



CEOIndustries, Inc.

Penetration Test Report

Critical Role Productions, LLC

September 25, 2023

Critical Role Productions, LLC

3727 W Magnolia Blvd.
#817
Burbank, CA 91505
United States of America

Tel: 1-913-649-1364
Email: info@critrole.com
Web: <https://critrole.com>

Table of Contents

Executive Summary and Overview	1
Summary of Results	2
Attack Narrative	3
Footprinting With Google	3
Incorporation and Business Structure	3
Footprinting with WHOIS and DNS Interrogation	7
Screenshots	
Recommendations	22
Appendix A: Resources	23



Executive Summary and Overview

CEO Industries, Inc. (“CEO Industries”) was contracted by Critical Role Productions, LLC (“Critical Role”) to conduct a black-box penetration test in order to determine the company’s potential exposure to a targeted attack. Critical Role is a multimedia entertainment production company incorporated in 2015 by the members of the creator-owned streaming shows. The main streaming show is a weekly livestream that uses roleplaying game mechanics to explore and develop stories designed to provide an exciting escape from reality and change reality for the better. Critical Role is committed to ensuring that their produced content maintains its confidentiality, integrity, and availability.

All activities were conducted in a manner that simulated a malicious actor engaged in the beginning stages of reconnaissance to build up an attack against Critical Role with the goals of:

- Assessing the ability of a remote attacker to penetrate Critical Role’s defenses simply by searching publicly available information with no internal knowledge of Critical Role’s systems or architecture.
- Determining the likelihood of a security breach based on the types and amount of information a passive actor could obtain, including:
 - Confidential and Personally Identifiable Information (PII) such as trade secrets, financial information, or confidential assets
 - Internal infrastructure and vulnerabilities of Critical Role’s information systems

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have. The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 (<http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf>) with all tests and actions being conducted in a passive and nonintrusive manner.



Summary of Results

Initial reconnaissance of the Critical Role network resulted in mining and accumulating data and information specific to Critical Role and its Internet resources. The results provided us with a vast amount of data that could potentially be used in future, more active and intrusive, stages of pentesting for the company. An examination of Critical Role's main website led to accessible corporate information such as its business registration, subsidiaries, affiliates, trademark filings, etc. After creating a list identifying such entities and associations, it was simple to delve deeper to obtain information regarding the company's business operations.

An examination of the business operations then gave us access to a list of executives and employees, along with their pictures, titles, roles, active social media accounts, and a host of other information. After a closer examination, we determined that despite possessing so much information about the company and its employees, because Critical Role does not own its IP domain (having two IP addresses) or DNS server, there is not a huge risk of an actor gaining access to the company's internal network at this stage. Social engineering and active attacks such as SQL injections, brute force password attempts, and perhaps physical access to the headquarters would be needed to determine the true security of the network and security systems.

We recommend additional, active black-box testing as well as perhaps a minimal white-box assessment, in order to identify any vulnerabilities that could be taken advantage of at the next level of attacks/testing.



Attack Narrative

Footprinting With Google

For the purposes of this assessment, Critical Role provided minimal information outside of the organizational domain name: critrole.com. The intent was to closely simulate an adversary without any internal information. To avoid targeting systems that were both owned and not owned by Critical Role, there were no active attacks conducted.

In an attempt to gather as much information as possible to identify the potential attack surface, we first examine Critical Role's website: <https://critrole.com>. By using both simple and advanced Google searches with operators I was able to gather the necessary basic company information needed to proceed with a more active attack. Resources and tools used have been listed in Appendix A – Resources.

Incorporation and Business Structure:

Main Company:	Critical Role Productions, LLC (alias "Critical Role") Status: Active and in Good Standing Incorporated In: 2015 State of Incorporation: California, USA Type: Privately Held Limited Liability Company Headquarters Address: 3727 W Magnolia Blvd #817, Burbank, CA 91505 Number of Employees: Approximately 40 Website: https://critrole.com
Other Subsidiaries/Affiliates:	Critical Role Foundation Status: Active and in Good Standing TaxID: 82-2787844 Incorporated In: 2019 State of Incorporation: Delaware, USA Type: 501(c)3 Nonprofit Organization Headquarters Address: 2025 North Lincoln Street, Burbank, CA 91504 Email: info@criticalrolefoundation.org
	Critical Role LLC Status: Active and in Good Standing Incorporated In: 2020 State of Incorporation: California, USA Type: Privately Held Limited Liability Company Key Principle: Kyle Shire Headquarters Address: 2025 North Lincoln Street, Burbank, CA 91504



