VOLKIS™

Volkis sample report

Prepared for Client, 28 April 2022

Table of Contents

Executive summary 3

Overview 4

Scope . . . 4
Root cause analysis . . . 5
Effective security practices . . . 6
Additional recommendations . . . 7
Conclusion . . . 7

Attack Walkthrough 9

Information gathering . . . 9
Privilege escalation . . . 10
Post-exploitation . . . 10

Detailed Vulnerabilities 11

Vulnerability 1: API endpoints leak client and user data . . . 11
Vulnerability 2: Name resolution poisoning . . . 14
Vulnerability 3: Guest wireless network was not sufficiently segmented . . . 16

Appendices 17

Appendix A: Internal penetration testing methodology . . . 17
Appendix B: External penetration testing methodology . . . 21
Appendix C: Risk assessment methodology . . . 24
Appendix D: Document control . . . 26

Executive summary

This is a sample report for penetration testing from Volkis.

Volkis reports are aimed to be informative and actionable. It includes not just a listing of vulnerabilities and recommendations, but business relevant high level findings that allow you to move forward with your security and ensure that the systems you roll out in the future won't have the same vulnerabilities in them.

This sample report includes some representative high level findings as well as a small sample of vulnerabilities that are similar to real vulnerabilities found in Volkis penetration testing.

If you opt for some of the additional services Volkis provides that enhance your penetration testing such as Pentest Response, a root cause analysis workshop, alert triggering, or compliance checks, the results of these activities may also be included in your penetration testing report or attached as an appendix.

For more information about this report or to book services that could help you in your security journey, please contact Volkis:

- Email: info@volkis.com.au

	Title	Risk
1	API endpoints leak client and user data	High
2	Name resolution poisoning	High
3	Guest wireless network was not sufficiently segmented	Medium

Overview

Client engaged Volkis to perform penetration testing on their internet accessible web applications and infrastructure as well as their internal environment. This testing is part of a yearly testing cycle, with penetration testing being performed as part of the security due diligence.

Testing was performed over a two-week window.

Scope

The scope of the penetration testing included the internal and internet-accessible network environments of Client.

Internal penetration testing

The tester connected to the user subnet of the internal network. All accessible systems and services were in scope for testing.

Wireless penetration testing

The following SSIDs were in scope:

- CLIENT_GUEST
- CLIENT_CORPORATE

Both the network configurations and the wireless infrastructure were in scope for testing. Connected clients and user devices may also be affected and should be considered in scope.

Web application penetration testing

The following web applications were in scope:

- www.client.com.au
- api.client.com.au
- purchase.client.com.au

Both the web applications and web servers were in scope for testing. Backend services such as databases and data processing systems may also be affected and should be considered in scope.

External penetration testing

The following IP range was in scope:

- 0.0.0.0/29

All systems and hosted services in this IP address range are in scope for testing. Additional services used by systems in this range such as DNS, load balancers, and reverse proxies may be affected even if it lies outside this range and should be considered in scope. Similarly, backend services such as databases may also be affected.

Root cause analysis

This section highlights what we determined to be the likely root cause of the vulnerabilities discovered. By addressing the root cause, you reduce the chances of introducing new vulnerabilities of the same class.

Information security awareness training

Even though most employees have no experience in information security, security is never-the-less becoming a key part of the work of every person who works with computers. This means the employees need training on the information security requirements and expectations for their work.

Effective Information Security Awareness Training (ISAT) programmes incorporate a mixture of class-room style presentations or computer-based training, regular updates using emails or announcements in team meetings, and posters in visible locations.

Client should consider implementing an ISAT programme for its staff. This will help to grow the security culture of the organisation and protect the company from social engineering attacks.

Password handling

The password handling of Client was ineffective to ensure that accounts were resilient to password guessing, password spraying, brute forcing, and other password attacks. The insecure handling of passwords included:

- Shared accounts;
- Accounts without multi-factor authentication;
- Reuse of passwords between accounts;
- Weak passwords based on dictionary words;
- Weak password requirements and group policy;
- Weak password storage.

