National College of Ireland

How can threat intelligence gathered from the dark web enhance organizational vulnerability management process?

MSc Research Project
MSc in Cybersecurity

Neha Sawant
Student ID: x23267291

School of Computing
National College of Ireland

Supervisor: Kamil Mahajan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Neha Dnyandeo Sawant
Student ID:	X23267291
Programme:	Msc in Cybersecurity **Year:** 2024-25
Module:	MSc (Research) Practicum/Internship Part 2
Supervisor:	Kamil Mahajan
Submission Due Date:	15th September 2025
Project Title:	How can threat intelligence gathered from the dark web enhance organizational vulnerability management process?
Word Count:	6817 **Page Count** 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Neha Dnyandeo Sawant

Date: 12-09-2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

How can threat intelligence gathered from the dark web enhance organizational vulnerability management process?

Neha Sawant
x23267291

Abstract

In the age of the digital world there is rise of cyberattacks where multiple organizations are targeted by various threat actors. It is important for every organization to have a very strong cybersecurity foundation. Vulnerability management is one of the parts of cybersecurity which helps organizations stay ahead of threats by identifying and fixing weaknesses before attackers can exploit them. This research paper explores research where threat intelligence related to vulnerabilities can be identified and gathered from dark web and can be used to prevent the organization and it can increase the efficiency of vulnerability management.

The purpose of the research paper is to explore and find a proactive solution to prevent cyberattacks by monitoring the dark web. The research discusses various threats which are present on dark web and how monitoring those threats can help to improve the security of the organization. The research paper explores different traditional scanning such as Active Scanning and passive scanning and delves into dark web monitoring methods. The research paper discusses certain limitations for manual dark web monitoring due to the recent circumstances as multiple forums have been blocked and taken down by government agencies.

Keywords: [Dark web monitoring, Vulnerability Management, Zero Day vulnerabilities, Hacker Forums, Malware, Exploit]

1 Introduction

Internet is a superhighway of information which consists of three layers of surface web, deep web and dark web. The surface web is the one which is available to the public through search engines such as Google, yahoo, Firefox and Bing. The Deep web is not directly available as they are not indexed by search engines as these are password protected. They require the user to login using password . Users can still access these using appropriate passwords(Ijraset.com, 2023).

Dark Web:

In 2011, Dark web became famous due to the launch of silk Road, it is an online black market which is known for illegal drug marketplace. It enables internet users to sell and buy products and services anonymously using bitcoin. In 2013, it was shut down by the Federal Bureau of Investigation (FBI). Dark web can be used for legitimate purposes, but it still is the platform of illegal activities such as drug dealing ,human trafficking, arms dealing etc. Dark web is used by multiple threat actors to conduct cyberattacks and there are forums where these threat forums share information and have a conversation(Ijraset.com, 2023).

The dark web requires special attention as it is hidden and anonymous so many cybercriminals operate here, and it can be useful for the researchers to gather information from Dark web to protect the company(Ijraset.com, 2023).
Cybercriminals have used the dark web's anonymity to carry out a number of illegal operations, including buying zero-day vulnerabilities, running C34 servers for botnets and malware exfiltration, and hiring experienced criminals. Advanced Persistent Threat(APT) actors have been responsible for high-profile instances of espionage on significant organizations and nation states, focusing on their digital assets. There are markets which sell ransomware as a service and hacking as a service on the Dark web(Ngo, Marcum and Belshaw, 2023).
So, the main aim of the research is to find the threat intelligence data from the dark web which can be used to prevent organization. This is a proactive technique as it will prevent any future damage to the company .

Vulnerability management :
Vulnerability management is a process which includes identification, classification, remediation and mitigation of the security vulnerabilities. The main components of a vulnerability management system are asset identification of the assets, vulnerability identification, vulnerability assessment, remediation and mitigation, reporting and continuous monitoring. There are multiple frameworks such as NIST Cybersecurity Framework (CSF), ISO/IEC 27001 and OWASP Vulnerability Management(Kotha, 2015).
The main aim of research is to combine dark web monitoring with vulnerability management systems to improve efficiency and proactively secure the organization from cyberattacks.

Cyber Threat Intelligence:
Threat Intelligence is gathering information, processing information and analyzing data to prevent cyber-attacks. These are the data which is acquired from different sources that have been analyzed. Cyber Threat Intelligence provides information about who, what, where, how and when. The sources can be from network event logs, firewall logs, alerts or external. Cyber Threat Intelligence includes Open-Source Intelligence (OSINT), Social Media Intelligence (SOCMINT), Measurement and Signature Intelligence (MASINT), Human Intelligence (HUMINT), and Technical Intelligence (TECHINT) (Basheer and Alkhatib, 2021).

2 Related Work

2.1 Dark Web Threat Intelligence

There is a research paper which performed a review on previous hacker community studies, as past work provides context and helps guide the formulation of this research. The 3 types of hacker community were discussed such as hacker forums, carding shops and hacker Internet-Relay-Chat (IRC) (Benjamin et al., 2015).

There are different types of products and threats such as Tools, Services, exposed credentials, insider threats, hacked information, vulnerability information etc. on Dark web.

Tools:

Tools such as exploit kits and zero-day vulnerabilities which can be used to deliver different payloads and gain access to the systems are sold on dark web. Viruses, worms and trojans are also sold with a unique technique where the sellers use packers, binders etc. to provide the users with different and unique malware that bypasses the detection. Examples of exploit kits are Icepack, Nuclear, Luckysploit and Crimepack. Zero-day exploits can be very profitable for the sellers as they are sold at an expensive price. These sales are done privately and advertised only in some areas(Burgess, 2017).

Services:

The service offered is provided by hackers and cyber-crime groups which offer services such as DDos (Distributed Denial of Service), spam services, spyware etc. Hackers are renting botnets as a service to the buyers. These services are rented on an hourly, daily, weekly, and monthly basis by the buyers depending on their needs. There are even services where hackers and hacker groups offer to loan their skills to customers who have a specific target they want to hack but don't have skills to carry it out themselves(Burgess, 2017).

Exposed Credentials:

Credentials are exposed on dark web which are part of data breaches, credential stuffing etc. These credentials are used by attackers to gain access to the account and can be used for further attacks on a target or organization. If the organization does not have proper and strong password policies then this can be very harmful as attackers can snoop and enter into the network using legitimate credentials . They can hide in plain sight(Bitsight, 2025).

Insider Threats:

These are the threats which are inside from the organization . It may be an old or former employee , partner , vendor which has access to sensitive data. It may be even current working employee who is not happy with organization and can sell sensitive information on dark web. They are very harmful threats as they already have access to the organization's data(Bitsight, 2025).

Hacked Accounts:

Hacked accounts are the accounts which are commonly sold on dark web . These accounts include financial accounts, email, social media and other online accounts. Many hacked corporate accounts are also sold here which provide access to the organization data to the buyer(Bitsight, 2025).

Vulnerability information:

Many software vulnerabilities are discussed on dark web. If a vulnerability is officially reported and patch is released the vulnerability report is not published. This vulnerability, which is not yet officially published can be found on dark web as these attackers try to exploit this vulnerability. These vulnerabilities are discussed in multiple hackers and dark web forums(Bitsight, 2025).

