JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A NEW ERA OF CYBER THREATS : EVALUATING ACCESS CONTROL VULNERABILITIES POST-COVID AND APPROACHES TO STRENGTHENING SECURITY

Sanjana Kunnackal Santhosh , Zaheeruddin Ahmed
IT Project Lead/ Student , Professor
School of Engineering & IT, School of Engineering & IT

Manipal Academy of Higher Education, Dubai Campus, Dubai, U.A.E

Abstract : The COVID-19 pandemic reshaped the digital environment, leading to a swift shift towards remote work and cloud-based technologies across various sectors. While these changes brought enhanced flexibility and operational efficiency, they also exposed new security weaknesses, particularly in systems that control user access and permissions. Cyber attackers quickly capitalized on these vulnerabilities to breach organizational defences. This study explores how access control vulnerabilities have evolved in the aftermath of the pandemic and the tactics attackers have used to exploit these weaknesses. By examining recent cyberattacks that targeted access control systems, this paper highlights key areas where conventional security measures have fallen short, including inadequate multi-factor authentication (MFA), weak encryption protocols, and insufficient real-time monitoring. Additionally, the rapid adoption of cloud infrastructures and the increased reliance on remote work have created new entry points for attackers. This research provides valuable insights into the post-pandemic cybersecurity landscape, offering recommendations to strengthen defences and safeguard critical data and assets. The goal is to help organizations better prepare for and counter the growing sophistication of cyber threats in today's digital world.

IndexTerms - IoT, MFA for Access Controls.

I. INTRODUCTION

The global COVID-19 pandemic has brought about transformative changes across nearly every facet of society, with digitalization and remote work becoming the norm for countless organizations. While these shifts have enabled businesses to continue operations in unprecedented circumstances, they have also introduced a host of new cybersecurity challenges. Among the most significant of these challenges are access control vulnerabilities—weaknesses in the systems that govern who can access sensitive data and resources within an organization. As companies adapt to a hybrid or entirely remote workforce, many have found that their existing access control mechanisms are no longer sufficient to address the complexities of this new environment.

The purpose of this project is to assess the increased risks posed by these vulnerabilities in the post-COVID era and to explore strategies for reinforcing security protocols. The growing reliance on cloud computing, collaboration tools, and BYOD (Bring Your Own Device) policies has expanded the attack surface, creating more opportunities for cybercriminals to exploit system weaknesses. Traditional access control models, which were once effective in more controlled office environments, have struggled to keep pace with these rapid technological shifts.

In this context, the proposal aims to identify key areas of vulnerability, evaluate the impact of these risks on organizational security, and recommend approaches to mitigate them. By strengthening access control practices, organizations can better safeguard their critical data and ensure compliance with emerging privacy regulations. This project will provide insights into how businesses can adapt to the evolving cybersecurity landscape and build a more resilient security posture that aligns with both current and future threats.

II. LITERATURE REVIEW

[20] Parkinson, S., & Khan, S. (2022, April 27). A survey on empirical security analysis of access control systems: A real-world perspective. ACM Digital Library. https://dl.acm.org/doi/10.1145/3533703

The paper "A Survey on Empirical Security Analysis of Access-control Systems: A Real-world Perspective" by Simon Parkinson and Saad Khan reviews the empirical studies on access-control systems, emphasizing their importance in restricting access to

sensitive resources. It highlights the necessity of routine policy analysis to identify and mitigate problematic permissions that could lead to data theft or unintended modifications. The survey covers various models like RBAC, DAC, MAC, and ABAC, noting a significant gap in empirical evaluations within existing literature. Key findings include the complexity of policy analysis, the need for scalable solutions, and the importance of empirical validation. The paper discusses challenges such as policy size, processing requirements, and the difficulty of testing and empirical evaluation. Using a systematic approach, the authors identify, screen, and refine relevant studies, ensuring a comprehensive review. They suggest future research areas, including developing more efficient analysis techniques and standardized benchmarking datasets. The findings aim to help organizations improve their access-control systems by providing insights into effective policy analysis and management. The survey concludes that while progress has been made, more empirical research is needed to address practical challenges faced by organizations.

[18] Moore, M. (2022, August 1). Top Cybersecurity Threats in 2022. University of San Diego. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/
The literature review on the top cybersecurity threats highlights the evolving landscape of cyber threats and the increasing sophistication of attacks. It underscores the significant financial impact of cybercrime, projected to rise dramatically from $9.22 trillion in 2024 to $13.82 trillion by 2028. The review categorizes threats into several types, including malware, which encompasses viruses, ransomware, and spyware, and social engineering, which exploits human interactions to gain unauthorized access. Insider threats, both accidental and malicious, are also a major concern. The review emphasizes the role of advanced technologies like machine learning and artificial intelligence in both facilitating and combating cyber threats. It discusses the risks associated with the Internet of Things (IoT), where ransomware can hijack connected devices. The intentional spread of misinformation, particularly through bots and automated sources, is identified as a threat to the integrity of information. The review also highlights the challenges posed by conflicting national security and privacy regulations, which can hinder organizations' ability to control their information. The need for heightened vigilance and innovative cybersecurity strategies is stressed to protect against these diverse and evolving threats. Overall, the literature review provides a comprehensive overview of the current and emerging cybersecurity threats, emphasizing the critical need for robust defenses and proactive measures.

[9] Duchamps, W. (2022, July 22). 9 common access management myths debunked. LinkedIn. https://www.linkedin.com/pulse/9-common-access-management-myths-debunked-wardduchamps/
The literature review in "9 Common Access Management Myths Debunked" by Ward Duchamps addresses prevalent misconceptions about access management and highlights modern solutions. It begins by debunking the myth that access control is solely for business and employees, emphasizing that modern systems offer fine-grained access for both workforce and customers. The review also challenges the belief that centralized access administration inherently enhances security, advocating for delegated administration to manage access more flexibly. It dispels the notion that authorization depends on finding the organization's system administrator, highlighting the evolution from access control lists (ACLs) to more dynamic, policy-based management. The myth that access management is static and unchanging is countered by showcasing the adaptability of modern systems to evolving business needs. The review also addresses the misconception that access management solutions are overly complex and costly, noting that scalable solutions are available for organizations of all sizes. It emphasizes the importance of user experience, debunking the myth that security measures always complicate user access. The review highlights the role of advanced technologies like AI and machine learning in enhancing access management. It also dispels the myth that access management is only about preventing unauthorized access, stressing its role in enabling secure collaboration. The misconception that access management is a one-time setup is addressed by emphasizing the need for continuous monitoring and updating. Finally, the review underscores the importance of integrating access management with broader security strategies to ensure comprehensive protection.

[12] Global Fraud Report 2021. (2022). Cybersource. https://www.cybersource.com/content/dam/documents/campaign/fraud-report/global-fraudreport-2021.pdf
The literature review in the "Global Fraud Report 2021" by CyberSource provides a comprehensive analysis of the evolving landscape of eCommerce fraud. It highlights the increasing sophistication of fraud tactics and the significant financial impact on businesses worldwide. The report categorizes fraud into various types, including payment fraud, identity theft, and account takeover, emphasizing the need for robust fraud management strategies. It discusses the role of advanced technologies like machine learning and artificial intelligence in detecting and preventing fraud. The review underscores the importance of multi-layered security approaches, combining technology with human expertise. It also addresses the challenges posed by the rapid growth of eCommerce, which has led to an increase in fraud attempts. The report highlights the need for continuous monitoring and updating of fraud prevention measures to keep pace with evolving threats. It emphasizes the importance of collaboration between businesses, financial institutions, and technology providers to effectively combat fraud. The review provides insights into the latest trends in fraud management, including the use of data analytics and real-time monitoring. Overall, the literature review underscores the critical need for proactive and adaptive fraud prevention strategies to protect businesses and consumers in the digital age.

[14] Griffiths, C. (2022, November 21). The latest 2022 cyber crime statistics. AAG IT. https://aagit.com/the-latest-2022-cyber-crime-statistics/
The literature review in "The Latest 2022 Cyber Crime Statistics" by AAG IT Support highlights the alarming rise in cybercrime and its significant impact on businesses and individuals. It notes that 50% of UK businesses experienced cyber attacks in 2023, with nearly 1 billion emails exposed in a single year, affecting 1 in 5 internet users. The review categorizes cyber threats, emphasizing that phishing remains the most common form of cybercrime, with a 220% increase in incidents during the pandemic. Ransomware attacks are also a growing concern, with 236.1 million attacks reported globally in the first half of 2022. The financial impact of cybercrime is substantial, with data breaches costing businesses an average of $4.88 million in 2024. The review highlights the rapid increase in malware attacks, which surged by 358% in 2020 compared to 2019. It underscores the importance of robust cybersecurity measures, noting that 73% of small and medium-sized businesses (SMBs) recognize the need for action, with 78% planning to increase their cybersecurity investment. The review also discusses the challenges posed by the lack of cyber insurance, with around 1 in 10 US organizations having no coverage against cyber attacks. It emphasizes the need for continuous monitoring

and updating of security measures to keep pace with evolving threats. Overall, the literature review provides a comprehensive overview of the current cybercrime landscape, stressing the critical need for proactive and adaptive cybersecurity strategies.

[15] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. JMIR. https://doi.org/10.2196/21747

The literature review in "Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review" by Ying He, Aliyu Aliyu, Mark Evans, and Cunjin Luo highlights the significant impact of the COVID-19 pandemic on healthcare cybersecurity. It identifies nine main challenges, including increased cyberattacks on hospitals and healthcare organizations, driven by the rapid shift to remote work and telehealth services. The review emphasizes the rise in phishing, ransomware, distributed denial-of-service (DDoS) attacks, and malware targeting the healthcare sector. It discusses the vulnerabilities introduced by changes in working practices and the need for robust cybersecurity measures to protect sensitive health information. The review also identifies eleven key solutions adopted by healthcare organizations, such as enhancing staff training, implementing multi-factor authentication, and improving incident response capabilities. It highlights the importance of collaboration between healthcare providers, cybersecurity experts, and government agencies to address these challenges effectively. The review underscores the need for continuous monitoring and updating of cybersecurity practices to keep pace with evolving threats. It also points out four key areas that require strengthening, including cybersecurity capacity building, policy development, and investment in advanced security technologies. The review provides valuable insights into the cybersecurity issues faced by the healthcare sector during the pandemic and offers practical recommendations for improving resilience against future cyber threats.

[10] Eian, I. C., Yong, L. K., Li, M., Qi, Y. H., & Z, F. (2020). Cyber attacks in the era of COVID- 19 and possible solution domains. Preprints. https://doi.org/10.20944/preprints202009.0630.v1

The literature review in "Cyber Attacks in the Era of COVID-19 and Possible Solution Domains" by Isaac Chin Eian, Lim Ka Yong, Majesty Yeap Xiao Li, Yeo Hui Qi, and Fatima-tuz-Zahra explores the surge in cyberattacks during the COVID-19 pandemic. It highlights the exponential increase in internet usage for activities like e-learning, remote working, and online shopping, which has led to heightened vulnerability to cybercrimes. The review categorizes common types of cyberattacks, including phishing, malware, ransomware, social engineering, identity theft, and denial-of-service attacks. It discusses how attackers exploit these vulnerabilities to gain credential information or financial benefits. The review provides a detailed analysis of recent cyberattacks, emphasizing the critical need for robust cybersecurity measures. It proposes various solutions, including enhancing privacy protocols and implementing advanced security technologies. The review also addresses the reasons behind increased vulnerability, such as inadequate network security and the ability of attackers to exploit internet weaknesses. It emphasizes the importance of continuous monitoring and updating of cybersecurity practices to keep pace with evolving threats. The review concludes with an in-depth analysis of future directions for cybersecurity research, stressing the need for innovative solutions to combat cyber threats effectively. Overall, the literature review provides valuable insights into the cybersecurity challenges posed by the pandemic and offers practical recommendations for improving resilience against cyberattacks.

[7] Cybersecurity remains one of Malaysia's top concerns, says Hamzah. (2022, March 28).Free Malaysia Today. https://www.freemalaysiatoday.com/category/nation/2022/03/28/cybersecurity-remains-oneof-malaysias-top-concerns-says-hamzah/

The literature review in "Cybersecurity Remains One of Malaysia's Top Concerns, Says Hamzah" highlights the significant rise in cybercrime cases in Malaysia, with 3,273 cases reported up to February 2022, resulting in losses of RM114 million. It emphasizes the growing concern over cybersecurity due to the increasing number of online crimes. The review categorizes various types of cyber threats, including phishing, ransomware, and identity theft, which have become more prevalent during the pandemic. It discusses the vulnerabilities introduced by the rapid shift to digital platforms and remote work, which have been exploited by cybercriminals. The review underscores the importance of robust cybersecurity measures and the need for continuous monitoring and updating of security protocols to protect sensitive information. It highlights the role of government initiatives and collaborations with private sectors to enhance cybersecurity infrastructure. The review also addresses the challenges faced by small and medium-sized enterprises (SMEs) in implementing effective cybersecurity measures due to limited resources. It emphasizes the need for increased awareness and education on cybersecurity best practices among the general public. The review concludes by stressing the critical importance of proactive and adaptive cybersecurity strategies to mitigate the risks posed by evolving cyber threats.

[8] Dr.S., Mohanavel. (2021). Prevention from cyber security vulnerabilities in COVID-19 pandemic situation.

The literature review in "Prevention from Cyber Security Vulnerabilities in COVID-19 Pandemic Situation" by Dr. S. Mohanavel highlights the significant increase in cyber threats during the COVID-19 pandemic. It emphasizes the rapid shift to remote work and the corresponding rise in vulnerabilities as organizations adapted to new working environments. The review categorizes various types of cyber threats, including phishing, ransomware, and malware, which have become more prevalent during the pandemic. It discusses the challenges posed by inadequate network security and the exploitation of these weaknesses by cybercriminals. The review underscores the importance of robust cybersecurity measures, such as multi-factor authentication and regular software updates, to protect sensitive information. It highlights the role of employee training in enhancing cybersecurity awareness and reducing the risk of human error. The review also addresses the need for continuous monitoring and updating of security protocols to keep pace with evolving threats. It emphasizes the importance of collaboration between organizations, cybersecurity experts, and government agencies to effectively combat cyber threats. The review concludes by stressing the critical need for proactive and adaptive cybersecurity strategies to mitigate the risks posed by the pandemic and future crises. Overall, the literature review provides valuable insights into the cybersecurity challenges faced during the COVID-19 pandemic and offers practical recommendations for improving resilience against cyberattacks.

[2] Alshawi, A., Al-Razgan, M., AlKallas, F. H., Bin Suhaim, R. A., Al-Tamimi, R., Alharbi, N., & AlSaif, S. O. (2022). Data Privacy during pandemics: A systematic literature review of covid-19 smartphone applications. PeerJ Computer Science, 7. https://doi.org/10.7717/peerjcs.826
The literature review in "Data Privacy During Pandemics: A Systematic Literature Review of COVID-19 Smartphone Applications" by Amany Alshawi et al. explores the privacy concerns associated with COVID-19 contact tracing apps. It highlights the rapid deployment of these apps to control viral transmission and the subsequent privacy issues that arose. The review categorizes privacy concerns into centralized and decentralized models, discussing how each affects user privacy differently. It emphasizes the importance of balancing public health benefits with privacy protection, noting that many apps collected extensive personal data, raising significant privacy concerns. The review identifies various technologies used in these apps, such as Bluetooth and GPS, and their implications for privacy. It discusses the legal and ethical considerations, stressing the need for robust data protection laws to safeguard user privacy. The review also highlights the role of public trust in the success of contact tracing apps, noting that privacy breaches can undermine public confidence. It suggests solutions to improve data privacy, including enhancing transparency, implementing strict data governance policies, and ensuring data minimization. The review concludes by emphasizing the need for continuous monitoring and evaluation of these apps to address emerging privacy issues and improve their effectiveness. Overall, the literature review provides a comprehensive analysis of the privacy challenges posed by COVID-19 contact tracing apps and offers practical recommendations for enhancing data privacy.

[3] Clancy, R. (2022, October 12). What is broken access control vulnerability? EC-Council. https://www.eccouncil.org/cybersecurity-exchange/web-application-hacking/broken-accesscontrol-vulnerability/
The literature review on "Broken Access Control Vulnerability" by EC-Council highlights the critical security flaws that allow unauthorized users to access restricted resources. It emphasizes that broken access control vulnerabilities often arise from weak authentication and authorization mechanisms, enabling attackers to bypass standard security procedures and gain illegitimate privileges. The review categorizes common attack vectors, including injection flaws, cross-site scripting (XSS), and broken authentication and session management. It discusses how these vulnerabilities can be exploited to gain unauthorized access to sensitive data or modify application data. The review underscores the importance of implementing robust security measures such as input validation, proper session management, and strict authorization controls to mitigate these risks. It also highlights the need for continuous monitoring and updating of security protocols to address evolving threats. The review provides practical examples of broken access control vulnerabilities, such as applications that allow users to view or edit sensitive data without proper authentication. It stresses the significance of role-based access control to ensure that only authorized users can perform specific functions. The review concludes by emphasizing the critical need for organizations to adopt comprehensive security strategies to prevent broken access control vulnerabilities and protect their systems and data.

Needs/Problems

Sectors Affected by Cyber Attacks Post-COVID-19

Since the COVID-19 outbreak, cyberattacks have primarily targeted industries like banking and healthcare, taking advantage of weaknesses in access controls. The increased reliance on digital platforms and distant work situations has led to a boom in phishing, ransomware, and malware attacks.

• Healthcare Sector
March 2020: Ransomware attacks targeted hospitals, causing serious data breaches and serious disruptions to patient care. Cybercriminals took advantage of the pandemic's disarray and overburdened healthcare institutions.
May 2020: A spike in cyberattacks targeting the theft of private information pertaining to
COVID-19 research and patient data was reported by the U.S. Department of Health and
Human Services. This brought attention to the cybersecurity flaws in the healthcare industry.