Passwords are the key for accessing the sensitive data and business functions of the organisation. Weak passwords will lead to weak security and can lead to compromises in the organisation.

The following controls may assist in improving password handling at Client:

- Effective password policies combined with password selection being a part of user awareness training will help users to create stronger passwords.
- Regular password cracking exercises can ensure weak passwords are changed while providing users feedback on what are strong and weak passwords.
- Using a password manager to generate secure password and storing them in the password vault. Staff can be given access to shared accounts by allowing them access to the password object.
- Multi-factor authentication can decrease the reliance on passwords as the single factor of security.
- Limiting the usage of shared accounts will decrease the exposure of shared account passwords. Additional controls such as jump boxes or virtual environments can help protect shared accounts.

Effective security practices

Volkis likes to celebrate the positives! This section highlights some of the effective security practices and controls that were observed during the penetration test.

Patch management

The systems in the IT infrastructure of Client were mostly patched with the latest security updates. Many online attacks such as WannaCry and Petya target vulnerabilities that already have already been fixed in security updates. The attacks rely on organisations being lax with their patching or not installing patches properly. Client systems are resilient against such attacks due to their patch level.

Rapid response

During the project, Volkis disclosed multiple critical vulnerabilities to Client. Actions were taken immediately to reduce the risk of the vulnerabilities and ensure that attackers were unable to exploit them to the original, full extent. Client were receptive and proactive with fixing security vulnerabilities.

Strong passwords for wireless networks

The wireless networks used strong passwords that were unlikely to be broken in any reasonable length of time. Although using WPA2Enterprise would still give greater security by removing the need for passwords, the strong passwords will raise the resilience of the networks to attack by third parties.

Similar strength passwords in other areas would also help increase security.

Additional recommendations

Defence-in-depth is a security concept that teaches multiple layers of protection against adversaries. These recommendations are not specifically related to a vulnerability but will increase the overall security of the organisation.

Multi-factor authentication

Externally facing accounts, including accounts that Client held in third party cloud hosted environments, were found to not require Multi-Factor Authentication (MFA). An account that requires multiple factors will need not just a password for login, but also a secondary channel such as SMS's, soft tokens, device authentication, or hard tokens.

MFA reduces the over-reliance on passwords for security, meaning that even if the password is disclosed or compromised the account is still protected. This reduces the likelihood of successful account compromise.

Conclusion

Volkis performed a penetration test on Client and discovered vulnerabilities that could cause **High** impact to the organisation. We recommend remediating the vulnerabilities found in the report and address their root causes to protect the organisation from attacks.

We're here to help! If you find yourself needing assistance with fixing a vulnerability in this report or are unsure what the next step in your security strategy should be, reach out. Volkis' consultants are experts in the information security field who love to talk shop.

Thank you for letting us hack your web applications and thank you for reading.

Attack Walkthrough

This section describes the path the consultant took, starting with no access other than physical port access and eventually gaining full control over the network and sensitive company data. It demonstrates how combining multiple vulnerabilities and chaining exploits can result in a severe consequence for the organisation. Attackers in a similar position would likely gain the same result.

Information gathering

The attack started by accessing the network, receiving an IP address to the corporate network and identifying the Domain Controllers (DCs). Using a combination of the NTLM Relay attack and a name resolution poisoning attacker via LLMNR, the consultant created a new computer account on the DC. Although the account only had low privileges, it was a foothold in the internal network that the consultant could use to gather further information about the network and access some shares.

The following information was retrieved from the DC and member computers:

- All domain users
- All domain groups and group memberships
- Network shares
- Accounts with Service Principal Names (SPNs)
- Active sessions on each member computer
- Password policy

With this level of information, the consultant used BloodHound to create a visual map of domain object relationships, making it easier to understand the domain configuration.

Privilege escalation

Accessing a machine using administrator privileges allowed the consultant to fully compromise that machine, recover all data on that machine and compromise certain credentials. Specifically, the local password hashes were retrieved.

