VENDOR NAME:	Alliant Cybersecurity, LLC
BUYER:	Brandon L. Barr
SOLICITATION NO.:	CRFQ LOT2400000009
BID OPENING DATE:	March 28th, 2024
BID OPENING TIME:	1:30pm EDT
FAX NUMBER:	304-558-3970

RESPONSE TO

CENTRALIZED REQUEST FOR QUOTE

FOR

NETWORK PENETRATION TESTING AND CYBERSECURITY ASSESSMENTS

FOR

STATE OF WEST VIRGINIA

CYBERSECURITY

An alliantgroup Company

ALLIANT

CYBERSECURITY

An alliantgroup Company

Submitted To:	Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130
Submitted By:	Rizwan Virani Vice Chairman Alliant Cybersecurity rizwan.virani@alliantcybersecurity.com P: (713) 877-9600 F: (713) 877-9657
Date:	March 28, 2024

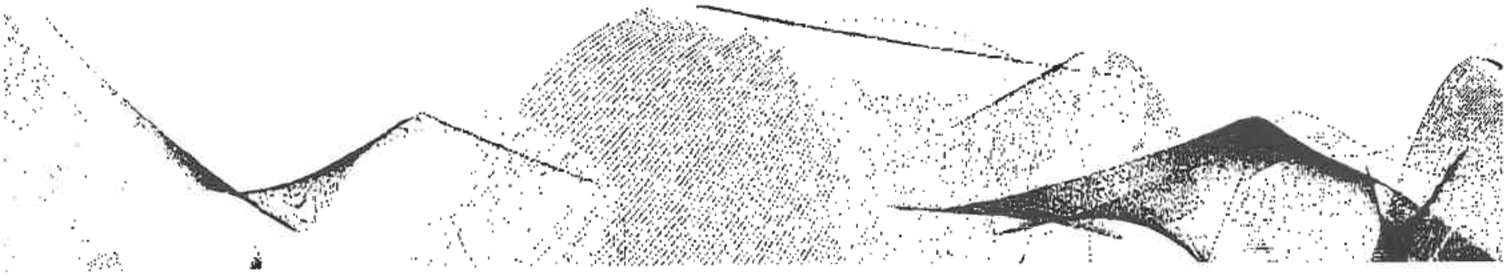


Table of Contents

ALLIANT
CYBERSECURITY

Subject: Network Penetration Testing and Cybersecurity Assessments

To whom it may concern,

We are extremely pleased to have the opportunity to respond to the request for a proposal for network penetration testing and cybersecurity assessment to the State of West Virginia for the West Virginia Lottery ("the Lottery"). We are confident that after reading our submission, you will be assured that Alliant Cybersecurity is the best option for your assessment needs.

Alliant Cybersecurity ("Alliant") is the information security division of alliantgroup providing customized solutions for the digital technology, security, and governance needs of entities all around the country. Our team of experts has extensive experience in delivering comprehensive cybersecurity assessment services to organizations of all sizes in both the public and private sectors.

At Alliant, we've built a reputation for a long-standing dedication to serving government entities, and our leadership team is focused on the needs of the government. Our board is led by former public servants, including IRS commissioners, senators, Members of Congress, and Presidential Cabinet Members. They are now helping direct our services to ensure the unique needs of local governments are addressed with a strong emphasis on the responsible stewardship of taxpayer dollars.

While we are the best fit for the Lottery at an organizational level, I also want to highlight that we are the best fit at a technical level. Our experts hold all relevant certifications to execute this project appropriately, including CISA, CISM, CISSP, HITRUST, CDPSE, PCI-DSS, PMP, and more. They also have experience with compliance frameworks such as GLBA, HIPAA, NIST Cybersecurity Framework, and Cyber Insurance. We guarantee accountability, professionalism, and innovation in every aspect of our work, making us the ideal partner for the Lottery.

Other providers may have similar certifications, but what makes Alliant the preferred provider of entities across the United States is our customized approach and our dedication to customer service, which stands as the central pillar of our approach. Be assured the solutions we propose to the Lottery will be tailored to your needs. Know that we will not rest until you are more than satisfied with our results. If there is ever an issue, your team will need to make only one call to have it resolved. We stand by our customer-centric approach, which is why we have been selected from so many competitors.