• Banking and Financial Services
April 2020: A noticeable rise in phishing attempts directed at bank clients. Cybercriminals took advantage of the pandemic's economic turmoil by posing as banks in order to steal personal information.
In October 2020: a significant ransomware attack impacted multiple financial institutions. The attackers threatened to reveal sensitive customer data if their demands were not fulfilled and demanded hefty ransoms.

• Government and Critical Infrastructure
July 2020: More government entities became the target of cyberattacks, especially in the United States. In order to interfere with services and steal important data, attackers targeted public health and safety systems.
December 2020: A number of US federal institutions were impacted by the SolarWinds cyberattack, which turned out to be one of the biggest breaches. Hackers were able to obtain private data, which had an effect on vital infrastructure and national security.

• Education Sector
September 2020: Cyberattacks on educational institutions increased as schools made the switch to online instruction. Ransomware attacks exposed the weaknesses in the education sector by interfering with classes and compromising student data.

Applications Targeted by Attackers

- Cloud-Based Applications:
- To obtain sensitive data without authorization, attackers have taken advantage of poorly configured cloud services and unsafe APIs.

- SaaS apps have been especially susceptible; reports of account hijacking and cookie poisoning have been made.

- Remote Work Tools:
- Unauthorized access has been attempted to applications used for remote work, including collaboration tools and video conferencing.
- Social engineering techniques have been employed by cybercriminals to fool users into disclosing login credentials for various platforms.

- Healthcare Applications:
- Attackers have used fake applications to steal personal information from COVID-19 tracking and vaccination apps.

- Financial Apps:

Phishing attacks have been used to target mobile banking and payment apps, tricking users into exposing login information.

Attacks across a wide range of industries and applications have significantly increased as a result of the COVID-19 epidemic, which has made hackers' habitat. To reduce these threats, organizations need to improve their security procedures, especially those related to access controls.

Post-COVID Surge in Cyberattacks

January 2021: According to reports, cyberattacks have increased by an astounding 400% since the beginning of the pandemic. Attackers targeted companies in a variety of industries by taking advantage of flaws in remote work configurations.

March 2021: The pandemic response was made more difficult in March 2021 when cybercriminals launched a series of attacks on vaccine distribution networks with the goal of stealing private information pertaining to vaccine research and distribution logistics.

Recent Trends

January 2025: The continued threat landscape was demonstrated in January 2025 when Russian hackers launched spear phishing operations against Kazakh diplomatic entities, inserting malicious code into diplomatic documents for the goal of cyber espionage.

January 2025: Chinese cyberattacks on Taiwan, which mostly targeted government networks, doubled. A change in the focus of cyber threats was indicated by this increase, which was ascribed to growing geopolitical tensions.

These instances highlight the urgent need for improved cybersecurity measures to protect sensitive data and infrastructure by illuminating the serious vulnerabilities across multiple domains during and after the COVID-19 pandemic.

ZOOM

Cyberattacks, most notably "Zoombombing," which took advantage of insufficient security settings to gain unauthorized access to meetings, undermined Zoom's access safeguards after COVID-19. Organizations can use strategies like waiting rooms, password protection, and frequent software updates to fix vulnerabilities in order to improve access control.

Impact on Zoom's Access Controls

Increased Vulnerabilities:
- Existing security vulnerabilities were brought to light by the pandemic's rapid increase in consumers.
- The chat feature and unsecured meeting links were two areas where attackers specifically took advantage of vulnerabilities.

Zoombombing Incidents:
- Meetings were interrupted by unauthorized users, resulting in harassment and privacy violations.
- This demonstrated the necessity of enhanced user awareness and access controls.

Weak Security Settings:
- A large number of users failed to make use of waiting rooms and password protection, among other security elements.
- If these features weren't activated, attackers might enter meetings with ease.

Response to Cyber Attacks:
- Zoom implemented several security measures, including:
- End-to-End Encryption: Improved meeting data security.
- Default Password Protection: To avoid unwanted access, meetings are now password-protected by default.
- Waiting Room Feature: Gives meeting hosts the ability to manage who attends.
- Ongoing Security Improvements:
- Zoom has promised to fix vulnerabilities with frequent updates and patches.

The organization is now more open about its security procedures and weaknesses.

Cyber Security Measures to Enhance Access Control

- Enable Password Protection:

To avoid unwanted access, all meetings should require passwords.

- Utilize Waiting Rooms:

Prior to attendees joining the meeting, screen them using the waiting room feature.

- Regular Software Updates:

To fix vulnerabilities, make sure Zoom and any associated software are updated on a regular basis.

- Educate Users:

Conduct training on Zoom security best practices, such as identifying phishing attempts and comprehending privacy settings.

- Restrict Screen Sharing:

To stop unwanted content sharing, restrict screen sharing to hosts only.

- Lock Meetings:

To keep new attendees out of meetings, lock sessions after everyone has joined.

- Remove Disruptive Participants:

Be ready to remove out anyone who interferes with the meeting or threatens everyone's safety.

Zoom's increased use during the COVID-19 epidemic created serious access control issues, which prompted the firm to strengthen its security protocols. Organizations can further defend their meetings and sensitive data from cyber threats by putting strong cybersecurity procedures into place.

3.1 Goals/Objectives

Attackers' strategies to get around or violate access rules are evolving along with cybersecurity technologies. The strategies used by cybercriminals to take advantage of weaknesses and obtain illegal access to networks, systems, and private information are always changing. The following are a few recent sophisticated assaults that target access controls:

1. Credential Stuffing Attacks

- Description: Attackers try to log into several services using username and password combinations that have already been compromised in past data breaches. This technique works quite well because many people repeat their passwords across platforms.

- How It Bypasses Access Control

  - Weak authentication methods, such as username/password combinations without MFA (Multi-Factor Authentication), are exploited by hackers.
  - Thousands of username/password combinations are tried on websites or enterprise systems by automated tools.

- Mitigation Techniques:

  - Implementing rate limiting and IP blocking after multiple failed login attempts.
  - Enforcing strong password policies and multi-factor authentication (MFA).

2. Brute Force Attacks

- Description: Attackers systematically try all possible combinations of credentials to gain unauthorized access.

- How It Bypasses Access Control:

  - Even with strong passwords, attackers may still succeed in breaking into systems by leveraging fast computational power and automated brute force tools.
  - These attacks can be aimed at breaking weak passwords, even those with some complexity.

- Mitigation Techniques:

  - Account lockout policies after a certain number of failed login attempts. o CAPTCHAs or time delays to prevent automated attacks.
  - Use of advanced MFA that goes beyond just passwords.

3. Social Engineering and Phishing Attacks

- Description: Attackers manipulate users into revealing their credentials or installing malware through deceptive means, such as fake emails, websites, or phone calls.

- How It Bypasses Access Control:

  - Phishing is particularly effective when users are tricked into disclosing credentials or clicking on malicious links that grant attackers access.

o If users are tricked into disabling MFA or other security features, attackers can bypass otherwise strong access controls.

- Mitigation Techniques:

o User education and awareness programs about phishing and social engineering attacks.

o Anti-phishing technologies like email filtering and web filtering.

o Multi-Factor Authentication (MFA) to prevent login even if credentials are compromised.

4. Password Spraying Attacks

- Description: Unlike brute force attacks, in password spraying, attackers attempt to log in with a single common password (e.g., "123456") across many user accounts instead of attempting different passwords for one account.

- How It Bypasses Access Control:

This method bypasses traditional brute force defenses (like account lockouts after too many failed attempts) by using only a few guesses per account, avoiding detection.

- Mitigation Techniques:

o Rate-limiting and account lockout policies for detecting suspicious login attempts. o Enforcing strong password policies and multi-factor authentication to reduce the chances of a successful attack.

5. Privilege Escalation

- Description: Attackers gain unauthorized access to higher levels of privileges or permissions within a system (e.g., from a standard user to admin or root privileges).

- How It Bypasses Access Control:

o Attackers can exploit software vulnerabilities, misconfigurations, or weak access controls to gain elevated privileges and access critical systems.

o Exploiting insecure direct object references (IDOR) or flaws in role-based access control (RBAC).

- Mitigation Techniques:

o Applying least privilege access and enforcing strict access control lists (ACLs). o Regular patching and updates to prevent the exploitation of known vulnerabilities.

o Implementing Privilege Access Management (PAM) solutions.

6. Pass-the-Hash (PTH) Attacks

- Description: Attackers steal and reuse hashed passwords (e.g., NTLM hashes) to authenticate as the victim, bypassing the need for plaintext credentials.

- How It Bypasses Access Control:

o This attack takes advantage of stored hashed password data, enabling attackers to impersonate users without needing to know their actual password.

o PTH attacks are often used in lateral movement across the network to escalate privileges or gain access to more sensitive systems.

- Mitigation Techniques:

Credential isolation and encrypted storage of hashes.

o Implementing multi-factor authentication even for privileged accounts. o Using network segmentation to prevent attackers from moving freely across systems.

7. Man-in-the-Middle (MitM) Attacks

- Description: Attackers intercept and potentially alter communications between a user and a service, gaining unauthorized access or capturing sensitive information like passwords or tokens.

- How It Bypasses Access Control:

o Attackers can intercept login credentials or session tokens, bypassing traditional access controls by injecting malicious code or altering data in transit.

o SSL/TLS stripping can downgrade secure connections, allowing attackers to view or manipulate traffic.

- Mitigation Techniques:

- End-to-end encryption using strong SSL/TLS protocols.
- Secure channels for authentication, such as using VPNs or SSH.
- Using public key infrastructure (PKI) to secure communications and ensure data integrity.

8. Session Hijacking

- Description: Attackers steal session cookies or tokens and impersonate a legitimate user to gain unauthorized access to systems.

- How It Bypasses Access Control:

- By stealing a session token or cookie, an attacker can bypass traditional authentication mechanisms and access the victim's account without needing to log in.

- Mitigation Techniques: Token expiration and re-authentication: Frequent session renewal and token expiration help minimize the window of opportunity for attackers.

- Secure cookie handling: Using HttpOnly and Secure flags to protect session cookies.

- Session timeout policies to automatically log users out after periods of inactivity.

9. Insider Threats and Abuse of Privileged Access

- Description: Malicious or negligent insiders (employees, contractors, etc.) misuse their legitimate access to steal, leak, or modify sensitive data.

- How It Bypasses Access Control:

- Insider threats bypass external access controls because they have authorized access to the system. They may exploit their permissions for malicious purposes.

- Mitigation Techniques:

- Enforcing least privilege and regularly auditing access logs to detect unusual activities.

- Implementing Privileged Access Management (PAM) tools to monitor and control privileged user activities. o User behavior analytics (UBA) to detect unusual patterns of activity, such as accessing sensitive data not required for their role.

10. Exploiting Misconfigurations in Cloud Environments

- Description: Attackers take advantage of misconfigured access controls in cloud environments, such as overly permissive access to cloud storage or services.

- How It Bypasses Access Control:

oMisconfigurations like open cloud storage buckets, improper identity management settings, or overly permissive roles allow attackers to gain unauthorized access to cloud systems.

- Mitigation Techniques:

Implementing cloud security posture management (CSPM) tools to detect and fix misconfigurations.

- Adopting Zero Trust principles to ensure all cloud-based access is continuously verified.
- Regular audits of access controls and permissions in cloud environments.

11. Sudo Caching Attacks

- Description: Attackers exploit the ability of sudo (on Linux/Unix systems) to cache credentials, enabling unauthorized users to escalate their privileges.

- How It Bypasses Access Control:

- Attackers can manipulate the cached credentials or exploit vulnerabilities in sudoers configuration to run commands with elevated privileges.

- Mitigation Techniques:

- Disabling sudo caching and requiring users to authenticate every time they attempt to elevate privileges.

- Regularly reviewing and restricting the sudoers file for excessive privileges.

The landscape of access control bypass methods is constantly evolving. Attackers are using increasingly sophisticated techniques to exploit weaknesses in access control mechanisms, from credential stuffing and social engineering to advanced attacks like privilege escalation and session hijacking. Organizations must stay vigilant and continuously enhance their access control policies, employ advanced security technologies like MFA, behavioral analytics, and zero trust, and ensure proper monitoring and auditing to mitigate these advancedthreats.

3.2 Procedures/Scope of Work

Provide detailed information about proposed procedures, if available, and the scope of work. Include information on activities such as recruiting, training, testing, and actual work required.

Access control mechanisms are critical in mitigating cyberattacks by ensuring that only authorized users and devices can access sensitive systems and data. With the increasing sophistication of cyber threats, modern access control technologies have evolved to provide better security. Here are some of the latest types of access controls that are helping organizations mitigate cyberattacks:

1. Zero Trust Access Control

- **Principle:** "Never trust, always verify."

- **Description:** In a Zero Trust model, every access request is treated as if it originates from an open network, regardless of its source. It assumes that threats could be internal or external and requires verification for every attempt to access systems, data, or applications.

- **Key Techniques:**

  - **Identity and Access Management (IAM)** with strict verification protocols. ○ **Continuous Authentication** using behavioral analytics and device health checks. ○ **Least Privilege Access** (access only to the resources necessary to perform a task).
  - **Micro-Segmentation**: Dividing the network into smaller, isolated segments to limit the lateral movement of attackers.

2. Identity and Access Management (IAM) with AI/ML Integration

- **Principle:** Utilize machine learning (ML) and artificial intelligence (AI) to enhance IAM processes.

- **Description:** Advanced IAM solutions now integrate AI and ML to automatically assess user behaviors and access patterns. These technologies can detect anomalies that may indicate malicious activities or unauthorized access attempts.

- **Key Features:**

  - **Behavioral Analytics**: Identifying deviations from normal usage patterns.
  - **Risk-based Authentication**: Adjusting access levels based on real-time risk assessments (e.g., based on the user's location, device, or network).
  - **Adaptive Authentication**: Continuously assessing access conditions and applying higher security measures when needed.

3. Multi-Factor Authentication (MFA) and Continuous Authentication

- **Principle:** Requiring multiple forms of verification to ensure a user's identity and continuing to authenticate during a session.

- **Description:** Traditional MFA uses two or more factors to authenticate users (e.g., a password and a fingerprint). Modern solutions take this a step further by continuously authenticating users during their session using biometrics, device behavior, or other contextual factors.

- **Key Technologies:**

  - **Biometric Authentication** (fingerprint, face recognition, etc.).
  - **Device-based Authentication** (using a trusted device for verification).
  - **Contextual Authentication** based on the user's environment, behavior, and location.

4. Privileged Access Management (PAM)

- **Principle:** Control and monitor the use of privileged accounts that have elevated access rights.
- **Description:** PAM tools ensure that privileged access to critical systems is restricted, tracked, and managed carefully to prevent misuse. It helps mitigate insider threats and reduces the risk of credential theft.
- **Key Features:**
  - **Least Privilege**: Ensuring users have only the minimum access needed for their role.
  - **Session Recording and Monitoring**: Monitoring and recording activities performed by users with elevated access.
  - **Time-bound Access**: Granting temporary access based on specific tasks or time limits.

5. Behavioral Biometrics

- **Principle:** Uses unique behavioral traits to authenticate and continuously verify users.
- **Description:** Instead of relying only on static factors like passwords or physical biometrics, behavioral biometrics monitor user actions such as typing speed, mouse movements, or even how they swipe a mobile device. Any irregularities in behavior can trigger additional security checks or alerts.
- **Applications:** This technology is gaining traction in both mobile apps and enterprise environments, providing continuous authentication.

6. Contextual Access Control

- **Principle:** Adjust access policies based on contextual data.
- **Description:** Access controls are applied based on the context of the request. Factors such as the user's location, device type, time of access, network conditions, and behavior patterns help determine the level of access granted.
- **Use Cases:**
  - A user accessing a system from a trusted office network may get different privileges compared to accessing it remotely.
  - Adjusting access rights based on whether the request is from a corporate network or a potentially compromised one.

7. Blockchain-based Access Control

- **Principle:** Using distributed ledger technology (DLT) to decentralize and secure access management.
- **Description:** Blockchain allows tamper-proof records of access events, enhancing accountability and reducing the risk of unauthorized access. It can be used to verify identities and enforce access policies.
- **Advantages:**
  - **Immutability**: Ensuring that access records cannot be altered or erased.
  - **Decentralization**: Reducing the reliance on a central authority, which can be a point of failure or attack.

8. Risk-Adaptive Access Control (RAAC)

- **Principle:** Adjusting access controls based on the risk level of the request.
- **Description:** RAAC evaluates the risk associated with each access request based on factors such as the user's profile, the sensitivity of the requested resource, and environmental conditions (e.g., time of day or geographical location). If a high-risk factor is detected, the system can require more stringent authentication or deny access altogether.

- **Key Features:**

○ **Dynamic Access Policies**: Adjusting access rules in real-time based on risk evaluations. ○ **Real-time Risk Assessment**: Analyzing user actions or requests in context and enforcing appropriate access restrictions.

9. Single Sign-On (SSO) with Federated Identity Management

- **Principle:** Allowing users to authenticate once and gain access to multiple systems or services without needing to log in again.

- **Description:** SSO solutions combined with Federated Identity Management (FIM) improve user convenience while maintaining high security. It reduces the need for multiple passwords, decreasing the risk of password fatigue and unauthorized access due to weak or reused credentials.

- **Integration with MFA**: Enhancing SSO by combining it with multi-factor authentication.

10. Access Control based on Device Security Posture

- **Principle:** Assessing the security status of the device before granting access.

- **Description:** Access to systems is conditional upon the security state of the device being used. This includes checks like whether the device has up-to-date antivirus software, proper encryption, and a secure configuration.
- **Use Cases:** If a user tries to access a sensitive resource from an outdated or unsecured device, the access attempt may be blocked or flagged for review.

11. AI-Powered Threat Detection and Response Systems

- **Principle:** Using AI to detect suspicious access patterns and automatically respond to threats.

- **Description:** AI-powered systems monitor for anomalous access behavior and can respond automatically (e.g., by locking accounts or adjusting access rights) in real time. This helps to rapidly contain threats before they escalate.

The evolving threat landscape demands more advanced and dynamic access control measures. Zero Trust, AI/ML-enhanced IAM, and multi-factor authentication are among the most effective access control mechanisms available today. By combining these techniques, organizations can significantly reduce the risk of cyberattacks and data breaches.