Using an attack called Pass-the-Hash, the consultant used the hash of a local administrator account to compromise other servers on the network. This was possible because multiple servers used the same password for the local administrator account.

This type of progress is known as lateral movement and allows attackers to increase the consequence of compromising a single account.

Having access to at least 10 servers, the consultant targeted CLIENT-Server knowing that a Domain Admin account had a session on that server. Since they had local administrator access to that server, it was possible to impersonate a Domain Admin delegation token and act on behalf of that user. A new account, Volkistest, was added to the domain and elevated to Domain Admin.

Post-exploitation

With this level of access, the consultant effectively has full control over the IT systems of Client. For any non-domain connected systems, it would be possible to install keyloggers and screen monitors to steal admin credentials to other critical systems.

As proof of consequence, the consultant retrieved all password hashes from the DC which proves technical risk to the business.

As a way to prove business risk, the consultant targeted customer data stored in the CLIENT-SQL database. From here, it was possible to retrieve personally identifiable information for all customers, their credit history and how much they have owing.

It was possible to decrypt the credit card information for all customers, since the decryption key was also stored in the database.

Although the card data is encrypted, poor management of the decryption key is in violation of the PCI-DSS compliance standard and could result in significant damage to Client including breaches of contract and trade restrictions.

If an attacker achieves the same level of compromise, Client would be required to disclose the breach under the Privacy Act, causing significant reputational damage.

Detailed Vulnerabilities

Vulnerability 1: API endpoints leak client and user data

Likelihood	Impact	Risk
Likely	Severe	**High**

Risk assessment

This vulnerability requires authentication to exploit, however given the ability for users to create their own accounts, this will not limit the exploitation of this vulnerability.

This vulnerability can be used to gain access to the sensitive personal information of all clients of Client, and the personal details of all advisers. The information exposed includes names, addresses, contact details, payment information, premium information, business and working information including business names and addresses, and medical information.

A compromise using this vulnerability would likely result in a mandatory disclosure to the Privacy Commissioner, potential fines and legal action, large impact to the reputation of Client and a large impact to the trust that customers have with Client. Given the level of trust required for new customers to submit their data, the compromise of this data would have a severe impact on the growth of the business.

Description

Website 1 is a single-page application with a user interface running in the browser that uses APIs to send traffic to and from the server. These APIs are hosted at api.client.com.au.

Although the user interface will usually only allow the user to access data and functionality that they are authorised to access, if a user directly interfaces with the APIs the user can bypass these restrictions.

Direct access to the API endpoints can be performed with any tool such as curl, standard web browsers, or specialist tools such as Burp Suite. When accessing the data, a valid authentication token must be supplied in the headers, along with the application's Ocp-Apim-Subscription-Key. These values are provided when the user authenticates, and with every valid API request that the browser makes when accessing the Website 1.

Accessing client data

The following API endpoint allows unrestricted access to client data:

- api.client.com.au/api/clientDetails?clientId=221

The API does not validate that the user should have access to the client referred to in clientId. When choosing a different ID, a different client's details will be shown. This request, when submitted by any authenticated user, will show details about the client's policy, including names, contact details, address, premium information, work information, super information, and basic medical details.

Using an automated tool, the entire client dataset could be retrieved by changing the clientId number:

B	C	D	E	F	G
Payload	Status	Response received	Error	Timeout	Length
	200	2059	false	false	994
0000	400	293	false	false	663
0001	400	675	false	false	636
0002	400	783	false	false	636
0003	400	1202	false	false	636
0004	400	620	false	false	636
0005	400	618	false	false	636
0006	400	716	false	false	636
0007	400	677	false	false	636
0010	400	581	false	false	637

Figure 1: Client data dump

Accessing user data

Details of all users of the application can also be accessed through the following API endpoint:

- api.client.com.au/api/userDetails?userId=221

This request will show a full listing of all users, including names, contact details, and rights within the application.

Although this endpoint wasn't referred to directly within the application, it could be seen by following the patterns of the API requests.

