record has public IP	Good! The IP address(es) of the A records returned for your WWW record have public IP addresses.

STATUS	TEST CASE	INFORMATION
OK	WWW CNAME lookup	OK! You don't have a CNAME entry for your WWW record! This is ok though because you have an A record for your WWW record. When people visit www.vabankers.org they will go to the IP address in the A record above.

Mapping / Enumeration:

Zone Dump Testing / Subdomain Enumeration:

dnsenum -noreverse -f 5000.txt vabankers.org
dnsenum VERSION:1.3.1

----- vabankers.org -----

Host's addresses:

_____

vabankers.org. 300 IN A 23.185.0.3

Name Servers:

_____

art.ns.cloudflare.com. 1212 IN A 172.64.33.102
art.ns.cloudflare.com. 1212 IN A 108.162.193.102
art.ns.cloudflare.com. 1212 IN A 173.245.59.102
lia.ns.cloudflare.com. 1203 IN A 172.64.32.185
lia.ns.cloudflare.com. 1203 IN A 173.245.58.185
lia.ns.cloudflare.com. 1203 IN A 108.162.192.185

Mail (MX) Servers:

_____

vabankers-org.mail.protection.outlook.com. 9 IN A 52.101.42.9
vabankers-org.mail.protection.outlook.com. 9 IN A 52.101.41.22
vabankers-org.mail.protection.outlook.com. 9 IN A 52.101.9.0
vabankers-org.mail.protection.outlook.com. 9 IN A 52.101.194.13

Trying Zone Transfers and getting Bind Versions:

_____

Trying Zone Transfer for vabankers.org on art.ns.cloudflare.com ...
AXFR record query failed: FORMERR

Trying Zone Transfer for vabankers.org on lia.ns.cloudflare.com ...
AXFR record query failed: FORMERR

Brute forcing with 5000.txt:

_____

www.vabankers.org. 300 IN A 23.185.0.3
mail.vabankers.org. 300 IN CNAME outlook.office365.com.
outlook.office365.com. 109 IN CNAME ooc-g2.tm-4.office.com.
ooc-g2.tm-4.office.com. 1 IN CNAME outlook.ms-acdc.office.com.
outlook.ms-acdc.office.com. 32 IN CNAME MDW-efz.ms-acdc.office.com.

```
MDW-efz.ms-acdc.office.com.          7       IN    A       52.96.79.162
MDW-efz.ms-acdc.office.com.          7       IN    A       52.96.157.162
MDW-efz.ms-acdc.office.com.          7       IN    A       52.96.79.114
MDW-efz.ms-acdc.office.com.          7       IN    A       52.96.191.194
autodiscover.vabankers.org.          300     IN    CNAME   autodiscover.outlook.com.
autodiscover.outlook.com.            60      IN    CNAME   atod-g2.tm-4.office.com.
atod-g2.tm-4.office.com.             10      IN    A       52.96.163.56
atod-g2.tm-4.office.com.             10      IN    A       52.96.156.8
atod-g2.tm-4.office.com.             10      IN    A       52.96.170.88
atod-g2.tm-4.office.com.             10      IN    A       52.96.156.24
atod-g2.tm-4.office.com.             10      IN    A       52.96.164.136
atod-g2.tm-4.office.com.             10      IN    A       52.96.73.56
atod-g2.tm-4.office.com.             10      IN    A       52.96.79.40
atod-g2.tm-4.office.com.             10      IN    A       52.96.79.168
sip.vabankers.org.                   300     IN    CNAME   sipdir.online.lync.com.
remote.vabankers.org.                300     IN    A       192.237.239.220
ssl.vabankers.org.                   300     IN    A       107.1.112.25
members.vabankers.org.               300     IN    A       104.21.60.31
members.vabankers.org.               300     IN    A       172.67.191.28
lyncdiscover.vabankers.org.          300     IN    CNAME   webdir.online.lync.com.
MAIL.vabankers.org.                  294     IN    CNAME   outlook.office365.com.
outlook.office365.com.               103     IN    CNAME   ooc-g2.tm-4.office.com.
ooc-g2.tm-4.office.com.              31      IN    CNAME   outlook.ms-acdc.office.com.
outlook.ms-acdc.office.com.          26      IN    CNAME   MDW-efz.ms-acdc.office.com.
MDW-efz.ms-acdc.office.com.          1       IN    A       52.96.157.162
MDW-efz.ms-acdc.office.com.          1       IN    A       52.96.79.114
MDW-efz.ms-acdc.office.com.          1       IN    A       52.96.191.194
MDW-efz.ms-acdc.office.com.          1       IN    A       52.96.79.162
WWW.vabankers.org.                   285     IN    A       23.185.0.3
rdp.vabankers.org.                   300     IN    A       192.237.239.220
```

