



Open-Source Intelligence External Security Assessment

ACME Solutions Inc.

July 14, 2023



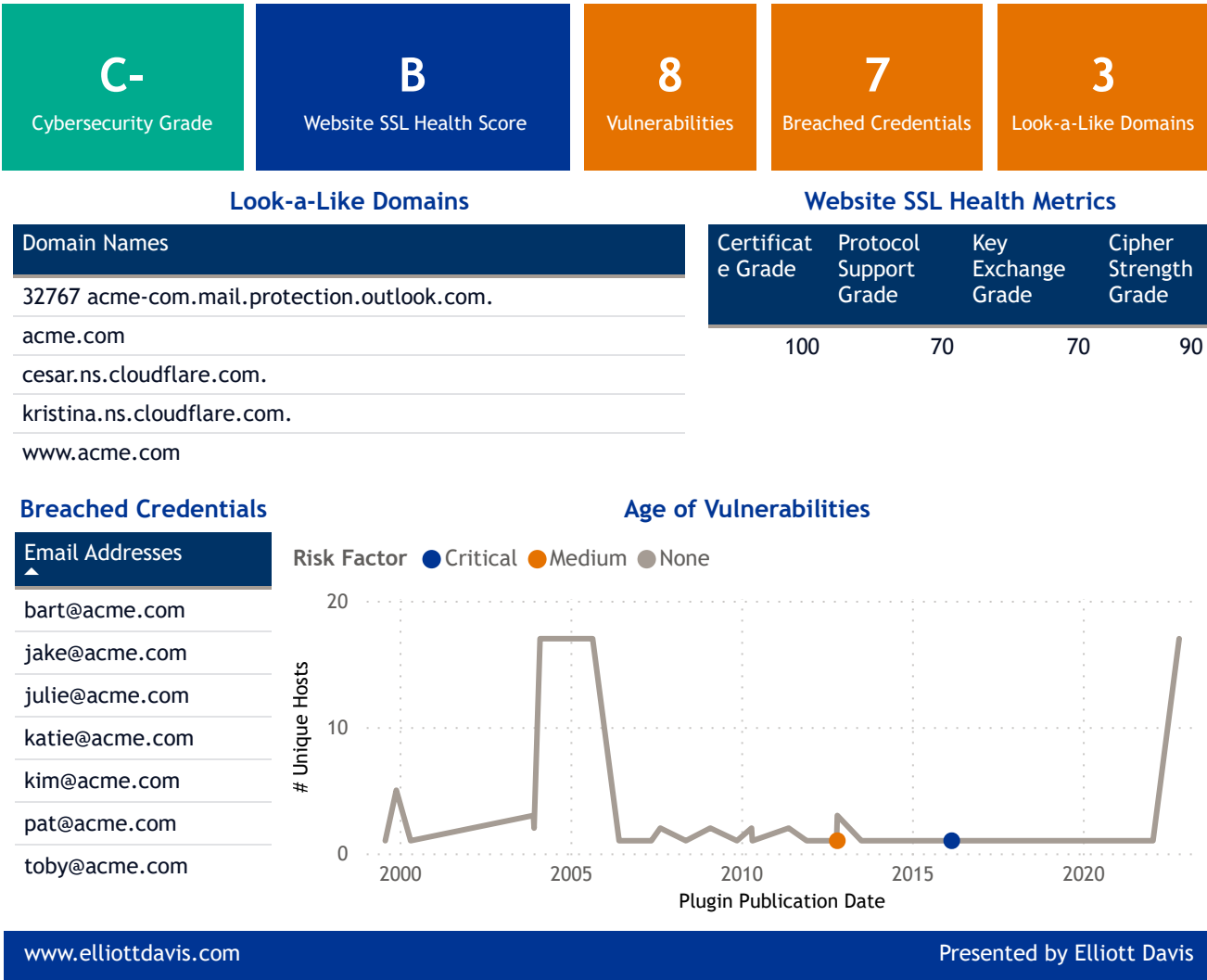
Executive Summary

We have conducted an Open-Source Intelligence (OSINT) external security assessment for ACME company, and our findings indicate that the company's public-facing online presence poses several security risks. Our assessment aimed to identify the information that the company inadvertently shares online and how this information could be leveraged by attackers to launch targeted attacks.

Our approach involved analyzing publicly available information on the company's website, social media profiles, and other publicly available information. We also analyzed the information available on third-party websites that could be used to attack the company's IT infrastructure, applications, and network.


The results of our assessment reveal that ACME company shares a significant amount of sensitive information on its website. We also found that the company's website contains outdated software and plugins that could be exploited by attackers to compromise the company's web servers and gain access to sensitive data.