Hacker Forums are forums which support cybercriminal activity. They share knowledge and tools , malware sample , source tools etc. here. There are tutorials which enable the readers to launch attacks such as denial of service attacks, SQL injections etc. (Benjamin et al., 2015).

These forums can carry malware which is intended to infect visitors, and they can attempt to exploit the web browser vulnerabilities. Hacker communities can also exist as Internet Relay chat(IRC) channels. IRC exists on a separate protocol and can support real-time, synchronous chat among thousands of users simultaneously. Hackers commonly use IRC for real-time communication, as forums are more slow-paced (Benjamin et al., 2015).

These hacker forums can be a great source of information for researchers and analysts to find if there is any discussion of vulnerability exploitation and if there is any new vulnerability which can be exploited (Benjamin et al., 2015).

To protect from all these threats, it is important for an organization to monitor dark web. Information on exposed credentials and hacked accounts can be useful for an organization so that they can act on these accounts by deleting and monitoring them. Targeted attacks can help identify unknown threats to the organization. By monitoring insider threats organizations can identify insider risks and prevent further attacks. By monitoring vulnerability information, companies can monitor the software and services which are exploited till the patch is released(Bitsight, 2025).

In on research, a researcher presented an approach that integrates information from social networks on Surface, Deep, and Dark Webs. This system matches terms from twitter, discussion on forums where they are using text mining methods which identify generate warnings about anticipated or current cyber threats(Sapienza et al., 2017).

2.2 Vulnerability Management using Scanners and tools(Nessus)

As per the research paper , the vulnerabilities and complexity of vulnerabilities are increasing which has made it very difficult for manual identification and remediation processes .As per National Vulnerability Database (NVD),the vulnerabilities have grown significantly, which has increased the use of automated tools for vulnerability scanning. The research has suggested that automation has reduced human error and have increased the speed of threat detection (Baskaran et al., 2024).

Many studies on vulnerability management say that organizations need flexible systems to help them decide which security weaknesses to fix first. The tools use a standard scoring system like CVSS (Common Vulnerability Scoring System) to rank how risky vulnerability is. But while CVSS is popular, it doesn't always consider what matters most for a specific company. For example, a hospital and a bank might face very different threats, so a one-size-fits-all score doesn't work well (Baskaran et al., 2024).

While automated vulnerability assessment tools exist, there is a lack of literature examining how to create exploit-vulnerability links using vulnerability text data. This prevents a holistic perspective on what exploits can target vulnerabilities and the development of advanced vulnerability severity metrics(Samtani, Chai and Chen, 2021).

Organizations often use assessment tools such as Nessus to automatically identify, categorize, and prioritize tens of thousands of vulnerabilities, including web application issues, unpatched technology, and default login (Bennouk *et al.*, 2024).

Each vulnerability in prevailing scanners provides description-based metadata such as name, synopsis, description, class (family) name, CVE, published and updated dates, and a list of vulnerable system versions.

Additionally, every vulnerability includes risk details such as CVSS score and risk factor. The vulnerability name is the only non-null value which appears in all records. Cybersecurity professionals formulate each name to summarize its key aspects such as the system, version, operations etc. CVSS is essential for prioritization and risk management.

Right now, security tools like vulnerability scanners and CVSS scores help to find and rate weaknesses in devices and software. But they don't tell which ones hackers are actually talking about or using in real life. On the Dark Web, hackers often share tools and tips to exploit certain vulnerabilities and that info is super valuable. If the names of known vulnerabilities can be matched with what hackers are discussing online, organization can know which ones are truly dangerous. No known study has yet explored how the textual content of vulnerability names like those in CVE entries could be leveraged to identify matching exploit discussions in these underground communities. By fusing structured vulnerability data with unstructured exploit chatter, security teams could develop smarter prioritization metrics that reflect not just technical severity but actual attacker interest and exploit availability. This approach would enable organizations to respond more proactively to emerging threats and allocate resources where they matter most. (Samtani, Chai and Chen, 2021).

2.3 Proactive Vulnerability Assessment

Organizations are currently just dependent on CVSS scores which are provided by The National Institute of Science and Technology that maintains a comprehensive list of publicly disclosed vulnerabilities in the National Vulnerability Database (NVD) to identify systems at risk. There are case studies which showcased the poor correlation between the CVSS score and the likelihood that a vulnerability on a system will be targeted by hackers. So, it is important for organizations to proactively identify vulnerabilities which are actively targeted by hackers. Threat Intelligence collected from Dark web can help identify vulnerabilities which are targeted by hackers and are being actively exploited. The limitation of that paper was identifying the discussions with no vulnerability identifiers (CVE) that are of interest to threat actors are not considered(Nunes, Shakarian and Simari, 2018).

Many organizations are increasingly turning to cyber threat intelligence (CTI) to help prioritize their vulnerabilities, but current CTI processes are often criticized as being reactive to known exploits. One promising data source that can help develop proactive CTI is the vast and ever-evolving Dark Web, especially hacker forums, which contain millions of hacking tools and exploits. Automatically linking the exploits from hacker forums to known vulnerabilities is a hectic task due to the non-natural language content and volume of data. This necessitates novel computational algorithms rooted in artificial intelligence(Samtani, Chai and Chen, 2021).

There is a research paper which performed a review on previous hacker community studies.

These hacker forums can be a great source of information for researchers and analysts to find if there is any discussion of vulnerability exploitation and if there is any new vulnerability which can be exploited(Nunes, Shakarian and Simari, 2018).

3 Research Methodology

This section includes the step-by-step method used for this research. There are three ways vulnerability will be done .The first is active scanning using Nessus , passive scanning using tools such as Shodan.io and Censys.io and the last part of the dark web monitoring threat intelligence gathering are vulnerability management system includes Nessus for the active scanning .

Vulnerability Management:

In this research, vulnerability management procedure was created as well with proper process of finding the scope which included all the updated company servers, assets, network devices etc. In this process different teams should be contacted to collect all the updated asset lists for vulnerability assessment.

A vulnerability policy was created which included detailed roles and responsibilities of different teams such as Infosec Team, Cloud Service Desk Team, Infra Team, Engineering team and Information Security Manager for the vulnerability management process. Different phases of vulnerability process were defined with proper SLA (Service Level Agreement) for different severity of vulnerabilities detected.

Data Collection:

- Active Scanning: Nessus is the main tool which is going to be used to perform active scanning. In active scanning the Nessus scanner sends the packet to the remote target to provide a snapshot of the network and application. This is then compared with the plugin database to identify if any vulnerabilities are present(Kotha, 2015).
- A host with public Ip address was scanned on Nessus Expert to find vulnerabilities on that. This was done multiple times to get a proper output .After that , the vulnerabilities were shown in the form of report in excel sheet .The excel sheet was extracted from Nessus and a final excel sheet was created with the vulnerabilities.

After performing an active scan Data can be collected in the form of a report where the vulnerabilities would be mentioned with cve details, description and severity.