Recommendations

The API endpoints should be changed to ensure user permissions are checked each time an API is requested. The following API endpoints were identified as having ineffective or insufficient user permissions checks:

- api.client.com.au/api/clientDetails?clientId=221
- api.client.com.au/api/userDetails?userId=221

Vulnerability 2: Name resolution poisoning

Likelihood	Impact	Risk
Likely	Severe	**High**

Risk assessment

Tools to exploit this vulnerability are publicly known and commonly employed when attacking internal networks making the attack likely to be performed if an attacker reaches the internal network. The impact to the business is severe as it could allow attackers to gain administrator access to potentially multiple systems if the right system is poisoned.

The result could be sensitive information disclosure about Client's clients, passwords and documents.

Description

Computers on the active directory domain use vulnerable name resolution protocols Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS).

There protocols are enabled by default and are used as a fallback mechanism for resolving hostnames when DNS fails. However, unlike DNS, both protocols use a broadcast message that is sent to all other machines in the subnet. In a normal use case, a machine will reply back if it has the requested name. Attackers can abuse this by listening for incoming requests and replying back to any requested name, giving the attacker's IP address.

The victim machine will now make further requests to the attacker's machine rather than the real one. This attack can be used to solicit SMB connections to gather the NetNTLM hash from the victim machine or to relay incoming connection to another host as part of an NTLM relay attack.

Whether the password is cracked, or the connection is relayed, the attacker can gain the privileges on the victim user and perform actions on their behalf.

Recommendations

Disable the use of these protocols. For LLMNR, change the following Group Policy Object to Enabled:

Computer Configuration > Administrative Templates > Network > DNS Client > Turn Off Multicast Name Resolution

As there is no GPO for disabling NBT-NS, the use of a logon script is recommended.

1. Create a PowerShell file (*.ps1) and add the following contents:

   ```
   $regkey = "HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\
   Interfaces"Get-ChildItem $regkey |foreach { Set-ItemProperty -Path "
   $regkey$($_.pschildname)"-Name NetbiosOptions -Value 2 -Verbose}
   ```

2. Put the file in the in the following GPO location:

   Computer Configuration > Policies > Windows Settings > Scripts > Startup > PowerShell Scripts

3. You may confirm that the script is working by running the following PowerShell command on each host:

   Get-ChildItem “HKLM:SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces”

4. Ensure that each interface has the setting NetbiosOptions set to 2.

Vulnerability 3: Guest wireless network was not sufficiently segmented

Likelihood	Impact	Risk
Possible	Moderate	**Medium**

Risk assessment

The guest wireless network can be used to attack internal systems. Exploitation requires physical proximity, either at the office, at a nearby building, or at the café downstairs.

Description

After connecting to the guest wireless network named Client_Guest, Volkis ran scans to check the network segmentation between the wireless network and the internal infrastructure. These scans showed that we could connect to all internal systems:

```
root@kali:~# nmap -v -q 192.168.0.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-13 19:17 EST
Initiating Ping Scan at 19:17
Scanning 256 hosts [4 ports/host]
Completed Ping Scan at 19:17, 2.75s elapsed (256 total hosts)
Initiating Parallel DNS resolution of 256 hosts. at 19:17
Completed Parallel DNS resolution of 256 hosts. at 19:17, 0.10s elapsed
Initiating SYN Stealth Scan at 19:17
Scanning 64 hosts [1000 ports/host]
Discovered open port 53/tcp on 192.168.0.21
Discovered open port 53/tcp on 192.168.0.20
Discovered open port 53/tcp on 192.168.0.22
Discovered open port 53/tcp on 192.168.0.23
Discovered open port 53/tcp on 192.168.0.24
Discovered open port 139/tcp on 192.168.0.20
Discovered open port 139/tcp on 192.168.0.21
Discovered open port 139/tcp on 192.168.0.27
Discovered open port 139/tcp on 192.168.0.56
Discovered open port 139/tcp on 192.168.0.59
Discovered open port 139/tcp on 192.168.0.22
```

Figure 2: Successfully connecting to systems in the internal network from the guest WiFi

This issue was reported and then fixed straight away. There were different segmentation rules between the two wireless access points, with one of the access points not properly segmenting systems.

