**PENETRATION TEST REPORT**

**Executive summary: -**

Montoya Gin wanted to perform penetration test, to explore all the vulnerabilities and undergo cybersecurity risk assessment, to get the cyber security insurance.

**Objective: -**

* The main objective was to demonstrate the effectiveness of these controls and identify any potential vulnerabilities that could lead to data breaches or exploitations.
* Successful access into underlying OS or any password protected applications is considered a successful exploit.
* Any elevation of privilege is considered a successful exploit.
* Document vulnerabilities that you can successfully exploit on the server and the method used.
* Document potentially sensitive information that you can obtain from the server. That could include credentials, employee files etc.

Montoya Gin primarily was a liquor supplier organization and wanted to expand their network by saturating the market with their product such that every store has their product. The company intentionally did not give much information regarding their network, to see what any outside hackers can do to their network.

After performing the test, we found the system has various vulnerabilities in which one of them was eternalblue, which makes it susceptible to data breaches and system takeovers. System files containing payment information can be easily compromised and altered, which puts the client at significant risk of compliance violations, which eventually leads to sustainable fines and loss of reputation.

**Prioritized Recommendations: -**

* Patch your vulnerabilities.
* Network segmentation.
* Implement a backup and recovery plan.
* Change the passwords.
* Limit the access.

**Authorization: -**

We are authorized to perform the agreed upon vulnerability assessment of the Montoya Gin server site. Our scope of engagement is exclusively limited to the specific server assigned.

The target server is locally hosted on premise at the Montoya Gin offices and no additional consent is needed.

**Liability: -**

Montoya Gin accepts any risk and liability related to the outcomes of this test. There are no additional legal or regulatory parameters that govern Montoya Gin.

**Scope: -**

**In scope: -**

* Access the server through any technological means available.
* Carry out activities that may crash the server.
* Include in the evidence any employee names, passwords, or confidential files found.

**Out of scope: -**

* Social engineering any Montoya Gin employees.
* Sabotage the work of any other consultancy team hired by Montoya Gin.
* Disclose to any other party any information discovered on the asset.

**Status updates and Incident handling: -**

No updates required, as Carlos Montoya (CEO) would like the report to be a surprise.

**Sensitive data handling: -**

Montoya Gin has no specific data storage or handling requirements.

**Tools used during the test: -**

There are few tools as follows which are used during the penetration black box test and are mentioned below,

**Searchsploit: -** Searchsploit is operated on the command line and is used by security experts, pen testers and hackers to find out the vulnerabilities. The exploit databases of Searchsploit consists of thorough collection of known vulnerabilities and exploits supervised by offensive cybersecurity.

Searchsploit is used to explore the exploit database by using various search parameters such as user’s id’s, keywords, author names, CVE numbers and many more. Users can also download and inspect the contents of specific exploits and vulnerabilities.

**Metasploit: -** Metasploit is a framework that is used by pen testers to identify, exploit, and verify vulnerabilities of the targeted systems, it is widely used by lot of security researchers to identify the security of the systems and networks.

Other than the primary framework, Metasploit web-interface, graphical interface and command-line interface which offers various ways to interact with the functionalities.

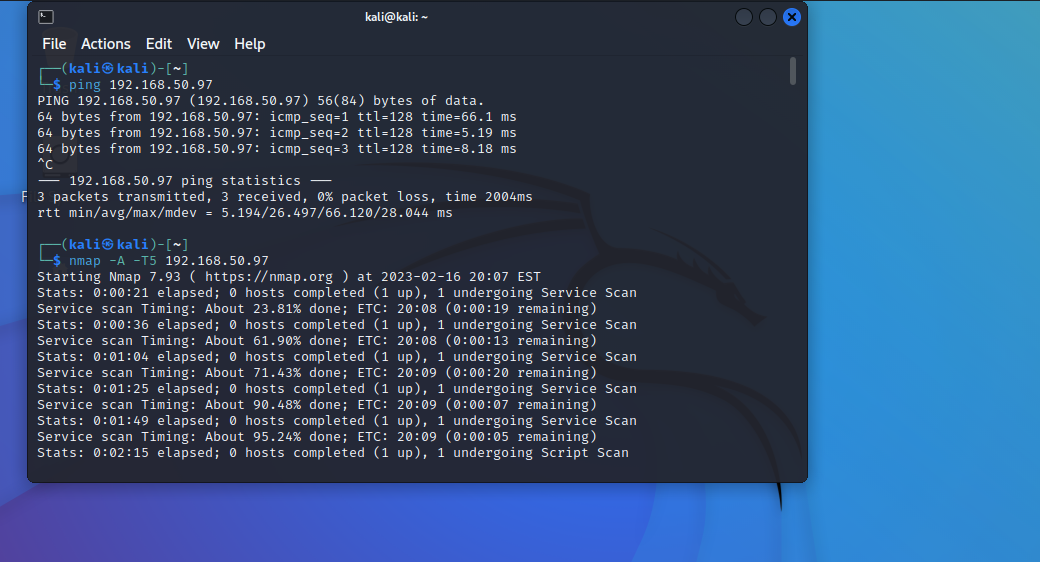
**Nmap: -** Nmap is used to discover various hosts and services on the given computer network. Nmap offers a range of functionalities which includes service enumeration, port scanning, version detection, OS detection and many more.