Finally, I want to highlight our commitment to promoting diversity, equity, and workforce inclusion that helps us better serve our clients. We believe diversity in knowledge, ideas, and opinions makes the services we provide to our clients superior. This is part of our organizational identity, as we are minority-led, and over 60% of our workforce and executive leadership is female. We are passionate about creating avenues for leadership and advocating education. Every year, Alliant donates school supplies to students in need, sponsors STEM field trips, and awards grants. We have also established programs like the alliantgroup Black Collaborative. This group was created to promote excellence in the African-American community and create more opportunities for Black leadership in our organization and organizations across America.

We are confident that we can exceed the expectations and remain committed to utilizing our experience and expertise to provide network penetration testing and cybersecurity assessment services. Thank you for considering our proposal response. We look forward to working with the Lottery.

Sincerely,

Rizwan H Virani

Rizwan Virani
Vice Chairman

Executive Summary

Our company is pleased to submit a response to the West Virginia Purchasing Division's RFP for Information Technology Cybersecurity Assessments on behalf of the West Virginia Lottery. We understand that the Lottery is seeking to establish a contract for external network, website, wireless, and internal/client-side penetration testing assessments, all of which must be conducted to the highest industry standards.

Our team is committed to providing thorough and comprehensive assessments that follow the Center for Internet Security methodology and employ the latest techniques and guidelines from the OWASP Top 10 Project and the NIST SP 800-115 Information Security Testing and Assessment technical guide. We will utilize a combination of automated tools and manual techniques to thoroughly assess and evaluate the Lottery's infrastructure and identify areas that present an exploitable vulnerability.

Our External Network Penetration Testing service will be performed remotely, while Website Penetration Testing, Internal/Client-Side Network Penetration Testing, and Wireless Penetration Testing will be conducted onsite at all Lottery locations. We will provide a four-phased structure methodology for each type of assessment, including reconnaissance, mapping, discovery, and exploitation.

After each assessment, we will provide an Executive Summary Report and a Technical Report detailing each vulnerability type discovered, along with a critical, high, medium, or low-risk rating. Additionally, we will provide a Findings Presentation to the Lottery management team that provides an overview of strengths, weaknesses, and vulnerabilities identified throughout the assessment.

Our team is highly experienced in performing these types of assessments and is committed to delivering high-quality results that meet the Lottery's needs. We look forward to the opportunity to work with the Lottery and provide the cybersecurity assessments needed to ensure the safety and security of their infrastructure.

Scope of Work

In recent years, the frequency and severity of cyber-attacks have increased significantly. According to reputable studies, an organization's average cost of cybercrime has increased by 15% yearly for the past five years. This highlights the importance of identifying and addressing vulnerabilities before malicious actors can exploit them.

Penetration testing provides organizations with a proactive approach to cybersecurity. It allows them to identify weaknesses in their systems and networks, evaluate their overall security posture, and take necessary measures to mitigate potential risks. This helps prevent cyber-attacks and reduces the impact and cost of a successful attack.

Benefits of Penetration Testing

1. **Identify Vulnerabilities:** The primary benefit of penetration testing is identifying vulnerabilities that hackers could potentially exploit. This allows organizations to take necessary steps to fix these vulnerabilities before they can be used against them.
2. **Ensure Compliance:** Many organizations, especially those in highly regulated industries, must conduct regular penetration testing as part of their compliance requirements. This helps them meet regulatory standards and avoid penalties.
3. **Cost-Effective:** While the upfront cost of penetration testing may seem high, it is much more cost-effective than being the victim of a cyber-attack. The average cost of a data breach for an organization is $3.86 million, while the average cost of a penetration test is significantly lower.
4. **Improved Security Posture:** Penetration testing identifies vulnerabilities and helps organizations improve their security posture. Organizations can strengthen their defenses against cyber-attacks by addressing weaknesses and implementing necessary changes.
5. **Build Customer Trust:** With the increasing number of data breaches and cyber-attacks, customers are becoming more concerned about the security of their personal information. Regular penetration testing and taking necessary security measures can help organizations build trust with their customers.