Recommendations

Ensure there are access control restrictions that prevent devices connected to guest wireless networks from connecting to internal systems.

Appendices

Appendix A: Internal penetration testing methodology

Volkis will perform penetration testing on the internal networks of the organisation. This will include the identification and enumeration of systems and services, passive and active reconnaissance, identifying vulnerabilities within systems and services, active interception and manipulation of traffic, targeting weak authentication and account credentials, exploiting identified vulnerabilities, and then analysing and reporting on the results.

Identification and enumeration

Volkis will investigate the subnets in scope using scanning methods, active enumeration to identify what systems and services are accessible, and Open Source Intelligence (OSINT).

Volkis will scan the entirety of the in-scope subnet using a port scanner, scanning for common TCP and UDP open ports. Where sensible and where systems can handle the traffic throughput, full TCP port scans may be launched against systems.

Accessible systems will be analysed to gather information about the system, including whether the system is running Microsoft Windows or Linux and the version including the operating system build or service pack information.

Open services and ports will be enumerated to identify what service is running and information about that service including the version, banner information, and any third party plugins and modules that could be installed. If there are open file shares, the tester may review them for sensitive information or account credentials.

A search for hidden assets and endpoints will also be performed. This is to expand the attack surface and find things such as:

- Non-linked admin/high value pages;
- Websites behind a virtual hostname;
- UAT pages/instances with live data.

The tester will use a network sniffer to capture traffic that is being broadcast on the network. This may include connection requests, domain requests, and other potentially useful information.

If the organisation is using Active Directory, the tester will attempt to retrieve information about the directory using null sessions or authentication credentials. This can provide information about the users, systems, and group policy of the organisation.

Responding to and relaying internal traffic

The tester will analyse the traffic that is being broadcast on the internal network for opportunities to respond or relay authenticated connections. Although many protocols may be vulnerable to relay attacks, common vulnerable protocols include SMB, LDAP and HTTP.

When a user attempts to connect to a server, the tester will respond to that connection as if it were the server. The tester will then pass any information sent through that connection to the server. From the users' perspective there will be no change as they will be seeing the information they are expecting, but the tester will be able to gain access as the user to the target server.

The tester will then attempt to use this access to run commands, create new account objects, retrieve password hashes, or view sensitive file shares.

Vulnerability identification

Each open system, service and asset will be investigated for potential vulnerabilities that could be used to compromise systems, gain access to information, make malicious changes to information or applications, or create impact on the availability of systems and information.

The vulnerability identification will begin with using automated vulnerability assessment tools on the environment. This will include running generalist network vulnerability assessment tools such as Tenable Nessus that will scan for potential misconfigurations, missing patches, out-of-date software, and other common vulnerabilities.

For specific services, more specialised vulnerability scanning, and assessment tools will be used. These specific tools will give greater depth of vulnerability assessment than the general vulnerability assessment tools.

Following the vulnerability assessment, and with assistance of the results of the identification, enumeration, and vulnerability assessment results, the tester will then use manual techniques to uncover vulnerabilities that automated techniques will not see. This will include targeting custom developed services, leveraging the OSINT information, investigating the feedback that the services provide when test cases are entered, and other manual techniques.

Vulnerabilities that are identified will not just be technical vulnerabilities, but could also include logic flaws, gaps in business process, or any other weakness of the application that could present risk to the organisation.

Exploitation

The tester will exploit identified vulnerabilities to better understand its impact and to eliminate the possibility of a false-positive.

The exploitation will occur alongside the vulnerability identification phase as vulnerabilities are identified. It will incorporate prioritisation, where vulnerabilities that tend to present higher risk to the organisation will be prioritised over low risk vulnerabilities. If there is a significant chance of service disruption, the tester will organise a window for exploitation, or not exploit it at all.

Exploitation will often involve the usage of publicly available tools, custom written tools, or specific actions taken by the tester.