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

	<p>Darrington Press LLC Status: Active and in Good Standing Incorporated In: 2020 State of Incorporation: California, USA Type: Privately Held Limited Liability Company Key Principles: Ivan Van Norman and Matthew Mercer Headquarters Address: 2025 North Lincoln Street, Burbank, CA 91504</p> <p>CR Real Estate Holdings LLC Status: Active and in Good Standing Incorporated In: 2022 State of Incorporation: California, USA Type: Privately Held Limited Liability Company Headquarters Address: 2025 North Lincoln Street, Burbank, CA 91504</p>
Executives and Employees:	<ul style="list-style-type: none">- Liam O'Brien → co-founder, cast member, executive producer of The Legend of Vox Machina animated series on Amazon Prime- Marisha Ray → Creative Director, cast member, executive producer of The Legend of Vox Machina animated series on Amazon Prime- Sam Riegel → co-founder, cast member, executive producer of The Legend of Vox Machina animated series on Amazon Prime- Travis Willingham → Chief Executive Officer, cast member, and executive producer of The Legend of Vox Machina animated series on Amazon Prime- Taliesin Jaffe → co-founder, cast member, executive producer of The Legend of Vox Machina animated series on Amazon Prime- Ashley Johnson → President of the Critical Role Foundation, cast member, and executive producer of The Legend of Vox Machina animated series on Amazon Prime- Matthew Mercer → Chief Creative Officer, cast member, and executive producer of The Legend of Vox Machina animated series on Amazon Prime- Laura Bailey → co-founder, cast member, and executive producer of The Legend of Vox Machina animated series on Amazon Prime- Ed Lopez → Chief Operating Officer acts in the role of (but not named) VP of Strategy and Operations being responsible for product strategy, lifecycle, and P&L for Alpha, subscriptions, content management, usability/beta testing, engineering, and quality assurance- Rachel Romero → SVP of Marketing and board member of Critical Role Foundation – consumer marketing,



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

	<p>promotion efforts, large-scale digital content distribution, online/offline events, mobile and OTT apps, and eCommerce, social media marketing campaigns, public relations</p> <ul style="list-style-type: none">- Ben Van Der Fluit → SVP of Business & Content Development to accelerate growth beyond the screen into new mediums and ventures.- Mark Koro → Board member of Critical Role Foundation- Aaron Monroy → Art Director- Nadia Dilbert → Director, Consumer Products & Project Manager, Soft Lines & Hard Goods- Allyson De Simone → Director, Procurement- Brittney Austin → Senior Manager, Marketing- Surena Marie → Manager, Marketing & Community- Jennifer Veloso → Customer Services Representative- Bryn Hubbard → Post Production Coordinator- Niki Chi → Online Operations Coordinator- Nicole Yonan → Marketing Coordinator- Max Schapiro → Editor- Jordyn Torrence → Graphic Designer- Ashleigh Fell → Senior Project Manager- Maxwell James → Senior Producer- Ashley Middlebrook → Producer- Vinnie Singh → Head of Production- Tal Levitas → Supervisor, Post Production- Dolores Verdiell → Contract Designer- Steven Failows → Producer- Dani Carr → Lorekeeper- Robert Doig → Agent
Other Information	<p>Public facing sites of interest, such as domains, websites, portals, etc:</p> <p>They have the following social media accounts:</p> <ul style="list-style-type: none">- Facebook- Instagram- Apple iTunes/Podcasts- Linked-In- Pinterest- Twitch



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

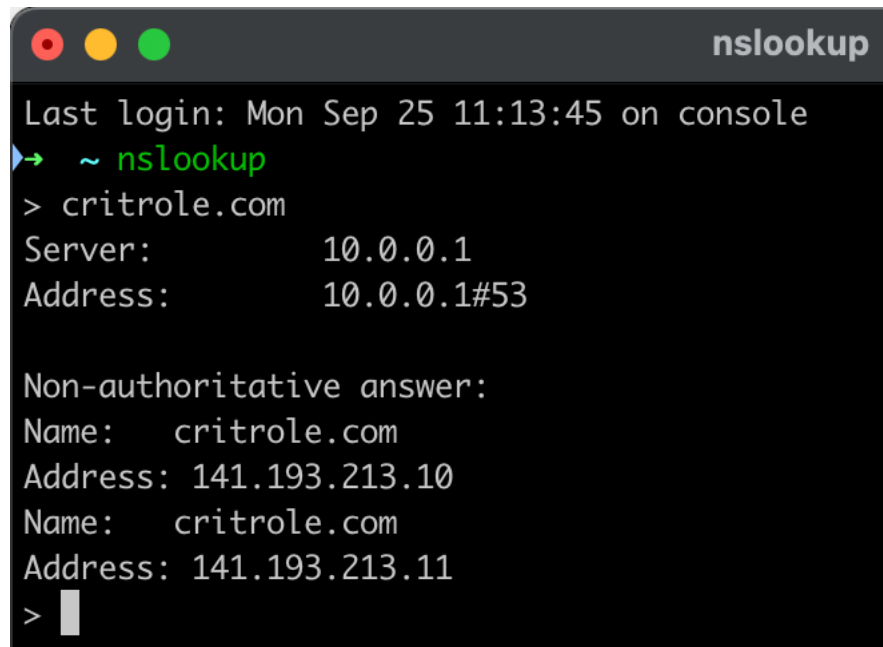
	<ul style="list-style-type: none">- Twitter (“X”)- Youtube- Spotify- Google Podcasts <p>Web Technology Spend in 2023: \$25,968 USD/year.</p> <p>Hired a third-party professional chat moderation service: to pay, train, and properly support moderation efforts on their Twitch channel.</p> <p>Trademarks, copyrights, logos: 8 trademarks found from the United States Patent Trademark Office, under attorney Mark A. Watkins at Vorys, Sater, Seymour and Pease LLP at P.O. Box 2255, Columbus, Ohio 43216.</p>
--	--



Footprinting with WHOIS and DNS Interrogation

Below, we have provided screenshots of our command line searches using NSLookup, WHOIS, and DNS Interrogation. At the end of this Section, there is a summary of our findings.