- Passive Scanning: Passive scanning is the collection of information of the systems, the network and the endpoints. It does not directly interact with these systems .These helps in identifying any software vulnerabilities and monitor the versions as well. It also gives information about the open ports present in the environment. There are multiple tools such as Shodan and Censys which will be used to perform passive scanning(Team, 2024).

Dark Web monitoring:

In this step dark web monitoring will be performed by visiting different dark web forums which give information and have chats about different vulnerabilities and exploit. These forums include details of vulnerability and the way it could be successfully exploited. These forums are updated by the members in the forums with different kinds of exploits. There are few which are always available but there are some which are not always available and can be taken down by the government for security purposes.

Dark web is used by many threat actors to discuss the vulnerabilities and the exploitation of those vulnerabilities. So, it is important to collect intel from the dark web to protect the organization . In this research, dark web threat intelligence is collected through manual exploration and analysis of dark web forums, marketplaces, and paste sites using the Tor browser. The automated crawlers can cause compliance issues by collecting unauthorized data.

Dark web can be visited using TOR .

- TOR : TOR browser is browser which was designed to maintain privacy and anonymity online. It was started by the Naval research Laboratory for private communication. Tor is used by legitimate as well as illegitimate users. The TOR browser has several routers called nodes which are much like going through the layers of an onion, making it difficult to track and identify users. Entry nodes form the first layer of encryption and enable the TOR network. The series of middle nodes fully encrypt web traffic to ensure anonymity, and the exit node further encrypts data before it reaches the final server (Kaspersky, 2023).

- Brave: Brave is lightweight and a safe browser which has multiple features such adblocking, tracker blocking etc. The important feature is Tor integration. Using that feature users can browse with Tor's privacy benefits without needing a separate Tor browser(Brave Software Inc, 2025).

So , dark web can be accessed using the Brave browser through its TOR functionality inbuild or feature.

- In this process different forums such as data breach forums, vulnerability forums, discussion board can be identified and accessed. These forums may contain information and discussion about the CVE which might be exploited in the wild or a new vulnerability which was exploited by the user .
- This process includes manual recording the CVE ,discussion on EDR bypass using zero-day vulnerabilities, exploit kits etc.
- The data will be collected and maintained in a spreadsheet with the information found.

Finding useful Dark web Forums:

As discussed earlier dark web data can be gathered using TOR, but the collection of threat intel is not as easy as it is important to do proper research on various forums available on Dark web . Initial access tools are available on dark web in form of exploit kits and zero-day vulnerabilities. Dark web has multiple forums for various purposes such data breach information, exploits, vulnerabilities, malware and viruses etc. For this research it is important to find forums where vulnerability exploitation is discussed . As the dark web is huge it is hard to just get that information easily. But to find the forums it is necessary to monitor LinkedIn, twitter , telegram etc. to get this information as these are the active platforms where researchers in dark web monitoring discuss the different hacker forums which can be accessed via TOR which has relevant information.

1. **LinkedIn**: LinkedIn can be used to follow different people from research background in dark web as they are actively working on dark web monitoring. So, for this research many analysts, researchers posts were read and analyzed to find information

related to the research. These posts give live and active information about the forums and information related to different groups of hackers . So, it is important to be active on LinkedIn and be updated on recent discussion made on the platform.

2. **Twitter:** Twitter is a very useful social media platform for all researchers and people working in cybersecurity as it gives many updates regarding any vulnerabilities as well as data breach platforms. For this research, it is important to follow various twitter accounts which work on many active forums to find information about the live forums as dark web forums are not always static, and they are moved to different domains most of the time. There are many twitter accounts such as Dark web Intelligence, Cyber detective, Dark web informer – Cyber Threat intelligence, cyber detective etc. which discusses about dark web forums and marketplaces .
3. **Telegram:** Telegram is also a useful tool in finding more information about dark web monitoring as many researchers and attackers have various telegram tools which discuss the different data breaches, 0-day vulnerability , forums etc. in the chats which can be very useful for a research person to get more information about the activity on dark web and different forums. It helps to find, visit and analyze useful dark web forums .

Data Cleaning and Processing:

In this , the data collected from all the sources will be processed for analysis. The data collected will be properly analyzed in an excel sheet with the CVE numbers found and vulnerabilities found on the dark web.

- Each source will contain different types of details such as Nessus will create a detailed report with the vulnerabilities details, Shodan will contain information in Json format and the dark web data will be manually researched, collected and updated in the excel.
- In this the Data which is duplicated will be removed such as same CVE and same vulnerabilities.
- The data such as low level vulnerabilities, irrelevant entries etc. will also be removed . Data will be cleaned and processed for further analysis.

The cleaned data will be generated and then it should be used for the analysis to get appropriate results for the research.

Data Analysis:

This step includes identifying the unique vulnerabilities which are found in the dark web. It includes comparing the processed data collected from all the sources from passive scanning, active scanning and dark web monitoring. The main purpose is to find unique vulnerabilities which are not detected in passive scanning and active scanning.

To find an effective way to analyze the data, a factor called Dark Web Intel Factor has been defined which will the number of critical vulnerabilities discovered exclusively through dark web monitoring, relative to those found using traditional scanning methods.

$$\mathbf{DWIG = | CVDW \ |/ CVTS}$$

DWIG = Dark Web Intel Gain

CVDW= Critical Vulnerabilities found on dark web

CVTS = Critical Vulnerabilities in traditional scanning

CVTS can be calculated by adding Critical Vulnerabilities in Nessus and Critical Vulnerabilities in Shodan/Censys.

So basically, the Critical vulnerabilities in traditional scanning will be all critical vulnerabilities found in Shodan, Nessus, censys etc. Using this formula will give a numerical value which will help to find unique contribution of dark web intelligence to critical vulnerability discovery. The more DWIG means the more critical vulnerabilities found in this research which are missed by the traditional scanners and vulnerability management process. The percentage will be marked as a contribution to the vulnerability management process which will increase proactiveness in the vulnerability management process.

4 Design Specification

The architecture for the research includes the main servers which is the host which will be scanned for the vulnerabilities. An active scan will be performed using the Nessus expert tool on this host which will scan for vulnerabilities. Once the vulnerabilities are found. The same host will be scanned using Shodan and censys which act as passive scanning tools. These tools will be used for reconnaissance and vulnerabilities.

This will show various vulnerabilities which are not detected actively by Nessus. After combining these vulnerabilities, data will be collected from dark web monitoring from different forums such as exploit[.]in, 0day[.]today etc. These forums will give information which will be manually collected in an excel sheet. These two data sets will be compared for analysis. The diagram below shows a basic architecture of the research of how the dark web intel will be collected and compared with the Nessus and Shodan/censys .