Due to the nature of certain vulnerabilities, not every vulnerability can be exploited by the tester. This could be due to the level of network or system access required for exploitation, privilege requirements for exploitation, or specific conditions that need to be in place. These vulnerabilities will still be reported on even if exploitation was not achieved. The lack of exploitation will be a consideration when assessing the risk rating during the risk assessment.

Due to time limitations and prioritisation, not all vulnerabilities that are identified will be exploited during this phase. For example, the tester may choose not to exploit vulnerabilities that present a low risk to the organisation or that have a known impact.

Sensible precautions will be used during the exploitation phase to minimise the risks of availability issues. This could include performing exploitation out-of-hours or using a development or testing server. If the risks of exploitation are considered greater than the benefit of exploitation, and those risks cannot be mitigated or managed, the exploitation of the vulnerability will be skipped.

Exploitation of vulnerabilities that specifically create Denial of Service (DoS) condition will not be performed, nor will any sort of Distributed Denial of Service (DDoS).

Post-exploitation

Successful exploitation of vulnerabilities will provide the tester with additional access to information, functionality, and potentially full control over all systems in the environment. This additional access will be used by the tester to determine and prove the full scope of compromise, including the true business impact of the vulnerability.

The additional access will be fed back into the previous stages to determine if additional services can be enumerated and additional vulnerabilities can be found and exploited.

As part of post-exploitation, the tester will seek out business-relevant information and functionality such as business critical applications, ERP systems, payroll, credit card information and customer databases, and procurement systems. This will be used to establish the real-world impact to the organisation of the compromise.

Appendix B: External penetration testing methodology

Volkis will perform penetration testing on the internet-accessible systems and services within the target subnet. This will include the identification and enumeration of systems and services, identifying vulnerabilities within those systems and services, targeting weak authentication and account credentials, exploiting identified vulnerabilities, and then analysing and reporting on the results.

Identification and enumeration

Volkis will investigate the subnets in scope using scanning methods, active enumeration to identify what systems and services are accessible from the internet, and Open Source Intelligence (OSINT).

Volkis will scan the entirety of the in-scope subnet using a port scanner, scanning for common TCP and UDP open ports. Where possible and where systems can handle the traffic throughput, full TCP port scans will be launched against systems.

Accessible systems will be analysed to gather information about the system, including whether the system is running Microsoft Windows or Linux and the version including the operating system build or service pack information.

Open services and ports will be enumerated to identify what service is running and information about that service including the version, banner information, and any third-party plugins and modules that could be installed.

A search for hidden assets and endpoints will also be performed. This is to expand the attack surface and find things such as:

- Non-linked admin/high value pages;
- Websites behind a virtual hostname;
- UAT pages/instances with live data.

The tester will investigate the organisation using common OSINT sources. This could include WHOIS information, social media sources and publicly available websites including the organisation's website. Other assets that may impact the security of the external network such as DNS, email, code repositories, third party hosting and Software as a Service providers will also be considered as part of the security posture.

Vulnerability identification

Each open system, service and asset will be investigated for potential vulnerabilities that could be used to compromise systems, gain access to information, make malicious changes to information or applications, or create impact on the availability of systems and information.

The vulnerability identification will begin with using automated vulnerability assessment tools on the environment. This will include running generalist network vulnerability assessment tools such as Tenable Nessus that will scan for potential misconfigurations, missing patches, out-of-date software, and other common vulnerabilities.

For specific services, more specialised vulnerability scanning and assessment tools will be used. These specific tools will give greater depth of vulnerability assessment than the general vulnerability assessment tools.

Following the vulnerability assessment, and with assistance of the results of the identification, enumeration, and vulnerability assessment results, the tester will then use manual techniques to uncover vulnerabilities that automated techniques will not see. This will include targeting custom developed services, leveraging the OSINT information, investigating the feedback that the services provide when test cases are entered, and other manual techniques.

Vulnerabilities that are identified will not just be technical vulnerabilities, but could also include logic flaws, gaps in business process, or any other weakness of the application that could present risk to the organisation.

Exploitation

The tester will exploit identified vulnerabilities to better understand its impact and to eliminate the possibility of a false-positive.