Penetration testing plays a crucial role in ensuring the cybersecurity of organizations. It helps them identify vulnerabilities, ensure compliance, improve security posture, and build customer trust. By conducting regular penetration testing, organizations can stay one step ahead of cybercriminals and protect themselves from potential attacks.

Penetration Testing Scope Components

It is important to consider the multiple tests that can be conducted during a penetration test. The penetration tests include physical security assessment, network assessment and surveillance, application assessment, social engineering, and wireless testing.

Selecting the most appropriate approach for a given scenario provides a more accurate and effective assessment of a system's security posture.

1. External Network Assessment

Gathering enough information about the targeted networks or systems is critical for proceeding with the Security Assessment phases. This can be achieved by employing various tools and techniques, such as network scanning and publicly available data. Furthermore, conducting offline and onsite intelligence gathering is essential to reveal any mishandling of sensitive data.

There are two distinct goals to keep in mind when it comes to security testing: the objectives of the client and those of Alliant. From the client's perspective, the aim is to evaluate the efficiency of all security measures in the operating environment. On the other hand, Alliant's objective during penetration testing is to gain access to systems and applications that contain confidential information or attempt to perform other malicious activities.

When testing a network, numerous components must be assessed to ensure the optimal performance of the system and network architecture designs. Experts typically evaluate several factors, including using IPv4 addresses, security protocols for internally hosted applications, domain controllers, and internal web servers. Potential attack vectors such as password cracking, buffer overflows, router testing, DoS and Distributed DoS testing, and containment measures testing are also analyzed. All heavy-load brute force or automated tasks and DoS and Distributed DoS testing will only be performed when approved/authorized.

Additionally, it's important to conduct external penetration tests to simulate attacks from outside the organization's network boundaries, mimicking the strategies employed by hackers attempting to breach the system from the internet. These tests primarily target externally accessible assets such as web applications, email systems, VPN gateways, firewalls, and other internet-facing services. Testers attempt to exploit vulnerabilities in these external systems to gain unauthorized access, escalate privileges, or extract sensitive information. They might use techniques like port scanning, vulnerability scanning, and exploitation of known vulnerabilities.

To meet the necessary goals of an external network penetrating test, our team of experts will conduct a series of tests, which include:

- Network scanning.
- Monitoring software review.

- Infrastructure analysis.
- Data transmission security assessment.
- Web application evaluation.
- Firewall effectiveness review.
- Intrusion Detection / Intrusion Prevention (IDS/IPS) systems assessment.

2. Internal Network Assessment

Internal Network Penetration Testing is a crucial aspect of network security that helps verify the effectiveness of security controls and policies designed to protect against cyber threats. It also focuses on simulating attacks that originate from within an organization's network perimeter. This type of testing is especially important for identifying vulnerabilities that could be exploited by malicious insiders or external attackers who have gained access to the internal network.

During Internal Penetration Testing, testers assess the security of assets within the internal network, such as servers, workstations, databases, and other resources. Testers typically start with a foothold within the network, which could be obtained through various means, such as phishing attacks or exploiting external vulnerabilities. Once inside, they attempt to escalate privileges, move laterally across the network, and access sensitive data. This may involve exploiting misconfigurations, weak access controls, or unpatched systems.

