Stage 1

Report

Title of the project

Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management

Overview: -

The "Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management" project aims to improve the organization's security posture through the implementation of the IBM Qradar SIEM solution. The project involves deploying and configuring Qradar to centralize log collection, perform real-time event correlation, and enhance threat detection and incident response capabilities.

Additionally, the project includes customizing the SOC dashboard to offer an intuitive and comprehensive view of security performance. The dashboard will be designed in collaboration with SOC analysts, identifying key performance indicators (KPIs), relevant metrics, and visualizations to support effective monitoring, detection, and response to security incidents. Furthermore, the SIEM system will be integrated with external threat intelligence feeds and vulnerability databases. This integration will enrich the analysis and detection capabilities by providing real-time information on emerging threats, known attack vectors, and potential vulnerabilities. This empowers the SOC team to proactively respond to emerging risks.

In summary, the project aims to enhance security operations by implementing Qradar SIEM, creating a tailored SOC dashboard, and integrating threat intelligence to bolster the organization's ability to detect and respond to security threats effectively.

Based on the case study we feel that this work may suffer from Security controls and Logging issues, which are one of the top OWASP issues “security misconfiguration” and “security logging and monitoring failures”.

List of Vulnerabilities Table: -

The following table shows the major list of vulnerabilities based on the given case study with its CWE.

S.no	Vulnerability Name	CWE – No
1	Configuration	16
2	Security Misconfiguration	1349
3	Security Misconfiguration	1032
4	Security Misconfiguration	933
5	Security Misconfiguration	815
6	Improper Output Neutralization for Logs	117
7	Insertion of Sensitive Information into Log File	532
8	Omission of Security-relevant Information	223
9	Security Logging and Monitoring Failures	1355
10	Insufficient Logging	778

REPORT

1) *Vulnerability Name:- Configuration*

CWE : - 16

OWASP Category:- Security Misconfiguration

Description:- Weaknesses in this category are typically introduced during the configuration of the software.

Business Impact::- Configuration vulnerabilities (CWE-16) can have severe repercussions for businesses. Inadequate or improper configuration settings in software, systems, or networks can lead to data breaches, service disruptions, financial losses, regulatory non-compliance, reputational damage, competitive disadvantages, resource drain, legal consequences, and long-term security risks. These vulnerabilities jeopardize customer trust, operational continuity, and overall business viability. Organizations must prioritize proactive security measures, regular assessments, and swift remediation to mitigate the potential impacts and safeguard their reputation and bottom line.

2) *Vulnerability Name:- Security Misconfiguration*

CWE : - 1349

OWASP Category:- Security Misconfiguration

Description:- Categories are informal organizational groupings of weaknesses that can help CWE users with data aggregation, navigation, and browsing. However, they are not weaknesses in themselves.

Business Impact::- Security misconfigurations (CWE-1349) can have significant business ramifications. When systems, applications, or networks are improperly configured, they become vulnerable to cyberattacks and data breaches. This can lead to unauthorized access, data leaks, service disruptions, financial losses, regulatory penalties, and reputational harm. Customer trust and confidence can erode, while operational integrity and regulatory compliance are compromised. It is imperative for businesses to diligently manage configurations, conduct regular audits, and promptly rectify misconfigurations to prevent these detrimental effects on their operations, finances, and reputation.

3) Vulnerability Name:- Security Misconfiguration

CWE : - 1032

OWASP Category:- Security Misconfiguration

Description:- Categories are informal organizational groupings of weaknesses that can help CWE users with data aggregation, navigation, and browsing.

Business Impact::- Vulnerabilities related to Security Misconfigurations (CWE-1032) can significantly impact businesses by exposing them to various security risks. Improperly configured software, systems, or platforms can create openings for cyberattacks and unauthorized access, potentially leading to data breaches, service disruptions, financial losses, and compliance violations. Such incidents undermine customer trust, disrupt operations, incur remediation costs, and trigger legal and regulatory consequences. To mitigate these risks, businesses must prioritize thorough configuration management, regular assessments, and swift resolution of misconfigurations to ensure robust cybersecurity and safeguard their reputation.

4) Vulnerability Name:- Security Misconfiguration

CWE : - 933

OWASP Category:- Security Misconfiguration

Description:- Categories are informal organizational groupings of weaknesses that can help CWE users with data aggregation, navigation, and browsing.

Business Impact::- Security Misconfiguration (CWE-933) vulnerabilities can have serious repercussions for businesses. Poorly configured systems or applications can be exploited by attackers, leading to unauthorized access, data leaks, service outages, financial losses, and non-compliance with regulations. Such incidents erode customer trust, disrupt operations, incur remediation expenses, and potentially result in legal actions. To mitigate these risks, businesses must prioritize meticulous configuration management, routine audits, and swift resolution of misconfigurations to ensure robust cybersecurity and maintain their reputation and bottom line.

5) Vulnerability Name:- Security Misconfiguration

CWE : - 815

OWASP Category:- Security Misconfiguration

Description:- Weaknesses in this category are related to the A6 category in the OWASP Top Ten 2010.

Business Impact::- Security Misconfiguration (CWE-815) vulnerabilities can have detrimental effects on businesses. When software, systems, or networks are improperly configured, they become susceptible to cyberattacks and data breaches. This can lead to unauthorized access, information disclosure, service disruptions, financial losses, and non-compliance with industry regulations. These incidents undermine customer trust, disrupt operations, incur financial costs, and potentially result in legal liabilities. To mitigate these risks, businesses must prioritize rigorous configuration management, regular assessments, and swift resolution of misconfigurations to ensure robust cybersecurity and safeguard their reputation and overall business continuity.

6) Vulnerability Name:- Improper Output Neutralization for Logs

CWE : - 117

OWASP Category:- Security Logging and Monitoring Failures

Description:- The product does not neutralize or incorrectly neutralizes output that is written to logs.

Business Impact::- The vulnerability known as Improper Output Neutralization for Logs (CWE-117) can have significant business implications. Failure to properly neutralize or sanitize output that is logged can enable attackers to inject malicious content into logs, potentially leading to unauthorized access, data manipulation, and system compromise. This can result in breaches of sensitive information, loss of customer trust, legal and regulatory repercussions, service disruptions, and reputational damage. To mitigate these risks, businesses must prioritize secure coding practices, implement proper output sanitization, and regularly audit and monitor log outputs to ensure the integrity and security of their systems and data.

7) Vulnerability Name:- Insertion of Sensitive Information into Log File

CWE : - 532

OWASP Category:- Security Logging and Monitoring Failures

Description:- Information written to log files can be of a sensitive nature and give valuable guidance to an attacker or expose sensitive user information.

Business Impact::- The vulnerability labeled "Insertion of Sensitive Information into Log File" (CWE-532) can have serious repercussions for businesses. When sensitive information such as passwords, financial data, or personally identifiable information is inadvertently logged, it becomes accessible to potential attackers. This can lead to data breaches, unauthorized access, identity theft, legal liabilities, regulatory non-compliance, and damage to the organization's reputation. Such incidents erode customer trust, disrupt operations, incur remediation costs, and can result in legal actions. To mitigate these risks, businesses must implement strict logging practices, sanitize sensitive data before logging, and regularly review and secure log files to ensure the confidentiality and integrity of the information they handle.

8) *Vulnerability Name:- Omission of Security-relevant Information*

CWE : - 223

OWASP Category:- Security Logging and Monitoring Failures

Description:- The product does not record or display information that would be important for identifying the source or nature of an attack, or determining if an action is safe.

Business Impact::- The vulnerability "Omission of Security-relevant Information" (CWE-223) can have serious business implications. Neglecting to include essential security details like error messages or logging can hinder the identification and resolution of security issues. This may lead to undetected breaches, prolonged incident response times, data exposure, reputational damage, and potential legal consequences. By failing to provide critical security information, organizations risk eroding customer trust, violating regulatory requirements, and experiencing financial losses. To mitigate these risks, businesses should prioritize comprehensive error handling, thorough logging practices, and effective reporting mechanisms to ensure prompt detection and response to security incidents, thus safeguarding their operations and preserving their reputation.

9) *Vulnerability Name:- Security Logging and Monitoring Failures*

CWE : - 1355

OWASP Category:- Security Logging and Monitoring Failures

Description:- Weaknesses in this category are related to the A09 category "Security Logging and Monitoring Failures" in the OWASP Top Ten 2021.