NSLookup for critrole.com:



```
nslookup
Last login: Mon Sep 25 11:13:45 on console
~ nslookup
> critrole.com
Server:          10.0.0.1
Address:         10.0.0.1#53

Non-authoritative answer:
Name:   critrole.com
Address: 141.193.213.10
Name:   critrole.com
Address: 141.193.213.11
> 
```

Figure 1 – Information gathering for critrole.com reveals two IP addresses.



NSLookup Type SOA for critrole.com:

```
> set type=SOA
> critrole.com
Server:          10.0.0.1
Address:         10.0.0.1#53

Non-authoritative answer:
critrole.com
      origin = carter.ns.cloudflare.com
      mail addr = dns.cloudflare.com
      serial = 2307583543
      refresh = 10000
      retry = 2400
      expire = 604800
      minimum = 3600

Authoritative answers can be found from:
> server carter.ns.cloudflare.com
Default server: carter.ns.cloudflare.com
Address: 172.64.33.80#53
Default server: carter.ns.cloudflare.com
Address: 108.162.193.80#53
Default server: carter.ns.cloudflare.com
Address: 173.245.59.80#53
```

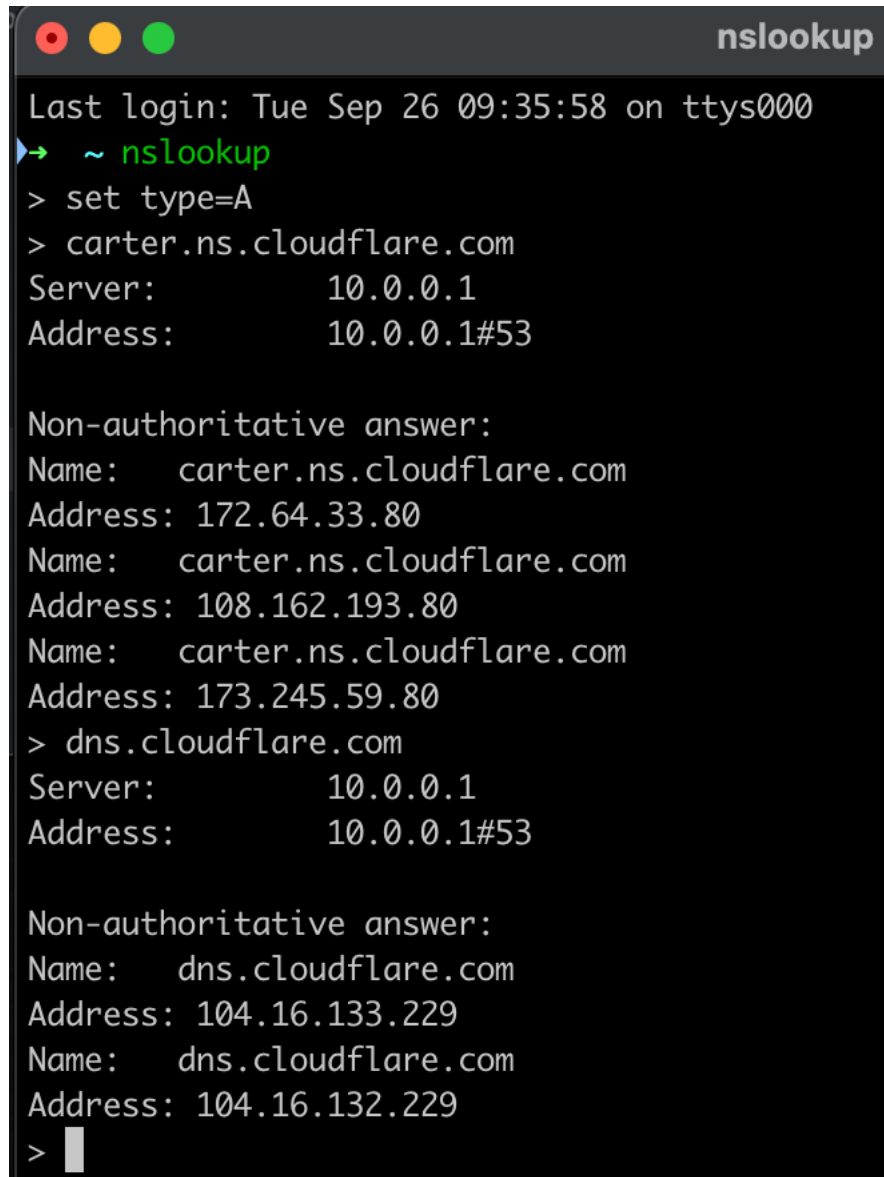
Figure 2 – Information gathering for critrole.com reveals Critical Role does not own their domain or DNS server.

```
> server dns.cloudflare.com
Default server: dns.cloudflare.com
Address: 104.16.133.229#53
Default server: dns.cloudflare.com
Address: 104.16.132.229#53
```

Figure 3 – DNS nameserver search confirms the above.