In conclusion, our OSINT external security assessment indicates that ACME company's public-facing online presence poses significant security risks that require immediate attention. We recommend that the company takes steps to secure their website, including updating software and plugins, removing sensitive information from public-facing platforms, and training employees on how to identify and report suspicious activity.



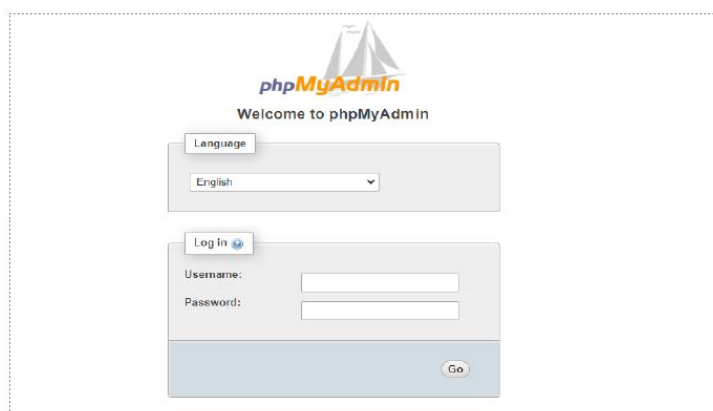


Sample Screenshots

PHP Version 7.3.27-9+ubuntu18.04.1+deb.sury.org+1	
	
System	Linux ubuntu-lpm-sifbm 4.15.0-140-generic #144-Ubuntu SMP Fri Mar 19 14:12:35 UTC 2021 x86_64
Build Date	Feb 23 2021 15:10:08
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-ldap.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysql.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sysmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.3/apache2/conf.d/20-xsl.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731.NTS
PHP Extension Build	API320180731.NTS

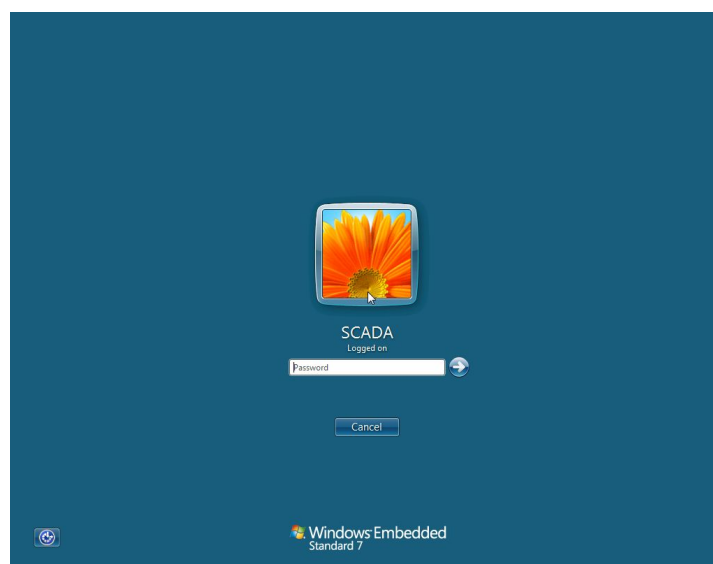
Information Disclosure

Elliott Davis' cybersecurity consultants identified through the use of Archive.org's Wayback machine a page disclosing information on the configuration of the Company's web server.



phpMyAdmin Exposed to the Internet

Elliott Davis' cybersecurity consultants identified through Tenable Nessus a phpMyAdmin page exposed to the Internet. It is best practice never to expose admin consoles to the Internet to avoid brute force login attempts.



Remote Desktop Exposed to the Internet

The Company has Remote Desktop services exposed to the Internet. It is best practice never to expose Remote Desktop to the Internet to avoid brute force login attempts. In addition, Tenable Nessus has identified a Remote Code Execution vulnerability within Remote Desktop that could be abused by an attacker to gain remote access to the device.



Assessment Details

Present Outside Hosts Detail

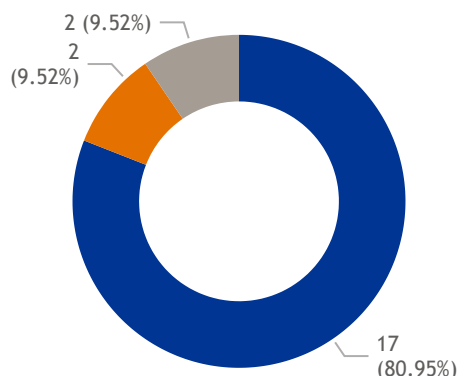
Hostname	IP Address	Type
32767 acme-com.mail.protection.outlook.com.	172.67.31.24	MX
acme.com	172.67.31.24	A
cesar.ns.cloudflare.com.	172.67.31.24	NS
kristina.ns.cloudflare.com.	172.67.31.24	NS
www.acme.com	172.67.31.24	A