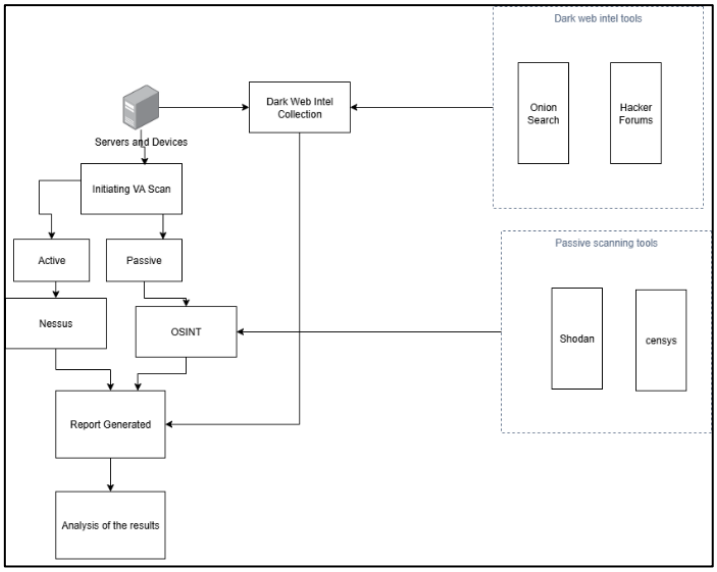

Fig 1: Architecture Diagram of the solution

5 Implementation

The implementation of the proposed solution was done where all the data collected was properly checked for any repeated CVE and vulnerability . Different data was collected using the tools such as Nessus, Shodan, Censys, Brave with TOR and Excel.

A Cisco AnyConnect VPN was used to connect to the internal server as Nessus expert is hosted on internal server. Once connecting to that Nessus Expert can be accessed . On Nessus Expert , a new scan should be started and configured with appropriate details such as the Target Ip and host domain. A basic network scan and web application scan should be done to get a proper report with vulnerabilities with CVE number. The reports consist of critical, high, medium and low vulnerabilities. The report can be exported in a excel format and html format . Nessus was used for active scanning and Shodan & censys was used for passive scanning.

- Shodan: It is a search engine for everything on the internet which includes web cams, water cams, water treatment facilities, medical devices etc. everything which can be connected via internet. Shodan can be used to check web applications and network devices information , software, ports and vulnerabilities as well(Jmporup, 2022).

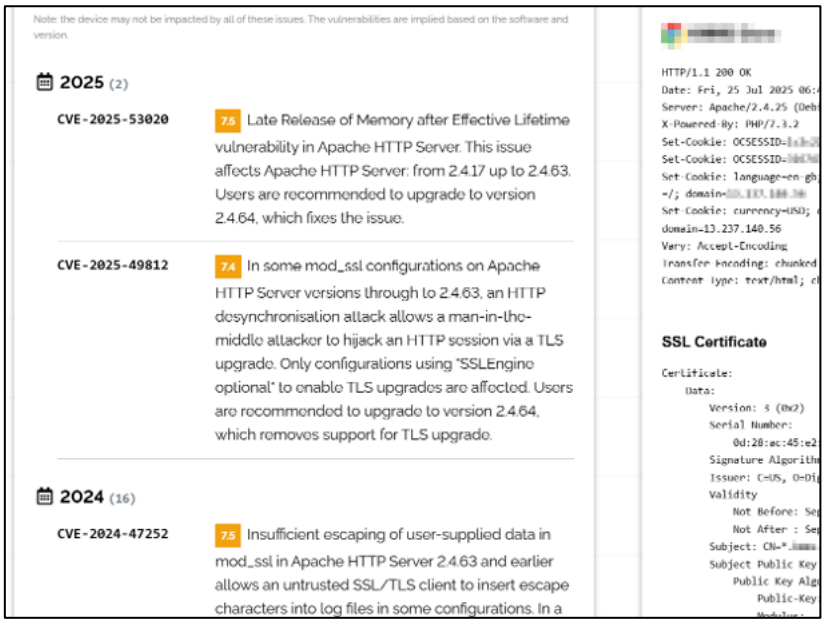

Fig 2.1: CVE Details found on shodan (passive scanning)

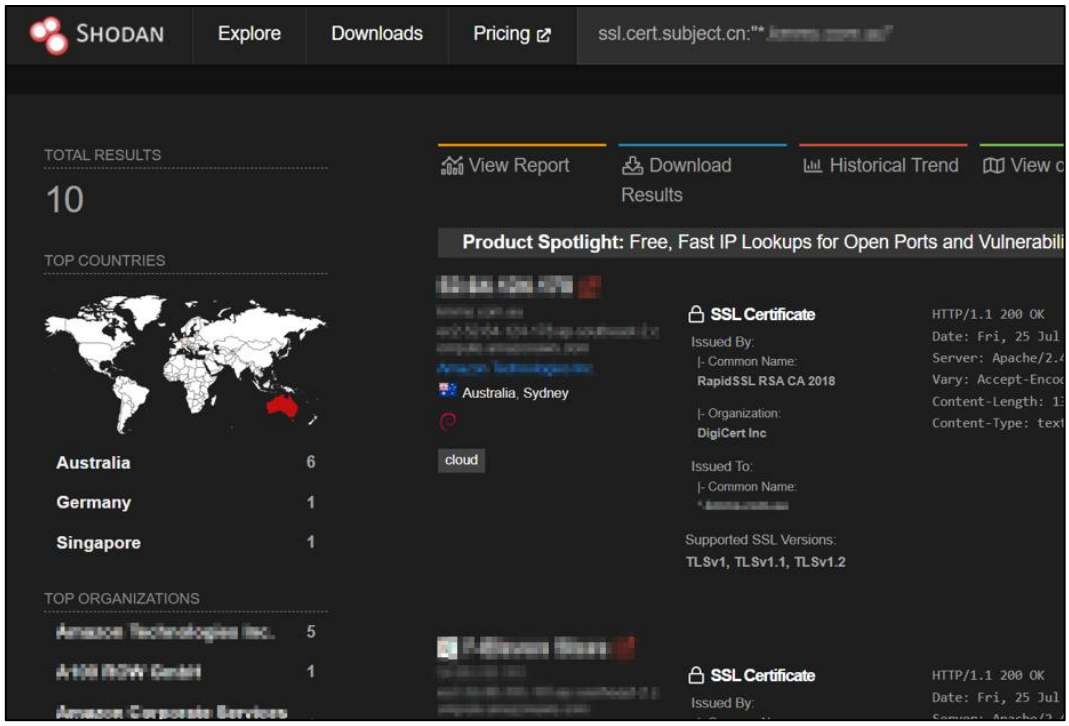

Fig 2.2: screenshots of finding more hosts and vulnerabilities on Shodan related to the domain

- Censys: It is similar to Shodan . It is used for OSINT(Open-Source Intelligence) and CTI(Cyber Threat Intelligence). Censys can be used to find Hosts, certificates, and names related to a host. It can also be used to find a specific combination of OS and application. It can be used to find more information about web applications and devices in detail(Warner, 2023).

The above tools will be helpful to find different information such as Open ports, SSL certificate information, detected software versions and CVE details.

Later for dark web intel, brave browser should be used to connect to TOR safely. Once Tor is securely connected , the dark web forums can be accessed via brave TOR browser.
As discussed earlier, LinkedIn, Twitter, Telegram etc were used to find relevant dark web Forums.