Business Impact::- The vulnerability "Security Logging and Monitoring Failures" (CWE-1355) can have significant business ramifications. Inadequate security logging and monitoring can lead to undetected cyber threats, breaches, and unauthorized activities. This may result in data compromises, financial losses, regulatory non-compliance, reputational damage, and legal liabilities. Failing to establish robust logging and monitoring mechanisms undermines incident response capabilities, customer trust, and operational continuity. To mitigate these risks, businesses must ensure effective security logging, real-time monitoring, and timely response to security events, thereby safeguarding sensitive data, maintaining compliance, and preserving their reputation in the face of potential security incidents.

10) Vulnerability Name:- Insufficient Logging

CWE : - 778

OWASP Category:- Security Logging and Monitoring Failures

Description:- When a security-critical event occurs, the product either does not record the event or omits important details about the event when logging it.

Business Impact::- The vulnerability "Insufficient Logging" (CWE-778) can have significant business consequences. Insufficient or inadequate logging practices can hamper the detection and response to security incidents, leaving organizations vulnerable to undetected breaches, data manipulation, and unauthorized access. This may result in financial losses, regulatory penalties, reputational damage, and legal liabilities. Inadequate logging undermines the ability to track and analyze security events, hindering incident investigations and potentially eroding customer trust. To mitigate these risks, businesses must prioritize robust logging mechanisms, comprehensive event recording, and timely analysis to ensure effective monitoring, incident response, and protection of their operations, data, and reputation.

Stage 2

Report

Overview: -

On performing a Basic network scan of a website, www.mits.ac.in with the domain 172.67.156.128, Nessus generated many reports based on Classifying Vulnerabilities by Plugins and Vulnerabilities by Host. In the Vulnerabilities by Plugins report, 8 vulnerabilities are identified. There are many ports found to be open. There is no risk factor identified. Whereas, we found totally 33 different types of Information in the Vulnerabilities by Host. We don't have any risk factors, as mentioned in the scan report. Yet, as few ports are open, there is a chance to enter into the system.

I understand Nessus as a widely-used vulnerability assessment tool developed by Tenable, a cybersecurity company. Nessus is designed to identify and evaluate security vulnerabilities within computer systems, networks, applications, and other IT infrastructure components. The tool operates by scanning target systems and assets, analyzing their configurations, and comparing them against a comprehensive database of known vulnerabilities and security issues.

Nessus provides detailed reports that outline the vulnerabilities it discovers, including their severity levels, potential impacts, and recommended remediation steps. This information enables organizations to prioritize and address security weaknesses to reduce the risk of exploitation by malicious actors. Key features of Nessus include its extensive plugin database, which contains a vast array of vulnerability detection plugins that are updated regularly to reflect the latest security threats. The tool also offers flexibility in customization, allowing users to tailor scans to specific requirements and environments. Additionally, Nessus supports both authenticated and unauthenticated scans, enabling deeper insights into target systems when proper credentials are provided.

Nessus is not just limited to vulnerability scanning; it also assists organizations in maintaining compliance with industry standards and regulations by auditing systems against predefined security policies. The tool can be integrated with other security and IT management solutions, enabling seamless workflows for vulnerability management and response.

Overall, Nessus plays a crucial role in helping organizations enhance their cybersecurity posture by identifying and mitigating vulnerabilities before they can be exploited, thereby contributing to the overall security and resilience of their IT infrastructure.

Target website: - www.mits.ac.in
Target ip address: - 172.67.156.128

List of Vulnerabilities Table: -

S.No	Vulnerability name	Severity	plugins
1	Common Platform Enumeration (CPE)	Info	45590
2	Device Type	Info	54615
3	Nessus SYN scanner	Info	11219
4	Nessus Scan Information	Info	19506
5	OS Identification	Info	11936
6	Service Detection	Info	22964
7	TCP/IP Timestamps Supported	Info	25220
8	Traceroute Information	Info	10287

REPORT: -

1) *Vulnerability Name:- Common Platform Enumeration (CPE)*

severity : - Info

Plugin:- 45590

Port :- (tcp/0)

Description:- By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host. Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

solution:- n/a

Business Impact::- Common Platform Enumeration (CPE) 45590 can have a significant business impact by streamlining the process of identifying and managing software and hardware components within an organization's IT infrastructure. CPE 45590, a unique identifier for a specific product, can enhance operational efficiency by providing a standardized and structured approach to cataloging assets. This, in turn, leads to improved asset tracking, vulnerability management, and compliance efforts. With CPE 45590, businesses can prioritize and address security vulnerabilities more effectively, reducing the risk of cyberattacks and data breaches. Furthermore, the ability to associate a specific CPE identifier with a product or service simplifies communication among stakeholders, enabling informed decision-making and fostering collaboration. Overall, CPE 45590 contributes to better risk management, increased cybersecurity resilience, and streamlined business operations, ultimately resulting in a positive impact on an organization's bottom line.

2) Vulnerability Name:- Device Type

severity : - Info

Plugin:- 54615

Port :- (tcp/0)

Description:- Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

solution:- n/a

Business Impact::- The vulnerability labeled as Device Type 54615 can have notable business implications by directly influencing an organization's cybersecurity posture and operational continuity. This specific vulnerability classification assists in identifying vulnerabilities associated with certain device types within an IT infrastructure. By promptly addressing vulnerabilities linked to Device Type 54615, businesses can mitigate potential security breaches, data leaks, and system disruptions. This proactive approach enhances the organization's ability to safeguard sensitive information, maintain customer trust, and avoid financial losses stemming from cyber incidents. Moreover, effectively managing vulnerabilities linked to Device Type 54615 enables businesses to uphold regulatory compliance standards and industry best practices. By bolstering their cybersecurity defenses, organizations can bolster their overall resilience and maintain their competitive edge, ensuring sustained growth and success.

3) Vulnerability Name:- Nessus SYN scanner

severity : - Info

Plugin:- 11219

Ports (14) :- (tcp/80/www), (tcp/443/www), (tcp/1720), (tcp/2052/www), (tcp/2053/www), (tcp/2082/www), (tcp/2083/www), (tcp/2086/www), (tcp/2087/www), (tcp/2095/www), (tcp/2096/www), (tcp/8080/www), (tcp/8443/www), (tcp/8880/www)

Description:- This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target. Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

solution:- Protect your target with an IP filter.

Business Impact::- The business impact of the vulnerability associated with the Nessus SYN scanner underscores the critical role this tool plays in fortifying an organization's cybersecurity framework. The Nessus SYN scanner vulnerability has the potential to expose weaknesses in network configurations, potentially leading to unauthorized access, data breaches, and service disruptions. Swiftly addressing vulnerabilities highlighted by the Nessus SYN scanner is imperative for businesses to safeguard sensitive information, protect customer trust, and avoid reputational damage. By taking proactive measures to rectify these vulnerabilities, organizations can demonstrate their commitment to robust cybersecurity practices, adhere to industry regulations, and maintain the integrity of their operations. Furthermore, mitigating vulnerabilities identified by the Nessus SYN scanner enhances the overall resilience of the business, ensuring uninterrupted services, bolstered risk management, and sustained growth in an increasingly interconnected digital landscape.

4) Vulnerability Name:- Nessus Scan Information

severity : - Info

Plugin:- 19506

Port:- (tcp/0)

Description:- This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

solution:- n/a

Business Impact::- The business impact of vulnerabilities discovered through Nessus scan information is of paramount importance in today's cybersecurity landscape. Nessus scan information provides insights into potential weaknesses within an organization's IT infrastructure, including networks, systems, and applications. Failing to address vulnerabilities exposed by Nessus scans could leave a business susceptible to cyberattacks, data breaches, and operational disruptions. The financial consequences of such incidents, including regulatory fines, legal liabilities, and reputational damage, can be substantial. Conversely, leveraging Nessus scan information to proactively identify and rectify vulnerabilities enables businesses to enhance their security posture, protect sensitive data, and maintain customer trust. By prioritizing remediation efforts based on Nessus scan results, organizations can demonstrate a commitment to cybersecurity best practices, compliance with industry standards, and the overall well-being of their operations. This approach not only minimizes potential risks but also fosters a resilient business environment capable of navigating evolving cyber threats with confidence.