NSLookup Type A for critrole.com:



```
nslookup
Last login: Tue Sep 26 09:35:58 on ttys000
~ nslookup
> set type=A
> carter.ns.cloudflare.com
Server:          10.0.0.1
Address:         10.0.0.1#53

Non-authoritative answer:
Name:   carter.ns.cloudflare.com
Address: 172.64.33.80
Name:   carter.ns.cloudflare.com
Address: 108.162.193.80
Name:   carter.ns.cloudflare.com
Address: 173.245.59.80
> dns.cloudflare.com
Server:          10.0.0.1
Address:         10.0.0.1#53

Non-authoritative answer:
Name:   dns.cloudflare.com
Address: 104.16.133.229
Name:   dns.cloudflare.com
Address: 104.16.132.229
> 
```

Figure 4 – NSLookup Type A search to confirm.



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

Dig +Trace for critrole.com:

```
ceotten1@M1-MacBook-Pro:~  
→ ~ dig +trace critrole.com  
  
; <> DiG 9.10.6 <> +trace critrole.com  
;; global options: +cmd  
.  
229161 IN NS i.root-servers.net.  
229161 IN NS a.root-servers.net.  
229161 IN NS f.root-servers.net.  
229161 IN NS e.root-servers.net.  
229161 IN NS l.root-servers.net.  
229161 IN NS h.root-servers.net.  
229161 IN NS b.root-servers.net.  
229161 IN NS j.root-servers.net.  
229161 IN NS k.root-servers.net.  
229161 IN NS g.root-servers.net.  
229161 IN NS m.root-servers.net.  
229161 IN NS d.root-servers.net.  
229161 IN NS c.root-servers.net.  
229161 IN RRSIG NS 8 0 518400 20231009050000 202  
30926040000 11019 . qxBQ9qLiP9o72uIhpCWZU31LyeHn0vCwcPej53zZvqgjsBCgW63r+Ue jiJ  
DDctoTG2TsNIq1jF3xFfgHrn5w0Tf0zuasnrxFhQqsSf0ZV/P03U rspE3B9tupmTzbQ1fe/N+FRKGJ  
K06St5h9kUKJJfie/7ABX5fqwJRoLL voiP0VVHp7EsS/TsWw/aUyN1bf4h78LABZ64ggnKKJOXZLJql  
BCc/BDC Na0zad8R1XUC0qa9YWI1i99Fm6Sgl3pvcInqzQdh+gnGqgJSVesFUjD4 rCa/CubUf9r2e/W  
Jkn49zM3tJfseyGsqrw/iwASTf7wv3Et8zLhd9Qtw 6DQF7w==  
;; Received 1097 bytes from 10.0.0.1#53(10.0.0.1) in 22 ms  
  
com. 172800 IN NS e.gtld-servers.net.  
com. 172800 IN NS b.gtld-servers.net.  
com. 172800 IN NS a.gtld-servers.net.  
com. 172800 IN NS d.gtld-servers.net.  
com. 172800 IN NS i.gtld-servers.net.  
com. 172800 IN NS f.gtld-servers.net.  
com. 172800 IN NS j.gtld-servers.net.  
com. 172800 IN NS k.gtld-servers.net.  
com. 172800 IN NS c.gtld-servers.net.  
com. 172800 IN NS g.gtld-servers.net.  
com. 172800 IN NS h.gtld-servers.net.  
com. 172800 IN NS l.gtld-servers.net.  
com. 172800 IN NS m.gtld-servers.net.  
com. 86400 IN DS 30909 8 2 E2D3C916F6DEEAC73294E8  
268FB5885044A833FC5459588F4A9184CF C41A5766  
com. 86400 IN RRSIG DS 8 1 86400 20231009050000 2023  
0926040000 11019 . b5nT6zFilbldu8iHwLNndfEmDyLm06sK+XcWibagEgJ03kIYXftfFRc3 orSC  
4/cipWjbXeL0eEESFCf/Fs3sN4V8xAh+0gDPLybMiD1N7rXnlz6n rimAnx1YxpySzSg05W7gUJDb2AC  
0sGc6vA0GDQBx2CBYnyzxjmCEMBQH Uik55I+69h4eUw/+2iBJ5lvtklEkz3c0jpi6UOT7W/t0mCmidt  
V5N02U u/xxYYwVkvfGJlctyMBfH1SzDVESzdPqV0z+g2ZFLi6Hsy5HABhifVDq pinVizBamLSLujJP  
VTgOR6I0y6k+gpZVDhe/g+ecPzxv1nr1cXnte8kY 6/oJ3A==
```

Figure 5 – Dig +Trace search to confirm IP Addresses and lack of ownership.