vabankers.org class C netranges:

```
23.185.0.0/24
104.21.60.0/24
107.1.112.0/24
172.67.191.0/24
192.237.239.0/24
```

vabankers.org ip blocks:

```
23.185.0.3/32
104.21.60.31/32
107.1.112.25/32
172.67.191.28/32
192.237.239.220/32
```

done.

Ping Sweeping / Port Scanning:

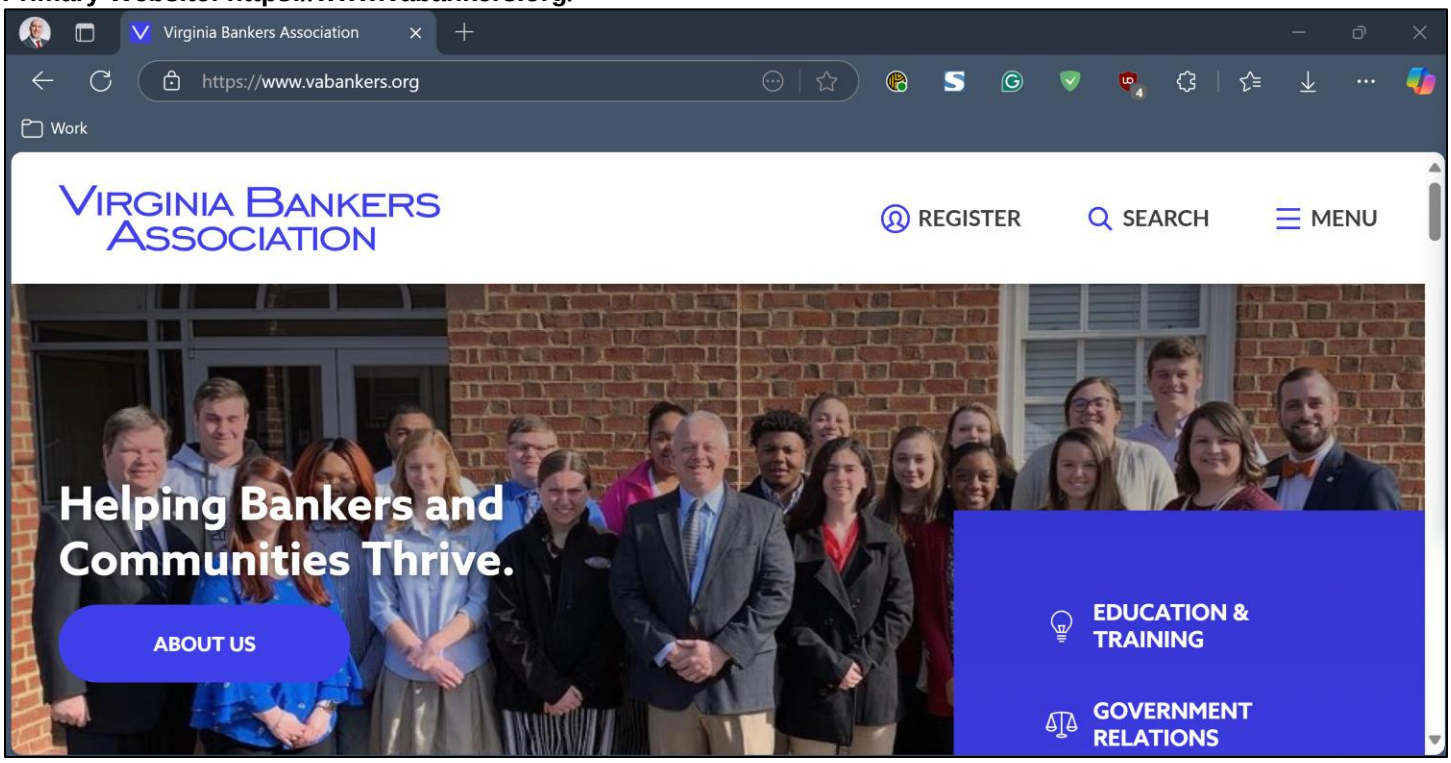
```
# Nmap 7.95 scan initiated Tue Feb 25 10:15:13 2025 as: /usr/lib/nmap/nmap --privileged -T4 -p- -Pn -iL ips.txt -oA vba
Nmap scan report for static-68-134-20-155.bltmmd.fios.verizon.net (68.134.20.155)
Host is up (0.039s latency).
Not shown: 65482 closed tcp ports (reset), 51 filtered tcp ports (no-response)
PORT     STATE SERVICE
443/tcp  open  https
4433/tcp open  vop

Nmap scan report for 107.1.82.170
Host is up.
All 65535 scanned ports on 107.1.82.170 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)

# Nmap done at Tue Feb 25 10:16:11 2025 -- 2 IP addresses (2 hosts up) scanned in 57.96 seconds
```