Different dark web forums were selected which were “zero-day[.]cz”, “0day[.]today”, “packetstorm[.]news”, “cracked[.]sh”, “exploit[.]in”, “xss[.]is”.

- **zero-day[.]cz** This is a foundation and created to raise awareness of zero-day vulnerabilities. The information gathered in these forums is from open source and is investigated by the cybersecurity team.

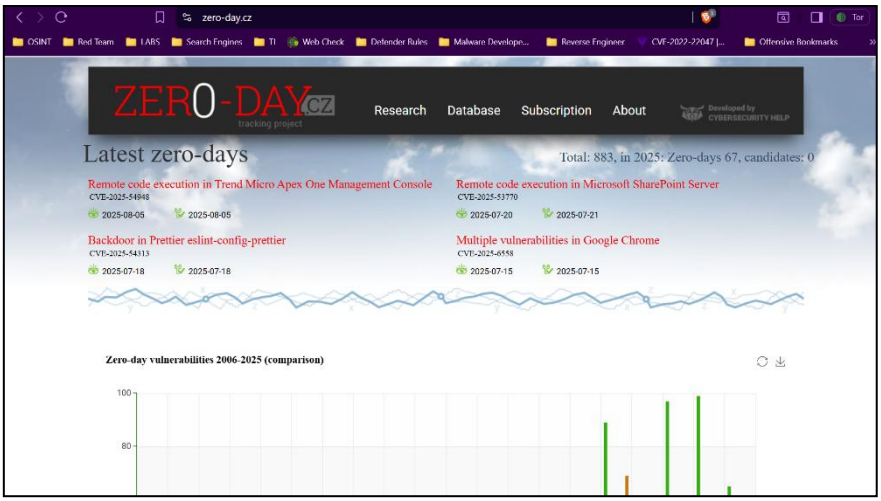

Fig 2.3: Zer0-Day forum

- **0day[.]today** : The 0day[.]today provides a database of standards and technology to protect the systems against possible threats. Some threats may be targeting the confidentiality or integrity of the information, processes and the availability of your information and services. They inform the company as soon as possible when new security breaches are discovered so organization can take appropriate action to prevent any cyber-attack (Baines, 2023).

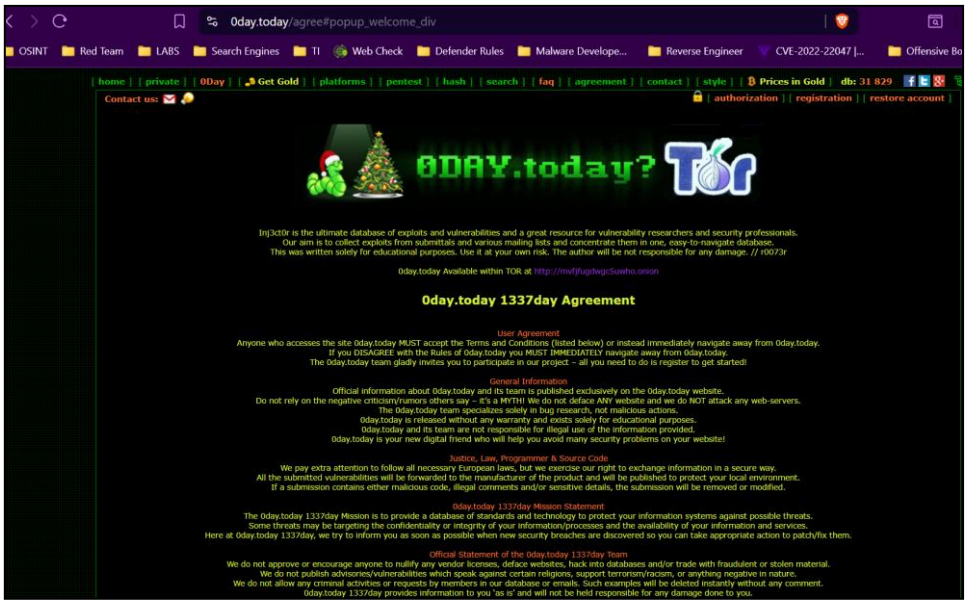

Fig 2.4: 0Day[.]today Forum

- **cracked[.]sh**: They provide cracking tutorials, tools, leaks, marketplace etc. . This is a place where there are live discussions about various things there.

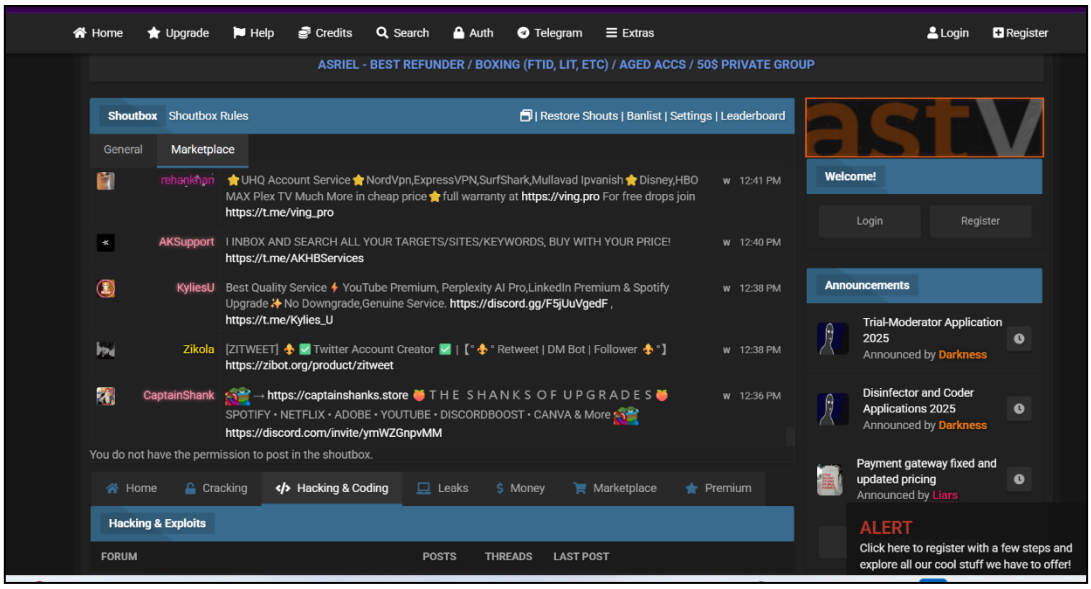

Fig 2.5: Cracked[.]sh Forum

- **exploit[.]in**: Exploit[.]in is Russian forum which includes a lot of information about vulnerabilities, malware, carding, hackers etc. It is a useful forum where many vulnerabilities which are exploitable are discussed in detail. This information can be helpful to the organization to keep them updated with the latest vulnerabilities (Baines, 2023).