5) Vulnerability Name:- OS Identification

severity : - Info

Plugin:- 11936

Port :- (tcp/0)

Description:- Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

solution:- n/a

Business Impact::- The business impact of vulnerabilities related to operating system (OS) identification underscores the essential role it plays in maintaining a robust cybersecurity stance. Accurate OS identification is crucial for understanding the security landscape of an organization's IT environment. Failing to address vulnerabilities in specific operating systems could leave businesses susceptible to targeted attacks, malware infiltration, and data breaches. The financial repercussions of such incidents, including potential legal liabilities, compliance penalties, and damage to brand reputation, can be severe. Conversely, actively managing vulnerabilities associated with OS identification empowers businesses to bolster their overall security posture, safeguard critical data, and instill confidence in customers and stakeholders. By proactively patching and securing identified vulnerabilities, organizations demonstrate their commitment to resilience, compliance with industry standards, and the protection of sensitive information. This approach not only mitigates potential risks but also fosters a secure digital ecosystem conducive to sustained growth and success.

6) Vulnerability Name:- Service Detection

severity : - Info

Plugin:- 22964

Ports (13) :- tcp/80/www), (tcp/443/www), (tcp/2052/www), (tcp/2053/www), (tcp/2082/www), (tcp/2083/www), (tcp/2086/www), (tcp/2087/www), (tcp/2095/www), (tcp/2096/www), (tcp/8080/www), (tcp/8443/www), (tcp/8880/www)

Description:- Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

solution:- n/a

Business Impact::- The business impact of vulnerabilities stemming from service detection is a critical consideration in the realm of cybersecurity. Accurate and comprehensive service detection is essential for understanding the various services and protocols running within an organization's network environment. Overlooking vulnerabilities related to service detection can expose businesses to a range of risks, including unauthorized access, data breaches, and service disruptions. The potential financial consequences of such incidents, including regulatory fines, legal actions, and reputational damage, can be significant. On the other hand, actively managing vulnerabilities associated with service detection allows businesses to enhance their security posture, protect sensitive data, and maintain trust among customers and partners. By promptly addressing and securing identified services and protocols, organizations demonstrate a commitment to proactive risk management, compliance with industry regulations, and the overall resilience of their operations. This approach not only reduces potential risks but also fosters a secure and dependable digital environment, facilitating continued growth and success in a dynamic threat landscape.

7) Vulnerability Name:- TCP/IP Timestamps Supported

severity : - Info

Plugin:- 25220

Port :- (tcp/0)

Description:- The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

solution:- n/a

Business Impact::- The business impact of vulnerabilities related to TCP/IP timestamps support is a critical concern in modern cybersecurity. TCP/IP timestamps support is often exploited by malicious actors to gain insight into network activity, potentially leading to unauthorized access, data breaches, and even advanced cyberattacks. Neglecting vulnerabilities associated with TCP/IP timestamp support could expose businesses to substantial risks, including compromised sensitive data, regulatory non-compliance, financial losses, and damage to reputation. Conversely, actively addressing these vulnerabilities enhances an organization's security posture, strengthens data protection measures, and preserves customer trust. By swiftly mitigating vulnerabilities tied to TCP/IP timestamp support, businesses demonstrate their commitment to proactive cybersecurity practices, adherence to industry standards, and the overall resilience of their operations. This approach not only minimizes potential risks but also cultivates a secure digital environment conducive to sustained growth and business continuity.

8) Vulnerability Name:- Traceroute Information

severity : - Info

Plugin:- 10287

Port :- (udp/0)

Description:- Makes a traceroute to the remote host.

solution:- n/a

Business Impact::- The business impact of vulnerabilities stemming from traceroute information is a crucial aspect of modern cybersecurity strategy. Traceroute, a network diagnostic tool, reveals the path that data packets take across a network, potentially exposing critical infrastructure details to attackers. Overlooking vulnerabilities related to traceroute information could lead to potential security breaches, unauthorized access, and data leaks. The financial consequences of such incidents, including regulatory fines, legal liabilities, and reputational damage, can be substantial. Conversely, actively managing vulnerabilities associated with traceroute information allows businesses to enhance their security posture, safeguard sensitive data, and maintain trust among stakeholders. By addressing and securing traceroute-related vulnerabilities promptly, organizations demonstrate a proactive commitment to risk management, compliance with industry standards, and the overall resilience of their operations. This approach not only mitigates potential risks but also cultivates a secure digital environment conducive to sustained growth and business continuity.

MITS scan

Fri, 04 Aug 2023 14:35:31 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Plugin

Collapse All | Expand All

Nessus Essentials

11219 (14) - Nessus SYN scanner -

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2023/06/20

Plugin Output

172.67.156.128 (tcp/80/www)

```
Port 80/tcp was found to be open
```

172.67.156.128 (tcp/443/www)

```
Port 443/tcp was found to be open
```

172.67.156.128 (tcp/1720)

```
Port 1720/tcp was found to be open
```

Nessus Essentials

172.67.156.128 (tcp/2052/www)

```
Port 2052/tcp was found to be open
```

172.67.156.128 (tcp/2053/www)

```
Port 2053/tcp was found to be open
```

172.67.156.128 (tcp/2082/www)

```
Port 2082/tcp was found to be open
```

172.67.156.128 (tcp/2083/www)

```
Port 2083/tcp was found to be open
```

172.67.156.128 (tcp/2086/www)

```
Port 2086/tcp was found to be open
```

172.67.156.128 (tcp/2087/www)

```
Port 2087/tcp was found to be open
```

172.67.156.128 (tcp/2095/www)

```
Port 2095/tcp was found to be open
```

172.67.156.128 (tcp/2096/www)

```
Port 2096/tcp was found to be open
```

172.67.156.128 (tcp/8080/www)

```
Port 8080/tcp was found to be open
```

172.67.156.128 (tcp/8443/www)

```
Port 8443/tcp was found to be open
```

172.67.156.128 (tcp/8880/www)

```
Port 8880/tcp was found to be open
```

22964 (13) - Service Detection -

Synopsis

The remote service could be identified.

Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Solution

n/a

Risk Factor

None

Plugin Information

Nessus Essentials

Published: 2007/08/19, Modified: 2023/07/10

Plugin Output

172.67.156.128 (tcp/80/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/443/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/2052/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/2053/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/2082/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/2083/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/2086/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/2087/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/2095/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/2096/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/8080/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/8443/www)

```
A web server is running on this port.
```

172.67.156.128 (tcp/8880/www)

```
A web server is running on this port.
```

10287 (1) - Traceroute Information -

Synopsis

It was possible to obtain traceroute information.

Nessus Essentials

Description

Makes a traceroute to the remote host.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 1999/11/27, Modified: 2023/06/26

Plugin Output

172.67.156.128 (udp/0)

```

For your information, here is the traceroute from 10.31.34.115 to 172.67.156.128 :
10.31.34.115

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.

An error was detected along the way.
?
10.30.0.5
10.11.0.2
10.10.1.21
136.233.9.2
?
172.67.156.128

Hop Count: 9
```

11936 (1) - OS Identification -

Synopsis

It is possible to guess the remote operating system.

Description

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2003/12/09, Modified: 2022/03/09

Plugin Output

172.67.156.128 (tcp/0)

```


Remote operating system : CentOS Linux 7 Linux Kernel 3.10
Confidence level : 56
Method : MLSinFP
```

Nessus Essentials

```
The remote host is running CentOS Linux 7 Linux Kernel 3.10
```

19506 (1) - Nessus Scan Information -

Nessus Essentials

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2023/07/31

Plugin Output

172.67.156.128 (tcp/0)

```
Information about this scan :

Nessus version : 10.5.4
Nessus build : 20013
Plugin feed version : 202308040201
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : MITS scan
Scan policy used : Basic Network Scan
Scanner IP : 10.31.34.115
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 78.823 ms
Thorough tests : no
Experimental tests : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin launched)
CGI scanning : disabled
Web application tests : disabled
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2023/8/4 14:24 India Standard Time
Scan duration : 687 sec
Scan for malware : no
```

Nessus Essentials

25220 (1) - TCP/IP Timestamps Supported -

Synopsis

The remote service implements TCP timestamps.

Description

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

See Also

http://www.ietf.org/rfc/rfc1323.txt

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/05/16, Modified: 2019/03/06

Plugin Output

172.67.156.128 (tcp/0)

45590 (1) - Common Platform Enumeration (CPE)

Synopsis

It was possible to enumerate CPE names that matched on the remote system.