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

```
;; Received 1172 bytes from 192.203.230.10#53(e.root-servers.net) in 22 ms

critrole.com.          172800  IN      NS      cheryl.ns.cloudflare.com.
critrole.com.          172800  IN      NS      carter.ns.cloudflare.com.
CK0P0JMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q2D6NI4I7EQH8NA3
0NS61048UL8G5  NS SOA RRSIG DNSKEY NSEC3PARAM
CK0P0JMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 8 2 86400 20231001042
431 20230924031431 4459 com. CYfdurJJWFTcayIwTCeute74buaGrR1BnrZ+pcsTNKjfLENKizi
CLW6w S9RVwi/yAUoRoYl30BL0ymN2xafBrJhgotqhYYSjX2Ap9jeKCjz32e8m 7NCR3L0zrA9ttlITW
Z36U7mU59jp8DxHovnGGK0Hli1HiJQDjA9lnyd6 MtPVUbPGI+FnhfLr1St5y2w2Rd2/wpkPCYP9+bD/
2mgtNQ==
A4N0MKH5GLRDNC78LB8APEV6SH0NS4NS.com. 86400 IN NSEC3 1 1 0 - A4N0PT66403M2A9LJTG
2TQC8QQRI8V1I  NS DS RRSIG
A4N0MKH5GLRDNC78LB8APEV6SH0NS4NS.com. 86400 IN RRSIG NSEC3 8 2 86400 20230930054
444 20230923043444 4459 com. QfuhHJ8t4jJggvB2zDc0eq+8bwq+iF0Y5x0++QSCcYcUjb35QYE
9rYr6 p6up08pj0AzWsNj1l+TwcTd93t7LYDXIYUxgT/UB9YEn4MAD+QI8e64H U5FjB1GLY00onmrrW
oAwZQ1GyphblJlo3RkR1s+xJOAN7Pj6AbRxxi8H QrlBvaz3dsmpTN1L2HML3/WBnXUYSlvycinLR7Y8
WMvgzQ==
;; Received 910 bytes from 192.41.162.30#53(l.gtld-servers.net) in 59 ms

critrole.com.          300      IN      A        141.193.213.10
critrole.com.          300      IN      A        141.193.213.11
;; Received 73 bytes from 173.245.58.83#53(cheryl.ns.cloudflare.com) in 22 ms

→ ~ █
```

Figure 6 – Cont'd: Dig +Trace search to confirm IP Addresses and lack of ownership.



NSLookup Type NS for critrole.com:

```
ceotten1@M1-MacBook-Pro:~  
→ ~ nslookup -type=ns critrole.com  
Server:      10.0.0.1  
Address:     10.0.0.1#53  
  
Non-authoritative answer:  
critrole.com  nameserver = cheryl.ns.cloudflare.com.  
critrole.com  nameserver = carter.ns.cloudflare.com.  
  
Authoritative answers can be found from:  
carter.ns.cloudflare.com  internet address = 108.162.193.80  
carter.ns.cloudflare.com  internet address = 172.64.33.80  
carter.ns.cloudflare.com  internet address = 173.245.59.80  
cheryl.ns.cloudflare.com  internet address = 173.245.58.83  
cheryl.ns.cloudflare.com  internet address = 108.162.192.83  
cheryl.ns.cloudflare.com  internet address = 172.64.32.83  
carter.ns.cloudflare.com  has AAAA address 2803:f800:50::6ca2:c150  
carter.ns.cloudflare.com  has AAAA address 2a06:98c1:50::ac40:2150  
carter.ns.cloudflare.com  has AAAA address 2606:4700:58::adf5:3b50  
cheryl.ns.cloudflare.com  has AAAA address 2803:f800:50::6ca2:c053  
cheryl.ns.cloudflare.com  has AAAA address 2a06:98c1:50::ac40:2053  
cheryl.ns.cloudflare.com  has AAAA address 2606:4700:50::adf5:3a53  
→ ~ █
```

Figure 7 – NSLookup Type NS confirming that the DNS servers are Cheryl and Carter owned by Cloudflare.



NSLookup Type MX for critrole.com:

```
➔ ~ nslookup -type=mx critrole.com
Server:          10.0.0.1
Address:         10.0.0.1#53

Non-authoritative answer:
critrole.com     mail exchanger = 5 alt1.aspmx.l.google.com.
critrole.com     mail exchanger = 10 alt3.aspmx.l.google.com.
critrole.com     mail exchanger = 5 alt2.aspmx.l.google.com.
critrole.com     mail exchanger = 1 aspmx.l.google.com.
critrole.com     mail exchanger = 10 alt4.aspmx.l.google.com.

Authoritative answers can be found from:
```

Figure 8 – NSLookup Type MX confirming that Critical Role does not own their email server.

NSLookup Type TXT for critrole.com:

```
➔ ~ nslookup
> set type=txt
> critrole.com
Server:          10.0.0.1
Address:         10.0.0.1#53

Non-authoritative answer:
critrole.com     text = "MS=ms83513853"
critrole.com     text = "google-site-verification=W1AeVpCSgjIRTDpaR8stPpjGB1n6oxL3wGSs0JZBWM4"
critrole.com     text = "v=spf1 include:_spf.google.com include:shops.shopify.com include:critrole.com ~all"

Authoritative answers can be found from:
>
```

Figure 9 – NSLookup Type TXT revealing that they use Shopify.