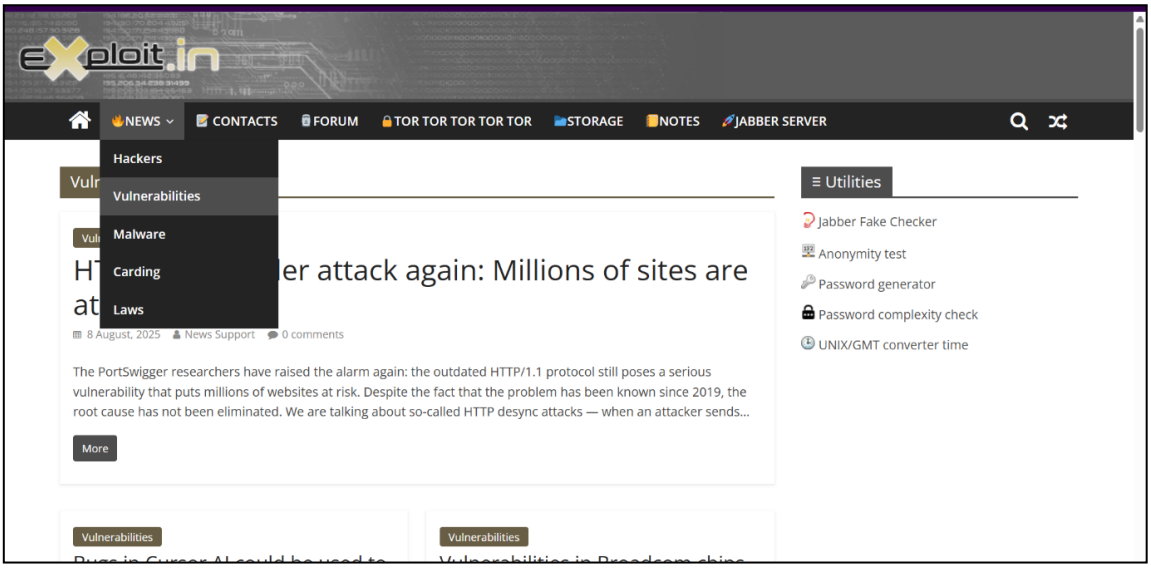

Fig 2.6: Exploit[.]in Forum

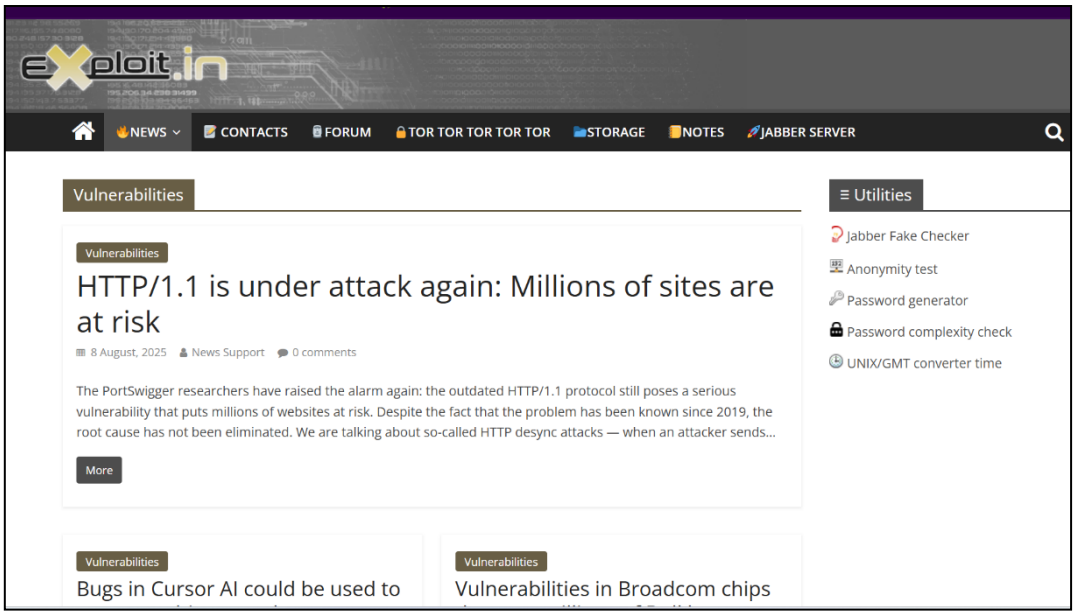

Fig 2.7: Vulnerability Details in the forum

- **xss[.]is**: Xss [.]is is a very old and useful forum where different users discuss the methods of exploiting any new vulnerabilities. It gives detailed steps about the exploitation of these vulnerabilities. However, currently it has been taken down by the government just while conducting research. Below is the screenshot which was before the website was taken down. As you can see it gives detailed information with the commands and steps to exploit a certain vulnerability (Owda, 2025).

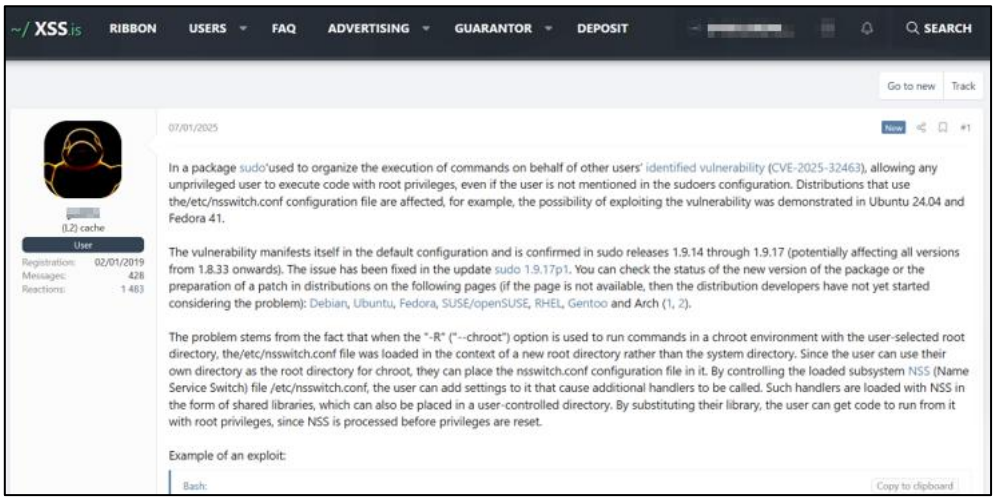

Fig 2.8: XSS[.]is Forum

6 Evaluation

Vulnerability Data was collected from various data sources for active(Nessus) and passive scanning(Shodan/censys) and manual dark web monitoring. In Nessus everything was generated in a report format with all the CVE, severity , description and remediation. In passive scanning various CVE were found for the same host which were not present during Nessus scan . So, all the CVE from both were collected and combined with the dark web monitoring

findings. In dark web monitoring around 15 critical and 5 high severity vulnerabilities related to the services present on the host were found which were not present in the Nessus nor in the Shodan. To find more information and details about different related host different commands can be used on Shodan with hostname and Ip which will give an overview of the hosts as well their vulnerabilities.

