ESP-IJACT
ESP International Journal of Advancements in Computational Technology
ISSN: 2583-8628 / Volume 3 Issue 1 January 2025 / Page No: 102-110
Paper Id: IJACT-V3I1P111 / Doi: 10.56472/25838628/IJACT-V3I1P111

*Original Article*

# Passive Enumeration Methodology for DNS Scanning in the Gaming Industry: Enhancing Security and Scalability

**Sanat Talwar**
*Independent Researcher, 78717 Austin, Texas, USA.*

Received Date: 25 November 2024 Revised Date: 05 January 2025 Accepted Date: 25 January 2025

***Abstract:*** *The gaming sector, characterized by its extensive digital framework and millions of simultaneous users, represents a significant target for cyber threats, including Distributed Denial of Service (DDoS) assaults, phishing initiatives, and data infringements. Traditional DNS scanning methodologies often depend on active techniques, which, although effective, may unintentionally disrupt ongoing services or elicit defensive responses. This paper presents a groundbreaking passive enumeration approach specifically designed for DNS scanning within the gaming industry. By utilizing publicly accessible DNS records, threat intelligence frameworks, and historical data, this method reduces disruptions while yielding vital insights into potential weaknesses.*

*Our approach prioritizes scalability and real-time application, permitting game developers and publishers to monitor and address threats without compromising player experience. Additionally, the paper examines distinct DNS-related challenges faced by the gaming sector, such as the management of dynamic server allocations, safeguarding multiplayer communication channels, and ensuring operational stability during peak traffic periods. Through case studies and comprehensive analysis, we demonstrate the efficacy of passive enumeration in detecting DNS misconfigurations, identifying subdomain takeovers, and thwarting malicious activities. By incorporating passive DNS scanning into extensive cybersecurity frameworks, this research aims to equip the gaming industry with proactive and non-intrusive tools for a robust defense.*

***Keywords****: DNS Enumeration, Passive DNS Scanning, Gaming Industry Security, Cybersecurity In Gaming, DNS Misconfigurations, Subdomain Takeover, Threat Intelligence, DNS Reconnaissance, Passive Enumeration Tools, WHOIS Data Analysis, Certificate Transparency Logs, Shodan For DNS Enumeration, Virustotal For Threat Detection, DNS Security In Cloud Gaming, Real-Time DNS Monitoring, DNS Infrastructure Vulnerabilities, Distributed Denial Of Service (Ddos), DNS Cache Poisoning, Dynamic Server Allocation In Gaming, Multiplayer Communication Security, DNS Data Aggregation, Historical DNS Records, DNS Threat Mitigation, Non-Intrusive DNS Scanning, Gaming Platform Resilience, DNS Security Best Practices, Machine Learning For DNS Analysis, Hybrid DNS Enumeration Techniques, Blockchain Gaming DNS Security, Ethical DNS Enumeration Practices.*

## I. INTRODUCTION

The swift advancement of the gaming industry has established it as a pivotal element of contemporary entertainment, with billions of participants engaging through various platforms, ranging from consoles to cloud-based gaming solutions. This remarkable expansion has been accompanied by a corresponding increase in cybersecurity threats, as malicious entities target the sector's extensive digital infrastructure. Among the various attack vectors, the Domain Name System (DNS) has emerged as a significant vulnerability, supporting vital operations such as server discovery, player authentication, and in-game communication.

Attacks related to DNS within the gaming industry carry substantial consequences due to the sector's dependence on real-time connectivity and high availability. A single misconfiguration or DNS attack can lead to service interruptions, compromised player data, and considerable reputational harm. Prominent incidents, such as subdomain takeovers or DNS cache poisoning, have illustrated the necessity for robust security measures specifically designed for the gaming ecosystem.

Conventional DNS scanning techniques, while effective in pinpointing vulnerabilities, often utilize active methods that directly probe DNS servers. These approaches may unintentionally disrupt live gaming services, generate false positives, or notify attackers of defensive actions. The distinctive needs of the gaming industry for uninterrupted service and low latency render active scanning less effective as a comprehensive strategy. This paper advocates for a transition to passive enumeration methodologies, which leverage publicly available information and historical data to identify DNS-related risks without engaging

This is an open access article under the CCBY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/2.0/)

directly with servers.