3.3 Case Study

Case Study – (1)Incident of Credential Stuffing Attack

Scenario: A popular online service, such as an e-commerce platform, experiences a credential stuffing attack. Cybercriminals have obtained a list of usernames and passwords from a data breach of another service (e.g., a social media platform). They use automated bots to attempt to log in to the e-commerce platform using these credentials.

Data Example:

Stolen Credentials from a Data Breach:

Username: user1@example.com, Password: password123

Username: user2@example.com, Password: 123456 Username: user3@example.com, Password: qwerty Attack Process:Automated Login Attempts: The attackers use a script or bot to automate login attempts on the e-commerce platform, trying thousands of combinations of the stolen credentials.

Success Rate: Even if only a small percentage of users reuse passwords across different services, the attackers can gain access to multiple accounts. For example, if 1% of users have reused their passwords, and the attackers try 10,000 credentials, they could potentially gain access to 100 accounts.

Consequences: Once inside, attackers can make unauthorized purchases, steal personal information, or engage in other malicious activities.

Mitigation Strategies

1. Implementing Rate Limiting

What is Rate Limiting? Rate limiting restricts the number of requests a user can make to a server in a given time frame. This helps to prevent automated scripts from making too many login attempts.

Implementation Example:

Threshold Setting: Limit login attempts to 5 per minute per IP address.

Response to Exceeding Limit: If an IP exceeds this limit, return a 429 Too Many Requests HTTP status code and temporarily block further attempts for a specified duration (e.g., 15 minutes).

Sample Code (Pseudocode): python # Pseudocode for rate limiting from time import time
Dictionary to store login attempts

login_attempts = {} def login(username, password, ip_address): current_time = time()
# Initialize login attempts for the IP if not present

if ip_address not in login_attempts:

login_attempts[ip_address] = []

# Remove attempts older than 1 minute
login_attempts[ip_address] = [attempt for attempt in login_attempts[ip_address] if attempt >

current_time - 60]

Check if the limit is exceeded if len(login_attempts[ip_address]) >= 5: return "429 Too Many Requests: Please try again later."# Proceed with login logic if authenticate (username, password): login_attempts[ip_address].append(current_time)
Log the attempt return "Login successful" else: login_attempts[ip_address].append(current_time)
Log the attempt return "Invalid credentials"

2. IP Blocking

What is IP Blocking? IP blocking involves preventing specific IP addresses from accessing the server, especially those identified as malicious or exhibiting suspicious behavior.

Implementation Example:

Identify Malicious IPs: Use threat intelligence feeds or logs to identify IP addresses that are known to be associated with credential stuffing attacks.

Block IPs: Add these IPs to a blacklist that prevents them from making requests to the login endpoint.
Sample Code (Pseudocode): python # Pseudocode for IP blocking
blocked_ips = {"192.168.1.100", "203.0.113.5"}

Example of known malicious IPs

def login(username, password, ip_address):

Check if the IP is blocked if ip_address in blocked_ips: return "403 Forbidden: Your IP has been blocked due to suspicious activity."
Proceed with login logic if authenticate(username, password):
return "Login successful"

else return "Invalid credentials"
Conclusion

By implementing rate limiting and IP blocking, organizations can significantly reduce the risk of credential stuffing attacks. Rate limiting slows down automated attempts, while IP blocking prevents known malicious actors from accessing the system. Together, these strategies enhance the security posture of online services and protect user accounts from unauthorized access.
Case Study – (2) DDoS attack

A DDoS attack was launched against the U.S. Department of Health and Human Services (HHS) during the COVID-19 pandemic with the intention of interfering with its response activities. By using DDoS defense measures, the attack was lessened, enabling HHS to continue providing vital services and sustaining its vital operations throughout the crisis.
Overview of the HHS DDoS Attack

- The U.S. Department of Health and Human Services (HHS) was targeted by cybercriminals in early 2020 as the COVID-19 epidemic worsened.
- The goal of the attack was to interfere with HHS's capacity to deliver timely pandemic-related information and services.

Details of the Attack

- HHS's online services were subjected to a tremendous rush of traffic during the DDoS attack, which threatened to render its systems inoperable.
- The timing of the attack was especially nefarious because it occurred during a crucial time when people were looking for trustworthy information regarding COVID-19.

Mitigation Efforts

- HHS quickly activated its DDoS protection measures, which included traffic filtering and rate limiting to manage the influx of malicious requests.
- The agency collaborated with cybersecurity experts and federal partners to enhance their defence's and ensure continuity of service.

Impact of the Attack

- **Operational Continuity**: Thanks to the DDoS protection measures, HHS was able to maintain its online services, ensuring that the public had access to vital health information and resources during the pandemic.
- **Increased Awareness**: The incident highlighted the importance of cybersecurity in public health infrastructure, prompting HHS to strengthen its overall security posture against future threats.

Lessons Learned

- **Cybersecurity Preparedness**: The attack underscored the necessity for government agencies and organizations to be prepared for cyber threats, especially during crises when their services are in high demand.
- **Importance of DDoS Protection**: Effective DDoS protection is crucial for maintaining operational integrity and public trust, particularly in sectors dealing with critical information and services.

Conclusion

The DDoS attack on the U.S. Department of Health and Human Services during the COVID19 pandemic serves as a significant case study in the realm of cybersecurity. It illustrates the vulnerabilities faced by essential services and the critical role of DDoS protection in safeguarding public health operations during unprecedented times.

Case Study – (3) SQL Injection AttackThe main purpose of this research is to introduce an accurate concept about SQL injection attack supported with an experiment that has been done. The content of the report will assist people to be aware and conscious about this type of harmful attack, therefore they can protect their data from being exposed to attacks.

SQLi Attack Definition

The starting point for this type of attack is some kind of user-friendly text that interacts with the database, usually the field for entering search information, the user registration field, and the like. When an application vulnerability is found, the attacker will concentrate on identifying the database data he is targeting in order to make accurate changes. In certain instances, the attacker's objective is to get around some authentication procedures, including username verification and passwords during login, rather than alter the database's contents. Like the majority of hacking techniques, this approach relies on trial-and-error techniques and is based on searching the structure, attribute names, tables, and SQL queries (inquiries made inside the database).

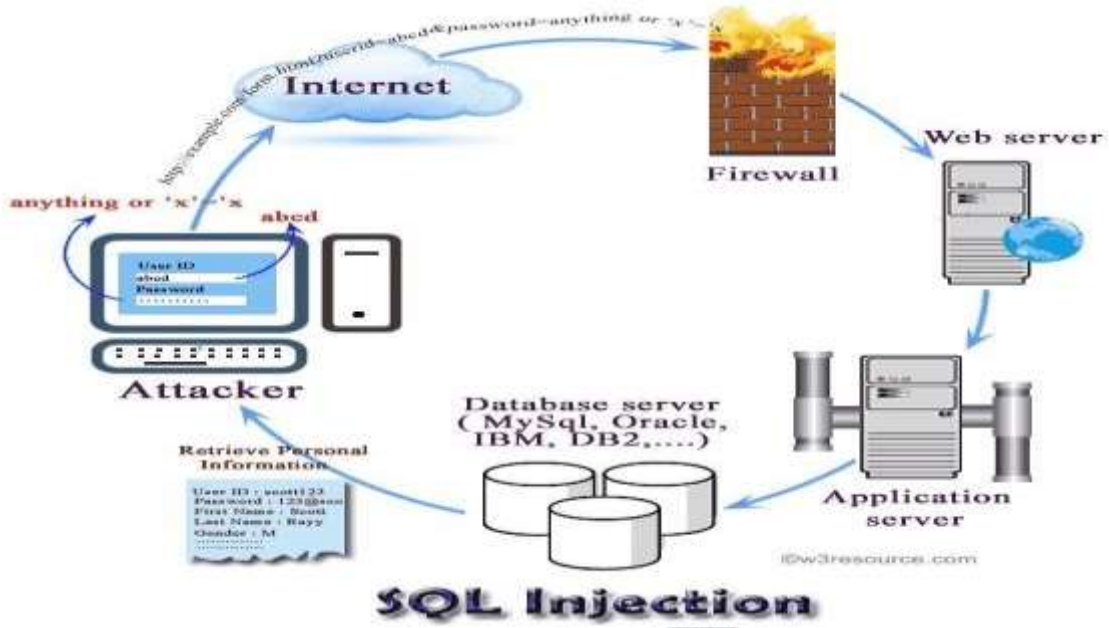


Diagram.1

Attack by inserting SQL code affects:

Confidentiality - Databases typically include sensitive information, including user personal data. Attackers are able to find out user email address information, which they may then utilize for more attacks.

Authentication - In order to bypass standard system login, SQL Server insertion attacks are frequently employed. This type of attack allows an attacker to pose as a different user without having the correct password.

Authorization - By using database information to log in as an administrator, the attacker can obtain further control over the database or website.

Data Integrity - Is the ability of an attacker to read and alter data from a database. In the end, the attacker has the ability to wipe out the entire database.

Types of SQLi attacks

SQL Manipulation - means adapting the SQL command through a set of processes, or by modifying a WHERE section to return a dissimilar outcome. The most famous attack is the change of the WHERE section of customer authentication clause, and the WHERE clause each time returns the TRUE result (Mahapatra, 2012).

Code Injection - attack when the attacker insets a new SQL command or database command into a SQL command. Standard Code Injection attack is when SQL Server is added PERFORM command in a defenseless SQL command. Code Injection is working only while numerous SQL commands are supported on one database request. This option has

PostgreSQL and SQL Server and sometimes it is likely to insert a compound SQL command in Oracle. (acunetix.com, n.d.)

Function Call Injection - Is the supplement of Oracle roles or customize functions in a susceptible SQL command. These call functions can be used to demand commands to the OS or manipulate data from the folder data.

Buffer Overflows - subset of Function Call Injection.

There are vulnerabilities in several types of system database operations in various functional or "open-source" databases that could lead to a shortage of buffers. Most of these vulnerabilities have patches available, but some databases that are currently in use are still patched-unprotected.

Depending on the attacker's aims, a variety of attack types are not utilized in isolation in many attacks; rather, they are used in groups or in succession. Similar to this, there are several assault variations for each strategy; however, this study will focus on a few exemplary examples of these attacks (Mahapatra, 2012).

SQL Tautologies

Objectives of the attack: sidestepping authentication, recognizing vulnerable parameters, extract data.

Explanation: The main objective of a redundancy attack is to insert the code into one or extra provisional commands so that they permanently return the value of TRUE. The imports of this attack hang on the impact of the returned inquiry results on the app. Most frequently, it is employed to get around data extraction and user authentication. The attacker employs a form field whose contents are compared to the WHERE clause inquiry in this type of injection. All of the target table's rows will be returned in the database when the conditions in the tautology are changed. (Pais, Balakrishnan, Chandrasekaran, & Thilagam, 2011)

Example: In the example of an attack, the attacker inserts the code in the form of “or 1=1 – “in “login” place, which results in the enquiry in the database:

CHOICErightAccess FROM users WHERE UserImage = “or 1=1 - THEN Code = ”’THEN

Pin =

Code inserted in the condition (OR 1=1) converts the complete WHERE section into the tautology. Database uses the condition as the base for assessing every row and decides which rows will yield as feedback to the app.

Logically/Illegal Incorrect QueriesObjectives of the attack: Recognizing vulnerable strictures, performing “fingerprinting” databases, extract data.

Explanation: The target of an occurrence is that an attacker collects significant data about the form and configuration of the backend database used by the web application. This type of attack is known as purposeful primary assault, which is the gathering of data for further attacks. The vulnerability of this attack is that the application server's default "error" page is typically very expressive. For instance, an attacker's weak parameters can frequently be found with a brief error notice. Kosta (2008)

Example: This example represents an attack to produce a data conversion error in order to retrieve relevant data. In order to make this error the attacker enters the code in the input field:

The result of this query is: CHOICErightAccess FROM users WHERE Username = “or 1 = 1

- AND Code = “THEN Pin = convert (int, (choice top 1 term from sys-objects where xtype =

“u”))

9

In the attacker's strings, the “choice” query is trying draw the primary user table (xtype = “u”) from metadata table (assuming the application uses ms SQL server, whose metadata table is named sys-objects). After that, the query attempts to convert the table term into digit data type (Mahapatra, 2012).

Union-based SQL injection

Objectives of the attack: To circumvent authentication, extract data.

Explanation: The attacker alters the data set that answers the query in UNION attacks by using weak parameters. By using this technique, an attacker can make an application return data from a different board instead of the table that the developer created the code for. Attackers type their code, UNION SELECT <Inserts remaining query>, to do this. The attackers may easily grab the data from the table because they have taken over the query. As a result of this assault, the database inserts the data requested by the additional query and proceeds with the set of data required by the unique query (Rolston, 2005).

Storage procedures

Objectives of the attack: Denial of application services, remote execution of commands. *Description:* Attackers attempt to carry out stored activities that are already present in the database in these attacks. Manufacturers of the majority of databases nowadays create stored processes that expand the database's capabilities and allow for OS connection. Regretfully, the attacker can carry out operating system operations once they have access to database information. When developing online applications, programmers frequently make the error of assuming that by utilizing system-stored processes, they will be able to escape the SQL injection issue. However, they are unaware that the application is just as vulnerable as other apps. Fayo (2005) Furthermore, because stored processes are often written in different script languages, they may have further flaws like cushion overflow, which gives hackers the ability to extend their privileges or path code control on the server (Rolston, 2005).

Experimental procedures:

We started the attack by searching for a vulnerable website by typing **php?id=1** to find websites that are vulnerable to SQL attacks. We did the attack using Kali Linux, and SQLmap tool. We implemented the attack by doing several steps.

We found three vulnerable websites, we will explain in detail one attack and show you the other two attacks. we started with this vulnerable website www.biblehistory.com/subcat.php?id=2 and we copied the URL and start the attack in Kali Linux.

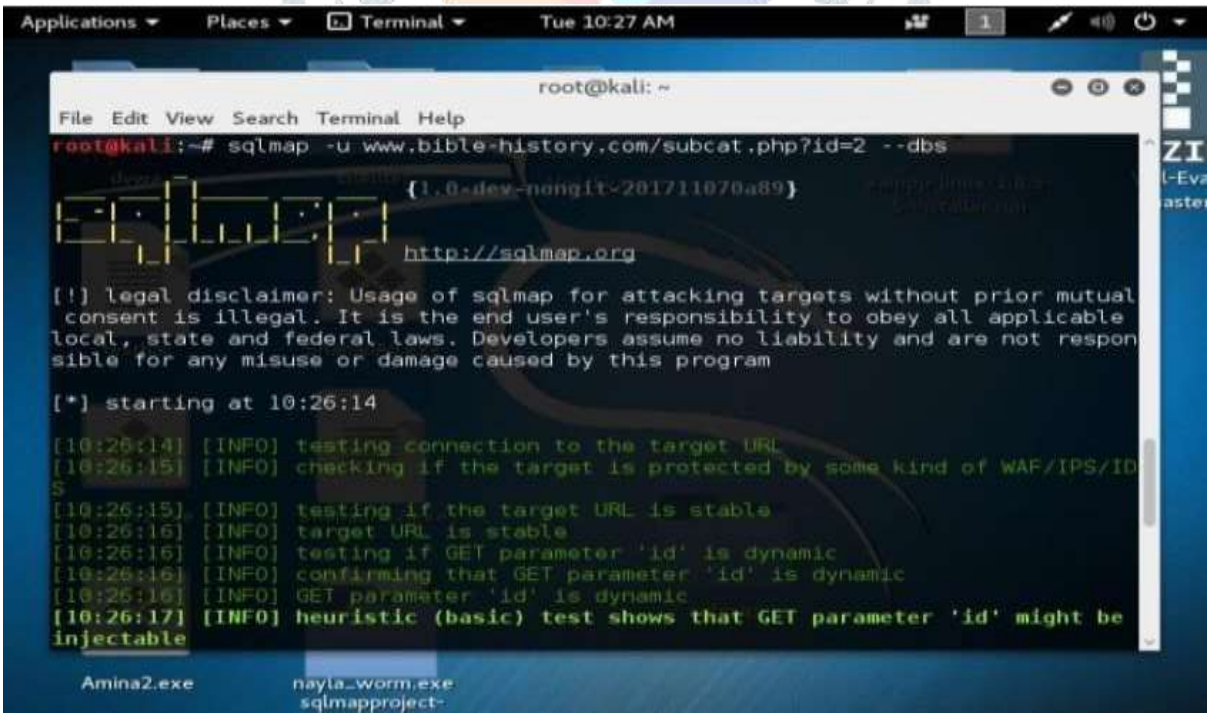


Diagram.2 Fig.1

In fig.1 we typed " Sqlmap –u www.bible-history.com/subcat.php?id=2 -- dbs, and by typing this command we will enter the database of this website.