Description

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

Nessus Essentials

See Also

http://cpe.mitre.org/
https://nvd.nist.gov/products/cpe

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2010/04/21, Modified: 2023/07/27

Plugin Output

172.67.156.128 (tcp/0)

```

The remote operating system matched the following CPE :

cpe:/o:centos:centos -> CentOS
```

54615 (1) - Device Type

Synopsis

It is possible to guess the remote device type.

Description

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2011/05/23, Modified: 2022/09/09

Plugin Output

172.67.156.128 (tcp/0)

```
Remote device type : unknown
Confidence level : 56
```

Nessus Es

© 2023 Tenable™, Inc. All rights reserved.

Stage 3
Report

Title of the project

Enhancing Security Operations: SIEM Qradar & SOC Dashboard Management

Security Operations Center (SOC): -

A Security Operations Center (SOC) in the context of SIEM, particularly IBM QRadar, is a dedicated facility or team responsible for monitoring, managing, and responding to security events and incidents within an organization's information technology infrastructure. The SOC leverages the capabilities of SIEM solutions like QRadar to collect, correlate, and analyze vast amounts of security data from various sources. This data includes logs, alerts, and event information generated by network devices, applications, servers, and endpoints.

The SOC's primary objective is to detect, investigate, and mitigate potential cybersecurity threats in real-time or near-real-time. This involves proactive monitoring, threat hunting, incident response coordination, and collaboration with other IT and security teams. By utilizing QRadar's advanced analytics, correlation rules, and reporting functionalities, the SOC aims to ensure a swift and effective response to security incidents, minimize the impact of breaches, and maintain a robust security posture for the organization's digital assets.

SOC – cycle: -

The Security Operations Center (SOC) cycle within SIEM, such as IBM QRadar, represents a structured and iterative process that enables a proactive and comprehensive approach to cybersecurity. This cycle typically involves several key stages. First, the SOC collects vast amounts of security data from various sources across the organization's IT landscape. This data includes logs, events, and alerts generated by network devices, applications, and endpoints.

Next, the collected data is aggregated and normalized, allowing the SOC to gain a unified view of the organization's security landscape. The SOC then employs QRadar's advanced correlation and analysis capabilities to detect patterns, anomalies, and potential threats. Once potential security incidents are identified, the SOC initiates a thorough investigation, leveraging QRadar's capabilities for in-depth forensics and threat hunting. Following the investigation, the SOC assesses the severity and impact of the incidents, determining whether they pose a significant risk to the organization. Based on this assessment, the SOC takes appropriate actions to mitigate the threats, contain the incident, and prevent further damage. These actions can range from applying patches and configurations to isolating affected systems.

Throughout the entire SOC cycle, continuous monitoring and real-time alerting are maintained, enabling the SOC to respond swiftly to emerging threats. The cycle also emphasizes collaboration and communication with other IT and security teams, ensuring a cohesive and coordinated response. Furthermore, the SOC cycle includes a feedback loop where lessons learned from each incident are analyzed and used to fine-tune QRadar's rules, correlation logic, and incident response procedures. This iterative process aims to enhance the SOC's ability to detect and respond effectively to future security incidents.

In essence, the SOC cycle within SIEM QRadar provides a structured framework for proactive threat detection, rapid incident response, continuous improvement, and collaboration across the organization, ultimately bolstering its cybersecurity resilience.

SIEM: -

SIEM (Security Information and Event Management) in the context of IBM QRadar represents a sophisticated and comprehensive solution that empowers organizations to proactively manage and enhance their cybersecurity posture. SIEM serves as a centralized platform that collects, correlates, and analyzes vast volumes of security data generated across an organization's IT infrastructure. In the case of QRadar, this entails aggregating information from various sources such as network devices, servers, applications, and endpoints.

QRadar's SIEM capabilities provide real-time monitoring and correlation of security events, enabling the detection of patterns, anomalies, and potential threats. This results in the timely identification of security incidents that might otherwise go unnoticed. QRadar also facilitates incident investigation by offering advanced analytics, data visualization, and forensic tools, aiding security teams in understanding the scope and impact of incidents.

One of the core strengths of QRadar's SIEM is its ability to provide context to security events by integrating threat intelligence feeds and contextual information. This enriched analysis enhances the accuracy of threat detection and helps organizations prioritize and respond to the most critical risks effectively. Furthermore, QRadar enables proactive incident response through automated alerting, customizable workflows, and orchestrated actions. This accelerates the process of containment, mitigation, and recovery in the event of a security breach.

In summary, SIEM within QRadar is a pivotal component of modern cybersecurity, offering organizations the means to efficiently collect, analyze, and respond to security-related data, ultimately safeguarding sensitive information, mitigating risks, and maintaining a resilient defense against evolving cyber threats.

SIEM Cycle: -

The SIEM cycle within IBM QRadar embodies a systematic and dynamic approach to cybersecurity that encompasses critical stages in threat detection, analysis, response, and continuous improvement. This cycle typically begins with data collection, where QRadar aggregates and normalizes security events and logs from diverse sources across the organization's IT environment. Once collected, the data is subjected to correlation and analysis, leveraging QRadar's advanced capabilities to identify patterns, anomalies, and potential security threats.

The next phase involves detection and alerting, where QRadar's real-time monitoring and rule-based correlation engine identify and prioritize security incidents based on predefined criteria. Upon detection, the system triggers alerts, notifying security teams of potential threats. Subsequently, the investigation and analysis stage commences, where QRadar's comprehensive tools aid in dissecting and understanding the nature, scope, and impact of security incidents. Following analysis, the response phase comes into play, with QRadar facilitating orchestrated actions, automated workflows, and threat containment strategies. This accelerates incident mitigation, minimizing potential damage. Throughout the entire SIEM cycle, continuous monitoring is maintained to ensure that ongoing activities and events are scrutinized for emerging threats.

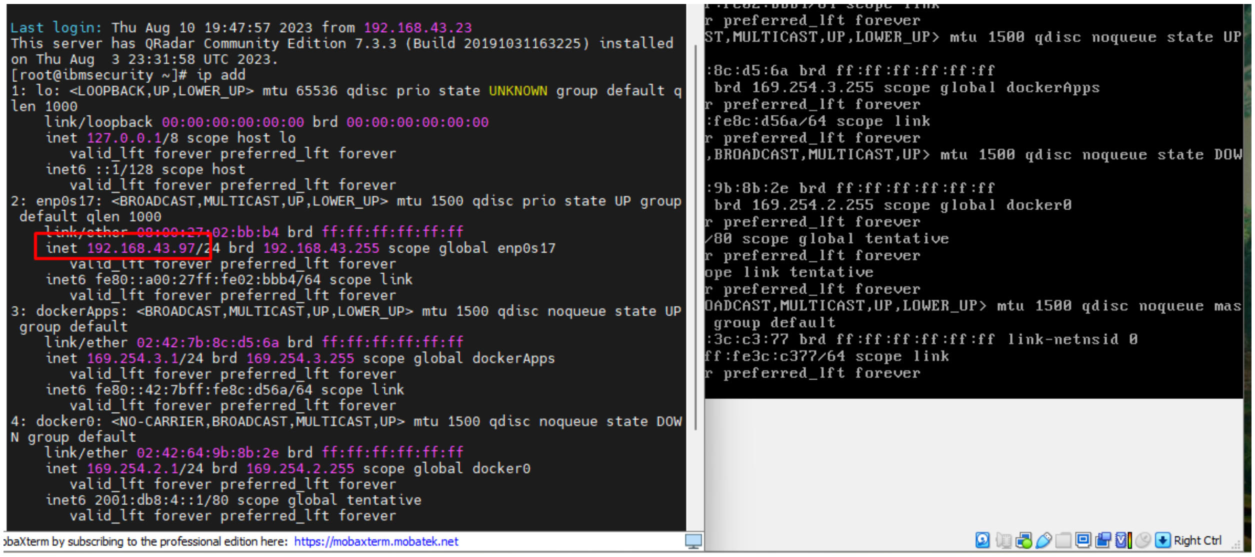
Moreover, the SIEM cycle integrates a feedback loop for learning and improvement. Lessons gleaned from past incidents are applied to fine-tune QRadar's rules, correlation logic, and incident response procedures. This iterative process enhances the system's accuracy, adaptability, and effectiveness in detecting and responding to future threats. In essence, the SIEM cycle within QRadar orchestrates a synchronized dance between data collection, analysis, detection, response, and enhancement. By providing a structured framework for tackling cyber threats, QRadar's SIEM cycle strengthens an organization's cybersecurity posture and contributes to its overall resilience in the face of an ever-evolving threat landscape.