IKE Testing:

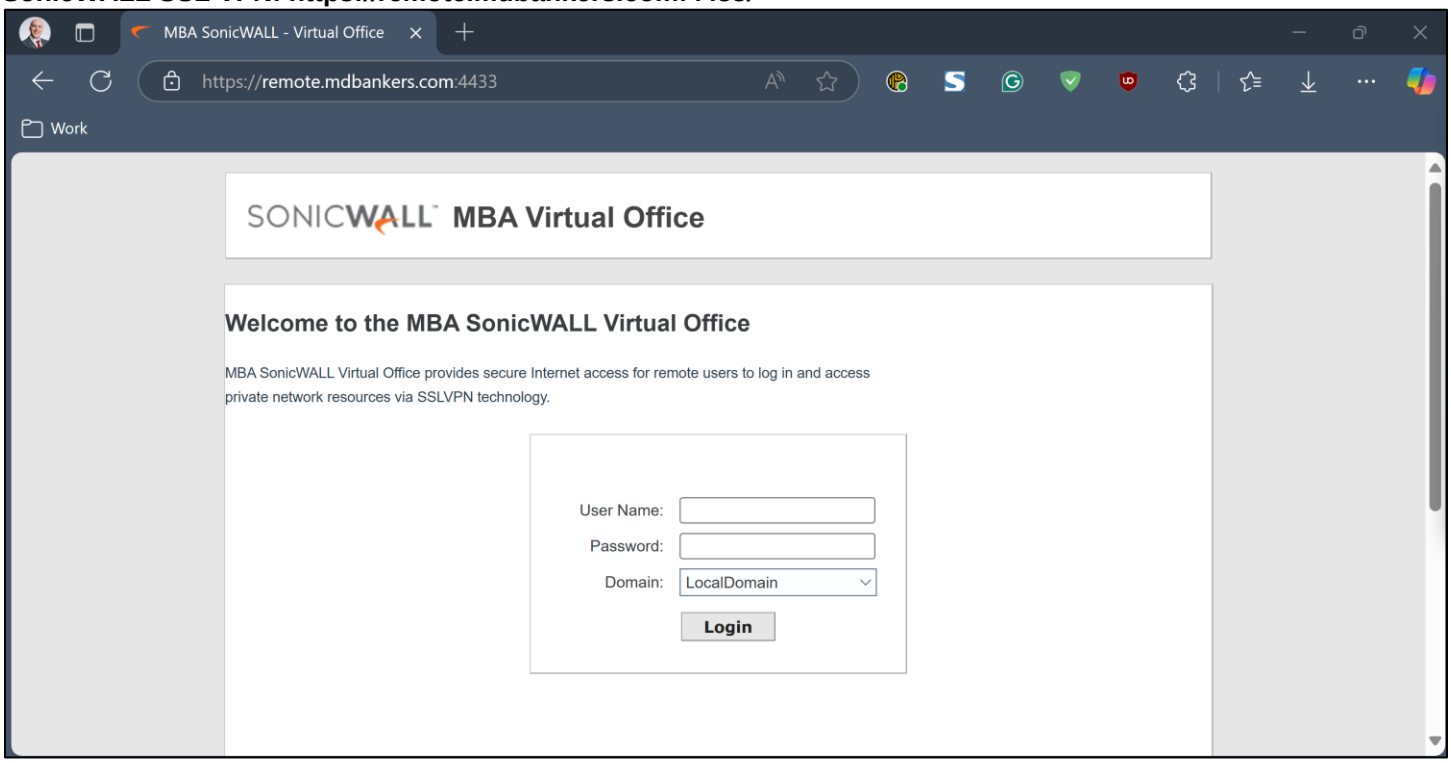
```
ike-scan -N -file ips.txt
Starting ike-scan 1.9.6 with 2 hosts (http://www.nta-monitor.com/tools/ike-scan/)
68.134.20.155   Notify message 14 (NO-PROPOSAL-CHOSEN) HDR=(CKY-R=93fd904c698afddf)
Ending ike-scan 1.9.6: 2 hosts scanned in 2.488 seconds (0.80 hosts/sec).  0 returned handshake; 1 returned notify

ike-scan -A -file ips.txt
Starting ike-scan 1.9.6 with 2 hosts (http://www.nta-monitor.com/tools/ike-scan/)
68.134.20.155   Notify message 18 (INVALID-ID-INFORMATION) HDR=(CKY-R=dc4381da816ffe9b)
Ending ike-scan 1.9.6: 2 hosts scanned in 2.494 seconds (0.80 hosts/sec).  0 returned handshake; 1 returned notify

ike-scan -2 -file ips.txt
Starting ike-scan 1.9.6 with 2 hosts (http://www.nta-monitor.com/tools/ike-scan/)
68.134.20.155   Notify message 7 (INVALID_SYNTAX) HDR=(CKY-R=0000000000000000, IKEv2)
Ending ike-scan 1.9.6: 2 hosts scanned in 2.476 seconds (0.81 hosts/sec).  0 returned handshake; 1 returned notify
```