Nmap has an advanced features where it can adapt to the network conditions.

Some of the features that nmap include are fast scan, TCP/IP stack finger printing and scriptable interaction with target.

**Vulnerability found through port 1617: -**

**Exploitation steps for the below vulnerability is as follows: -**



Whenever the test is being performed, we make sure that the server is up and working for which we ran the command starting with ping and the server’s IP address, which lets us know if the ping is successful or not.

After the successful result of ping then to know what the open ports are and what are the vulnerabilities running on the server we ran the nmap command. Nmap command is mostly used for evaluating security and network exploitation. After the successful execution the command we get to know all the open port on the server which can be seen on the below snapshot. ‘-A’ in the above command is used for the aggressive scan and to collect more information using different method of the targeted hosts. ‘-T5’ is used to speed up the process of running or scanning time.

A computer screen capture

Description automatically generated with medium confidence

After successfully knowing what are the open ports and their services and versions, we can start to find out if there are any vulnerabilities in those ports. In the order of exploiting vulnerabilities we need to enter into msfconsole. Msfconsole is the part of Metasploit framework which provides access to various Metasploit frameworks and allows to run various security scans and helps to place attacks on targets. This tool is mainly used to test and improve the security features of the system. Execution of the command can be seen in the below snapshot.

A screenshot of a computer

Description automatically generated with medium confidence

After successfully entered the console then we performed search operation on all the ports to find any vulnerabilities. To do that we used a command as follows.

nmap -A -p1617 192.168.50.97 -T5.

The above command performs a comprehensive scan where it includes port and network scans on the port 1617 for the given IP address. Then we will get to know what services are running on that port and what search commands we need to use. After performing the command we get to know that we need to use search jmx command in order to enter into the port 1617. Command used for search jmx is shown in the below snapshot.

Text

Description automatically generated

Graphical user interface

Description automatically generated

**Vulnerability summary: -**

The above command resulted in all the modules that port has, with their ranks and description. jmx is basically a technology used to manage and monitor java-based applications.

The CVE associated with the vulnerability is CVE-2016-3427, and this effects the Java SE and Java SE Embedded. When coming to the criticality of this vulnerability is has 8.5 CVSS which is considered as high risk vulnerability. Normally CVSS will issues scores in between 1 to 10 where 10 is considered as the most severe.

**CVSS: - 8.5 which is critical.**

**CVE: - CVE-2016-3427**

After finding all the modules on the port then we used one by one to break into the system according to their ranks. If the rank is mentioned as excellent then it might be the best to break in as it will the weakest module.

To get reply from the ports for which we are trying to break into, we set the LHOSTS as our machine IP address and RHOSTS as the remote server’s IP address on which we are trying to break into. LHOSTS means Local Hosts and RHOSTS means Remote Hosts.

After setting LHOSTS and RHOSTS, we set LPORT as 4447, for the remote host to communicate back to us through that port. All the commands are executed as show in below snapshots.

Text

Description automatically generated

Text

Description automatically generated

After using all the modules to exploit, 7th module in the above snapshots was found vulnerable which gave us the access by allowing us into meterpreter, run command is used to execute after we set all the required ports and hosts, it can be seen in below snapshot.

Text

Description automatically generated

After a system has been compromised, Meterpreter can be used as a payload by taking advantage of a vulnerability, allowing it to be injected into the targeted system.

After entering installing meterpreter, it offers a command-line interface to the attacker, enabling remote access to the compromised system, execution of arbitrary code and kind of actions that include screenshotting and data extraction.

As we can see in the above last snapshot where we ran a command called getuid, to know who the user is currently using that system.

**Vulnerability found through port 9200: -**

**Exploitation steps for the below vulnerability is as follows: -**

9200 is an open port which is using wap-wsp? as its service.