MISP: -

MISP (Malware Information Sharing Platform) in the context of SIEM (Security Information and Event Management) QRadar refers to a valuable integration that enhances an organization's ability to gather, analyze, and share actionable threat intelligence. MISP serves as a collaborative platform designed to facilitate the exchange of detailed information about malware, threats, and vulnerabilities among cybersecurity professionals and organizations. When integrated with QRadar, MISP enables the seamless incorporation of external threat data into the SIEM environment. By utilizing MISP in QRadar, organizations can enrich their security data with contextual information from a wide range of sources, including open-source threat feeds, industry partners, and proprietary intelligence. This integration empowers QRadar to correlate events and alerts with real-time threat intelligence, enhancing the accuracy of threat detection and enabling rapid response to emerging risks.

MISP's capabilities extend beyond mere threat detection. It facilitates the sharing of indicators of compromise (IoCs), threat actor profiles, and attack patterns, enabling organizations to proactively defend against known and emerging cyber threats. Moreover, MISP in QRadar supports collaborative efforts within the security community, enabling organizations to collectively pool their expertise and resources to combat cyber threats effectively. In essence, MISP's integration within QRadar enriches the SIEM environment with actionable threat intelligence, enabling organizations to stay ahead of cyber adversaries, bolster their defenses, and foster a united front against the ever-evolving landscape of cybersecurity challenges.

Network information: -



```
Last login: Thu Aug 10 19:47:57 2023 from 192.168.43.23
This server has QRadar Community Edition 7.3.3 (Build 20191031163225) installed
on Thu Aug  3 23:31:58 UTC 2023.
[root@ibmsecurity ~]# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc prio state UNKNOWN group default q
len 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s17: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc prio state UP group
 default qlen 1000
    link/ether 08:00:27:02:bb:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.97/24 brd 192.168.43.255 scope global enp0s17
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe02:bbb4/64 scope link
       valid_lft forever preferred_lft forever
3: dockerApps: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
 group default
    link/ether 02:42:7b:8c:d5:6a brd ff:ff:ff:ff:ff:ff
    inet 169.254.3.1/24 brd 169.254.3.255 scope global dockerApps
       valid_lft forever preferred_lft forever
    inet6 fe80::42:7bff:fe8c:d56a/64 scope link
       valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOW
N group default
    link/ether 02:42:64:9b:8b:2e brd ff:ff:ff:ff:ff:ff
    inet 169.254.2.1/24 brd 169.254.2.255 scope global docker0
       valid_lft forever preferred_lft forever
    inet6 2001:db8:4::1/80 scope global tentative
       valid_lft forever preferred_lft forever
```

obaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net

```
r preferred_lft forever
ST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP

:8c:d5:6a brd ff:ff:ff:ff:ff:ff
 brd 169.254.3.255 scope global dockerApps
r preferred_lft forever
:fe8c:d56a/64 scope link
r preferred_lft forever
,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOW

:9b:8b:2e brd ff:ff:ff:ff:ff:ff
 brd 169.254.2.255 scope global docker0
r preferred_lft forever
/80 scope global tentative
r preferred_lft forever
ope link tentative
r preferred_lft forever
OADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue mas
 group default
:3c:c3:77 brd ff:ff:ff:ff:ff:ff link-netnsid 0
ff:fe3c:c377/64 scope link
r preferred_lft forever
```

How you think you deploy soc in your college: -

Deploying a Security Operations Center (SOC) in a college environment involves careful planning, resource allocation, and collaboration among various stakeholders. The below steps show us to deploy a SOC in the college environment:

- Assessment and Planning: Begin by conducting a comprehensive assessment of your college's IT infrastructure, existing security measures, and potential vulnerabilities. Identify the scope, objectives, and specific requirements of the SOC. Determine the budget, staffing needs, and technologies that will be required for effective operation.
- Stakeholder Buy-In: Gain support from key stakeholders, including college administrators, IT department, and security personnel. Clearly communicate the benefits of a SOC in enhancing cybersecurity, protecting sensitive data, and maintaining operational continuity.
- Infrastructure Setup: Design and establish the physical and technical infrastructure needed for the SOC. This includes dedicated workspace, hardware, software, and networking resources. Choose an appropriate location that allows for centralized monitoring and quick response.
- Technology Selection: Select a suitable SIEM solution, such as QRadar, and other necessary tools for monitoring, alerting, incident response, and threat intelligence integration. Ensure that the chosen technologies align with the college's needs and capabilities.
- Staffing and Training: Recruit and train a team of skilled cybersecurity professionals to staff the SOC. These experts should have knowledge of threat detection, incident response, and the selected SIEM platform. Training should be ongoing to keep the team up-to-date with the latest threats and best practices.
- Integration and Configuration: Integrate the SIEM solution (e.g., QRadar) with the college's network and systems. Configure data sources, such as firewalls, intrusion detection systems, and endpoints, to feed relevant security events into the SOC for analysis.
- Rule Development: Develop custom correlation rules and use cases within the SIEM to match the college's specific security requirements.

These rules will help detect and alert on potential threats and anomalies.

- Threat Intelligence Integration: Integrate threat intelligence feeds and sources, including MISP, to enrich the SIEM's analysis capabilities and enhance threat detection accuracy.
- Incident Response Planning: Develop detailed incident response procedures and playbooks. Define roles, responsibilities, and escalation paths for handling different types of security incidents.
- Continuous Monitoring and Optimization: Continuously monitor security events and alerts in real-time. Regularly review and fine-tune the SIEM rules, correlation logic, and incident response procedures based on lessons learned and evolving threat landscape.
- Collaboration and Communication: Foster collaboration between the SOC team, IT department, and other relevant stakeholders. Maintain open lines of communication to ensure coordinated responses to security incidents.
- Education and Awareness: Educate college staff and students about the importance of cybersecurity, safe online practices, and how to report potential security concerns.

Deploying a SOC in a college environment is a complex undertaking that requires dedication, resources, and expertise. It is crucial to align the SOC's goals with the college's security needs and strategic objectives, ensuring that it contributes effectively to maintaining a secure and resilient digital environment.

Threat intelligence: -

Threat intelligence refers to the strategic use of external and internal data sources to enhance the accuracy and effectiveness of cybersecurity operations. Threat intelligence provides valuable context about potential security threats, attack techniques, malicious actors, and vulnerabilities. When integrated into QRadar, threat intelligence enriches the analysis of security events and alerts by enabling the SIEM to correlate incoming data with known threat indicators and patterns. Threat intelligence feeds, which can be obtained from commercial providers, open-source communities, and proprietary sources like MISP, offer real-time updates about emerging threats and trends. These feeds contain information such as malicious IP addresses, domain names, file hashes, and attack signatures. QRadar's threat intelligence capabilities enable organizations to automatically match incoming events against these indicators, facilitating early detection of potential cyberattacks. By leveraging threat intelligence in QRadar, organizations can proactively identify and respond to threats, prioritize security incidents, and allocate resources effectively. This integration enhances the ability to detect sophisticated and targeted attacks that might otherwise go unnoticed, thus contributing to a stronger cybersecurity posture and an improved capacity to safeguard sensitive data and digital assets.