Screenshots of Identifiable Services:

Primary Website: https://www.vabankers.org/



SonicWALL SSL VPN: https://remote.mdbankers.com:4433/



Vulnerability / Penetration Testing:

SSL Analysis:

Primary Website: https://www.vabankers.org/

SSL Report: www.vabankers.org (23.185.0.3)

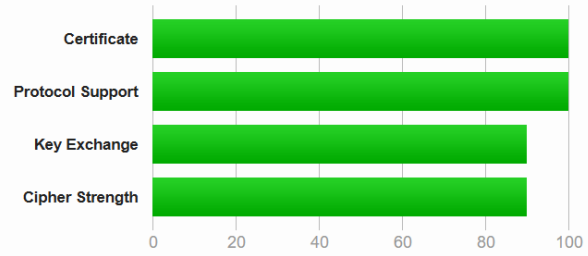
Assessed on: Mon, 24 Feb 2025 17:19:03 UTC | **HIDDEN** | Clear cache

Scan Another

Summary

Overall Rating

A+



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

This site works only in browsers with SNI support.

This server supports TLS 1.3.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	vabankers.org Fingerprint SHA256: da1f60f10178d66dd410a332b016c400b786ecbebb20cf9f81424ad64403eff0 Pin SHA256: 0HVDr3FAOfOiVrT3mDYXjrdGEvFrD1Kgvqb0VgrgaVs=
Common names	vabankers.org
Alternative names	vabankers.org vba.ddsandbox.net www.vabankers.org
Serial Number	0469999fcad0017b52f95803da3d88180b72
Valid from	Mon, 06 Jan 2025 01:46:18 UTC
Valid until	Sun, 06 Apr 2025 01:46:17 UTC (expires in 1 month and 12 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No

Server Key and Certificate #1

Issuer	R11 AIA: http://r11.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r11.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	2 (2590 bytes)
Chain issues	None

#2

Subject	R11 Fingerprint SHA256: 591e9ce6c863d3a079e9fabe1478c7339a26b21269dde795211361024ae31a44 Pin SHA256: bdrBhpj38ffhxpubzkINl0rG+UyossdhcBYj+Zx2fcc=
Valid until	Fri, 12 Mar 2027 23:59:59 UTC (expires in 2 years)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Certificate #2: RSA 2048 bits (SHA256withRSA) No SNI

Click here to expand

Configuration

Protocols

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

(*) Experimental: Server negotiated using No-SNI

Cipher Suites

 # TLS 1.3 (suites in server-preferred order)

TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256P

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	256

(P) This server prefers ChaCha20 suites with clients that don't have AES-NI (e.g., Android devices)

Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

Handshake Simulation

Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Android 8.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Android 9.0	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
IE 11 / Win 7 R	Server sent fatal alert: handshake_failure		
IE 11 / Win 8.1 R	Server sent fatal alert: handshake_failure		
IE 11 / Win Phone 8.1 R	Server sent fatal alert: handshake_failure		
IE 11 / Win Phone 8.1 Update R	Server sent fatal alert: handshake_failure		
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS

Handshake Simulation

Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH x25519 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_128_GCM_SHA256 ECDH x25519 FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure		
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure		
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure		
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure		
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure		
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_CHACHA20_POLY1305_SHA256 ECDH x25519 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Handshake Simulation

Not simulated clients (Protocol mismatch)

Click here to expand

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	**Yes, TLS_FALLBACK_SCSV supported** (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**Yes (with most browsers) ROBUST** (more info)
ALPN	Yes h2 http/1.1
NPN	No
Session resumption (caching)	**No (IDs assigned but not accepted)**

Protocol Details

Session resumption (tickets)	Yes
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	**Yes** max-age=31536000
HSTS Preloading	**Not in: Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No, DHE suites not supported
DH public server param (Ys) reuse	No, DHE suites not supported
ECDH public server param reuse	No
Supported Named Groups	x25519, secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	Yes

SonicWALL SSL VPN: https://remote.mdbankers.com:4433/

SSL Report: remote.mdbankers.com (68.134.20.155)

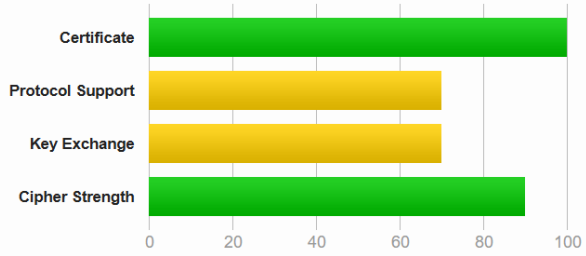
Assessed on: Wed, 26 Feb 2025 15:43:34 UTC | **HIDDEN** | Clear cache

Scan Another

Summary

Overall Rating

B



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

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

This server supports TLS 1.0. Grade capped to B. MORE INFO »

Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	remote.mdbankers.com Fingerprint SHA256: ea6493567e6f270855c016aa06942ecb36bf7929fd8f7410d7ce832ef2dc0bc4 Pin SHA256: 6ZQCoPGCMV4kbIMPQ7gpLfdeZCRoZeSJKeCQH6Ufzfw=
Common names	remote.mdbankers.com
Alternative names	remote.mdbankers.com
Serial Number	06b20948811468298842cb65c466dc98
Valid from	Mon, 29 Apr 2024 00:00:00 UTC
Valid until	Tue, 29 Apr 2025 23:59:59 UTC (expires in 2 months and 3 days)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	RapidSSL TLS RSA CA G1 AIA: http://cacerts.rapidssl.com/RapidSSLTLSRSACAG1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	**Yes (certificate)**
OCSP Must Staple	No

Server Key and Certificate #1

Revocation information	CRL, OCSP CRL: http://cdp.rapidssl.com/RapidSSLTLSRSACAG1.crl OCSP: http://status.rapidssl.com
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	**Yes** **Mozilla Apple Android Java Windows**

Additional Certificates (if supplied)

Certificates provided	2 (2789 bytes)
Chain issues	None

#2

Subject	RapidSSL TLS RSA CA G1 Fingerprint SHA256: 4422e963ee53cd58cc9f85cd40bf5ffec0095fdf1a154535661c1c06bcadc69b Pin SHA256: E3tYcwo9CiqATmKtpMLW5V+pzIq+ZoDmpXSiJlXGmTo=
Valid until	Tue, 02 Nov 2027 12:24:33 UTC (expires in 2 years and 8 months)
Key	RSA 2048 bits (e 65537)
Issuer	DigiCert Global Root G2
Signature algorithm	SHA256withRSA

Certification Paths

Click here to expand

Configuration

Protocols

TLS 1.3	No
TLS 1.2	Yes
TLS 1.1	No

Protocols

TLS 1.0	Yes
SSL 3	No
SSL 2	No

Cipher Suites

TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e) DH 1024 bits FS **WEAK**	128
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 1024 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x33) DH 1024 bits FS **WEAK**	128
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK**	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK**	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK**	128

TLS 1.0 (suites in server-preferred order)