The exploitation will occur alongside the vulnerability identification phase as vulnerabilities are identified. It will incorporate prioritisation, where vulnerabilities that tend to present higher risk to the organisation will be prioritised over low risk vulnerabilities. If there is a significant chance of service disruption, the tester will organise a window for exploitation, or not exploit it at all.

Exploitation will often involve the usage of publicly available tools, custom written tools, or specific actions taken by the tester.

Due to the nature of certain vulnerabilities, not every vulnerability can be exploited by the tester. This could be due to the level of network or system access required for exploitation, privilege requirements for exploitation, or specific conditions that need to be in place. These vulnerabilities will still be reported on even if exploitation was not achieved. The lack of exploitation will be a consideration when assessing the risk rating during the risk assessment.

Due to time limitations and prioritisation, not all vulnerabilities that are identified will be exploited during this phase. For example, the tester may choose not to exploit vulnerabilities that present a low risk to the organisation or that have a known impact.

Sensible precautions will be used during the exploitation phase to minimise the risks of availability issues. This could include performing exploitation out-of-hours or using a development or testing server. If the risks of exploitation are considered greater than the benefit of exploitation, and those risks cannot be mitigated or managed, the exploitation of the vulnerability will be skipped.

Exploitation of vulnerabilities that specifically create Denial of Service (DoS) condition will not be performed, nor will any sort of Distributed Denial of Service (DDoS).

Post-exploitation

Successful exploitation of vulnerabilities will provide the tester with additional access to information, functionality, and potential access to the internal environment. This additional access will be used by the tester to determine and prove the full scope of compromise, including the true business impact of the vulnerability.

The additional access will be fed back into the previous stages to determine if additional services can be enumerated and additional vulnerabilities can be found and exploited.

Appendix C: Risk assessment methodology

A qualitative risk assessment is performed on each vulnerability to determine the impact and likelihood of the vulnerability being exploited. An overall risk is calculated based on the table below:

Impact \ Likelihood	Rare	Unlikely	Possible	Likely
Critical	Medium	High	Critical	Critical
Severe	Low	Medium	High	High
Moderate	Low	Medium	Medium	High
Low	Low	Low	Low	Medium

The risk assessment methodology is derived from industry standards such as ISO 31000[1] and OWASP Risk Rating Methodology[2].

The impact rating is deduced from multiple factors that consider both technical impact and business impact:

- **Loss of confidentiality**: How much sensitive information could be accessed or leaked and how sensitive was it?
- **Loss of integrity**: How much data could be corrupted and what degree of corruption was possible? Was it possible to perform actions on behalf of others?
- **Loss of availability**: How much services could be disrupted, preventing users from performing their tasks? What was the degree of impairment?
- **Financial damage**: How much money could be lost as a result?
- **Reputational damage**: How badly would the company's reputation be damaged and how much trust could customers lose?
- **Non-compliance**: Would the business be in breach of certain compliance standards they are obliged to comply with? (E.g. Privacy Act)

The likelihood is deduced from considering who the adversary may be and factors around the vulnerability:

- **Skill of adversary**: How skilful is the attacker likely to be?
- **Motive**: What are the motivating factors that the adversary may have?
- **Resources**: How much time and economic resources does the adversary have?
- **Ease of discovery**: How likely is the adversary to discover the vulnerability?
- **Ease of exploitation**: How easy is the vulnerability to exploit and are there publicly available tools to aid in doing so?

[1] https://www.iso.org/iso-31000-risk-management.html
[2] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

- **Detection**: How likely is the attack to be discovered by the organisation?

An overall rating (from Low to Critical) is given to each vulnerability. The vulnerabilities are then sorted in order from importance and urgency to remediate.

Appendix D: Document control

Document information

Client	Client
Document name	Volkis sample report
Document version	1.0

Document changes

Version	Date	Name	Changes
1.0	2022-04-28	Volkis	April 2022 sample report

Document contributors

Name	Role	Phone number	Email address
Volkis			info@volkis.com.au

VOLKIS™