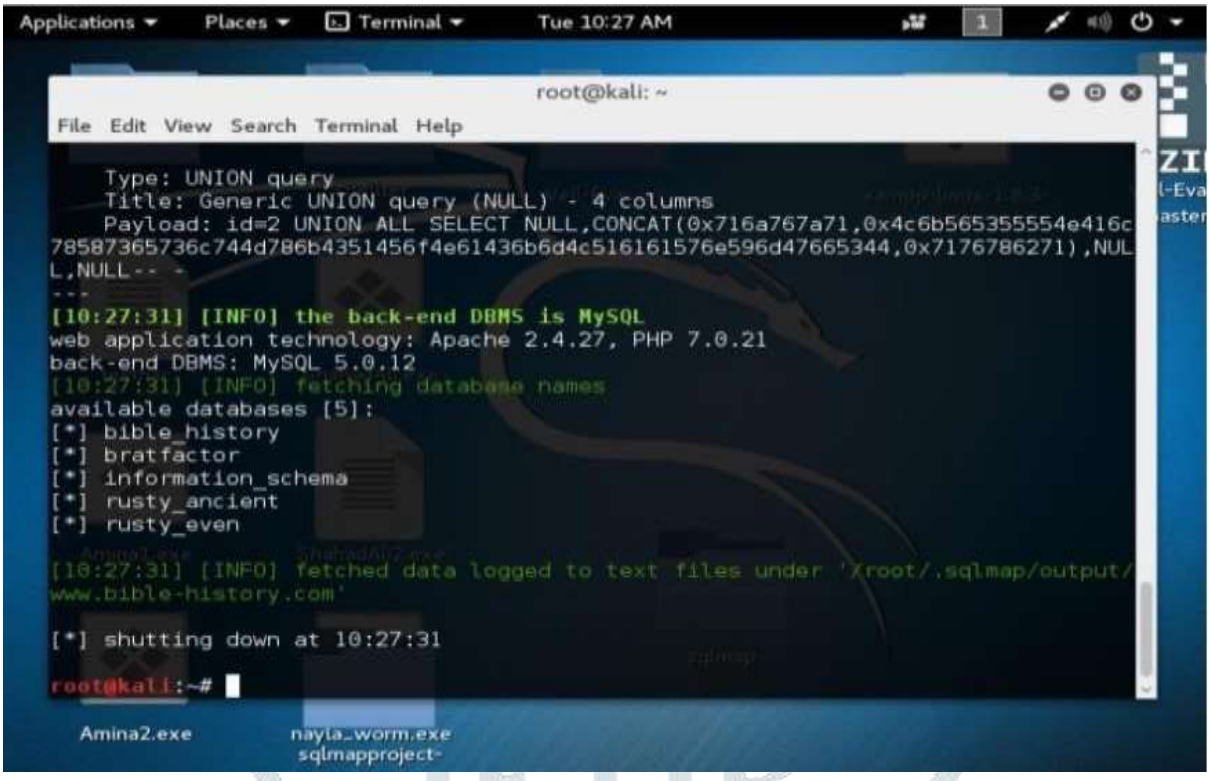


Diagram.3 Fig.2

The result of the previous command in fig.2; we can see that there are 5 available databases.

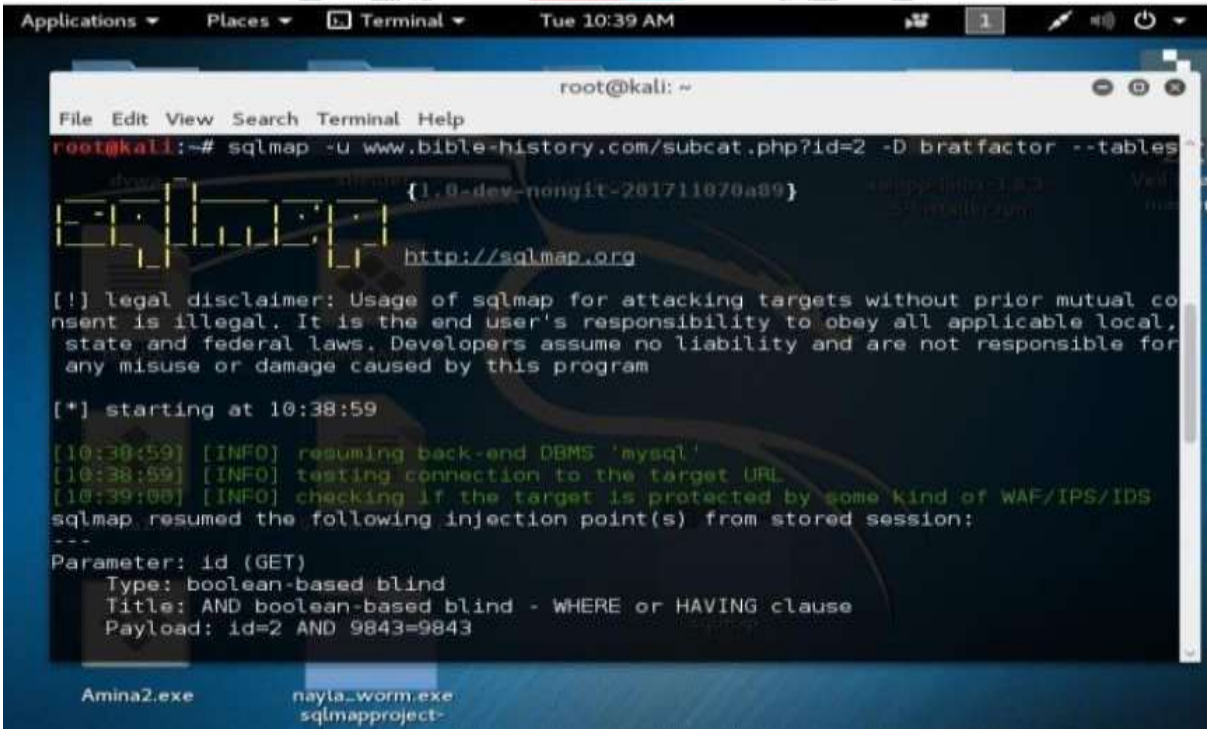


Diagram.4 Fig.3

In fig.3 we choose one of the available databases and used this command; Sqlmap –u www.bible-history.com/subcat.php?id=2 -D bratfactor –tables

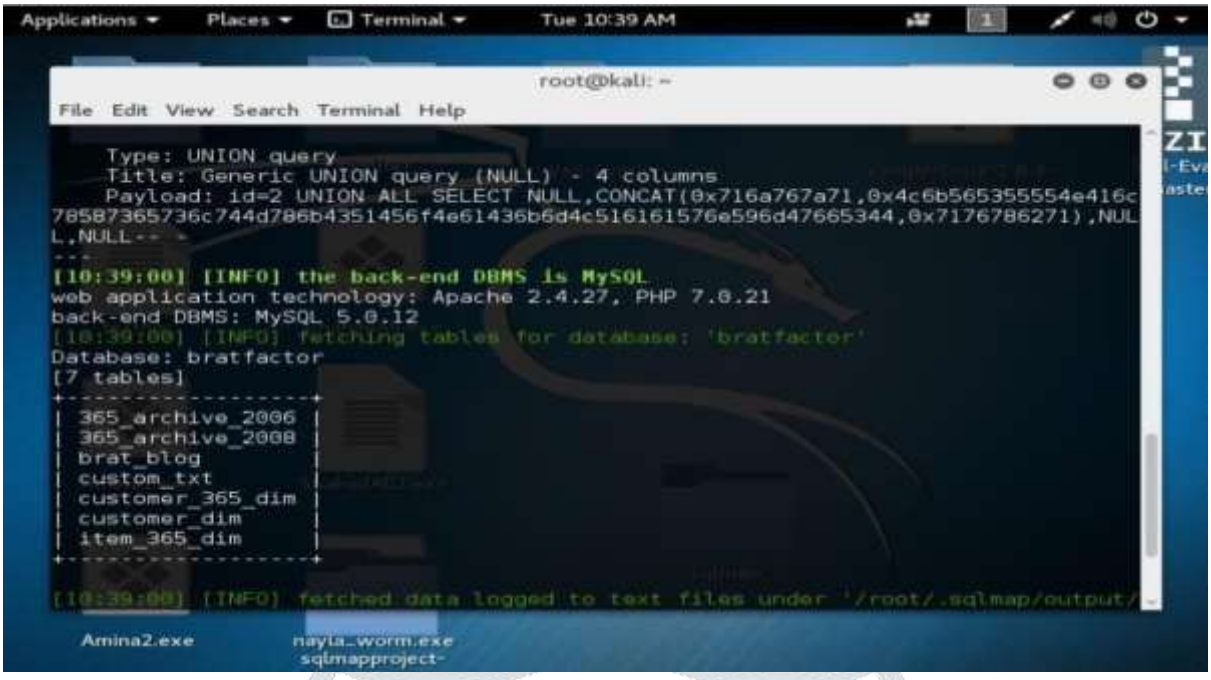


Diagram.5 Fig.4

After that we were able to see the items that are in this database, so we choose one of them to view the details of it by writing this command Sqlmap –u www.biblehistory.com/subcat.php?id=2 -D bratfactor –T customer_365_dim –columns as shown in fig.4

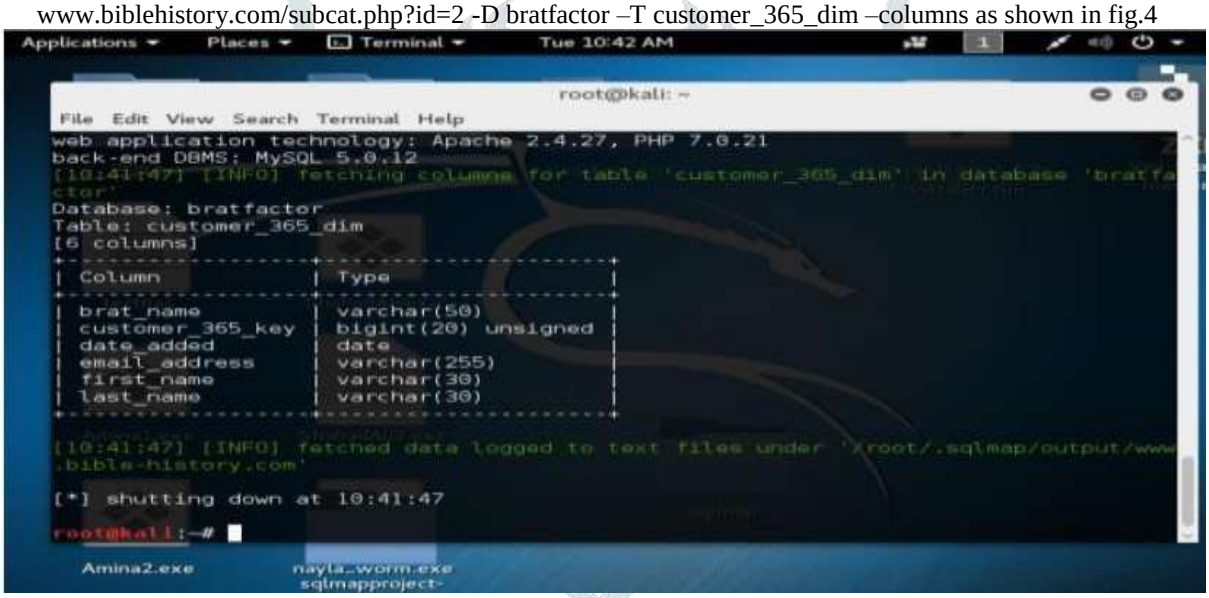


Diagram.6 Fig.5



Diagram.7 Fig.6

As expected the details of the item is displayed now, and we can see that we are able to view the customers private email address, their first and last name and many other details, and to view the details we used this command; Sqlmap –u www.bible-history.com/subcat.php?id=2 D bratfactor – T customer_365_dim –C brat_name,email_address, first_name --dump as shown in Fig 6

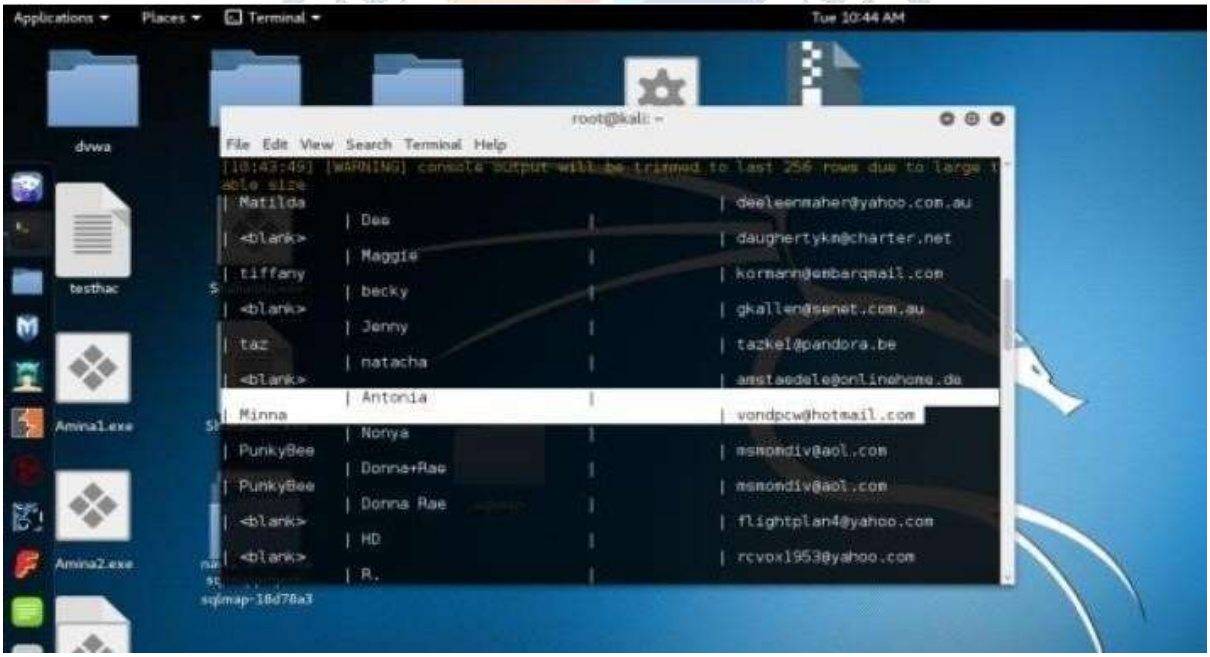


Diagram.8 Fig.7

As we can see now in fig.7 we are able to view the private details of the customers

In addition, we did two more attacks with the same steps in two different websites and here is some captures of the attacks: SQL injection attack 2 in www.uselitewine.com/index.php?id=1 website:

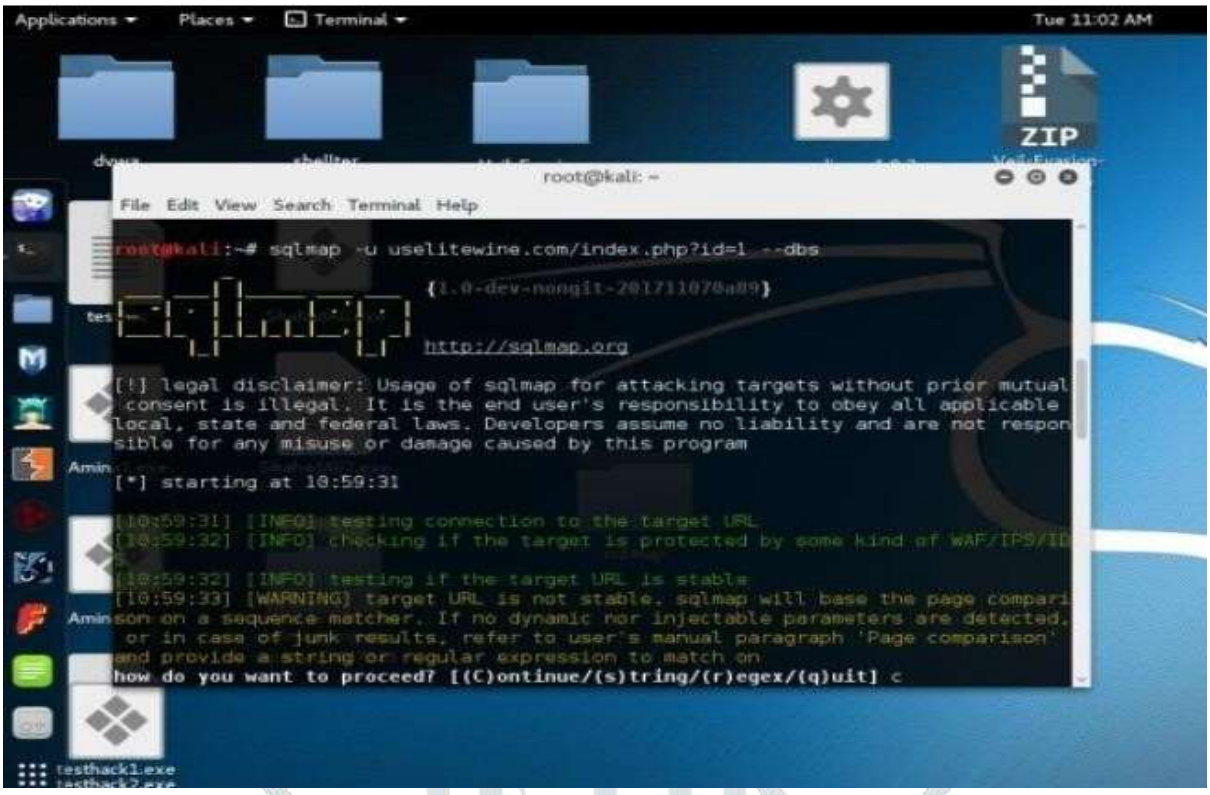


Diagram.9 Fig.1

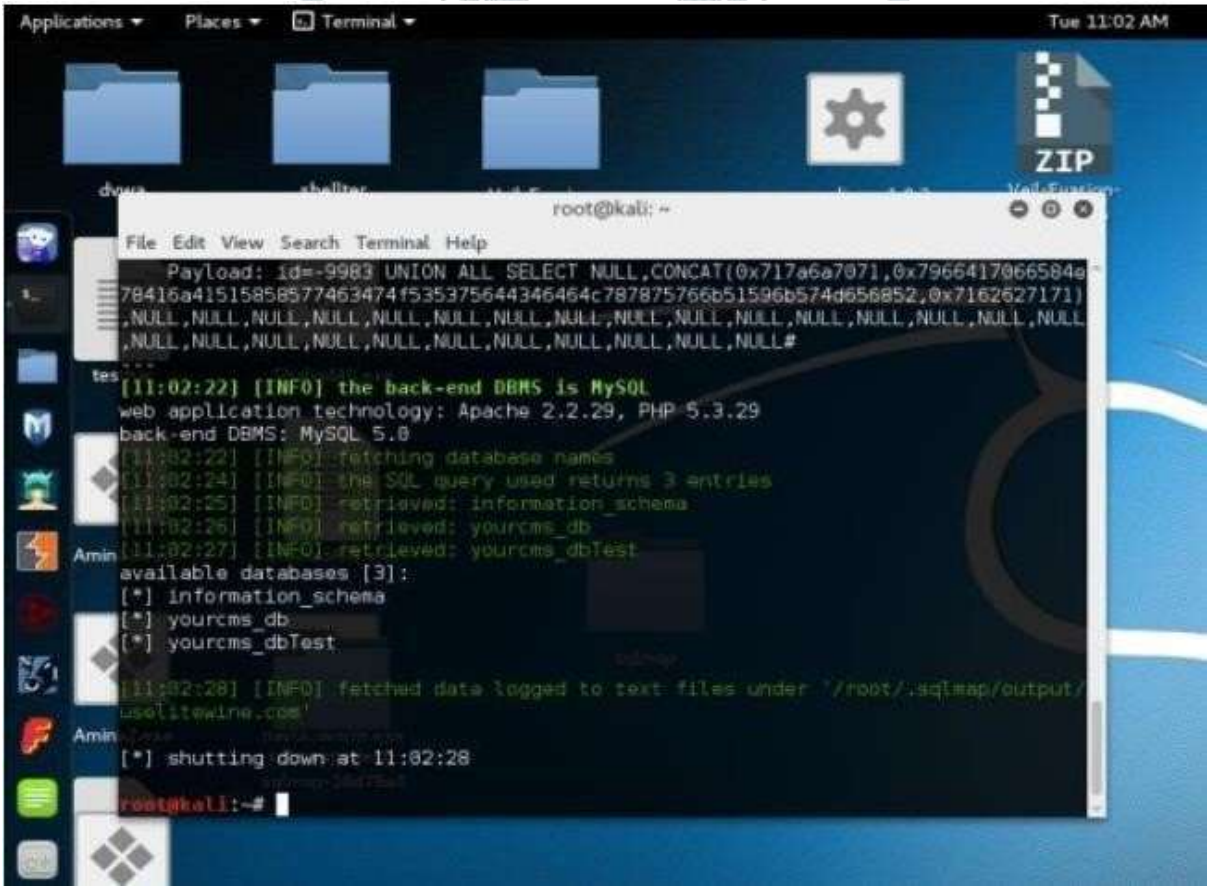


Diagram.10 Fig.2

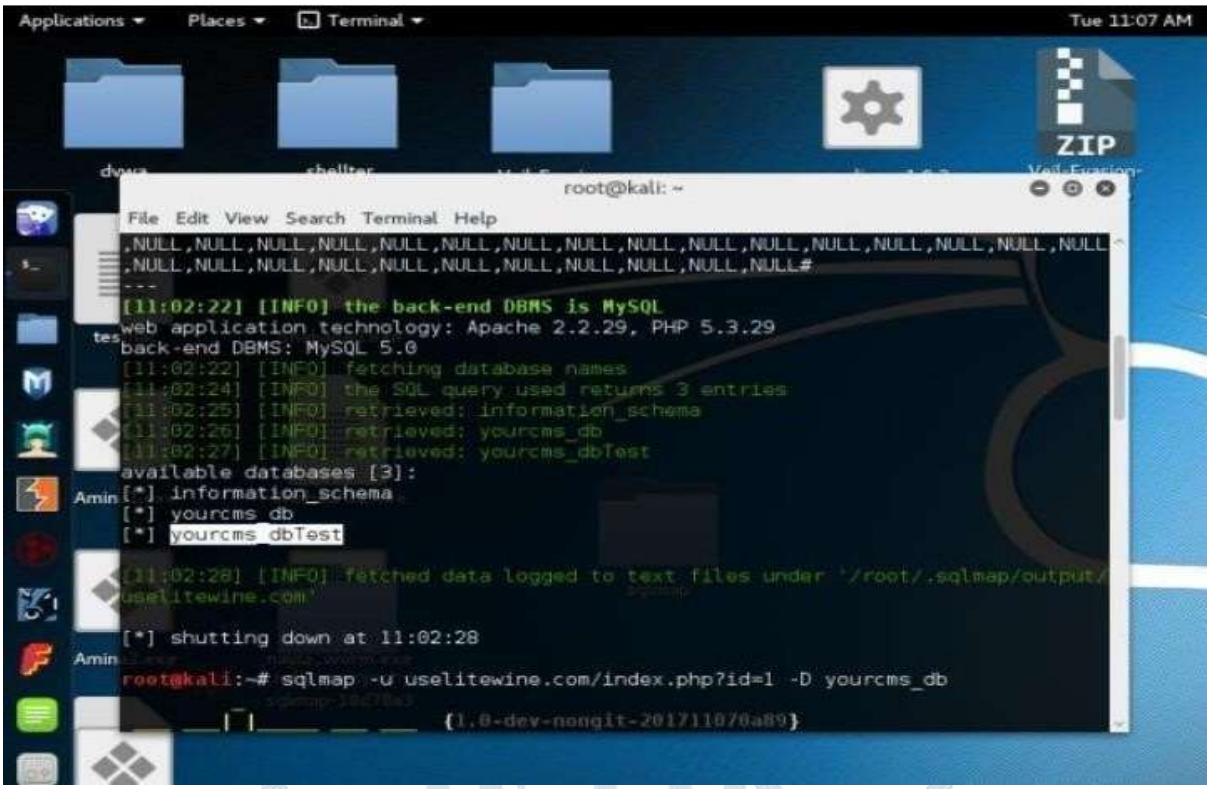


Diagram.11 Fig.3

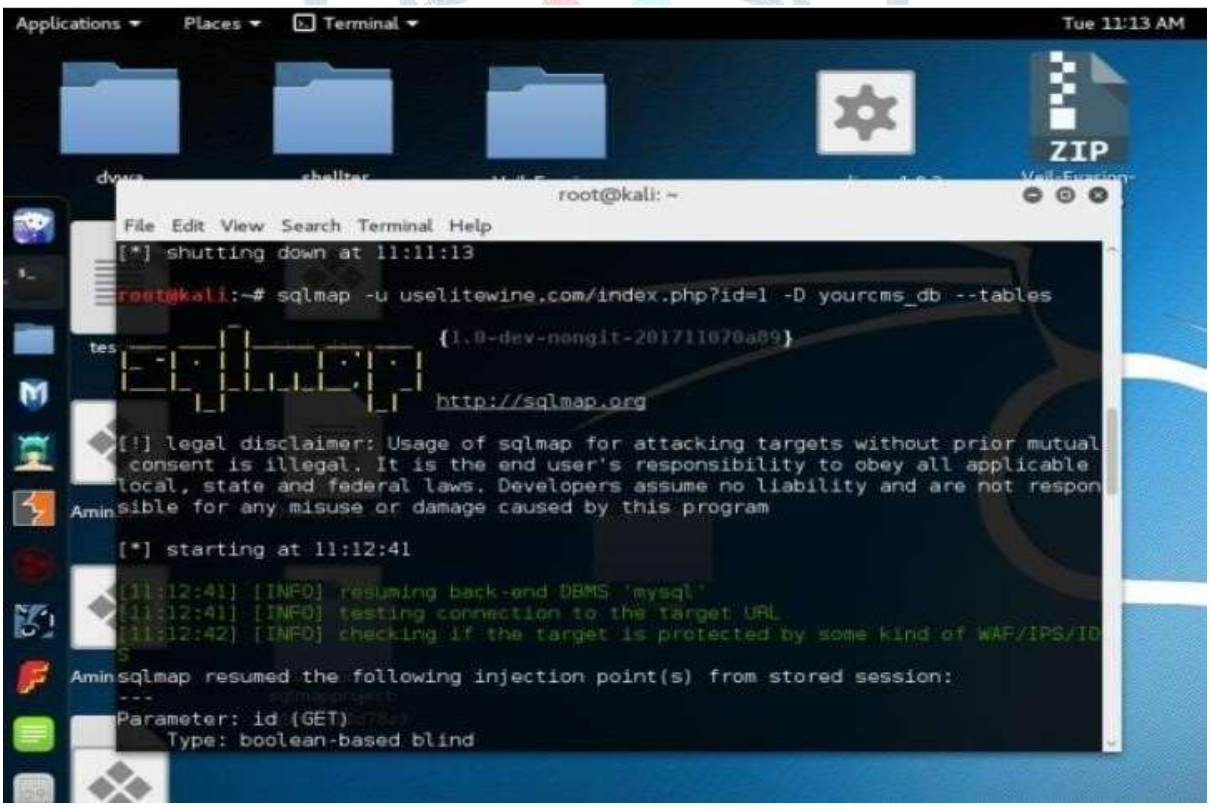


Diagram.12 Fig.4

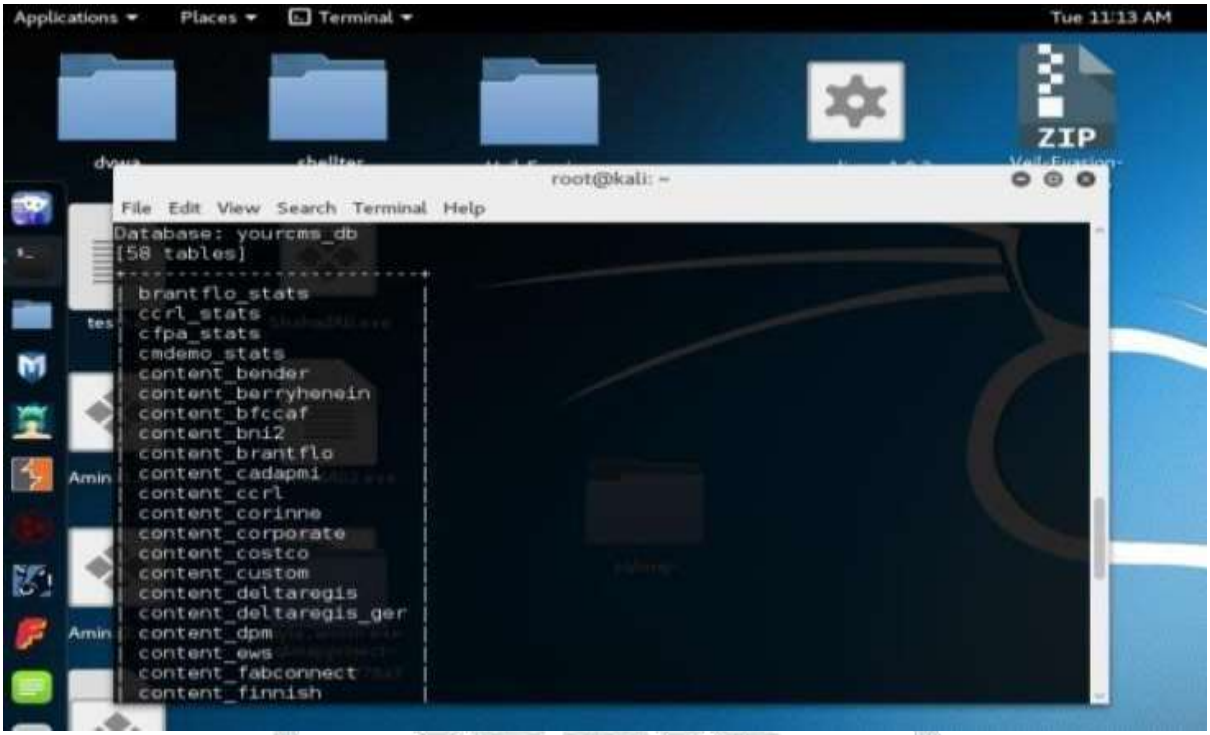


Diagram.13 Fig.5

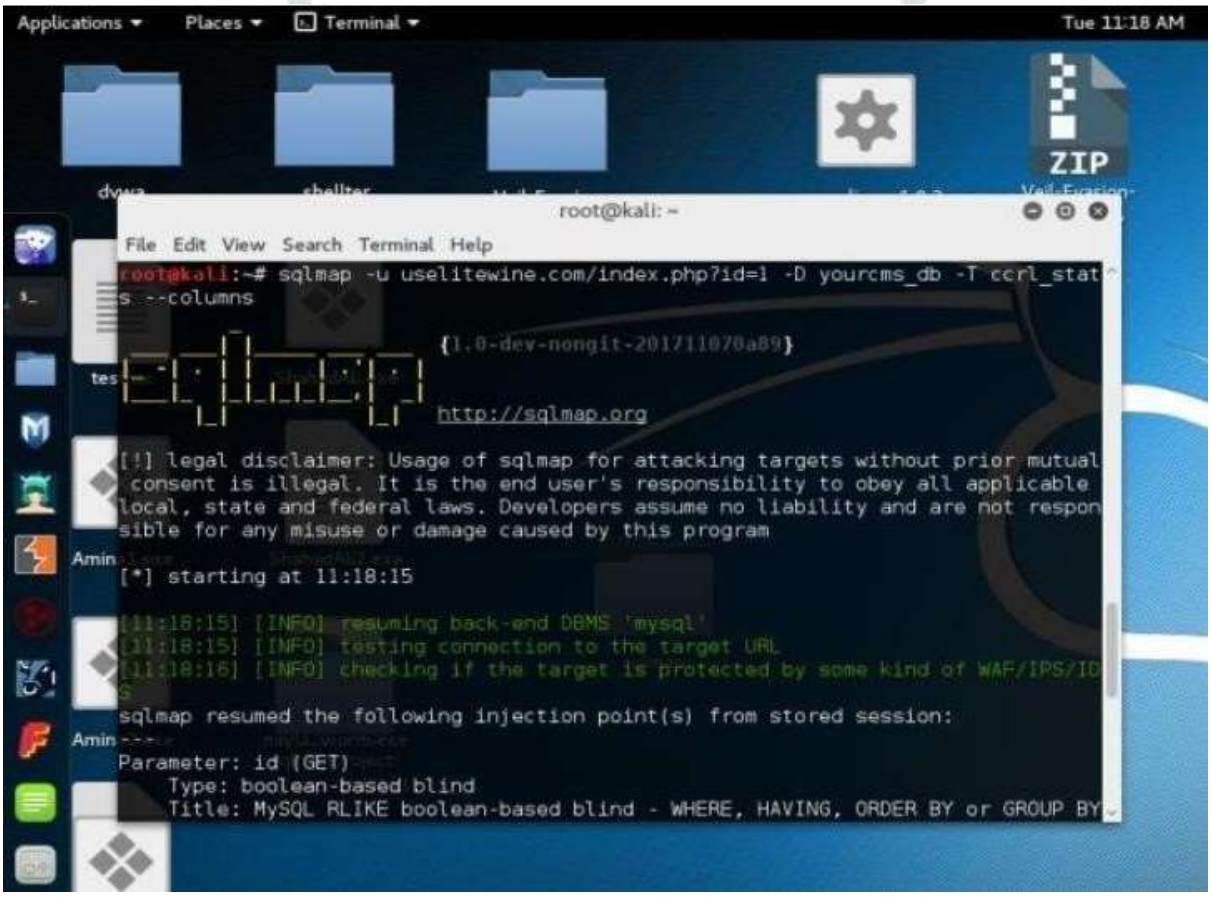


Diagram.14 Fig.6

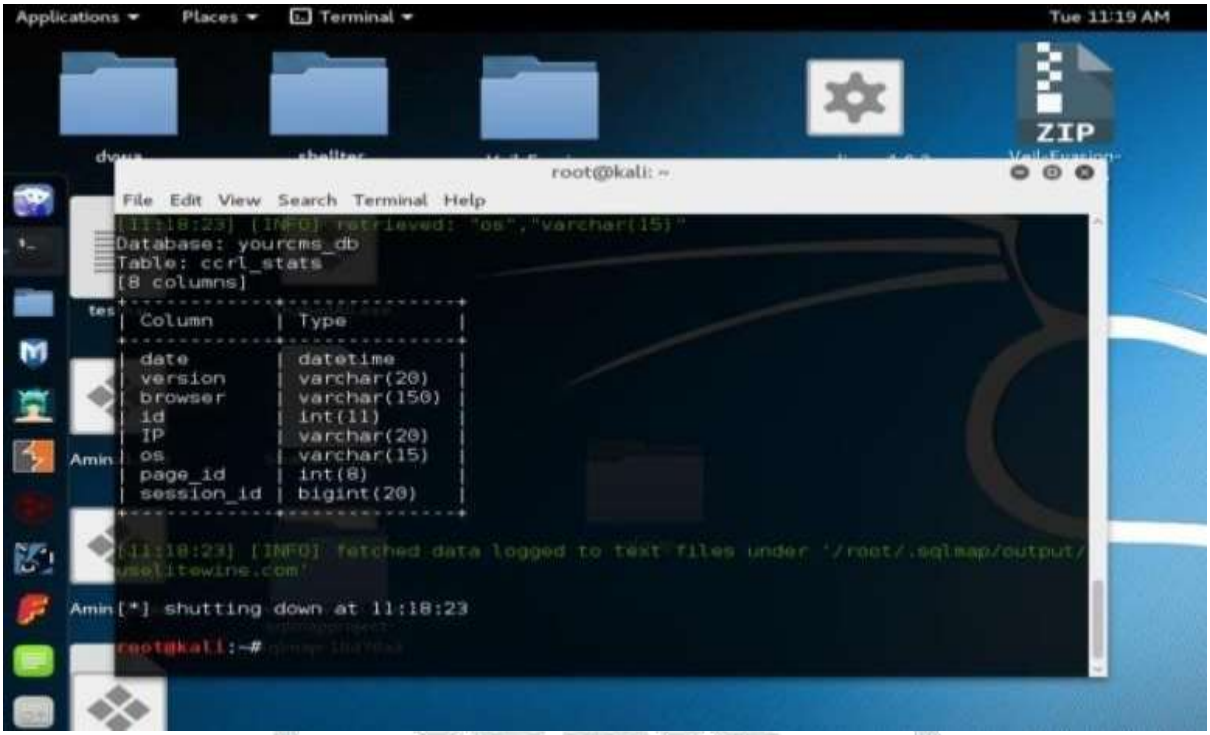


Diagram.15 Fig.7

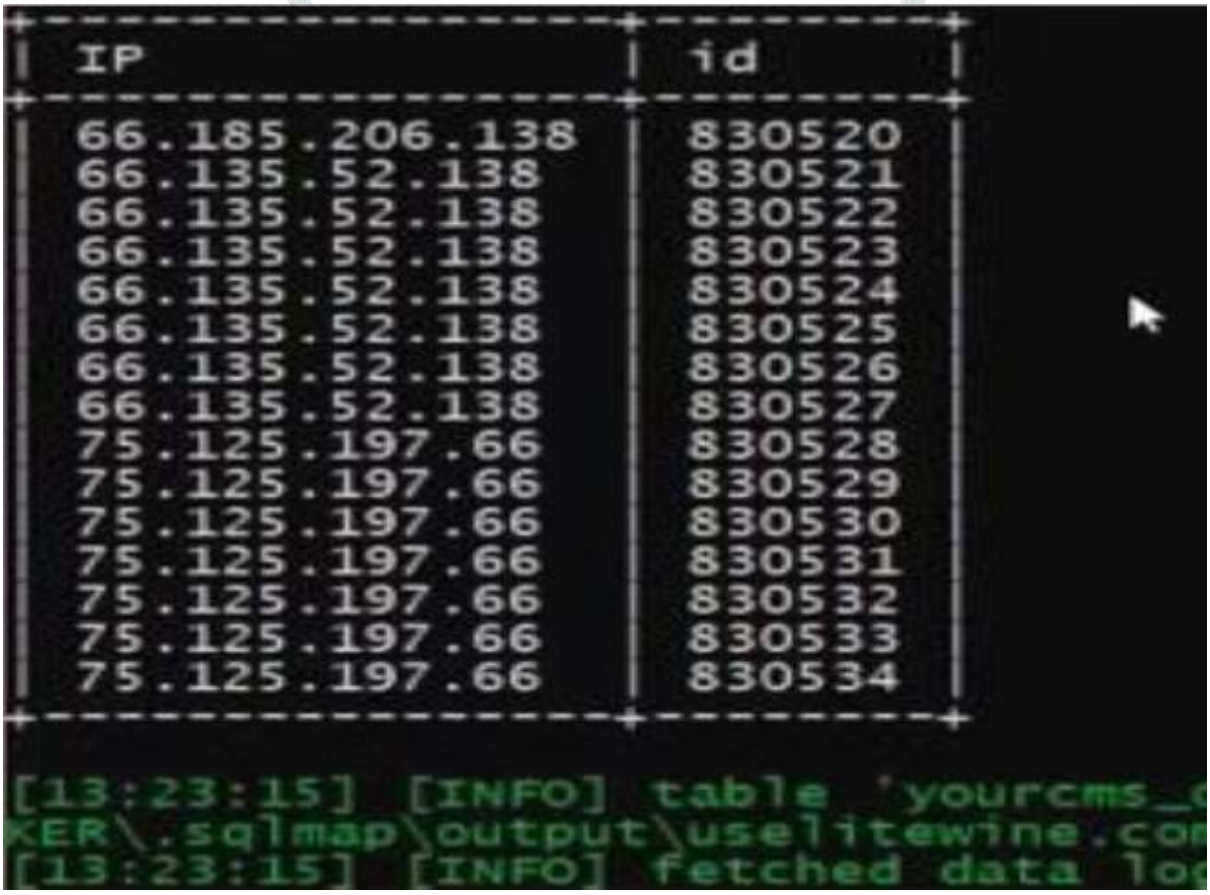


Diagram.16 Fig:8

SQL injection attack 3 in http://ssy.org/detail.php?id=1 website:

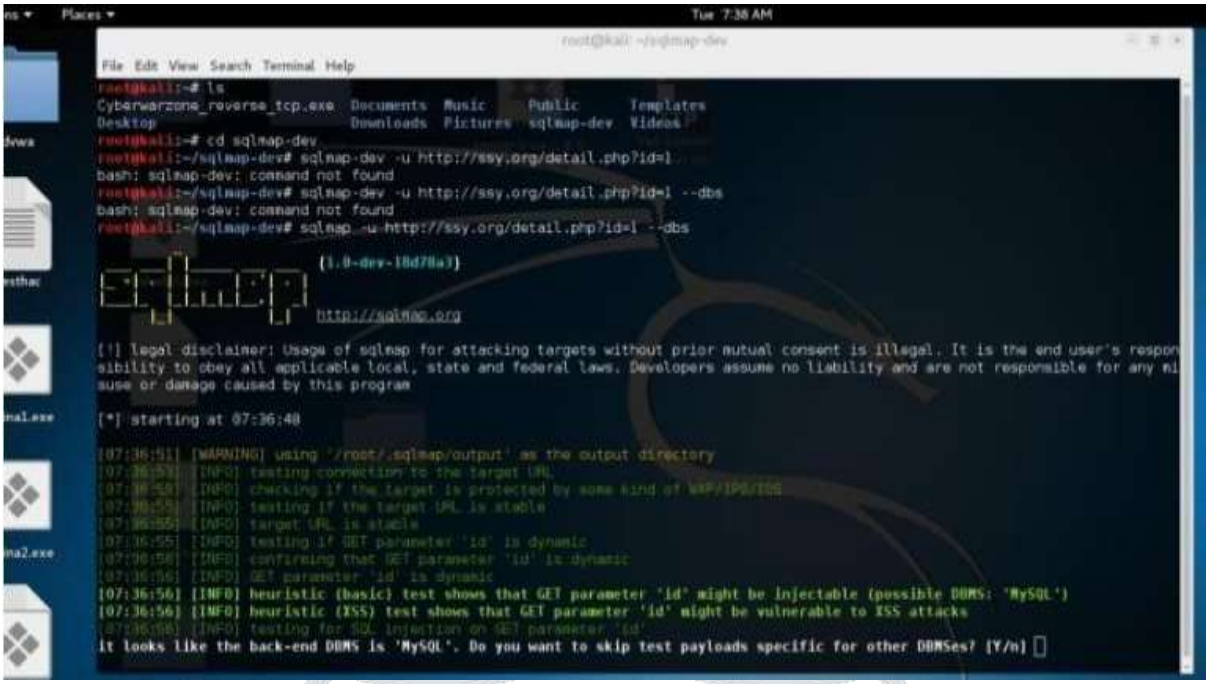


Diagram.17 Fig.1

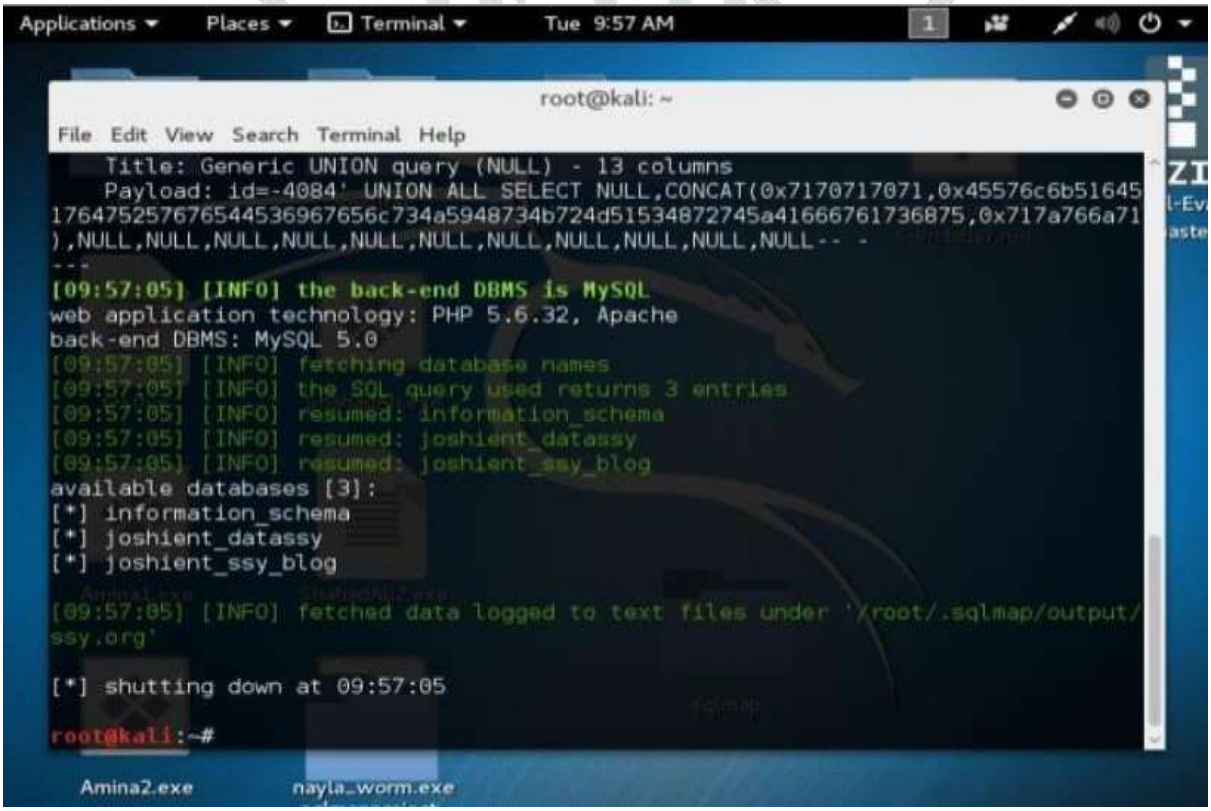


Diagram.18 Fig.2

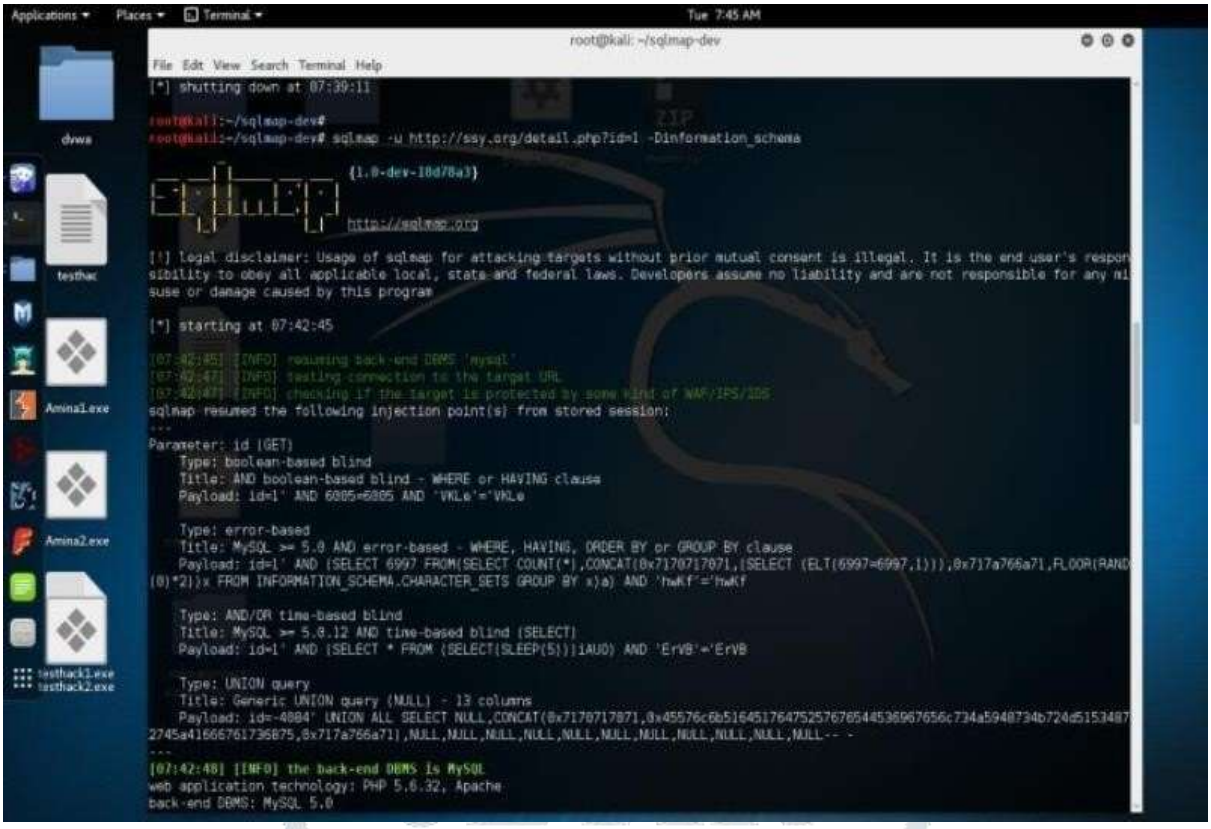


Diagram.19 Fig.3

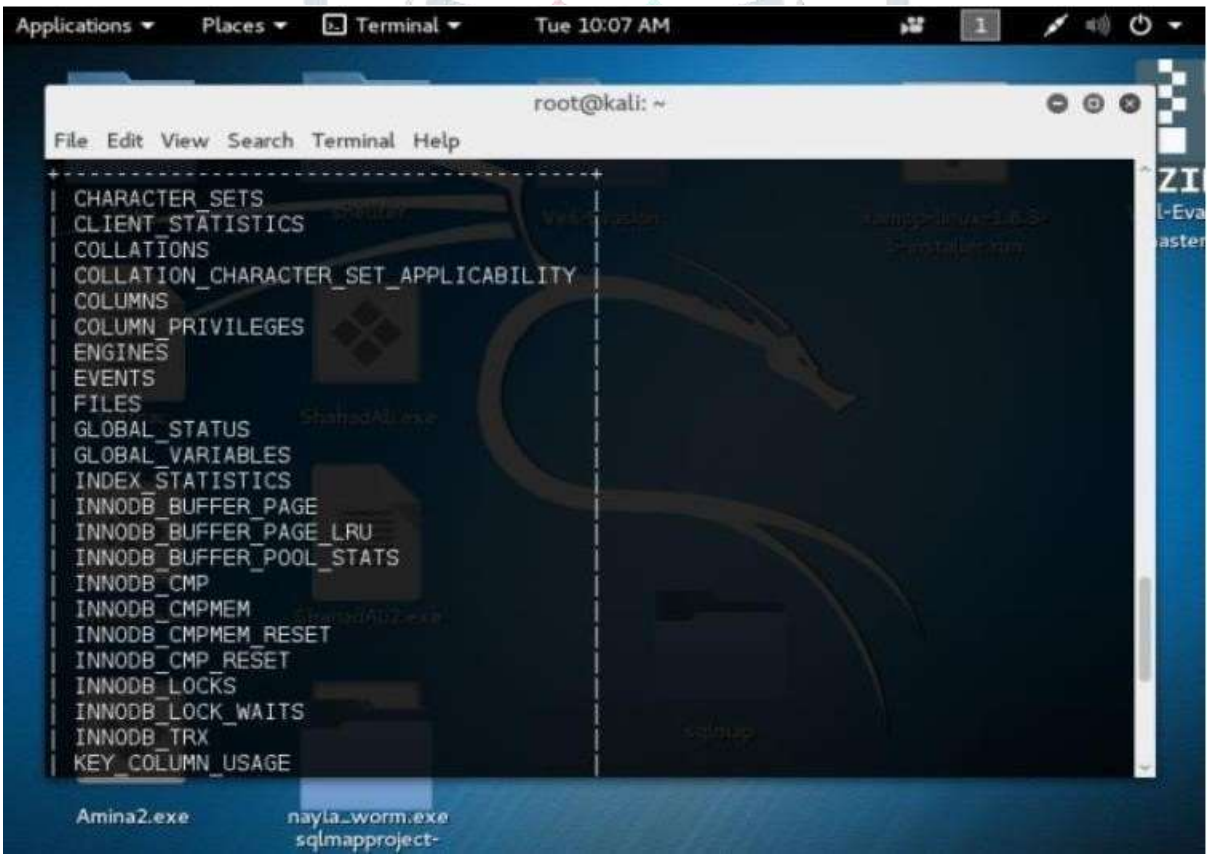


Diagram.20 Fig.4

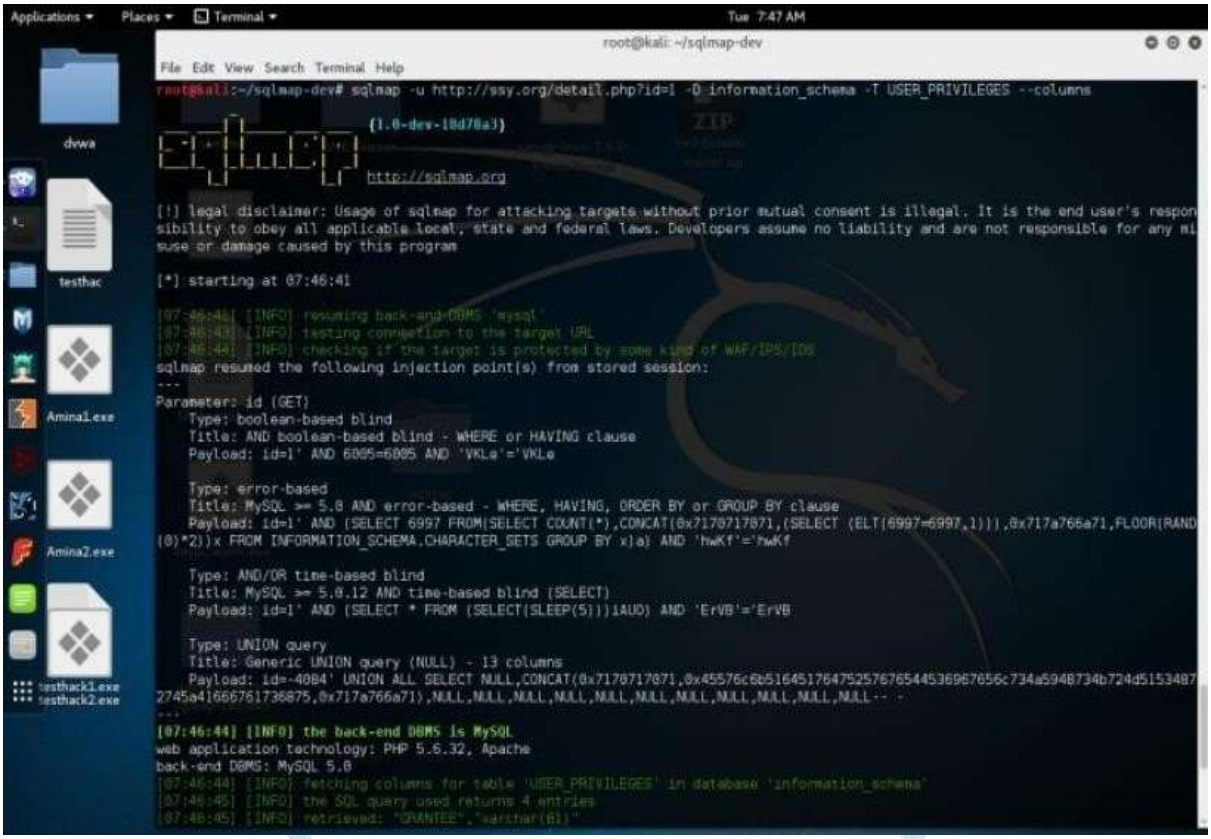


Diagram.21 Fig.5



Diagram.22 Fig.6

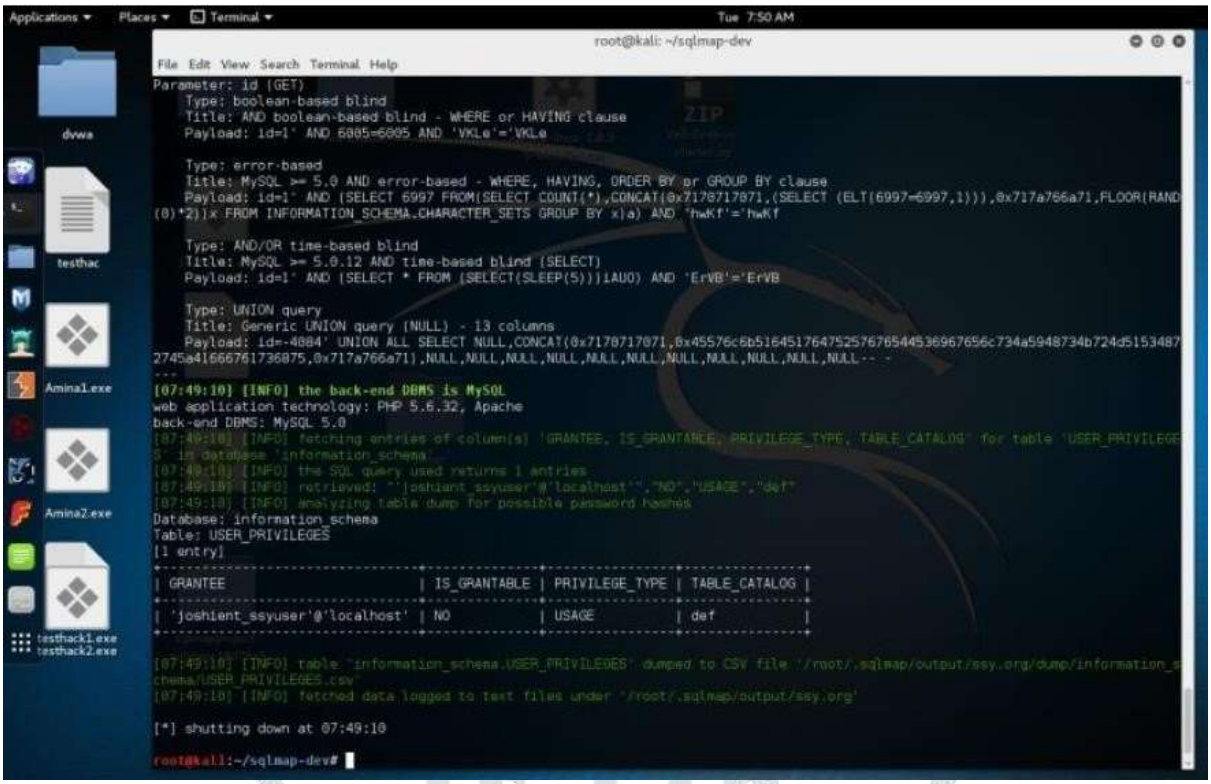


Diagram.23 Fig.7

To protect your application from *SQL Injection, you should follow these key precautions and best practices:

1. Use Prepared Statements (Parameterized Queries)

This is the 1 defense.

Python (with SQLite or MySQL): python

BAD (vulnerable to SQL injection)

cursor.execute("SELECT * FROM users WHERE username = '%s'" % user_input)

GOOD (safe) cursor.execute("SELECT * FROM users WHERE username = ?", (user_input,)) In other languages:

- PHP: Use PDO with bound parameters.
- Java: Use PreparedStatement.
- C#: Use parameterized queries with SqlCommand.

2. Use ORM (Object-Relational Mapping) Tools

Frameworks like SQLAlchemy, Django ORM, Hibernate, and Entity Framework abstract away raw SQL, reducing injection risks.

3. Validate and Sanitize User Input - Only accept expected characters.

- Use regex or allowlists (e.g., letters only, numeric only).
- Reject or escape special characters when necessary (though parameterized queries are still better).

4. Limit Database Permissions

- Avoid connecting as a root/admin user.
- Create a DB user with only the permissions needed.

- This limits damage if an injection does occur.

5. Avoid Displaying Raw SQL Errors

- Show user-friendly messages.

- Log detailed errors *securely* on the server side.

6. Use Web Application Firewalls (WAFs)

A WAF can detect and block known SQL injection patterns.

7. Keep Software Updated

- Regularly update your DBMS, frameworks, and libraries.

- Patches often include security fixes.

8. Escaping (If Necessary)

If you must build dynamic SQL (e.g., for table or column names), sanitize and escape inputs properly. But avoid this if you can.

Real Example of Injection (and why to avoid dynamic SQL) Vulnerable: sql
SELECT * FROM users WHERE username = 'admin' --' AND password = 'anything'

The -- turns the rest into a comment, letting the attacker log in without a password.

SCENARIO

SELECT * FROM users WHERE username = 'user_input' AND password = 'user_passw ord';

Test Case

1. **Normal Login Attempt:**

- Input:
- Username: admin
- Password: password123

2. **SQL Query:**

SELECT * FROM users WHERE username = 'admin' AND password = 'password123';

- Expected Result The user is authenticated if the credentials are correct.

3. **SQL Injection Attempt** :

- Input
  1. Username: `admin' --`
  2. Password: `anything`
- SQL Query

SELECT * FROM users WHERE username = 'admin' --' AND password = 'anything';

Explanation: The -- sequence is a comment in SQL, so everything after it is ignored.

The query effectively becomes:

SELECT * FROM users WHERE username = 'admin';

• Expected Result: The attacker is authenticated as the admin user without needing to know the password.

PREVENTION

To prevent SQL injection, use prepared statements or parameterized queries. Here's an example using Python with the sqlite3 library:

```
import sqlite3

# Connect to the database conn = sqlite3.connect('example.db') cursor = conn.cursor()

# User inputs username = input("Enter username: ") password = input("Enter password: ")

# Use parameterized query to prevent SQL injection cursor.execute("SELECT * FROM users WHERE username = ? AND password = ?",
(username, password)) result = cursor.fetchone()

if result: print("Login successful!") else:
print("Login failed!")

# Close the connection conn.close()
```

You have a web application with a login form that takes a username and password. The application uses the following SQL query to authenticate users:

Best Practices for Preventing SQL Injection

1. **Use Prepared Statements**: Always use prepared statements with parameterized queries.
2. **Input Validation**: Validate and sanitize user inputs to ensure they conform to expected formats.
3. **Least Privilege**: Use the principle of least privilege for database accounts. Ensure that the database user has only the necessary permissions.
4. **Stored Procedures**: Use stored procedures to encapsulate SQL queries.
5. **Error Handling**: Avoid displaying detailed error messages to users. Use generic error messages and log detailed errors on the server side.
6. **Regular Security Audits**: Conduct regular security audits and code reviews to identify and fix vulnerabilities.

RESEARCH METHODOLOGY

In the wake of the COVID-19 pandemic, many IT organizations find themselves scrambling to meet the sudden spike in VPN traffic as most employees are choosing to (or have been mandated to) work from home. Unfortunately, this also presents a golden opportunity for malicious attackers to disrupt their targets by launching various types of attacks on the enterprise VPN infrastructure itself.

A large number of organizations still utilize outdated, hub-spoke concentrators and remote VPN apps. This is due to the fact that VPNs have long been viewed as a "fill the gap" component of the IT infrastructure, intended for employees traveling on business or for users accessing company resources during non-business hours. A tiny percentage of all IT traffic was anticipated to pass through the VPN.

One of our key customers in the pharmaceutical industry actually prepped for this day. They built their DDoS defenses based on the premise that the majority of their employees would eventually need to work from home. In order to assess the durability of the various components, they also engaged an outside DDoS testing organization to launch attacks on the VPN infrastructure.

Below are the lessons learnt from the DDoS attack run on their VPN infrastructure.

Lesson #1

It is easy to exhaust resources on VPN concentrators and firewalls, even with a low volume attack.

A carefully designed TCP Blend attack, in which the attacker sends a small number of TCP packets with the SYN flag checked, another batch of TCP packets with the ACK flag, another set of URG packets, and so on, was able to bring the network firewalls

to the point where they could no longer handle any more new connections, even at an attack volume as low as 1 Mbps. Because the volume thresholds don't activate, the majority of DDoS defenses don't either.

You must adjust your hosts, firewalls, and DDoS policies to defend against this kind of attack. A "SYN defender" or "embryonic connection" function included in many network firewalls can guard against SYN Floods. Use characteristics that enable out-of-state packet identification and prevention for the DDoS policy.
Since the policies are entirely under the control of the customer and are not shared with other cloud users, an on-premise DDoS mitigation appliance will typically offer more choices for fine-tuning during an attack than a cloud-based DDoS service. Since many mitigation devices have default settings that don't always function well for VPN applications, it's important to specify thresholds that correspond to the number of VPN connections you anticipate using if you utilize rate limiting.

Lesson #2
SSL VPNs are susceptible to SSL floods, just like your web servers.
Two of the DDoS tests were variations of an SSL flood attack. The first attack was a highvolume SSL connection flood. This attack tries to exhaust the server resources using a high volume of SSL handshake requests.

Stateful devices, such as load balancers, firewalls, and VPN concentrators, should be closely watched for TCP sessions and states in order to defend against this attack. Additionally, it will be easier to troubleshoot during a real assault if you create baselines and set up alarms against them.
Reduce session timeouts for connections with no data packets by utilizing firewall capabilities like "concurrent connection limit." Permit a certain number of connections to be made simultaneously from a specified source IP address under the DDoS policy. Reduce session timeouts as well to clear the firewall's connection tables.

Finally, Radware provides a few proprietary defense methods that can assist with SSL floods in the cloud as well as on-premises: DefenseSSL uses behavioral analysis to identify suspicious communication, after which it triggers the built-in SSL module for decryption. The attack is detected and stopped by using a series of challenge response methods that are only applied to suspect communications. A new TLS/SSL session is established between the client and the protected SSL server if the client successfully completes all of the challenges.