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

IP2Location for critrole.com domains 141.193.213.11 (141.193.213.10 not shown):


IP2LOCATION Home Products ▾ Pricing	
Permalink	https://www.ip2location.com/141.193.213.11
<input checked="" type="checkbox"/> IP Address	141.193.213.11
<input checked="" type="checkbox"/> Country	 United States of America [US]
<input type="checkbox"/> Region	Texas
<input type="checkbox"/> City	Austin
<input type="checkbox"/> Coordinates of City ⓘ	30.271158, -97.741701 (30°16'16"N 97°44'30"W)
<input type="checkbox"/> ISP	WPEngine Inc.
<input type="checkbox"/> Local Time	26 Sep, 2023 10:34 AM (UTC -05:00)
<input type="checkbox"/> Domain	wpengine.com
<input type="checkbox"/> Net Speed	(T1) Data Center/Transit
<input type="checkbox"/> IDD & Area Code	(1) 512
<input type="checkbox"/> ZIP Code	78701
<input type="checkbox"/> Weather Station	Austin (USTX0057)
<input type="checkbox"/> Mobile Carrier	-
<input type="checkbox"/> Mobile Country Code - MCC	-

Figure 10 – IP2Location search reveals the host/owner of Critical Role’s website.



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

<input type="checkbox"/> Mobile Network Code - MNC	-
<input type="checkbox"/> Elevation	147m
<input type="checkbox"/> Usage Type	(DCH) Data Center/Web Hosting/Transit
<input type="checkbox"/> Address Type	Anycast
<input type="checkbox"/> Category	Technology & Computing
<input type="checkbox"/> District	Travis County
<input type="checkbox"/> ASN	AS209242 CloudFlare London LLC
<input type="checkbox"/> Anonymous Proxy	Yes
<input type="checkbox"/> Proxy Type	PUB
<input type="checkbox"/> Proxy ASN	AS209242
<input type="checkbox"/> Threat	BOTNET
<input type="checkbox"/> Last Seen	10 ago
<input type="checkbox"/> Provider	-
Olson Time Zone	America/Chicago

Figure 11 – Cont'd: IP2Location search reveals the host/owner of Critical Role's website.



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

U.S. Patent and Trademark Office Search for Critical Role trademarks:

Trademark registrations ⓘ



MARK TEXT	IMAGE	REGISTER	NICE CLASSIFICATIONS	REGISTRATION DATE	EXPIRY DATE
MIGHTY NEIN	MIGHTY NEIN	United States Patent and Trademark Office	21	2021-06-01	details
MIGHTY NEIN	MIGHTY NEIN	United States Patent and Trademark Office	9, 16, 25, 28, 38, 41	2020-12-22	details
		United States Patent and Trademark Office	16, 25, 28, 41	2020-08-25	details
CRITICAL ROLE	CRITICAL ROLE	United States Patent and Trademark Office	16, 21, 25, 28, 38, 41	2020-08-11	details
VOX MACHINA	VOX MACHINA	United States Patent and Trademark Office	9, 16, 21, 25, 28, 38, 41	2020-08-11	details
HOW DO YOU WANT TO DO THIS?	How do you want to do this?	United States Patent and Trademark Office	25, 41	2018-12-04	details
CRITICAL ROLE		United States Patent and Trademark Office	25, 41	2017-08-15	details
CRITICAL ROLE	CRITICAL ROLE	United States Patent and Trademark Office	38, 41	2016-03-01	details

Figure 12 – A U.S. Patent search reveals 8 trademarks in the name of Critical Role and their attorney information.



NSLookup for criticalrolefoundation.org:

```
~ nslookup criticalrolefoundation.org
Server:      10.0.0.1
Address:     10.0.0.1#53

Non-authoritative answer:
Name:   criticalrolefoundation.ORG
Address: 143.244.220.150

~ nslookup -type=
unknown query type:
> exit

~ nslookup
> set type=SOA
> criticalrolefoundation.org
Server:      10.0.0.1
Address:     10.0.0.1#53

Non-authoritative answer:
criticalrolefoundation.org
    origin = ns1063.ui-dns.org
    mail addr = hostmaster.1und1.com
    serial = 2017060125
    refresh = 28800
    retry = 7200
    expire = 604800
    minimum = 600

Authoritative answers can be found from:
> exit

~ clear
~ nslookup
> criticalrolefoundation.org
Server:      10.0.0.1
Address:     10.0.0.1#53

Non-authoritative answer:
Name:   criticalrolefoundation.org
Address: 74.208.236.74
> set type=SOA
> criticalrolefoundation.org
Server:      10.0.0.1
Address:     10.0.0.1#53

Non-authoritative answer:
```

Figure 13 – NSLookup for criticalrolefoundation.org revealing that this domain is owned by 1&1.