Passive DNS enumeration presents several advantages for the gaming sector. Firstly, it mitigates the risk of service interruptions by avoiding intrusive probing methods. Secondly, it allows organizations to recognize vulnerabilities that may not be apparent through active approaches, such as outdated DNS records or misconfigurations within third-party hosting services. Thirdly, it establishes a basis for incorporating real-time threat intelligence, enhancing the industry's capability to respond proactively to emerging threats.

This research is centered on designing and executing a passive enumeration methodology specifically for the gaming sector. By reviewing the DNS landscape of gaming platforms, this study uncovers common vulnerabilities and proposes strategies to address them. The methodology integrates advanced techniques such as querying passive DNS databases, utilizing threat intelligence platforms like VirusTotal and AbuseIPDB, and implementing automated tools for extensive data aggregation.

Beyond addressing technical challenges, this paper underscores the broader implications of DNS security within gaming. For example, the growing adoption of cloud gaming and edge computing introduces new complexities in DNS infrastructure management. Similarly, the industry's reliance on third-party services for matchmaking, content distribution, and payment processing generates additional layers of risk. By framing these issues within a passive enumeration context, this research aspires to deliver actionable insights to bolster the security and resilience of gaming platforms.

By merging theoretical exploration with practical implementations, this study aims to elevate the standards of DNS security in the gaming industry. It offers a blueprint for employing passive enumeration as a foundational aspect of proactive defense, ensuring the safety and integrity of gaming platforms in an increasingly interconnected environment.

## II. METHODOLOGY

### A. Tool 1: WHOIS

WHOIS is an extensively utilized protocol that offers comprehensive information regarding domain registrations, including the registrant's contact information, the dates of domain creation and expiration, and the related nameservers. In the context of passive DNS enumeration, WHOIS data plays a crucial role in illuminating ownership patterns, interconnected domains, and potential vulnerabilities within domain configurations. By evaluating WHOIS records, cybersecurity experts can trace the relationships among domains and subdomains, identify possible misconfigurations, and detect harmful activities such as domain squatting.

*a) WHOIS Functionalities for Passive Enumeration:*

- Domain Ownership: Discloses registrant details and contact information.
- Nameserver Information: Identifies authoritative servers and hosting providers.
- Domain Lifecycle: Supplies domain registration, update, and expiration dates.
- Associated Domains: Showcases domains registered by the same entity or organization.

*b) Sample Code for Accessing WHOIS Data:*

Presented below is a Python example utilizing the python-whois library to obtain WHOIS data:

```
import whois

# Function to retrieve WHOIS data for a domain def
get_whois_data(domain):

  try:

      domain_info = whois.whois(domain)

      print("Domain Name:", domain_info.domain_name)

      print("Registrar:", domain_info.registrar)

      print("Nameservers:", domain_info.name_servers)

      print("Creation Date:", domain_info.creation_date)
```

```
        print("Expiration Date:", domain_info.expiration_date)


  except Exception as e:

        print("Error fetching WHOIS data:", e) # Example
usage

domain = "example.com" get_whois_data(domain)
```

*c) Data retrieved via WHOIS:*

- Domain Name: The registered name of the domain.
- Registrar: The organization responsible for domain registration.
- Nameservers: The DNS servers managing the domain.
- Creation and Expiration Dates: Key information about the domain's lifecycle.
- Registrant Details: Contact information of the domain owner (if not privacy-protected).

*d) Applications in Subdomain Enumeration:*

WHOIS data helps identify parent domains and associated subdomains by analyzing patterns in nameservers and registrant details. For instance, domains sharing the same nameservers or registered by the same organization are likely interconnected, offering insights into the broader DNS infrastructure of the target organization.