Steps that we have gone through to find the vulnerabilities in 9200 port will be similar to what it is in port 1617. Below are the snapshots of how we break into the system,

Text

Description automatically generated

In the above snapshot we got the list of all open ports with their state, service, and versions, so that we can then perform executions on those to find the vulnerabilities.Text

Description automatically generated

**Vulnerability summary: -**

Search elastic is basically a search engine which is used to send queries and retrieve data from the elastic search database.

We used mvel\_rce module to exploit. As mentioned before excellent rank modules are more vulnerable and easier to crack.

**CVSS Score: - 9.8 which is critical.**

**CVE: - CVE-2018-14667.**

Text

Description automatically generated

Text

Description automatically generated

As seen in the above snapshot RHOSTS was not configured, so remote host is configured in the next step as show shown in below snapshot.

Text

Description automatically generated

‘Setg’ refers to configuring that rhosts globally, to not repeat the command again when we make any changes.

Text

Description automatically generated

In the above snapshot we can see observe that LHOSTS and LPORT have been configured already in the background, so in this instance there is no need to change any of those.

Text

Description automatically generated

After successfully given all the values, finally ‘run’ or ‘exploit’ command will be executed in order to break into the system.

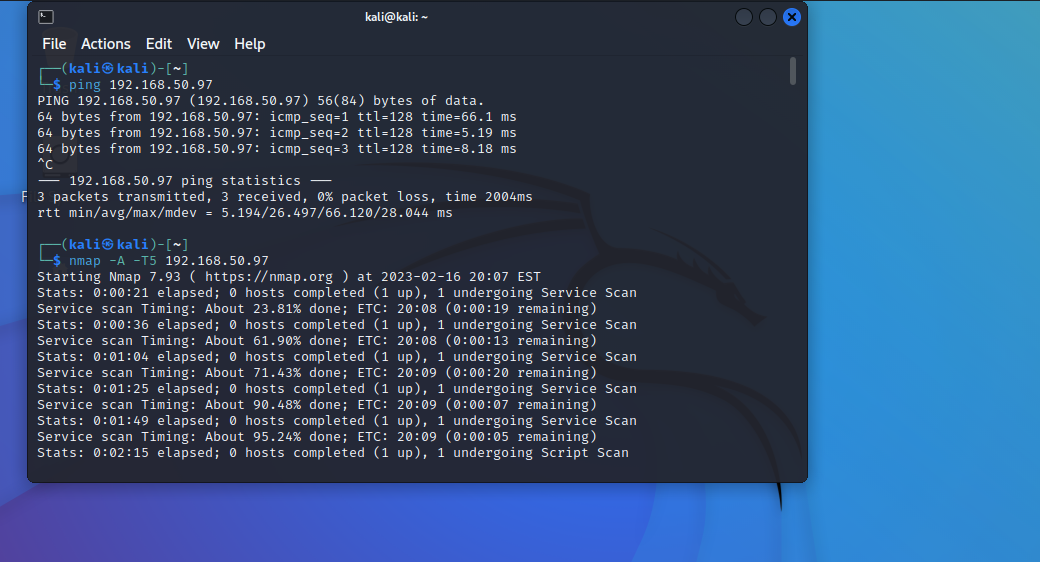
Finally, we can see on the above snapshot that we got the access and entered into meterpreter and got the id of the user who’s running the system at that particular time.

**Vulnerability found through port 445: -**

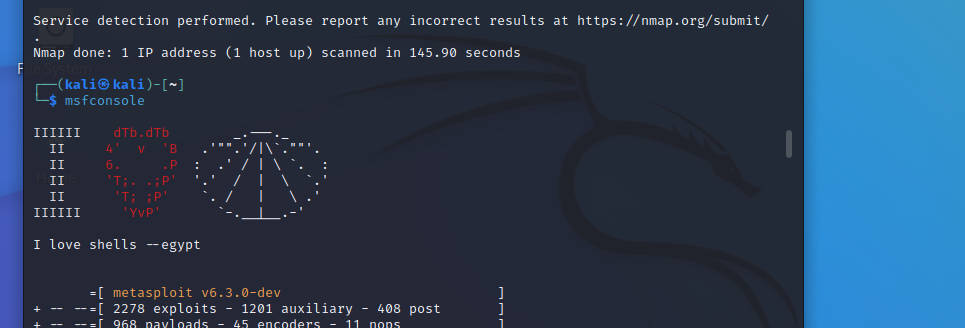
**Exploitation steps for the below vulnerability is as follows: -**

445 is an open port which is using Microsoft-ds as its service.

Steps that we have gone through to find the vulnerabilities in 445 port will be similar to what it is in port 1617and 9200. Below are the snapshots of how we break into the system,



To find any exploit the first thing is to make sure whether the server is up and running or not, for which the ping command will be used as show in the above snapshot. And nmap is used to get all the open ports and services running on that server.