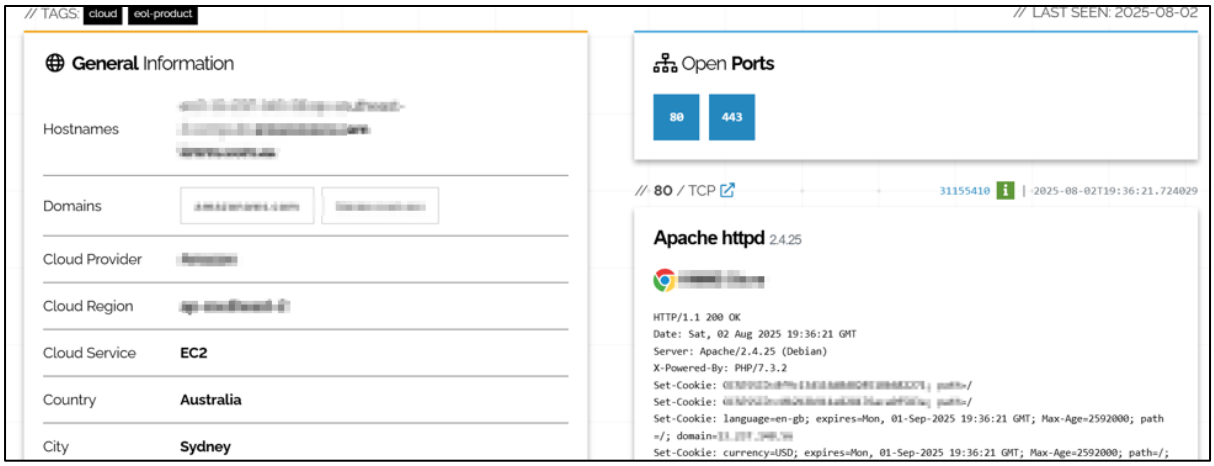

Fig 3.1: Information of the host on Shodan

These vulnerabilities were heavily exploited and were highly discussed on dark web. The forums had detailed information about the vulnerability with CVE number, description, how it can be exploited and remediation steps. The result comparison was very hard to calculate as most of the dark web forums are currently seized by the government, so this was performed multiple times to get appropriate results as well data.

After applying the formula for Dark web gain factor,

$$DWIG = |CVDW| / |CVTS|,$$

$$DWIG = |15| / (25+32),$$

$$= 15/57$$

$$\approx 0.263$$

So, after converting this value to percentage the output is 26%

The DWIG was 0.263 which means 26% more critical vulnerabilities were discovered on dark web monitoring beyond traditional scanning. Below is a detailed graph of the results which were found .

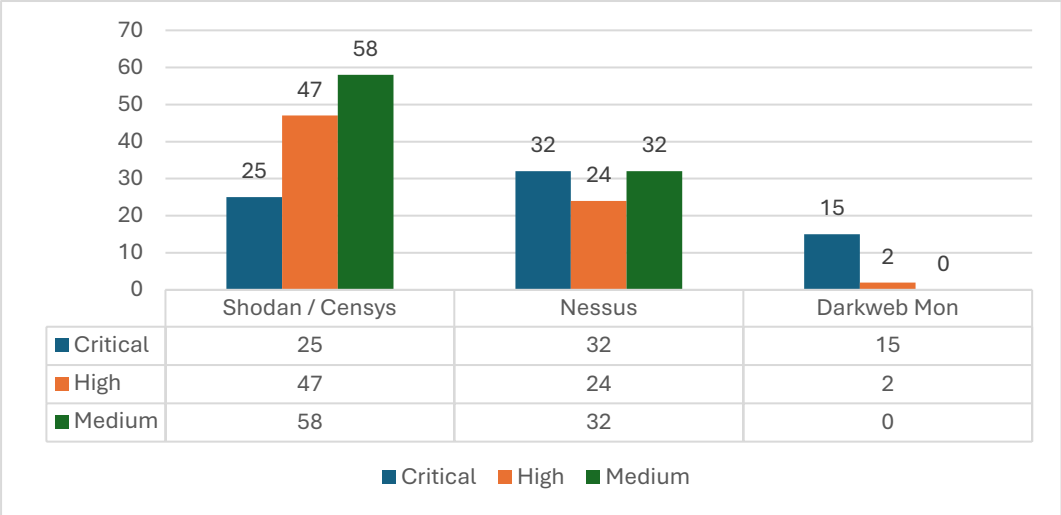

Fig 3.2: Graphic representation of the results

6.1 Discussion

As per the results, it can be stated that dark web monitoring helps identify vulnerabilities that Nessus and Shodan miss, making vulnerability management more proactive. However, it is important to later check if these vulnerabilities are exploitable in the environment or not .

As some of the vulnerabilities may not be directly present in the environment but this research proves that there is an intelligence gap which can be filled by passive scanning and dark web monitoring . As some organizations do not even conduct passive scanning using Shodan or censys and they just depend on Nessus which can be risky .

The DWIG percentage, which is 26% proves that there are so many critical vulnerabilities which are present on dark web, which are not detected by the traditional methods. In this the vulnerabilities consist of many services which are used by many companies and organizations such as chrome, Microsoft windows, SharePoint, Firefox, Nvidia, Cisco etc. Out of these vulnerabilities most of them can be present on many servers and desktops.

7 Conclusion and Future Work

As per the results, the research concludes that threat intelligence gathered from dark web monitoring can enhance vulnerability management process. This can help vulnerability management to be more proactive. The manual dark web monitoring was very hard as most of the websites were taken down by the government during research such as xss[.]is.

The government and law enforcement are working to take down multiple forums which can affect dark web monitoring as many dark webs monitoring are using these same forums as a base for detecting vulnerabilities. This research successfully demonstrates that dark web monitoring reveals unique critical vulnerabilities not detected by traditional scanners like Nessus or passive tools like Shodan/Censys.

As per the conclusion, it can be concluded that there is so much information which is available on the dark web which can be very useful for protecting the organization proactively. Dark web is part of web where the attackers connect with different other

attackers from the world for a similar goal. The goals could be financial gain, state sponsored attacks, hacktivism etc. Dark web should be monitored to identify early signs of a cyber-attack. Many government authorities monitor dark web to find threats which can be harmful to the country. They are monitoring the dark web to find the cybercriminal behind big attacks.

The previous research was done on what kind of threat intel are present on dark web and how they can be used but there was no direct comparison between the active scanner , passive scanning and dark web monitoring. This research shows explicitly how there is a huge gap in vulnerability assessment process by not considering the threat intel of dark web.

The research concludes that dark web monitoring is not a replacement for the traditional scanning methods but rather a strategic expansion as combining these can close the huge gap and identify the threats more efficiently.

Corporate companies can also monitor dark web to prevent these threats. There are many commercial tools available which can be deployed to monitor dark web. This research manually researched the dark web to find forums which discuss vulnerability and exploits. It has been predicted that malware and zero-day markets will continue to grow in popularity . As media attention continues to increase there will be multiple takedowns of these websites which offer these services and forums offering information about those. There are multiple new technologies which are emerging which can create a new way for hackers and attackers to find a way to exploit any vulnerabilities in these technologies.