Top 5 Vulnerability Risks

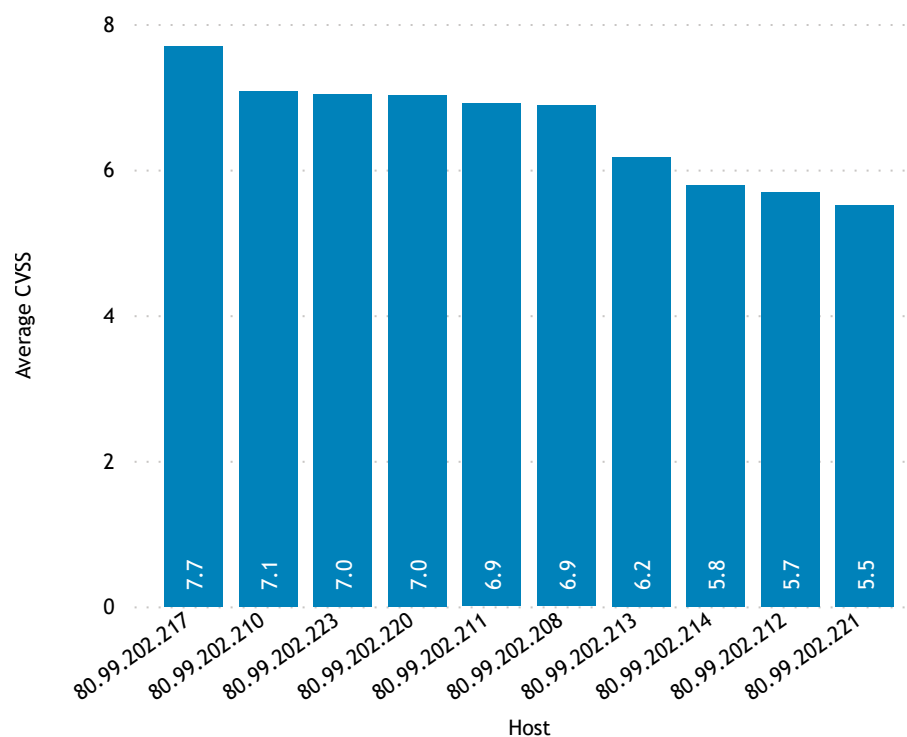
Port	Risk	Host	Protocol	Name	CVSS v3.0 Base Score
443	Medium	80.99.202.214	tcp	Nessus SYN scanner	9.56
443	Medium	80.99.202.214	tcp	SSL Cipher Block Chaining Cipher Suites Supported	7.83
500	Critical	80.99.202.212	udp	Cisco ASA / IOS IKE Fragmentation Vulnerability	6.50
443	Critical	80.99.202.214	tcp	TLS Version 1.3 Protocol Detection	4.99
500	Critical	80.99.202.212	udp	Cisco ASA / IOS IKE Fragmentation Vulnerability	4.49

Risk by Host Count

Risk ● None ● Critical ● Medium



Top 10 Hosts with the Highest CVSS Vulnerability Rating





Appendix A: Executive Summary Legend

Cybersecurity Grade - The assigned cybersecurity grade by the Elliott Davis team is an assessment of the Company's external presence at a specific point in time. It considers various factors and combines qualitative and quantitative analysis of findings from network vulnerability scanning and open-source intelligence research. The assessment considers the Company's size and industry, allowing Elliott Davis cybersecurity consultants to generate a grade that benchmarks it against similar organizations.

Website SSL Health Score - SSL health refers to the security of a website's SSL certificate. An SSL certificate is a digital security certificate that encrypts the data that is transmitted between a web server and a web browser. This ensures that the data is secure and cannot be intercepted or read by unauthorized third parties.

Vulnerabilities - Are known problems with network hardware and web applications discovered through network scans by Tenable Nessus and Shodan. This information is acquired through port scans, service fingerprinting, and vulnerability scans.