Incident response: -

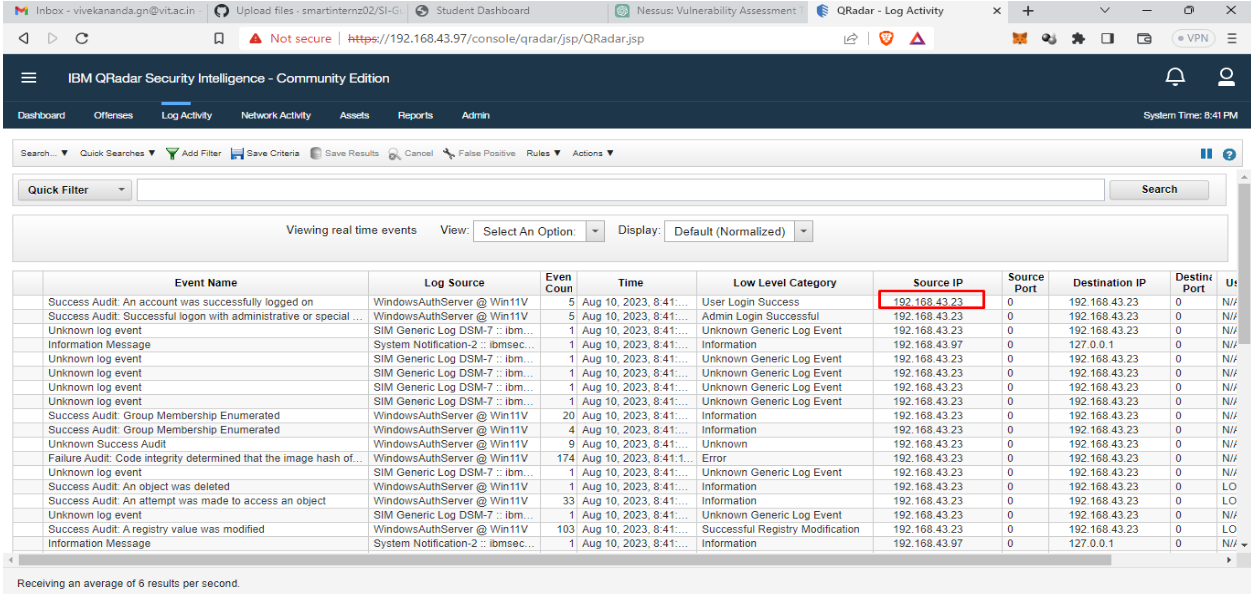
Incident response in the context of SIEM (Security Information and Event Management) QRadar refers to the structured and coordinated process of detecting, analyzing, mitigating, and recovering from security incidents within an organization's IT environment. QRadar's incident response capabilities enable cybersecurity teams to swiftly and effectively address potential threats and breaches, minimizing the impact on the organization. When an incident is detected through QRadar's real-time monitoring and correlation capabilities, the incident response process is initiated. This involves a series of steps, including validating the incident, determining its severity and scope, containing the threat, and eradicating it from affected systems. QRadar's forensic tools aid in understanding the attack vectors, techniques, and potential damage caused by the incident.

QRadar's incident response features extend beyond technical aspects. They encompass collaboration tools, automated workflows, and customizable playbooks that guide security teams through predefined response actions. This promotes consistent and efficient decision-making, particularly during high-stress situations. Additionally, QRadar facilitates post-incident analysis and reporting, enabling organizations to learn from past incidents and enhance their defenses. Lessons gleaned from the incident response process contribute to fine-tuning QRadar's correlation rules, improving threat detection, and ensuring a more resilient security posture over time. In essence, incident response in QRadar empowers organizations to promptly detect, analyze, and mitigate security incidents, thereby reducing the potential impact of breaches and maintaining the integrity of their digital infrastructure. By leveraging QRadar's robust incident response capabilities, organizations can effectively navigate the challenges posed by evolving cyber threats.

Qradar & understanding about tool: -

QRadar is a powerful and comprehensive security intelligence platform developed by IBM. At its core, QRadar is a Security Information and Event Management (SIEM) solution that provides organizations with advanced capabilities for monitoring, detecting, analyzing, and responding to cybersecurity threats and incidents. It offers a centralized platform for collecting, correlating, and analyzing security data from various sources across an organization's IT infrastructure. QRadar excels in its ability to ingest and process vast amounts of security event data, including logs, alerts, network flows, and user activity. Its advanced correlation and analytics capabilities enable the detection of patterns, anomalies, and potential threats in real-time or near-real-time. This empowers security teams to identify and respond to security incidents promptly, reducing the risk of data breaches and system compromises.

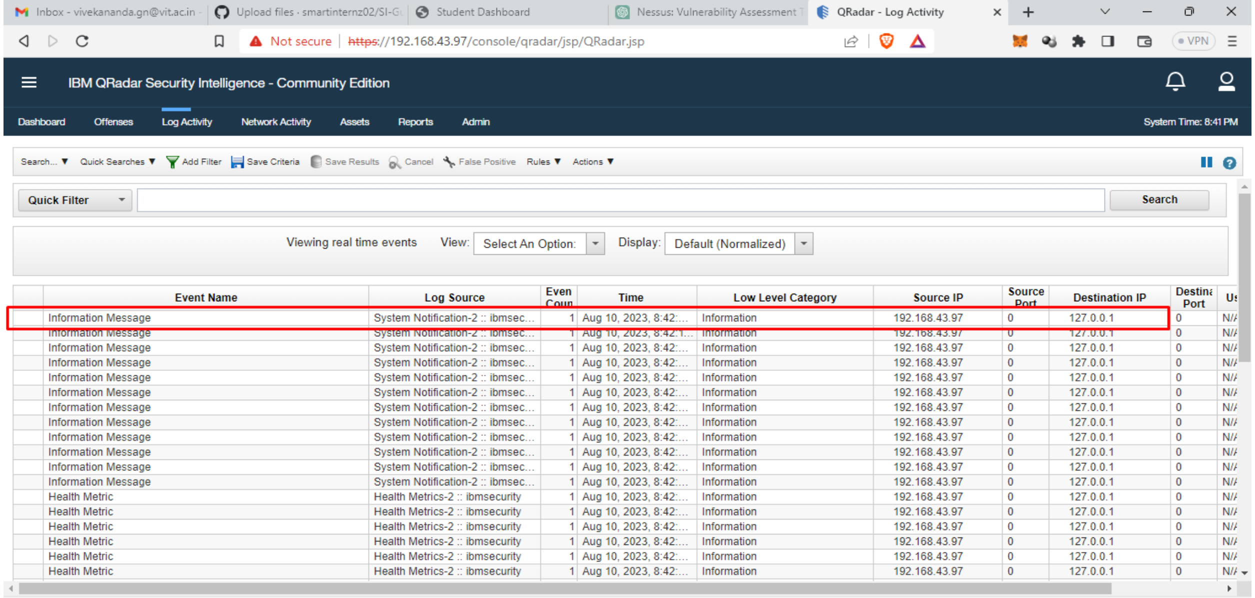
The tool's user-friendly interface and customizable dashboards provide security professionals with actionable insights and visualizations, making it easier to interpret complex data and make informed decisions. QRadar also supports the integration of threat intelligence feeds, allowing organizations to enrich their analysis with external context and stay updated on emerging threats. Furthermore, QRadar offers incident response features that guide security teams through predefined workflows and playbooks, ensuring a coordinated and efficient response to security incidents. The tool's reporting and compliance capabilities aid in generating detailed reports and meeting regulatory requirements. Overall, QRadar serves as a critical component of modern cybersecurity strategies, providing organizations with the tools and insights needed to proactively defend against cyber threats, enhance their security posture, and maintain the integrity of their digital assets.



Viewing real time events View: Select An Option: Display: Default (Normalized)