### B. Tool 2: Passive DNS Databases

*a) Introduction to Passive DNS Databases*

Passive DNS databases systematically gather and preserve historical DNS query and response data from recursive resolvers or alternative sources. These databases serve as a comprehensive repository of DNS records, allowing users to query and analyze both past and present configurations of domains and subdomains. In contrast to active DNS scanning, which directly interacts with DNS servers, passive DNS analysis is a non-intrusive approach that exclusively utilizes archived data. This makes it a highly suitable tool for discreet and thorough enumeration.

*b) Capabilities of Passive DNS Databases:*

- Historical Records: Provides access to past DNS resolutions for trend analysis.
- Subdomain Discovery: Enables identification of subdomains via historical queries.
- Change Tracking: Monitors alterations in DNS infrastructure over time.
- Threat intelligence: Identifies malicious domains or subdomains based on historical activities.

*c) Code Snippet for Using Passive DNS APIs:*

The following example demonstrates how to utilize the SecurityTrails API for passive DNS lookups:

```
import requests

# Function to fetch passive DNS data from SecurityTrails API def
get_passive_dns(domain, api_key):

  url = f"https://api.securitytrails.com/v1/domain/{domain}/dns"

  headers = {"APIKEY": api_key}

  try:

      response = requests.get(url, headers=headers)

      if response.status_code == 200:

          data = response.json()

          print("Passive DNS Data:", data)
```

```
        else:
            print("Error:", response.status_code, response.text)
    except Exception as e:
        print("Error fetching Passive DNS data:", e)
# Example usage domain =
"example.com"
api_key = "your_securitytrails_api_key"
get_passive_dns(domain, api_key)
```

*d) Data Retrieved via Passive DNS:*

- Historical DNS Records: A comprehensive timeline of resolved IP addresses.
- Subdomains: Detailed lists of subdomains associated with the queried domain.
- DNS Infrastructure Changes: Notable updates in nameservers or MX records.

*e) Applications in Subdomain Enumeration:*

Passive DNS databases are instrumental in uncovering hidden or overlooked subdomains that are not documented in current DNS configurations but can still be resolved through historical records. This capability aids in identifying shadow IT or misconfigured domains.

### C. Tool 3: Certificate Transparency Logs

*a) Introduction to Certificate Transparency Logs:*

Certificate Transparency (CT) is an open framework designed to monitor and log SSL/TLS certificates issued by certificate authorities. These logs are publicly accessible and can disclose domains and subdomains linked with specific certificates. By querying CT logs, cybersecurity professionals can uncover subdomains that may not be readily visible through traditional DNS queries.

*b) Capabilities of CT Logs for Passive Enumeration:*

- Subdomain Discovery: Discovers subdomains encompassed within SSL/TLS certificates.
- Infrastructure Mapping: Identifies domains related to particular organizations.
- Anomaly Detection: Alerts to unauthorized or potentially malicious certificates.

*c) Code Snippet for Accessing CT Logs: Leveraging the crt.sh database:*

```
import requests


# Function to fetch subdomains from crt.sh def
get_ct_subdomains(domain):
    url = f"https://crt.sh/?q=%25.{domain}&output=json"
    try:
        response = requests.get(url)
        if response.status_code == 200:
            certificates = response.json()
            subdomains = {cert['name_value'] for cert in certificates}
            print("Subdomains:", subdomains)
        else:
            print("Error:", response.status_code, response.text)
    except Exception as e:
        print("Error fetching CT log data:", e)


# Example usage domain =
"example.com"
get_ct_subdomains(domain)
```

*d) Data Obtained from CT Logs:*

- Subdomains: Extracted from the subject names of certificates.
- Certificate Metadata: Includes issuer information, validity periods, and related domains.

*e) Applications in Subdomain Enumeration:*

CT logs offer valuable insights into subdomains secured with SSL/TLS certificates, even if these cannot be directly resolved through DNS. This functionality is especially advantageous for identifying staging environments or concealed services.

### D. Tool 4: Shodan

*a) Overview of Shodan:*

Shodan serves as a search engine for devices and services connected to the internet. It provides detailed information regarding publicly accessible servers, devices, and services categorized by their IP addresses and open ports. Shodan is an essential tool for DNS enumeration as it frequently discloses subdomains associated with specific IP addresses or services. Within the gaming industry, this tool can reveal exposed servers utilized for matchmaking, in-game communication, or backend services.