This allows subsequent HTTPS requests to go straight to the protected server.

Only on the initial HTTPS session per client, this special deployment strategy allows a solution that introduces zero delay during peacetime and minimal latency during an attack. Behavioral SSL protection can be utilized in situations where a certificate cannot be used for decryption. This can prevent SSL floods without requiring the SSL connection to be decrypted.
[adbutler zone_id="276005"]
A flood of SSL restructuring was the second SSL assault. The processing power required to negotiate a secure TLS connection on the server side can be utilized by an SSL/TLS renegotiation attack. It continuously requests for a revision of the TLS connection or sends the server incorrect data, thereby overusing the server's resources.

Disable of SSL re-negotiation on the server to defend against this attack. It is also necessary to disable weak cipher suites. Another way to relieve your firewall or VPN concentrator is to use SSL offloading with large capacity external load balancers. Radware is capable of defending against this kind of attack in both cloud-based and on-premise situations.

Lesson #3
VPNs are susceptible to UDP floods.
Two of the attack scenarios included UDP floods. One was a randomized UDP flood and the second was an IKE flood. IKE is used for IPSec VPNs for authentication and encryption. Because the UDP port numbers are randomized, use a behavior-based DDoS defense mechanism - e.g. Radware's BDoS - which is capable of detecting UDP floods using real time signature generation.

Lesson #4
Monitoring and alerting are mandatory.
Real-time visibility and parameter adjustment on the DDoS policy, network firewalls, and VPN concentrators were necessary for the prevention of many of the attacks that were carried out. It is essential to have a comprehensive awareness of your typical VPN traffic, including the volume (in Mbps or Gbps) and the typical number of connections that are expected, in order to properly adjust the thresholds. A SIEM can make it simpler to keep an eye on connections across many devices. Additionally, knowing the typical baselines makes realtime tactics like rate limitation and session timeout reduction more effective.
Many of the types of attacks used in the test are similar to what one might expect from a threat entities, even though the lessons above were taken from a controlled DDoS test. Please remember to prepare for DDoS protection while you rush to fill your VPNs to capacity in order to accommodate the growing number of remote workers.

3.1 How to Defend the Network and Applications with End-to-End DDoS Protection Solutions

DDoS attacks pose an increasing risk to companies and organizations as they become more common, powerful and advanced over time. Additionally, the number of potential attacks has increased due to the expansion of attack tools available online. In order reduce the impact of these attacks and guarantee that their network and application resources are still accessible to authorized users, companies must take the initiative to deploy complete DDoS security solutions.

Using advanced behavioral-based detection for both network-layer (L3/4) and applicationlayer (L7) attacks, DDoS security solutions protect organizations against the most powerful DDoS attacks of today. Additionally, it offers unique SSL DDoS

protection, customizable appliance, cloud-based, and hybrid deployment options to meet the needs of each customer, and automatic real-time signature creation to defend against zero-day attacks.

The Challenges of the Modern DDoS Threat Environment

The number of DDoS attacks worldwide is currently at an all-time high. The Russian invasion of Ukraine is at the core of a confluence of events that have led to a surge in the size, frequency, and complexity of DDoS attacks. As a result, the threat landscape is more complicated and hazardous than it has ever been.

Here are some of the key factors impacting DDoS attack activity today:

- Emergence of State Actors

The involvement of state-sponsored groups has resulted in a substantial change in the attack landscape, particularly since Russia invaded Ukraine. These groups, which include separate state-backed organizations such as Killnet, Passion, Zarya, and
NoName057(16), work in tandem with the Russian military, continually emerging, reforming, merging, and splintering. This breakthrough has increased the scope and sophistication of FfoS attacks.

- Increase in Size and Complexity

DDoS attacks have expanded in magnitude and complexity, due to the growth of state-sponsored hacking groups. These groups have created new attack tools that enable larger and more complex attacks. Attackers now use many attack vectors in a single assault, using short bursts of one vector before quickly switching to another. This additional complexity poses a challenge to typical DDoS mitigation solutions.

- Shift to the Application Layer

DDoS attacks are increasingly targeting the application layer, following a longstanding pattern. Botnets, such as the Mirai botnet in 2017, pioneered the use of application-layer HTTP/S vulnerabilities. However, newer botnets established in the aftermath of the conflict in Ukraine have substantially improved these skills. They use complex online DDOS assault tools like as Blood, MHDDoS, and Saphyra, which leverage many attack vectors and mitigation bypass techniques, making them especially difficult to mitigate with traditional solutions.

Key Features of DDoS Protection Solutions

- Behavioural-based Detection

Behaviour-based detection uses advanced, patented machine-learning algorithms to protect against both known and undiscovered threats. It uses machine learning algorithms to automatically discriminate between legitimate user traffic and attack traffic. This enables for more accurate detection with fewer false positives.

- Real-Time Signature Creation

Real-time signature creation techniques offer zero-day security against network and application-layer DDoS attacks such as burst attacks, dynamic IP, DNS attacks, and others. It creates an optimal signature to prevent unknown attacks with a low false-positive rate, even if no prior knowledge of the specific vulnerability exists.

- Advanced Web DDoS Protection

Mitigation of L7 attacks uses the similar behavioural and machine-learning mechanisms as L3/4 DDoS attacks. L7 DDoS

- Managed Services and Attack-Time Protection

The Cloud DDoS Protection Service is fully maintained and supported by the Emergency Response Team (ERT). ERT provides consumers with a single point of contact for both normal and emergency needs, resulting in improved security and cheaper overhead than doing it themselves.

- Industry Leadership

Radware has continually been recognized as a leader in DDoS prevention by leading research organizations such as Gartner, Forrester, IDC, and others. This means you can trust Radware to safeguard your network and applications.

FLEXIBLE DEPLOYMENT MODELS

Diagram.24

Cloud Service

• Infrastructure DDoS Protection

Protects the organization's networks and infrastructure from network-layer (L3/4) volumetric floods, including SSY floods, TCP handshake violations, RFC violations, TCP RST attacks,
ACK floods, UDP floods, and others. Furthermore, it defends DNS infrastructure from DNS DDoS attacks such as DNS query floods, DNS amplification assaults, DNS randomized subdomain attacks, and others.

• Web DDoS Protection

Protects against both volumetric and non-volumetric application-layer (L7) DDoS attacks, including HTTP/S floods, SSL negotiation attacks, SSL floods, low- and slow attacks, and others. The Web DDoS protection add-on employs advanced L7 behavioralbased detection and mitigation to prevent sophisticated Web DDoS Tsunami attacks that employ advanced evasion techniques such as attack vector randomization, dynamic argument parameters, IP spoofing, forged X-Forwarded-For IP, cookie harvesting, and others.

Cloud Service supports both BGP and DNS traffic diversion and can be deployed in multiple deployment models, such as :

o On-Demand Cloud Service

Activated only when a volumetric DDoS attack threatens to take over the organization's internet pipe. Recommended for companies that do not commonly face attacks and for assets that are not mission important.

o Always-on Cloud Service

Provides always-on protection by routing traffic to cloud security scrubbing centers, eliminating the need for on-premises detection and mitigation devices. Radware will analyze and scrub every traffic, eliminating the need for traffic diversions. Recommended for applications that are often attacked, as well as assets that require constant uptime.