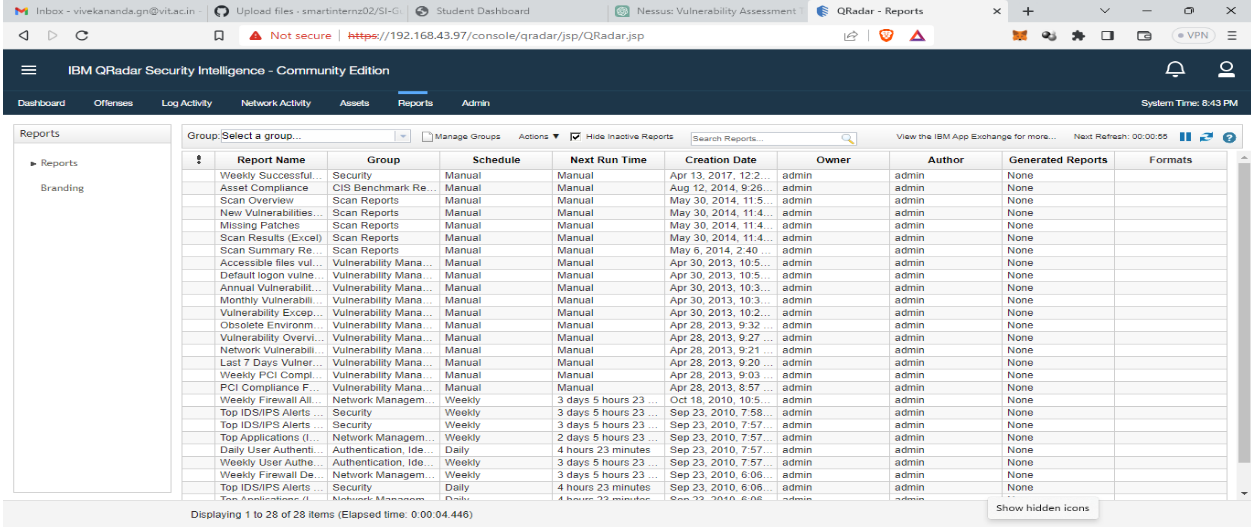
Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Us
Success Audit: An account was successfully logged on	WindowsAuthServer @ Win11V	5	Aug 10, 2023, 8:41:...	User Login Success	192.168.43.23	0	192.168.43.23	0	N/A
Success Audit: Successful logon with administrative or special ...	WindowsAuthServer @ Win11V	5	Aug 10, 2023, 8:41:...	Admin Login Successful	192.168.43.23	0	192.168.43.23	0	N/A
Unknown log event	SIM Generic Log DSM-7 :: ibm...	1	Aug 10, 2023, 8:41:...	Unknown Generic Log Event	192.168.43.23	0	192.168.43.23	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:41:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Unknown log event	SIM Generic Log DSM-7 :: ibm...	1	Aug 10, 2023, 8:41:...	Unknown Generic Log Event	192.168.43.23	0	192.168.43.23	0	N/A
Unknown log event	SIM Generic Log DSM-7 :: ibm...	1	Aug 10, 2023, 8:41:...	Unknown Generic Log Event	192.168.43.23	0	192.168.43.23	0	N/A
Unknown log event	SIM Generic Log DSM-7 :: ibm...	1	Aug 10, 2023, 8:41:...	Unknown Generic Log Event	192.168.43.23	0	192.168.43.23	0	N/A
Unknown log event	SIM Generic Log DSM-7 :: ibm...	1	Aug 10, 2023, 8:41:...	Unknown Generic Log Event	192.168.43.23	0	192.168.43.23	0	N/A
Success Audit: Group Membership Enumerated	WindowsAuthServer @ Win11V	20	Aug 10, 2023, 8:41:...	Information	192.168.43.23	0	192.168.43.23	0	N/A
Success Audit: Group Membership Enumerated	WindowsAuthServer @ Win11V	4	Aug 10, 2023, 8:41:...	Information	192.168.43.23	0	192.168.43.23	0	N/A
Unknown Success Audit	WindowsAuthServer @ Win11V	9	Aug 10, 2023, 8:41:...	Unknown	192.168.43.23	0	192.168.43.23	0	N/A
Failure Audit: Code integrity determined that the image hash of...	WindowsAuthServer @ Win11V	174	Aug 10, 2023, 8:41:1...	Error	192.168.43.23	0	192.168.43.23	0	N/A
Unknown log event	SIM Generic Log DSM-7 :: ibm...	1	Aug 10, 2023, 8:41:...	Unknown Generic Log Event	192.168.43.23	0	192.168.43.23	0	N/A
Success Audit: An object was deleted	WindowsAuthServer @ Win11V	1	Aug 10, 2023, 8:41:...	Information	192.168.43.23	0	192.168.43.23	0	LO
Success Audit: An attempt was made to access an object	WindowsAuthServer @ Win11V	33	Aug 10, 2023, 8:41:...	Information	192.168.43.23	0	192.168.43.23	0	LO
Unknown log event	SIM Generic Log DSM-7 :: ibm...	1	Aug 10, 2023, 8:41:...	Unknown Generic Log Event	192.168.43.23	0	192.168.43.23	0	N/A
Success Audit: A registry value was modified	WindowsAuthServer @ Win11V	103	Aug 10, 2023, 8:41:...	Successful Registry Modification	192.168.43.23	0	192.168.43.23	0	LO
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:41:...	Information	192.168.43.97	0	127.0.0.1	0	N/A

Receiving an average of 6 results per second.



Viewing real time events View: Select An Option: Display: Default (Normalized)

Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Us
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:1...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Information Message	System Notification-2 :: ibmsec...	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: ibmsecurity	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: ibmsecurity	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: ibmsecurity	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: ibmsecurity	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: ibmsecurity	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A
Health Metric	Health Metrics-2 :: ibmsecurity	1	Aug 10, 2023, 8:42:...	Information	192.168.43.97	0	127.0.0.1	0	N/A



!	Report Name	Group	Schedule	Next Run Time	Creation Date	Owner	Author	Generated Reports	Formats
	Weekly Successful...	Security	Manual	Manual	Apr 13, 2017, 12:2...	admin	admin	None	
	Asset Compliance	CIS Benchmark Re...	Manual	Manual	Aug 12, 2014, 9:26...	admin	admin	None	
	Scan Overview	Scan Reports	Manual	Manual	May 30, 2014, 11:5...	admin	admin	None	
	New Vulnerabilities...	Scan Reports	Manual	Manual	May 30, 2014, 11:4...	admin	admin	None	
	Missing Patches	Scan Reports	Manual	Manual	May 30, 2014, 11:4...	admin	admin	None	
	Scan Results (Excel)	Scan Reports	Manual	Manual	May 30, 2014, 11:4...	admin	admin	None	
	Scan Summary Re...	Scan Reports	Manual	Manual	May 6, 2014, 2:40 ...	admin	admin	None	
	Accessible files vul...	Vulnerability Mana...	Manual	Manual	Apr 30, 2013, 10:5...	admin	admin	None	
	Default logon vulne...	Vulnerability Mana...	Manual	Manual	Apr 30, 2013, 10:5...	admin	admin	None	
	Annual Vulnerabilit...	Vulnerability Mana...	Manual	Manual	Apr 30, 2013, 10:3...	admin	admin	None	
	Monthly Vulnerabili...	Vulnerability Mana...	Manual	Manual	Apr 30, 2013, 10:3...	admin	admin	None	
	Vulnerability Excep...	Vulnerability Mana...	Manual	Manual	Apr 30, 2013, 10:2...	admin	admin	None	
	Obsolete Environm...	Vulnerability Mana...	Manual	Manual	Apr 28, 2013, 9:32 ...	admin	admin	None	
	Vulnerability Overvi...	Vulnerability Mana...	Manual	Manual	Apr 28, 2013, 9:27 ...	admin	admin	None	
	Network Vulnerabili...	Vulnerability Mana...	Manual	Manual	Apr 28, 2013, 9:21 ...	admin	admin	None	
	Last 7 Days Vulner...	Vulnerability Mana...	Manual	Manual	Apr 28, 2013, 9:20 ...	admin	admin	None	
	Weekly PCI Compl...	Vulnerability Mana...	Manual	Manual	Apr 28, 2013, 9:03 ...	admin	admin	None	
	PCI Compliance F...	Vulnerability Mana...	Manual	Manual	Apr 28, 2013, 8:57 ...	admin	admin	None	
	Weekly Firewall All...	Network Managem...	Weekly	3 days 5 hours 23 ...	Oct 18, 2010, 10:5...	admin	admin	None	
	Top IDS/IPS Alerts ...	Security	Weekly	3 days 5 hours 23 ...	Sep 23, 2010, 7:58...	admin	admin	None	
	Top IDS/IPS Alerts ...	Security	Weekly	3 days 5 hours 23 ...	Sep 23, 2010, 7:57...	admin	admin	None	
	Top Applications (I...	Network Managem...	Weekly	2 days 5 hours 23 ...	Sep 23, 2010, 7:57...	admin	admin	None	
	Daily User Authenti...	Authentication, Ide...	Daily	4 hours 23 minutes	Sep 23, 2010, 7:57...	admin	admin	None	
	Weekly User Authe...	Authentication, Ide...	Weekly	3 days 5 hours 23 ...	Sep 23, 2010, 7:57...	admin	admin	None	
	Weekly Firewall De...	Network Managem...	Weekly	3 days 5 hours 23 ...	Sep 23, 2010, 6:06...	admin	admin	None	
	Top IDS/IPS Alerts ...	Security	Daily	4 hours 23 minutes	Sep 23, 2010, 6:06...	admin	admin	None	
	Top Applications (I...	Network Managem...	Daily	4 hours 23 minutes	Sep 23, 2010, 6:06...	admin	admin		

Displaying 1 to 28 of 28 items (Elapsed time: 0:00:04.446)

Conclusion: -

Web application testing refers to the systematic process of evaluating the functionality, performance, security, and overall quality of a software application that is accessed through web browsers. It involves a series of assessments, validations, and analyses to ensure that the web application operates as intended, providing a seamless and secure user experience. Testers rigorously examine different aspects, such as user interface interactions, data processing, navigation, and data integrity, while also identifying potential vulnerabilities or defects that could compromise the application's performance or compromise its security. The goal of web application testing is to uncover issues early in the development lifecycle, allowing for timely corrections and enhancements that result in a robust, user-friendly, and reliable web application that meets both user expectations and industry standards.