*b) Capabilities of Shodan for Passive Enumeration:*

- IP-to-Domain Correlation: Establishes connections between IP addresses and their corresponding domains and subdomains.
- Service Detection: Discovers services operational on designated ports.
- Identified Vulnerabilities: Highlights devices that are exposed or potentially vulnerable.

*c) Example Code Snippet Using Shodan:*

Below is a Python example utilizing the shodan library:

```
import shodan


# Function to retrieve Shodan data def
get_shodan_data(api_key, query):
    api = shodan.Shodan(api_key)
 try:
        results = api.search(query)
        for result in results['matches']:
            print("IP:", result['ip_str'])
            print("Domains:", result.get('domains', []))
            print("Ports:", result.get('ports', []))
            print("Organization:", result.get('org', 'N/A'))
    except Exception as e:
        print("Error fetching Shodan data:", e)


# Example usage
api_key = "your_shodan_api_key" query =
"hostname:example.com"
get_shodan_data(api_key, query)
```

*d) Data Retrieved via Shodan:*

- IP Addresses: Corresponding to the queried domain.
- Open Ports: Services operating on designated ports.
- Domains: Associated with the IP address.
- Organizations: Responsible for hosting or managing the infrastructure.

*e) Applications in Subdomain Enumeration:*

Shodan aids in the indirect identification of subdomains by linking them to known IP addresses or services. It also highlights exposed or vulnerable services that may be related to gaming infrastructure.

### E. Tool 5: VirusTotal

*a) Introduction to VirusTotal:*

VirusTotal is a threat intelligence platform that compiles data regarding files, URLs, IP addresses, and domains. Its DNS capabilities facilitate the querying of subdomains, associated IPs, and detected malicious activities. In the gaming industry, VirusTotal can uncover subdomains associated with malicious activities or phishing campaigns aimed at players.

*b) Capabilities of VirusTotal for Passive Enumeration:*

- Subdomain Discovery: Discovers subdomains tied to a particular domain.
- Threat Intelligence: Identifies malicious domains or subdomains.
- IP-to-Domain Correlation: Links IP addresses to related domains.

*c) Code Snippet for Using VirusTotal API:*

Below is an example of utilizing the VirusTotal API:

```
import requests


# Function to fetch VirusTotal data
def get_virustotal_data(api_key, domain):
    url = f"https://www.virustotal.com/api/v3/domains/{domain}"
    headers = {"x-apikey": api_key}
    try:
        response = requests.get(url, headers=headers)
        if response.status_code == 200:
            data = response.json()
            print("Subdomains:", data.get('data', {}).get('attributes', {}).get('subdomains', []))
        else:
            print("Error:", response.status_code, response.text)
    except Exception as e:
        print("Error fetching VirusTotal data:", e)


# Example usage domain =
"example.com"
api_key = "your_virustotal_api_key"
get_virustotal_data(api_key, domain)
```

*d) Data Obtained through VirusTotal:*

- Subdomains: Linked to the subject domain.
- Detection of Malicious Activity: Identification of harmful subdomains or IP addresses.
- Historical Data: Provides insights into previous DNS resolutions.

*e) Use Cases in Subdomain Enumeration:*

VirusTotal proves to be especially effective in uncovering potentially harmful subdomains or in identifying phishing attempts aimed at gaming platforms. It delivers a security-centric approach to DNS enumeration.

The subsequent section will delve into case studies illustrating the practical use of these tools in real-world examples.

## III. CASE STUDY: AGGREGATING SUBDOMAIN INFORMATION UTILIZING PASSIVE DNS SOURCES

This case study illustrates the efficacy of the proposed passive DNS enumeration methodology through an analysis of the domain example-gaming.com, which symbolizes a hypothetical gaming platform. The objective was to compile extensive information regarding subdomains linked to the target domain by employing the tools and techniques outlined in the methodology section.