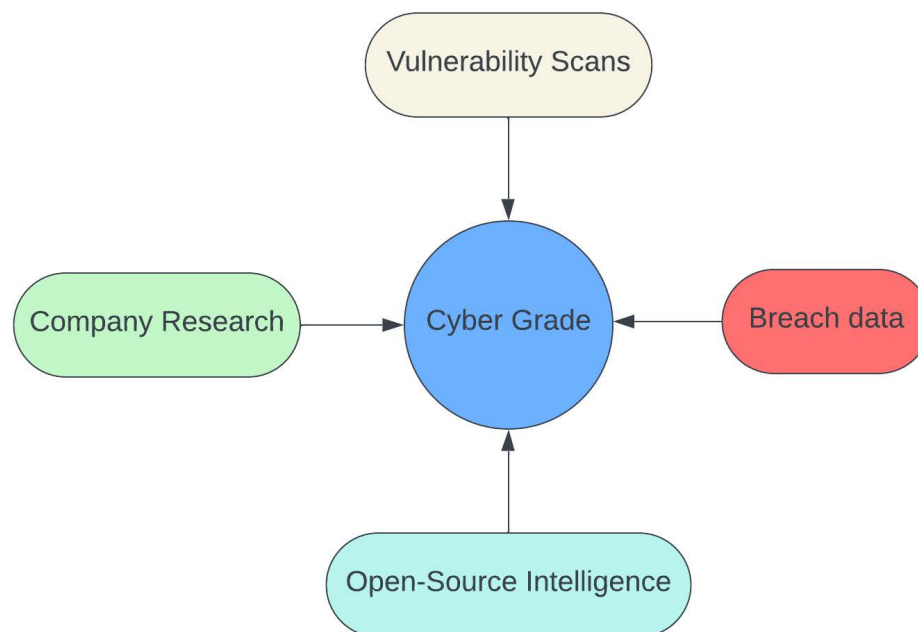
Breached Credentials - Breached credentials are usernames and passwords that have been stolen from a data breach. This type of data breach can happen when a company's security is compromised, and hackers are able to access sensitive information, such as user login credentials.

Look-a-Like Domains - A look-a-like domain is a domain name that is similar to a legitimate domain name but with one or more small changes. These changes can be in the spelling of the domain name, the order of the letters, or the addition of a hyphen or other character. Look-a-like domains are often used in phishing attacks. In a phishing attack, the attacker sends an email that appears to be from a legitimate company, such as a bank or credit card company. The email will often contain a link that, when clicked, will take the victim to a look-a-like domain that is controlled by the attacker.



Appendix B: Cyber Grade Explained

The assigned cybersecurity grade by Elliott Davis team is an assessment of the Company's external presence at a specific point in time. It considers various factors and combines qualitative and quantitative analysis of findings from network vulnerability scanning and open-source intelligence research. The assessment considers the Company's size and industry, allowing Elliott Davis cybersecurity consultants to generate a grade that benchmarks it against similar organizations.





Appendix C: Data Sources for the Assessment

The Common Vulnerability Scoring System (CVSS) - Software, hardware and firmware vulnerabilities pose a critical risk to any organization operating a computer network, and can be difficult to categorize and mitigate. The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, as well as a textual representation of that score. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes.

DeHashed - DeHashed is a hacked-database search-engine. A user can search for their e-mail address or their company's domain and find out if any of their e-mail account's passwords have been breached.

DNS Dumpster - DNS Dumpster is a domain research tool that can be used to perform DNS reconnaissance on a target domain. It can be used to find subdomains, MX records, web application firewall detection and more fingerprinting and lookups.

DNSTwist - DNSTwist is tool that is used to discover look alike domains, typosquatting, and other methods of creating look-alike domains for the purpose of tricking users into visiting them. Discovering look-alike domains can allow an organization to be aware of others that maybe trying to abuse their brand or be preparing to phish them.

Tenable Nessus - Tenable Nessus is a vulnerability scanner that helps identify vulnerabilities within IT infrastructure. It is a remote scanner, which means that it can scan devices without having to be installed on them. Tenable Nessus uses a variety of methods to scan for vulnerabilities, including port scanning, service fingerprinting, and vulnerability checks.

Qualys SSL Labs - A free online service that provides comprehensive analysis of SSL/TLS configurations on web servers. The service analyzes a wide range of factors, including the supported protocols, cipher strength, and certificate health. This information can be used to identify potential security vulnerabilities and improve the overall security of a web server. The Qualys SSL Labs rating system is based on a scale of A to F. A rating of A indicates that the web server is configured securely, while a rating of F indicates that the web server is vulnerable to a number of security threats. The rating is updated automatically whenever there is a change to the web server's configuration."

Shodan - Shodan is a search engine that lets users search for open services on IP addresses or ASNs that are searched for. Shodan is also capable of discovering known vulnerabilities that may be present on a certain service.

Wayback Machine - The Wayback Machine is a digital archive of the World Wide Web founded by the Internet Archive, a nonprofit based in San Francisco, California. The Wayback machine allows users to go see how websites looked in the past, changes that were made, and what web pages are still being maintained. This data can also expose pages that may not have originally meant to be public.

Urlscan.io - URLScan.io is a free service that scans and analyzes websites. It does this by submitting a URL to an automated process that browses to the URL like a regular user and records the activity that this page navigation creates. This includes the domains and IPs contacted, the resources (JavaScript, CSS, etc.) requested from those domains, as well as additional information about the page itself. URLScan.io will also take a screenshot of the page, record the DOM content, JavaScript global variables, cookies created by the page, and a myriad of other observations. If the site is targeting the users of one of the more than 900 brands tracked by URLScan.io, it will be highlighted as potentially malicious in the scan results.