A Nessus report is a comprehensive document generated by the Nessus vulnerability assessment tool, detailing the findings of security scans conducted on a specific target system or network. The report provides an in-depth analysis of identified vulnerabilities, misconfigurations, and potential security risks within the scanned environment. It includes essential information such as the severity levels of vulnerabilities based on industry standards like the Common Vulnerability Scoring System (CVSS), descriptions of the issues, affected systems, and recommended steps for remediation. The Nessus report serves as a valuable resource for security professionals and IT teams, offering actionable insights to prioritize and address vulnerabilities, enhance the overall cybersecurity posture, and mitigate potential threats before they can be exploited by malicious actors.

A Security Operations Center (SOC) is a centralized facility or team responsible for monitoring, detecting, analyzing, and responding to cybersecurity threats and incidents within an organization. SOC teams utilize tools like Security Information and Event Management (SIEM) systems to aggregate and correlate data from various sources across the IT infrastructure. A SIEM system, such as IBM QRadar, plays a crucial role in the SOC's operations by collecting and analyzing security events, logs, and data. The QRadar Dashboard is a graphical interface within the SIEM that provides a visual representation of the organization's security posture and threat landscape. It offers real-time insights, visualizations, and customizable widgets that allow SOC analysts to monitor network activity, detect anomalies, and promptly respond to potential security incidents. The QRadar Dashboard serves as a vital tool for SOC teams, aiding in quick decision-making, proactive threat hunting, and effective incident response by presenting a clear and intuitive overview of the organization's security environment.

Future Scope: -

The future scope of web application testing is poised for transformative growth as technological advancements and evolving user expectations reshape the digital landscape. With the proliferation of progressive web applications, single-page applications, and microservices architecture, testing methodologies will evolve to ensure seamless user experiences across diverse platforms and devices. Automation will take center stage, leveraging AI and machine learning to enhance test coverage, accelerate test cycles, and facilitate efficient regression testing.

As cybersecurity threats become more sophisticated, web application testing will increasingly prioritize robust security assessments. Penetration testing, vulnerability analysis, and code reviews will integrate advanced threat modeling techniques to preemptively identify and address potential vulnerabilities. Moreover, the proliferation of Internet of Things (IoT) devices and edge computing will extend the scope of testing to encompass the integration, compatibility, and security of web applications within interconnected ecosystems.

Performance testing will transcend traditional metrics, considering factors like energy efficiency, resource optimization, and responsiveness under variable network conditions. User-centric testing, including accessibility, usability, and localization, will be paramount to accommodate diverse user demographics and global audiences. Web application testing will be seamlessly integrated into DevOps and continuous delivery pipelines, ensuring that quality assurance remains an integral part of rapid development cycles. Collaborative tools and shared repositories will facilitate efficient communication among development, testing, and operations teams.

In the future, web application testing will transcend its current boundaries, embracing new technologies, methodologies, and paradigms. It will be a driving force in safeguarding user trust, promoting innovation, and enabling businesses to deliver secure, high-quality digital experiences in an increasingly interconnected and dynamic digital world.

The future scope of the testing process, as understood in Nessus, holds immense potential for addressing evolving cybersecurity challenges and ensuring the resilience of digital ecosystems. With the continuous proliferation of complex IT environments, the testing process within Nessus is likely to expand its focus on comprehensive vulnerability assessment and management. Advanced automation, machine learning, and AI integration will drive enhanced scanning efficiency, accuracy, and the ability to detect emerging vulnerabilities.

The testing process will increasingly emphasize real-time threat intelligence integration, enabling organizations to proactively identify and mitigate risks by aligning their strategies with the ever-evolving threat landscape. This integration will provide contextual insights that empower cybersecurity teams to prioritize vulnerabilities based on potential impact and exploitability. Furthermore, the scope of the testing process in Nessus will likely encompass a broader array of technologies, including cloud services, IoT devices, and containerized applications. The integration of these emerging technologies will demand specialized testing methodologies and tools to ensure their security and compliance.

As regulations and compliance requirements continue to evolve, the testing process will adapt to provide organizations with the means to validate adherence to industry standards and data protection regulations. Additionally, integration with incident response workflows and security orchestration will enable faster and more efficient incident mitigation and recovery. In conclusion, the future of the testing process within Nessus holds exciting prospects for advancing cybersecurity resilience. By embracing automation, real-time intelligence, and adaptability to emerging technologies, Nessus will play a pivotal role in safeguarding digital assets and supporting organizations in effectively managing the ever-changing threat landscape.

The future scope of Security Operations Centers (SOCs) and Security Information and Event Management (SIEM) systems is poised to undergo transformative developments as cybersecurity challenges continue to evolve. SOC and SIEM technologies will play an increasingly vital role in maintaining robust cyber defenses and enabling proactive threat detection and response.

Advancements in artificial intelligence and machine learning will lead to smarter and more adaptive SOC and SIEM solutions. These technologies will enhance anomaly detection, behavior analysis, and predictive analytics, enabling faster identification of sophisticated and evolving threats. Automation will streamline incident response workflows, allowing SOC teams to respond swiftly and effectively to security incidents. The future SOC and SIEM landscape will place a stronger emphasis on threat intelligence integration, enabling organizations to leverage real-time contextual information to enhance threat detection and decision-making. Collaboration and information-sharing among SOC teams and across organizations will be facilitated through interconnected threat intelligence platforms.

Furthermore, the convergence of IT and operational technology (OT) will extend the scope of SOCs to encompass industrial control systems (ICS) and critical infrastructure. SOC capabilities will be adapted to monitor and defend against cyber threats targeting these vital sectors. As cybersecurity regulations and compliance requirements become more stringent, SOCs and SIEM systems will evolve to provide comprehensive auditing, reporting, and compliance capabilities. The integration of SOAR (Security Orchestration, Automation, and Response) tools will streamline incident management and remediation processes. In conclusion, the future scope of SOCs and SIEM systems promises an era of heightened intelligence, automation, collaboration, and adaptability. By embracing these advancements, organizations will be better equipped to navigate the increasingly complex and sophisticated threat landscape, ensuring the security, resilience, and continuity of their digital operations.

Topics explored: -

- Data breach
- Web APIs, web hooks
- Data protection
- Vulnerability stack
- Digital ecosystem
- Introduction to networking
- Antivirus
- Essential terminology
- QRadar
- Cloud service and cloud security
- Introduction to cybersecurity
- Firewall
- Types of cyber attacks
- Data sanity
- OWASP top 10 applications
- SOC
- SIEM
- Growth of cybersecurity
- Web shell concepts

Tools explored: -

- **QRadar for SOC dashboard presentation**
- **OSINT framework**
- **sqlmap**
- **thehackersone.com**
- **Kali Linux**
- **Gamma (AI based PPT)**
- **metasploitable**
- **live websites-bugcrowd**
- **chaptgpt**

- **OWASP top 10 vulnerabilities (2021)**
- **virtual box**
- **IBM fix central**
- **cybermap.kaspersky.com**
- **CWE**
- **tools-nmtui**
- **QRadar Installation**
- **wepik.com (AI image editor)**
- **Nmap**
- **thehackersnews.com**
- **metasploit**
- **Data breach**
- **Virtual machine**
- **mobaxterm**
- **malware bytes**
- **Identify fixes-wincollect agent**
- **Nessus**
- **nslookup.io**