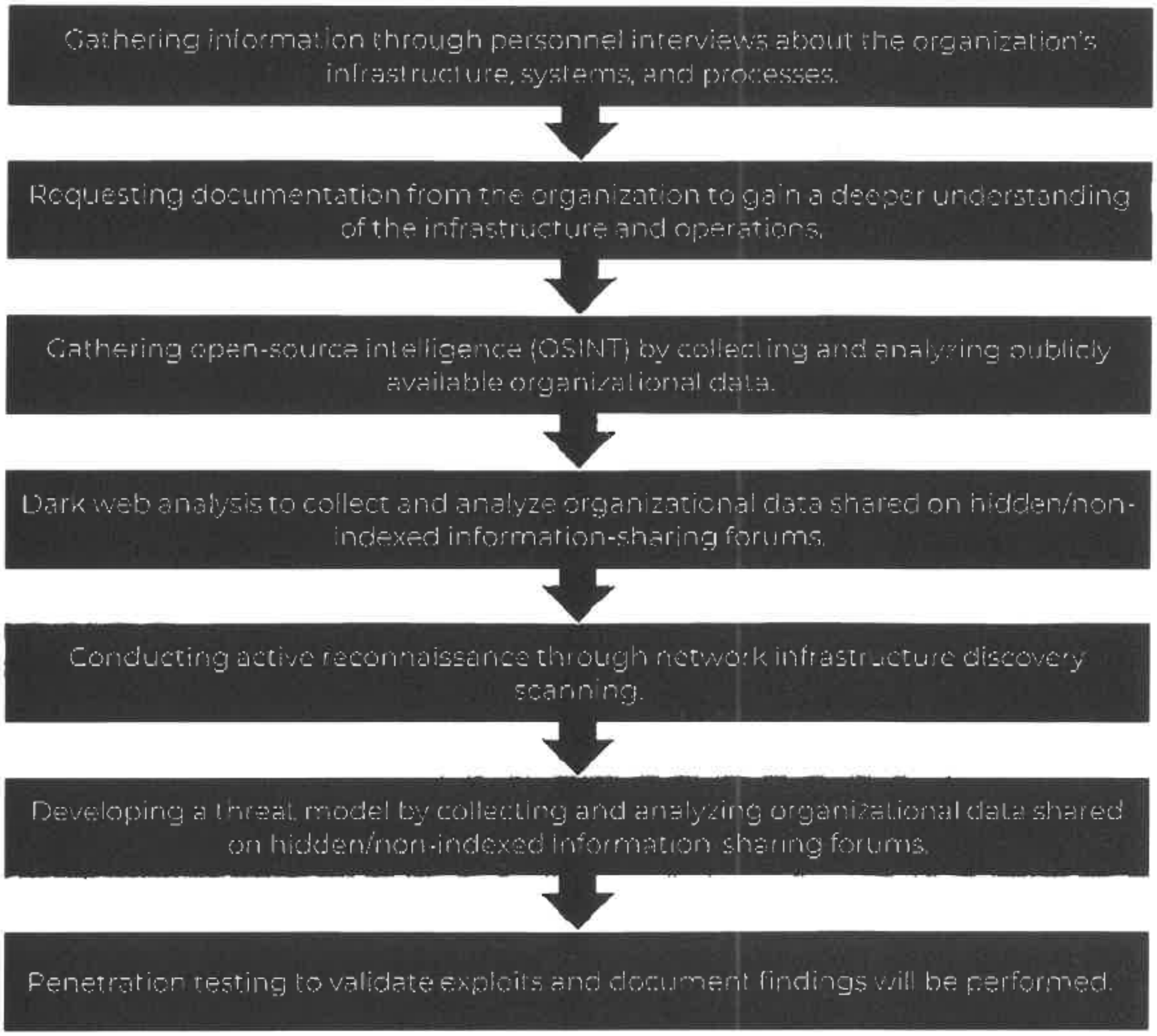
The goal of Internal Penetration Testing is to identify weaknesses in the internal network and assess the efficacy of security controls and policies designed to prevent and detect unauthorized access. This type of testing is critical to ensuring the confidentiality, integrity, and availability of sensitive data within the organization.

To meet the necessary goals of an external network penetrating test, our team of experts will conduct a series of tests, which include:

- Network scanning.
- Monitoring software review.
- Infrastructure analysis.
- Data transmission security assessment.

By meticulously examining each component, our experts ensure that the network operates effectively, efficiently, and securely.

Figure 1: External and Internal Assessment Methodology



Gathering information through personnel interviews about the organization's infrastructure, systems, and processes.

Requesting documentation from the organization to gain a deeper understanding of the infrastructure and operations.

Gathering open-source intelligence (OSINT) by collecting and analyzing publicly available organizational data.

Dark web analysis to collect and analyze organizational data shared on hidden/non-indexed information-sharing forums.

Conducting active reconnaissance through network infrastructure discovery scanning.