- Hybrid DDoS Protection

• Hybrid DDoS defense combines on-premises and cloud-based protection to prevent and mitigate advanced DDoS attacks. This enables organizations to detect and mitigate DDoS attacks at both the network and application layers, regardless of size or complexity.

• This hybrid solution offers a comprehensive and effective solution for businesses seeking to protect themselves against the growing threat of DDoS attacks – tier 1 enterprises that must protect their business and cannot afford downtime at all.

Summary

As distributed denial-of-service (DDoS) attacks become more common, powerful, and advanced, organizations face substantial hurdles in protecting their network and application resources. The expanding number of attack tools available online has broadened the scope of prospective attacks, demanding proactive actions to develop complete DDoS security systems. Radware's DDoS protection solutions efficiently protect organizations from advanced DDoS attacks by combining powerful behavioral-based detection, automatic realtime signature development, unique SSL DDoS protection, and flexible deployment choices.

Businesses who deploy Radware's DDoS protection solutions can effectively fight against today's most sophisticated DDoS attacks, mitigate risks, and ensure the availability and reliability of their network and application resources. With a complete set of capabilities and deployment options, Radware enables businesses to proactively safeguard their digital assets, maintain a secure online presence, and keep ahead of changing threats in the dynamic DDoS environment.

3.2 TOP 10 CYBER SECURITY PREDICTIONS FOR 2025

AI-Driven Cyber Attacks

1.AI is now a hacker's weapon – cybercriminals leverage machine learning for automated hacking, deepfake social engineering, and malware evolution.
2.The rise of Cybercrime-as-a- Service (CaaS) with AI-enhanced phishing, exploit kits, and automated attack tools makes cyber threats more scalable and precise.

Cyber Espionage & Nation-State Threats

1.Geopolitical tensions are driving statesponsored cyber warfare, espionage, and critical infrastructure sabotage worldwide.
2.The push for centralized/localized infrastructure increases the risk of single points of failure, exposing power grids, communication systems, and data centers to cyberattacks

Deepfake & Synthetic Media Exploits

1.AI-powered deepfakes bypass biometric authentication, enabling fraud, identity theft, and unauthorized access to sensitive systems.
2.Fake AI-generated news and propaganda manipulate public perception, financial markets, and political landscapes with alarming efficiency.

Cyber Espionage, Sabotage, and Nation-State Threats

1.Geopolitical cyber conflicts are intensifying, with state-sponsored actors launching attacks on critical infrastructure, finance, and defense systems to destabilize adversaries.
2.Decentralized security risks are growing as nations shift towards localized infrastructures, creating single points of failure that cybercriminals exploit.

3.3 Major Cyber Incidents in 2024

1.LockBit Ransomware Attack (Indonesia) Targeted Indonesia's National Data Center (PDN), disrupting immigration & licensing systems, impacting national services.

2.Undersea Cable Sabotage (Red & Baltic Seas) Coordinated cyber-physical attack on global communication infrastructure, crippling connectivity between Europe, Africa, and Asia.

Shapeshifting & Hyper-Scaling Fraud

1.Fraud-as-a-Service (FaaS) is evolving to enable criminals to exploit AI-generated credentials, automated frauds, and sophisticated financial fraud.

2.Criminals are increasingly exploiting victims through call center scams, false job postings, and internet fraud networks.

Autonomous System Hacks

1.AI-Driven IoT (Internet of Things) devices are extremely vulnerable, since hackers utilize competitive approaches and backdoors to access smart networks.

2.Increased hacks target networked AI-powered technologies that businesses rely on but cannot fully manage.

•Deepfake attacks are expected to expand by 50-60% by 2024, with an estimated 140,000-150,000 global instances.

•From late 2022 to late 2023, there was a 1,265% increase in malicious phishing emails, ascribed to attackers using generative AI tools.

Cloud Infrastructure Attack

1.Cloud misconfigurations, insecure APIs, and insufficient encryption are causing significant breaches in corporate and government environments.

2.Multi-tenant cloud services are vulnerable to sophisticated phishing and supply chain attacks, allowing hackers to access many firms simultaneously.

Identity-Based Attacks

1.Attackers attempt to disable multi-factor authentication (MFA) via compromised credentials, session hijacking, and SIM-swapping tactics.

2.As fake identity ecosystems grow, criminals can build synthetic accounts to avoid standard fraud detection systems.

•AI-powered malware can spread and adapt to security protections in real time, rendering traditional antivirus solutions ineffective.

•Dark GPT" models - Custom-trained AI systems automate phishing, deepfake frauds, and malware production, speeding up and spreading crimes.

"Nearest Neighbor" AI Attacks

1."Nearest neighbor attack" is a new threat that exploits vulnerabilities in networked systems.

2.To prevent lateral attacks from non-owned or managed devices, organizations should use extended perimeter security measures.

Quantum-Powered Cyber Attacks

1.Quantum decryption could make standard encryption algorithms (RSA, ECC) useless, enabling attackers to quickly crack passwords and access critical data.

2.Nation- states and cybercriminals are gathering encrypted data ("Harvest Now, Decrypt Later") to unlock it quickly when quantum computers become powerful enough.

• Why It's Cool & Dangerous?

Quantum computing will transform cybersecurity; defenders must prepare for postquantum cryptography (PQC) before hackers use quantum technology.

3.4Cybersecurity Predictions for 2025

Information technology (IT) has changed dramatically over the past few years, with advances in virtually every aspect of the industry. Cybersecurity, specifically, has evolved from its previous form.

1. The Evolution of Ransomware

The rising incidence of ransomware assaults is the first item on our cybersecurity 2025 forecast. An 81% increase from 2023 to 2024 shows that these attacks are getting more frequent and sophisticated.

Until the ransom is paid, ransomware prevents users from accessing specific computers or even entire networks. Even then, there's no assurance you'll get back everything the attack damaged.

Ransomware that just uses encryption is getting much less frequent. Double extortion is the main strategy used by attackers to coerce victims into paying the ransom. Double extortion is a sophisticated strategy used by attackers to raise pressure on victims to pay the ransom by combining data encryption and data theft.

April 30, 2024 Research from Black Kite analysed nearly 4,900 ransomware attacks to understand malicious actors and their new techniques, their evolving operations and their global impact. Some key findings from the report include:

- Between April 2023 and March 2024, there were 4,893 ransomware attacks reported.
- The United States was the most targeted country, with approximately 2300 attacks.
- Out of the 15 most active ransomware groups, nine are newcomers.

According to the report, attacks are not only increasing in frequency but also speeding up, which implies that ransomware organizations are growing more hostile. Attacks are occurring more often, sometimes in a matter of days. This implies that ransomware groups are keeping an eye on one another's actions in order to take advantage of a vulnerability in a company following an earlier attack. In addition, ransomware gangs are now focusing on smaller enterprises (those with less than $20 million in revenue) instead of the resource-rich organizations they used to target.

April 29, 2024
State of Ransomware 2024: A Year of Surges and Shuffling
Unveiling cybercriminal tactics, collusion, and industry targeting to help you fortify your defenses. Attacks of ransomware have nearly doubled from 2,700+ in 2022 to roughly 4,900 in 2023, which is a concerning increase. This study exposes the changing techniques of these cybercriminals, such as their increasingly complex schemes, intergroup cooperation, and the alarming tendency to target sectors that were previously thought to be off-limits.
Important conclusions include:

- The increase in assaults on healthcare organizations indicates a change in ransomware methods; ransomware attacks have evolved into sophisticated operations coordinated by organized cybercrime syndicates.
- Trends in geographic targeting and recurring victimization highlight ransomware's tenacity and worldwide influence.
- Understanding your supply chain's vulnerability to ransomware risk and implementing proactive cybersecurity measures are crucial for safeguarding your company.

Understanding the dynamics of ransomware attacks is crucial for organizations to bolster defenses and safeguard against potential extortion and supply chain disruptions.

2. Internet of Things Expansion

Another of the most important 2025 cybersecurity threats is the rapid expansion of the Internet of Things (IoT). The IoT refers to a network of internet-connected devices other than smartphones, tablets and computers, such as:

- Smartwatches.
- Wearable fitness trackers.
- Smart home appliances.
- Voice assistants like Amazon Echo and Google Home.
- Car infotainment systems.
- Radio-frequency identification (RFID) tags.

According to projections, there will be more than 32 billion IoT devices in operation globally by 2030.
Your attack surface grows as the number of devices connected to your network increases. Because of all the new endpoints your expansion has created, cybercriminals can sneak into your system.

3. Artificial Intelligence Empowering Cybercriminals

- In 2023 and 2024, the broad application of artificial intelligence (AI) marked a dramatic shift. Companies were able to increase their efficiency, but it also provided new chances for bad actors.
- Here are a few instances:

- Optimized attacks: Even novice attackers can use generative AI and machine learning (ML) technology to produce more complex malware, remove common phishing email signs, or scale their attacks to target more people.
- Data poisoning: An AI's performance can be lowered and erroneous results can be produced when a hacker introduces tainted, biased, or incorrect data into the training datasets.
- Automated malware: Although ChatGPT and Google Gemini, two AI tools, contain safeguards against malicious code, skilled hackers can get around them and exploit the program to generate dangerous code automatically.
- Model stealing: Without having direct access to the original code or training data, attackers can copy an AI model by running queries on it and watching the results.
- Bias exploitation: Attackers may use biases that AI algorithms unintentionally pick up from training data to sway results in their favor.
- AI in deepfakes: AI is capable of producing lifelike spoof audio or video recordings that can be used to disseminate false information or impersonate people.
- Risks associated with autonomous decision-making: Attackers may target or influence AI systems that make decisions on their own, particularly when it comes to defense or vital infrastructure.

4. Public Cloud Growth

While most organizations have fully resumed in-person operations, many continue to offer remote-capable employees the option of working remotely.
Organizations now rely on resources and services from public cloud data centers, such as collaborative software platforms and infrastructure components, since the remote workforce has grown rapidly.
While cloud service providers normally use numerous security steps to safeguard data from intruders, some dangers are impossible to manage.

- Misconfigured cloud settings: Failing to comply with industry rules can result in exploitable vulnerabilities.
- Insider threats: Cybercriminals can readily access public clouds if remote workers willfully leak data or leave their account vulnerable to attackers.
- Sniffing or snooping: Using unsecured network connections to migrate data to the cloud can allow attackers to hijack it during transit.
- Insecure APIs: Public cloud services are frequently accessed through application programming interfaces. If these APIs are not properly secured, attackers can use them to gain illegal access.
- Denial of service (DoS) attacks: Attackers can target cloud services, overwhelming resources and making services unavailable.

5. Extended Reality Vulnerabilities

While extended reality (XR) technologies such as virtual reality (VR) and augmented reality (AR) are gaining popularity in both personal and professional settings, they still lack many of the cybersecurity safeguards provided by the other tools in your IT stack. Some of the potential risks this gap creates include:

- Social engineering: Many XR programs come from third-party developers, which increases the risk of unreliable content manipulating your users to perform specific actions. Vetting your software vendors is key.
- Ransomware: Hackers can insert malicious code or links into VR or AR programs to trick users into activating computer viruses.
- Lack of privacy: VR headsets and AR technologies collect user biometric data, such as retina scans, eye movements and typical behavior patterns. Hackers can use this data to recreate user actions and gain unauthorized access to your system.
- Man-in-the-middle attack: XR applications require real-time data communication between devices and servers. Attackers could intercept this data and change its content or implant malicious code.

3.4.1 Developing Solutions for the Future of Cybersecurity

As technology advances, the IT market gains opportunity to improve security measures against both external and internal threats. Here are some positive trends for the future of cybersecurity.

Immersive Cybersecurity Training
According to Verizon's most recent Data Breach Investigations Report, a nonmalicious human element plays a significant role in 68% of all data breaches. An engaging security awareness training program is one of the most effective strategies to reduce human risk. VR provides new, immersive security training alternatives for employees across multiple industries. Organizations can encourage employees to improve by gamifying learning in an engaging virtual reality.

Virtualized Security Operations Centers
Although security operations centers (SOCs) are essential for any cybersecurity provider, physical centers are becoming increasingly expensive to create and operate. XR technology may provide a cost-effective solution.
VR and AR can enable businesses to establish entirely virtual, interactive SOCs leveraging limitless office platforms, allowing security experts to operate remotely while maintaining the same standard of service. Virtualization could also allow SOC staff to automate timeconsuming and monotonous processes, streamlining workflows and freeing them up to focus on more difficult initiatives.

AI-Enhanced Tools
AI-powered cybersecurity tools can help your organization enhance its security posture with capabilities like:

- Predictive analytics: AI technologies enable your organization to adopt a more proactive stance by predicting potential cybersecurity risks and their outcomes.
- Advanced threat detection: AI algorithms can also identify abnormal behavior faster than a human cybersecurity professional, enabling you to stay on top of insider threats and compromised accounts.
- ML capabilities: ML enables a software program to learn from previous cycles, creating a security system that can continuously update its knowledge of threats and adapt appropriate responses.

REFERENCES

[1] Ahn, G., Hu, H., Lee, J., & Meng, Y. (2010). Representing and reasoning about web access control policies. IEEE. https://ieeexplore.ieee.org/document/5676253

[2] Alshawi, A., Al-Razgan, M., AlKallas, F. H., Bin Suhaim, R. A., Al-Tamimi, R., Alharbi, N., & AlSaif, S. O. (2022). Data Privacy during pandemics: A systematic literature review of covid-19 smartphone applications. PeerJ Computer Science, 7. https://doi.org/10.7717/peerjcs.826

[3]Clancy, R. (2022, October 12). What is broken access control vulnerability? EC-Council. https://www.eccouncil.org/cybersecurity-exchange/webapplication-hacking/broken-accesscontrol-vulnerability/

[4] Colombo, P., & Ferrari, E. (2019, January 24). Access Control Technologies for Big Data Management Systems: Literature review and future trends. Cybersecurity. https://cybersecurity.springeropen.com/articles/10.1186/s42400-018-0020-9

[5] Cross, C., Parker, M., & Sansom, D. (2018). Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach. Media, Culture & Society, 25(1). https://doi.org/10.1177/0269758017752410

[6] Cybercrime module 10 key issues: Cybercrime that Compromises Privacy. (2019). UNODC. https://www.unodc.org/e4j/en/cybercrime/module-10/keyissues/cybercrime-thatcompromises-privacy.html

[7] Cybersecurity remains one of Malaysia's top concerns, says Hamzah. (2022, March 28). Free Malaysia Today. https://www.freemalaysiatoday.com/category/nation/2022/03/28/cybersecurity-remains-oneof-malaysias-top-concerns-says-hamzah/

[8] Dr.S., Mohanavel. (2021). Prevention from cyber security vulnerabilities in COVID-19 pandemic situation.

[9] Duchamps, W. (2022, July 22). 9 common access management myths debunked. LinkedIn. https://www.linkedin.com/pulse/9-commonaccessmanagement-myths-debunked-wardduchamps/

[10] Eian, I. C., Yong, L. K., Li, M., Qi, Y. H., & Z, F. (2020). Cyber attacks in the era of COVID- 19 and possible solution domains. Preprints. https://doi.org/10.20944/preprints202009.0630.v1

[11] Georgescu, T. (2021, May 14). A study on how the pandemic changed the Cybersecurity Landscape. ResearchGate. https://www.researchgate.net/profile/TiberiuGeorgescu/publication/350833004_A_Study_on_How_the_Pandemic_Changed_the_Cyberse curity_Landscape/links/609e5ee2458515c2658d6ec1/A-Study-on-HowthePandemicChanged-the-Cybersecurity-Landscape.pdf

[12]GlobalFraudReport2021.(2022). Cybersource. https://www.cybersource.com/content/dam/documents/campaign/fraudreport/global-fraudreport-2021.pdf

[13]Goh, J., Kang, H., Koh, Z. X., Lim, J. W., Ng, C. W., Sher, G., & Yao, C. (2020, February). Cyber Risk Surveillance: A Case Study of Singapore. International Monetary Fund. https://www.imf.org/-/media/Files/Publications/WP/2020/English/wpiea2020028-printpdf.ashx

[14] Griffiths, C. (2022, November 21). The latest 2022 cyber crime statistics. AAG IT. https://aagit.com/the-latest-2022-cyber-crime-statistics/

[15] He, Y., Aliyu, A., Evans, M., & Luo, C. (2021). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. JMIR. https://doi.org/10.2196/21747

[16]Martin, J. A. (2019, August 21). What is access control? A key component of data security. CSO Online. https://www.csoonline.com/article/3251714/whatis-access-control-akeycomponent-of-data-security.html

[17]McGraw, G. (2015, October 01). McGraw: Seven myths of software security best practices. TechTarget. https://www.techtarget.com/searchsecurity/opinion/McGraw-Sevenmythsofsoftware-security-best-practices

[18] Moore, M. (2022, August 1). Top Cybersecurity Threats in 2022. University of San Diego. https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

[19] Neto, N. N., Madnick, S., Paula, A. M., & Borges, N. M. (2020, March 17). A Case Study of the Capital One Data Breach. SSRN.

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542567

[20] Parkinson, S., & Khan, S. (2022, April 27). A survey on empirical security analysis of access control systems: A real-world perspective. ACM Digital Library. https://dl.acm.org/doi/10.1145/3533703

[21] Pranggono, B., & Arabo, A. (2020, October 3). Covid-19 pandemic cybersecurity issues. Wiley Online Library. https://onlinelibrary.wiley.com/doi/10.1002/itl2.247

[22] National Cyber Security Centre. (2015, October 13). Reducing your exposure to cyber attack. https://www.ncsc.gov.uk/information/reducing-yourexposureto-cyber-attack

[23] Roa, R. E. (2017, June). RANSOMWARE ATTACKS ON THE HEALTHCARE INDUSTRY. ProQuest. https://www.proquest.com/openview/53149e53ad84f1cfeeba87b0a8c9d414/1? pqorigsite=gscholar&cbl=18750

[24] Rogers, G., & Ashford, T. (2015). Mitigating Higher Ed Cyber Attacks. ERIC. https://files.eric.ed.gov/fulltext/ED571277.pdf