A screenshot of a computer

Description automatically generated with medium confidence

**Vulnerability summary: -**

Search eternalblue itself refers to Microsoft windows OS. This vulnerability gave access to the attacker to execute the code remotely on a vulnerable system without the user interaction.

Graphical user interface, text

Description automatically generated

We have used the first module which is referred to as ‘0’ in the above snapshot. CVSS and CVE score for that is mentioned below as follows,

**CVSS Score: - 10 which is considered as critical.**

**CVE: - CVE-2017-0144.**

Graphical user interface, text

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

A picture containing graphical user interface

Description automatically generated

A screenshot of a computer

Description automatically generated with medium confidence

Text

Description automatically generated

On the above screen shots, we’ve got the access and entered meterpreter, from which we have got the id of the user and system’s information as show in the above snapshots.

**General Business Impact: -**

Some of the legal, privacy and security risks that impacts the business are mentioned below,

Privacy risks: - Once the attacker is in the meterpreter he can gain access to confidential information such as passwords, files, and network traffic.

Security risks: - All the attacks that are performed regarding data such as stealing the data or altering the data will comes under security risks, also attackers can alter the price of the items and install malware which will automatically lead to crash of the website.

Legal risk: - There will be legal risk not to the company but to whomever trying to attack the company’s server without proper authorization.

**Strategic recommendations and remediations: -**

For the kind of vulnerabilities that Montoya Gin have, such as eternal blue, java rmi, elastic, here are few steps that needs to be followed to make the system better.

**Patch your vulnerabilities: -** Make sure to patch your vulnerabilities and keep the systems up to date with all the updated software’s. As far as concerned about eternal blue it was discovered in the year 2017, so if the systems are up to date with all the 2023 versions, then this vulnerability will be no more.

**Network segmentation: -** If the network was segmented enough, it can limit the impact of any breaches and prevents the spread of viruses. When an attacker installs malware in the system, because of segmentation it will only be affected to that segment.

**Use a security solution: -** By implementing Intrusion Detection System or Intrusion Prevention System, it can help detect and block attacks that exploit the vulnerability.

**Secure elastic search and jmx instances: -** Company needs to ensure that the passwords are strong enough and couldn’t be accessible on public internet. Then needs to keep changing the passwords at regular intervals.

**Disable SMBv1: -** By disabling SMBv1 protocol we can prevent the exploitation from eternalblue, as eternalblue mainly targets the SMBv1 protocol.

**Disable remote access: -** If you don’t have the need of remote access, remove the access of anyone can access your server remotely.

**Monitoring: -** Monitoring the search instances on regular basis to identify if there is any suspicious activities or unauthorized access to detect and respond to the attacks.

**Train your employees: -** Social engineering is a common potential attack used by the attackers to exploit the database, so it is better to train the employees on how the vulnerabilities look like to help prevent the attacks.

**Implement a backup and recovery plan: -** To tackle any attacks, you need to have a backup plan, to minimize the downtime and risks.

**Limit the services: -** If any of the services are not being used then stop those services to reduce the risk of attacks from different platforms.

**Use a firewall: -** A properly configured firewall can help prevent the attacks that exploits the vulnerability.

**REFERENCES: -**

*Elasticsearch: Security Vulnerabilities*, https://www.cvedetails.com/vulnerability-list/vendor\_id-13554/Elasticsearch.html.

*Chat.openai.com*. <https://chat.openai.com/>.

“You Are Viewing This Page in an Unauthorized Frame Window.” *NVD*, https://nvd.nist.gov/vuln/detail/cve-2016-3427.

Buckbee, Michael. “What Is Metasploit? the Beginner's Guide.” *Varonis*, Varonis, 24 Feb. 2022, https://www.varonis.com/blog/what-is-metasploit.

“What Is Meterpreter? - Security Wiki.” *Secret Double Octopus*, 7 Sept. 2022, https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/.

“Offensive Security's Exploit Database Archive.” *Exploit Database*, https://www.exploit-db.com/searchsploit.

“Metasploit.” *Wikipedia*, Wikimedia Foundation, 12 Jan. 2023, https://en.wikipedia.org/wiki/Metasploit.

“Nmap.” *Wikipedia*, Wikimedia Foundation, 24 Feb. 2023, https://en.wikipedia.org/wiki/Nmap.

*Sample Network Vulnerability Assessment Report - Purplesec.us*. https://purplesec.us/wp-content/uploads/2019/03/Sample-Network-Security-Vulnerability-Assessment-Report-Purplesec.pdf.