Governments face constant threat of cyberattacks by many state-sponsored actors who try to disrupt services and compromise sensitive information so they monitor dark web for any intel and information which can be used to protect from any huge cyberattacks (Stealthmole.com, 2024).

For future research, the verification of all the identified vulnerabilities on dark web within the specific organizational environment can be done.

8 Challenges and Limitations:

Dark web monitoring poses some significant challenges. It is decentralized and there should be need for specialized software to make it difficult to access and monitor effectively. The dark web is vast and there are many active forums on dark web which can only be found through private groups or forums. The relevance of data collected from dark web can be uncertain. Security teams should properly classify real threats and false positive out of the alerts from dark web as some can be not relevant to the environment (Chachak, 2025).

However, the vulnerabilities identified via dark web sources were not deeply validated within the organization’s specific environment to confirm their exploitability or presence. This decision was made to focus the research on the intelligence-gathering and detection gaps between sources rather than on in-depth local asset validation. As a result, although the dark web revealed high-risk CVEs, their actual relevance to the organization’s infrastructure was not fully verified.

During the research , it was very challenging to find an appropriate forum as some of them were taken down during the research process. The forums xss[.]is was a very important part of

the dark web monitoring and it was a base for many commercial tools as well which are available in the market. Europol arrested an individual in Ukraine who was suspected of running the XSS forum and it was seized by the French authorities and taken down. It is a victory for the security world as it was not only just Dark Web marketplace but a very influential forum . So, it sends a strong message that Law enforcement is getting better at tracking and disrupting these networks(Wright, 2025).

The xss forums are not fully taken down as they are available on some onion website, but it is very hard to track them as they are changed again and again to avoid tracking. It is also important to consider legal and ethical dilemmas as an organization. It is important to access the Dark web privately and safely as it can be huge issue to the privacy. So, while investigating vulnerabilities and finding forums discussing vulnerabilities and exploits it is important to protect privacy by not accessing any illegal websites or engage in any kind of conversations on the forums as it may be risky to contact any user on dark web as most of them are malicious users and they can risk the researcher's privacy.

References

Baines, J. (2023). *A Comparison of Exploit-DB and 0day.today | Blog | VulnCheck*. [online] VulnCheck. Available at: https://www.vulncheck.com/blog/edb-0day-compare [Accessed 12 Aug. 2025].

Basheer, R., and Alkhatib, B. (2021) 'Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence,' *Journal of Computer Networks and Communications*, 2021, pp. 1–21. https://doi.org/10.1155/2021/1302999.

Baskaran, S., Susmitha, N.R.K., Sruthi, S. and Thirulogaveni, J., 2024. A Comparative Analysis of Vulnerability Management Tools: Evaluating Nessus, Acunetix, and Nikto for Risk-Based Security Solutions. [online] Available at: https://doi.org/10.13140/RG.2.2.30040.71687 [Accessed 13 Aug. 2025].

Benjamin, V., Li, W., Holt, T., and Chen, H. (2015). Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. *2015 IEEE International Conference on Intelligence and Security Informatics (ISI)*, [online] pp.85–90. doi:https://doi.org/10.1109/isi.2015.7165944.

Bennouk, K., Ait Aali, N., El Bouzekri El Idrissi, Y., Sebai, B., Faroukhi, A.Z. and Mahouachi, D., 2024. A comprehensive review and assessment of cybersecurity vulnerability detection methodologies. *Journal of Cybersecurity and Privacy*, *4*(4), pp.853-908.

Bitsight. (2025). A Guide to Dark Web Threat Intelligence | Bitsight. [online] Available at: https://www.bitsight.com/learn/cti/what-is-dark-web-threat-intelligence#:~:text=By%20monitoring%20dark%20web%20forums,proactively%20defend%20against%20cyber%20threats [Accessed 12 Aug. 2025].

Brave Software Inc (2025). Brave Software. [online] Brave. Available at: https://brave.com/ [Accessed 12 Aug. 2025].

Burgess, J. (2017). Malware and Exploits on the Dark Web. [online] Queen's University Belfast. Available at: https://pure.qub.ac.uk/en/publications/malware-and-exploits-on-the-dark-web [Accessed 12 Aug. 2025].

Chachak, E. (2025) *The role of dark web monitoring in cyber threat intelligence*. https://www.cyberdb.co/the-role-of-dark-web-monitoring-in-cyber-threat-intelligence/.

Ijraset.com. (2023). *A Comprehensive Study of Dark Net*. [online] Available at: https://www.ijraset.com/research-paper/comprehensive-study-of-dark-net [Accessed 12 Aug. 2025].

Jmporup (2022) What is Shodan? The search engine for everything on the internet. https://www.csoonline.com/article/565528/what-is-shodan-the-search-engine-for-everything-on-the-internet.html.

Kaspersky (2023). What is the Tor browser and is it safe? [online] /. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-the-tor-browser [Accessed 12 Aug. 2025].

Kotha, N.R., 2015. Vulnerability Management: Strategies, Challenges, and Future Directions. *NeuroQuantology*, *13*(2), pp.269-275.

Ngo, F.T., Marcum, C. and Belshaw, S. (2023) 'The dark web: what is it, how to access it, and why we need to study it,' *Journal of Contemporary Criminal Justice*, 39(2), pp. 160–166. https://doi.org/10.1177/10439862231159774.

Nunes, E., Shakarian, P. and Simari, G.I., 2018, May. At-risk system identification via analysis of discussions on the darkweb. In *2018 APWG symposium on electronic crime research (eCrime)* (pp. 1-12). IEEE.

Owda, A. (2025) 'Top 10 deep web and dark web forums - SOCRadar® Cyber Intelligence Inc.,' *SOCRadar® Cyber Intelligence Inc.*, 24 June. https://socradar.io/top-10-deep-web-and-dark-web-forums/.

Samtani, S., Chai, Y. and Chen, H., 2022. Linking exploits from the dark web to known vulnerabilities for proactive cyber threat intelligence: An attention-based deep structured semantic model1. *MIS quarterly*, *46*(2).

Sapienza, A., Bessi, A., Damodaran, S., Shakarian, P., Lerman, K. and Ferrara, E., 2017, November. Early warnings of cyber threats in online discussions. In *2017 IEEE International Conference on Data Mining Workshops (ICDMW)* (pp. 667-674). IEEE.

Stealthmole.com. (2024). Dark Web Threat Intelligence for Governments. [online] Available at: https://www.stealthmole.com/sectors/governments [Accessed 12 Aug. 2025].

Team, Z. (2024). *Vulnerability Scanners: Passive Scanning vs. Active Scanning*. [online] ZenGRC. Available at: https://www.zengrc.com/blog/vulnerability-scanners-passive-scanning-vs-active-scanning/ [Accessed 12 Aug. 2025].

Warner, C. (2023). Censys Search Engine Intro. [online] Medium. Available at: https://warnerchad.medium.com/censys-search-engine-intro-d502d9839c1c [Accessed 12 Aug. 2025].

Wright, R. (2025) Law enforcement cracks down on XSS — but will it last? https://www.darkreading.com/threat-intelligence/law-enforcement-cracks-down-xss.