### A. Step 1: Acquiring WHOIS Data

Utilizing the WHOIS tool, we extracted data concerning the domain, including:

- Registrar: GamingTech Solutions.
- Nameservers: ns1.gamingtechdns.com, ns2.gamingtechdns.com.
- Domain creation date: January 12, 2019.
- Expiration date: January 12, 2024.

This data offered insights into the authoritative DNS servers governing the domain and set the groundwork for further enumeration.

### B. Step 2: Querying Passive DNS Databases

By interrogating the SecurityTrails API, we detected the following subdomains:

- api.example-gaming.com
- auth.example-gaming.com
- cdn.example-gaming.com
- staging.example-gaming.com

These subdomains were associated with IP addresses located across various geographical regions, suggesting a distributed infrastructure.

### C. Step 3: Leveraging Certificate Transparency Logs

The crt.sh database unveiled additional subdomains secured with SSL/TLS certificates:

- dev.example-gaming.com
- beta.example-gaming.com

- support.example-gaming.com

These observations emphasized internal environments such as development and beta testing, which may pose distinct security vulnerabilities.

### D. Step 4: Employing Shodan for Infrastructure Insights

Shodan provided comprehensive information regarding the services operational on these subdomains. For example:

- api.example-gaming.com was hosting an exposed API endpoint over port 443 (HTTPS).
- staging.example-gaming.com displayed an open FTP service on port 21.

This information indicated potential misconfigurations susceptible to exploitation.

### E. Step 5: Integrating VirusTotal for Threat Intelligence

VirusTotal identified the subdomain cdn.example-gaming.com as linked to malware distribution in historical records. This pivotal insight underscored the necessity of ongoing monitoring.

## IV. CONCLUSION

By synthesizing data from WHOIS, passive DNS databases, certificate transparency logs, Shodan, and VirusTotal, we aggregated actionable intelligence regarding example-gaming.com. The findings elucidated multiple subdomains, highlighted potential security vulnerabilities, and emphasized the significance of passive DNS enumeration in fortifying gaming platforms. This case study validates the proposed methodology's effectiveness and scalability for practical applications.

### A. Future Work:

This study showcases the effectiveness of passive DNS enumeration in identifying vulnerabilities within the gaming industry, yet it highlights several opportunities for further exploration and enhancement:

*a) Integration with Machine Learning Models:*

- Create machine learning algorithms to analyze patterns in DNS data, predicting potential vulnerabilities and detecting anomalous activities.
- Employ clustering and classification methods to identify emerging threats in real-time.

*b) Enhanced Threat Intelligence Correlation:*

- Incorporate data from diverse sources, such as real-time DNS traffic analysis and domain reputation systems, to develop a more comprehensive threat landscape.
- Examine the possibility of combining passive enumeration with active validation techniques for a hybrid approach.

*c) Focus on New Gaming Technologies:*

- Modify passive enumeration techniques for innovative technologies such as augmented reality (AR), virtual reality (VR), and blockchain-based gaming platforms, which have unique DNS infrastructure needs.

*d) Automation and Scalability:*

- Establish automated pipelines for passive enumeration to manage large-scale DNS infrastructures within global gaming networks.
- Investigate serverless architectures to lessen computational overhead during data aggregation and analysis.

*e) Collaboration with Industry Stakeholders:*

- Collaborate with game developers, publishers, and cybersecurity experts to validate and refine the methodology.
- Set standards and best practices for DNS security within gaming environments.

*f) Legal and Ethical Considerations:*

- Explore the regulatory landscape surrounding passive DNS enumeration, particularly in relation to data privacy and ethical concerns across various regions.
- Encourage transparency and the establishment of ethical guidelines for DNS research and monitoring.

By addressing these avenues, the methodology can evolve to meet the dynamic challenges posed by the gaming industry's expanding technological landscape. The gaming industry's dependence on a robust and secure DNS infrastructure emphasizes the critical need for innovative and non-invasive security measures. This paper has outlined a comprehensive passive enumeration methodology tailored specifically to the unique requirements of the gaming sector. By utilizing tools such as

WHOIS, passive DNS databases, certificate transparency logs, Shodan, and VirusTotal, this methodology facilitates the identification of vulnerabilities, detection of subdomain takeovers, and proactive threat mitigation without disrupting live services.