NSLookup for criticalrolefoundation.org – Including Types: SOA, A, TXT and DNS Reverse Lookup:

```
Name: criticalrolefoundation.org
Address: 74.208.236.74
> set type=SOA
> criticalrolefoundation.org
Server: 10.0.0.1
Address: 10.0.0.1#53

Non-authoritative answer:
criticalrolefoundation.org
      origin = ns1063.ui-dns.org
      mail addr = hostmaster.1und1.com
      serial = 2017060125
      refresh = 28800
      retry = 7200
      expire = 604800
      minimum = 600

Authoritative answers can be found from:
> server ns1063.ui-dns.org
Default server: ns1063.ui-dns.org
Address: 217.160.83.63#53
> set type=A
> criticalrolefoundation.org
Server: ns1063.ui-dns.org
Address: 217.160.83.63#53

Name: criticalrolefoundation.org
Address: 74.208.236.74
> set type=txt
> criticalrolefoundation.org
Server: ns1063.ui-dns.org
Address: 217.160.83.63#53

criticalrolefoundation.org      text = "stripe-verification=72cbd6488fc30b7292a4f9c656803ae5be12201efd04d98107e1d8f
fdeea2897"
criticalrolefoundation.org      text = "google-site-verification=08NE9hvGjxiJK37W4PEekmsY0FaRrepGr9yWyYdPymw"
> > ns1063.-dns.org
Server: ns1063.ui-dns.org
Address: 217.160.83.63#53

** server can't find ns1063.ui-dns.org: REFUSED
> █
```

Figure 14 – NSLookup revealing Critical Role Foundation does not own the IP domains or DNS servers.



Dig +Trace for criticalrolefoundation.org:

```
ceotten1@M1-MacBook-Pro:~
➔ ~ dig +trace criticalrolefoundation.org

; <<>> DiG 9.10.6 <<>> +trace criticalrolefoundation.org
;; global options: +cmd

.      214304 IN      NS      a.root-servers.net.
.      214304 IN      NS      c.root-servers.net.
.      214304 IN      NS      b.root-servers.net.
.      214304 IN      NS      m.root-servers.net.
.      214304 IN      NS      h.root-servers.net.
.      214304 IN      NS      k.root-servers.net.
.      214304 IN      NS      i.root-servers.net.
.      214304 IN      NS      g.root-servers.net.
.      214304 IN      NS      e.root-servers.net.
.      214304 IN      NS      f.root-servers.net.
.      214304 IN      NS      l.root-servers.net.
.      214304 IN      NS      j.root-servers.net.
.      214304 IN      NS      d.root-servers.net.
.      247225 IN      RRSIG   NS 8 0 518400 20231009050000 20230926040000 11019 . qxBQ9qLiP9o72uIhpCWZU31LyeHn0vCwcPej53zZvqgjsB
CgW63r+Ue jiJDDctoTG2TsNIq1jF3xFFgHrn5w0TF0zuasnrxFhQqsSf0ZV/P03U rspE3B9tupmTzbQ1fe/N+FRKGJK06St5h9kUKJJfie/7ABX5fqwJRoLL voiP0VVHp7EsS/TsWw/aUyN
1bf4h78LABZ64gggnKKJ0XLJq1BCc/BDC NaOzad8R1XUC0qa9YWI1199Fm6Sgl3pvcInqZQdh+gnGqgJ5VesFUjD4 rCa/CubUf9r2e/WJkn49zM3tJfseyGsqrw/iwASTf7wv3Et8zLhD9Qtw
6DQF7W==
;; Received 1097 bytes from 10.0.0.1#53(10.0.0.1) in 25 ms

org.      172800 IN      NS      a2.org.afiliast-nst.info.
org.      172800 IN      NS      b2.org.afiliast-nst.org.
org.      172800 IN      NS      d0.org.afiliast-nst.org.
org.      172800 IN      NS      c0.org.afiliast-nst.info.
org.      172800 IN      NS      b0.org.afiliast-nst.org.
org.      172800 IN      NS      a0.org.afiliast-nst.info.
org.      86400 IN      DS      26974 8 2 4FEDE294C53F438A158C41D39489CD78A868EB0D8A0AEAFF14745C0D 16E1DE32
org.      86400 IN      RRSIG   DS 8 1 86400 20231009050000 20230926040000 11019 . l8tiGJ0+Ne+EcWgPtUe3DTcXg6khA0DgGroraUSe0lv+0t7
xp75/x6b /b/1v7qP7lFUVGwV/AJDCbK0hhBdxnTTcufmrjL4xUkfWqJg9Y0bq9T l8c1W5Yon9LTbNe+DA7f1HA1Zdlu+ixkD5k3q+4mf2V9A5ohrLIsZ9qk eYcCtREe2sRxiXL4FSFbf7x0
6F9gtj26eIvp95J6x/6w7d3HZsEWmXb E2XAFr/zrCL4pfnC+bRTUICsqcG0fz6Imi6nv40iPjfnz9PLo0VBmzIO xk+VkmFg69zf60fU8+/QcJw8JHRP1jEpEyMzuLIwVLPdEXtbV0h9o0q
+tcgoQ==
;; Received 795 bytes from 192.33.4.12#53(c.root-servers.net) in 44 ms

criticalrolefoundation.org. 3600 IN      NS      ns1040.ui-dns.com.
criticalrolefoundation.org. 3600 IN      NS      ns1063.ui-dns.org.
criticalrolefoundation.org. 3600 IN      NS      ns1076.ui-dns.biz.
criticalrolefoundation.org. 3600 IN      NS      ns1076.ui-dns.de.
gdtpongmpok61u9lvnipqor8lra914t0.org. 3600 IN NSEC3 1 1 0 332539EE7F95C32A GDTREA8KMJ2RNEQEN4M20GJ26KFSUKJ7 NS SOA RRSIG DNSKEY NSEC3PARAM
gdtpongmpok61u9lvnipqor8lra914t0.org. 3600 IN RRSIG NSEC3 8 2 3600 20231017152331 20230926142331 35418 org. mUteXR+R+jBngCe4uPovIADPuLMAC2SE2KIGFRb
6uZZTTY17JNrPb71L 4wG6szgvmQCd7Wk9acc0ylWy7NBzrXHiaoITcqXozZdurFUB/sqNzy2s JLeReszmTi2kQKH/htn1KKrdf30X9x7WP1CcnEPWJAVXe8iHz7FrTFVE CgQ=
1lsrcaqgtqn7qocomaoulsdekp04ens.org. 3600 IN NSEC3 1 1 0 332539EE7F95C32A 1LSTVGCJDC090CPRS7EVEU5B0BQ004KU NS DS RRSIG
1lsrcaqgtqn7qocomaoulsdekp04ens.org. 3600 IN RRSIG NSEC3 8 2 3600 20231016152622 20230925142622 35418 org. gPu/MkP1oASoS9aqIbox003iL887klJ8G2TaLYI
6MUuEg8S782GzKkC0_8vmbD3l1cK0SbFeib72n+7q0lL+ZfE7S7Zv0/BxFlu015lEmaDht3TR0/ ha8B85q4Y13ybC4HkFWoR43lpEWEqezBv0hPC96AFSoMKXjaK+Z+57_8Sq=
```