Handshake Simulation

Android 2.3.7 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH 1024 FS
Android 4.0.4	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.1.1	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.2.2	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.3	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1 FS
Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 FS

Handshake Simulation

Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Android 8.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Android 9.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Baidu Jan 2015	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Chrome 70 / Win 10	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Chrome 80 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Firefox 73 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 7 / Vista	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 8 / XP No FS [1] No SNI [2]	Server closed connection				
IE 8-10 / Win 7 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 10 / Win Phone 8.0	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1	FS
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS
Java 6u45 No SNI [2]	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	DH 1024	FS
Java 7u25	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1	FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS

Handshake Simulation

Java 11.0.3	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Java 12.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
OpenSSL 0.9.8y	RSA 2048 (SHA256)	TLS 1.0	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	DH 1024	FS	
OpenSSL 1.0.1l R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
OpenSSL 1.1.1c R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 5.1.9 / OS X 10.6.8	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
Safari 6 / iOS 6.0.1	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 6.0.4 / OS X 10.8.4 R	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	ECDH secp256r1	FS	
Safari 7 / iOS 7.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 7 / OS X 10.9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 8 / iOS 8.4 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 8 / OS X 10.10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 12.1.2 / MacOS 10.14.6 Beta R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Safari 12.1.1 / iOS 12.3.1 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDH secp256r1	FS	

Not simulated clients (Protocol mismatch)

IE 6 / XP	No FS [1]	No SNI [2]	Protocol mismatch (not simulated)

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.

Protocol Details

Secure Renegotiation	**Supported**
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Not mitigated server-side (more info) TLS 1.0: 0xc014
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info) TLS 1.2 : 0xc027
GOLDENDOODLE	No (more info) TLS 1.2 : 0xc027
OpenSSL 0-Length	No (more info) TLS 1.2 : 0xc027
Sleeping POODLE	No (more info) TLS 1.2 : 0xc027
Downgrade attack prevention	No, TLS_FALLBACK_SCSV not supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No
Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	**Weak key exchange WEAK**
ALPN	No
NPN	No
Session resumption (caching)	**No (IDs assigned but not accepted)**
Session resumption (tickets)	No
OCSP stapling	**Yes**
Strict Transport Security (HSTS)	No
HSTS Preloading	**Not in: Chrome Edge Firefox IE**
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	No (more info)
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No

Protocol Details

Uses common DH primes	**Yes** Replace with custom DH parameters if possible (more info)
DH public server param (Ys) reuse	**Yes**
ECDH public server param reuse	**Yes**
Supported Named Groups	secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	Yes

Vulnerability Scanning:

68.134.20.155

1	0	3	1	34
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	VPR Score	EPSS Score	Plugin	Name
CRITICAL	10.0	-	-	34460	Unsupported Web Server Detection
MEDIUM	6.5	-	-	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
LOW	3.7	4.5	0.9689	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	-	-	46180	Additional DNS Hostnames
INFO	N/A	-	-	33817	CGI Generic Tests Load Estimation (all tests)

INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	49704	External URLs
INFO	N/A	-	-	84502	HSTS Missing From HTTPS Server
INFO	N/A	-	-	43111	HTTP Methods Allowed (per directory)
INFO	N/A	-	-	10107	HTTP Server Type and Version
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	-	11935	IPSEC Internet Key Exchange (IKE) Version 1 Detection
INFO	N/A	-	-	62695	IPSEC Internet Key Exchange (IKE) Version 2 Detection
INFO	N/A	-	-	50344	Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	56984	SSL / TLS Versions Supported

INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	40773	Web Application Potentially Sensitive CGI Parameter Detection
INFO	N/A	-	-	91815	Web Application Sitemap
INFO	N/A	-	-	11032	Web Server Directory Enumeration
INFO	N/A	-	-	11422	Web Server Unconfigured - Default Install Page Present

INFO	N/A	-	-	10302	Web Server robots.txt Information Disclosure
INFO	N/A	-	-	10662	Web mirroring

* indicates the v3.0 score was not available; the v2.0 score is shown

107.1.82.170

0	0	0	0	2
CRITICAL	HIGH	MEDIUM	LOW	INFO

Penetration Testing:

[*] Finding exploits (via local magic)

[*] Sorting Exploits...

[*] Launching Exploits...

[*] Listing sessions...

msf5 > sessions -v

Active sessions

==========

No active sessions.

Verification of Results:
No externally exploitable services were identified.