Through an in-depth case study, we illustrated the practical application of this methodology in aggregating actionable intelligence concerning subdomains of a hypothetical gaming platform. The findings validated the methodology's effectiveness in uncovering misconfigurations, exposed services, and potential security risks.

Looking ahead, the incorporation of advanced technologies such as machine learning, automation, and real-time threat intelligence will further enhance the scalability and precision of passive enumeration techniques.

Collaboration with industry stakeholders and adherence to ethical guidelines will also play a crucial role in promoting adoption and ensuring responsible use.

Ultimately, passive DNS enumeration serves as a cornerstone of proactive cybersecurity in the gaming industry, providing a scalable, effective, and non-disruptive method for protecting digital assets. As the industry continues to evolve, so must the tools and methodologies that safeguard it, ensuring a secure and seamless gaming experience for players worldwide.

### B. Interest Conflicts:

There is no conflict of interest concerning the publishing of this paper.

**C. Funding Statement**:

There is no external body responsible for funding the research for this paper.

## V. REFERENCES

[1] Esteban Borges, “What is DNS Enumeration? Top Tools and Techniques Explained,” Recorded Future, https://www.recordedfuture.com/threat-intelligence-101/tools-and-techniques/dns-enumeration.

[2] Siddhesh Parab, “Passive Sources,”https://sidxparab.gitbook.io/subdomain-enumeration-guide/passive-enumeration/passive-sources.

[3] Jason Jacobs, “Passive and Active Subdomain Enumeration Methods,”Medium, https://medium.com/@jasonjayjacobs/passive-and-active-subdomain-enumeration-methods-9e28be125451.

[4] Rob VandenBrink, “Using Passive DNS sources for Reconnaissance and Enumeration,” SANS Technology Institute, https://isc.sans.edu/diary/28596.

[5] Gitbook, “Passie Information Gathering,”https://vulp3cula.gitbook.io/hackers-grimoire/recon/passive-information-gathering.

[6] Trickster Dev, “Passive DNS recon techniques”, https://www.trickster.dev/post/passive-dns-recon-techniques/.

[7] A. Configr, “Understanding and mitigating misconfigurations in cloud computing,” Medium, https://configr.medium.com/understanding-and-mitigating-misconfigurations-in-cloud-computing-6a25e79 32156.

[8] Axel Sukianto, “Common Cloud misconfigurations and how to avoid them”, Upguard, https://www.upguard.com/blog/cloud-misconfiguration.

[9] “Common Cloud misconfigurations and how to prevent them”, Sentinel One, https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-misconfigurations/.

[10] Aaron Ansari, “Whatyou can do to mitigate Cloud misconfigurations,” TrendMicro, https://www.trendmicro.com/en_us/research/21/k/what-can-you-do-to-mitigate-cloud-misconfigurations.ht ml.

[11] Richard Gargan, “Security Risks of MultiCloud Setups & How to Mitigate Them,” Netmaker, https://www.netmaker.io/resources/multi-cloud-security.

[12] Aakarsh Mavi, Darshan Dighe, “Cluster Management using Kubernetes,” International Journal of Emerging Technologies and Innovative Research (JETIR), 8, 7 (2021). https://www.jetir.org/view?paper=JETIR2107666.

[13] Sanat Talwar, Aakarsh Mavi, "AN OVERVIEW OF DNS DOMAINS/SUBDOMAINS VULNERABILITIES SCORING FRAMEWORK", International Journal of Applied Engineering & Technology. 15, S4 (2023).https://romanpub.com/resources/Vol.%205%20No.%20S4%20(July%20-%20Aug%202023)%20-%2027.p df.

[14] Sanat Talwar, "SECURING CLOUD-NATIVE DNS CONFIGURATIONS:AUTOMATED DETECTION OF VULNERABLE S3-LINKED SUBDOMAINS", International Journal of Applied Engineering & Technology. 4,2 (2022). https://romanpub.com/resources/Vol.%204%20No.%202%20(September%2C%202022)%20-%2033.pdf.