Figure 15 – Dig +Trace Search for criticalrolefoundation.org confirming the NSLookups.



[IP2Location for criticalrolefoundation.org:](https://www.ip2location.com/)

IP2LOCATION Home Products ▾ Pricing	
Share The Result	
Permalink	https://www.ip2location.com/74.208.236.74
<input checked="" type="checkbox"/> IP Address	74.208.236.74
<input checked="" type="checkbox"/> Country	United States of America [US]
<input type="checkbox"/> Region	Pennsylvania
<input type="checkbox"/> City	Philadelphia
<input type="checkbox"/> Coordinates of City ⓘ	39.962440, -75.199930 (39°57'45"N 75°11'60"W)
<input type="checkbox"/> ISP	IONOS Inc.
<input type="checkbox"/> Local Time	26 Sep, 2023 11:32 AM (UTC -04:00)
<input type="checkbox"/> Domain	ionos.com
<input type="checkbox"/> Net Speed	(T1) Data Center/Transit
<input type="checkbox"/> IDD & Area Code	(1) 215/267/484/610
<input type="checkbox"/> ZIP Code	19103
<input type="checkbox"/> Weather Station	Philadelphia (USPA1276)
<input type="checkbox"/> Mobile Carrier	-
<input type="checkbox"/> Mobile Country Code - MCC	-

Figure 16 – IP2Location search for Critical Role Foundation IP address revealing it is owned by IONOS.



PENETRATION TEST REPORT – CRITICAL ROLE PRODUCTIONS, LLC

<input type="checkbox"/> Elevation	15m
<input type="checkbox"/> Usage Type	(DCH) Data Center/Web Hosting/Transit
<input type="checkbox"/> Address Type	Unicast
<input type="checkbox"/> Category	Data Centers
<input type="checkbox"/> District	Philadelphia County
<input type="checkbox"/> ASN	AS8560 IONOS SE
<input type="checkbox"/> Anonymous Proxy	No
<input type="checkbox"/> Proxy Type	DCH
<input type="checkbox"/> Proxy ASN	-
<input type="checkbox"/> Threat	-
<input type="checkbox"/> Last Seen	24 ago
<input type="checkbox"/> Provider	-
Olson Time Zone	America/New_York

Figure 17 – Cont'd: IP2Location search for Critical Role Foundation IP address revealing it is owned by IONOS.



Recommendations

Because Critical Role does not own its domain or DNS server we did not perform scanning and were thus unable to build a composite that we feel reflects Critical Role's network.

CEOIndustries recommends that this information be used as the basis for an additional, more active and invasive pentest to more accurately assess Critical Role's security vulnerabilities to a threat from an outside actor. It was determined that while these steps would be possible, they would be considered outside the scope of the current engagement.

CEOIndustries, Inc.



Appendix A: Resources

- Critrole.com
- Criticalrolefoundation.com
- BuiltWith → builtwith.com
- OpenCorporates → https://opencorporates.com/companies/us_ca/201512810264
- Linked-In → <https://www.linkedin.com/company/critical-role>
- Dun & Bradstreet, Inc. → www.dnb.com
- California Secretary of State Business → <https://bizfileonline.sos.ca.gov/search/business>
- U.S. Patent and Trademark Office → [https://tsdr.uspto.gov/#caseNumber=86703125&caseSearchType=US APPLICATION&caseType=DEFAULT&searchType=statusSearch](https://tsdr.uspto.gov/#caseNumber=86703125&caseSearchType=US_APPLICATION&caseType=DEFAULT&searchType=statusSearch)

CEO Industries, Inc.