Developing a threat model by collecting and analyzing organizational data shared on hidden/non-indexed information sharing forums.

Penetration testing to validate exploits and document findings will be performed.

We conduct a comprehensive network assessment that guarantees the confidentiality of any information and tools used in the process. We keep our clients informed throughout the assessment and immediately notify them if we identify any vulnerabilities that could pose a risk to their critical business processes or IT services.

3. Web Application Assessment

Our Web Application Penetration Testing adopts a risk-based approach to manually detect essential security vulnerabilities in the organization's relevant applications, such as customer, patient, taxpayer, etc., by testing each interface to the application, which may include the server operating system, database, application platform, etc. We conduct tests by combining advanced scanning tools with manual testing to identify and verify vulnerabilities, configuration errors, and flaws in business logic. We can detect issues that automated scanners often overlook by conducting in-depth manual application testing.

Alliant will also review and conduct application security testing of source code repositories to ensure no vulnerabilities may be exploited. Critical findings will be immediately reported to the client's stakeholders and tested thoroughly during the penetration testing phase.

Using this approach, our comprehensive Application Penetration Test covers the classes of vulnerabilities outlined in the Open Web Application Security Project (OWASP) Top 10 2021 and beyond:

- A01: Broken Access Control.
- A02: Cryptographic Failures.
- A03: Injection.
- A04: Insecure Design.
- A05: Security Misconfiguration.
- A06: Vulnerable and Outdated Components.
- A07: Identification and Authentication Failures.
- A08: Software and Data Integrity Failures.
- A09: Security Logging and Monitoring Failures.
- A10: Server-Side Request Forgery.

The testing team will comprehensively evaluate user session management to prevent unauthorized access. This will involve various measures, such as verifying the input validation of login fields, assessing the security configurations of cookies, and conducting lockout testing. Furthermore, we will also perform penetration testing of mobile applications to identify any weaknesses or vulnerabilities that may exist.

4. Wireless Testing

A wireless test is a comprehensive process that involves evaluating the security of a wireless network infrastructure. It aims to identify vulnerabilities and potential attack vectors that malicious actors could exploit. By performing controlled simulations of real-world attacks, this test enables organizations to uncover weaknesses in their wireless networks and implement effective security measures.

This type of test plays a crucial role in enhancing organizations' overall security posture. Through meticulous vulnerability identification and thorough analysis, potential security risks and threats can be identified, allowing organizations to address and mitigate them proactively. By strengthening the security of their wireless networks, organizations can significantly reduce the risk of unauthorized access and data breaches.

Moreover, conducting a wireless penetration test is essential for regulatory compliance. Many industry-specific regulations and standards, such as PCI-DSS and HIPAA, mandate regular security assessments, including wireless security assessments. By adhering to these regulations, organizations can demonstrate their commitment to protecting sensitive information and maintaining the trust of their customers.

5. Social Engineering

The Alliant team prepares a unique and relevant Social Engineering Test to be conducted by email to a selected set of users. The social engineering simulation will be defined by the scope after meeting key stakeholders to tailor the exercise to the organization's unique needs and context. As per the requirements, we will include a social engineering exercise during the external network penetration testing.

Next, realistic and relevant phishing scenarios will be developed, representing plausible threats to the organization, which can involve creating fake websites, phone numbers, or text messages. For the Lottery, a phishing email scenario will be developed targeting the 200 active Lottery staff. The users will be selected within the organization, either randomly or focused on specific departments or roles, and the content of the simulated attacks will be prepared, aligning it with the chosen scenarios. Technical preparations will be made to send emails, track user interactions, and ensure the simulation does not interfere with the organization's security measures. All activities will comply with applicable laws and regulations, and necessary permissions or consents are obtained.

Following the simulation, debriefing and feedback will be provided as part of the Assessment's final reporting, including individual or group discussions on the users' actions and opportunities for improvement. A comprehensive report outlining the process, findings, and recommendations will be compiled and presented to the organization.

Ongoing support, training, or other resources will be offered to help your organization address any identified vulnerabilities and enhance its overall resilience against social engineering attacks. The process aims to provide a valuable opportunity to test employees' awareness and build more robust cybersecurity defenses.

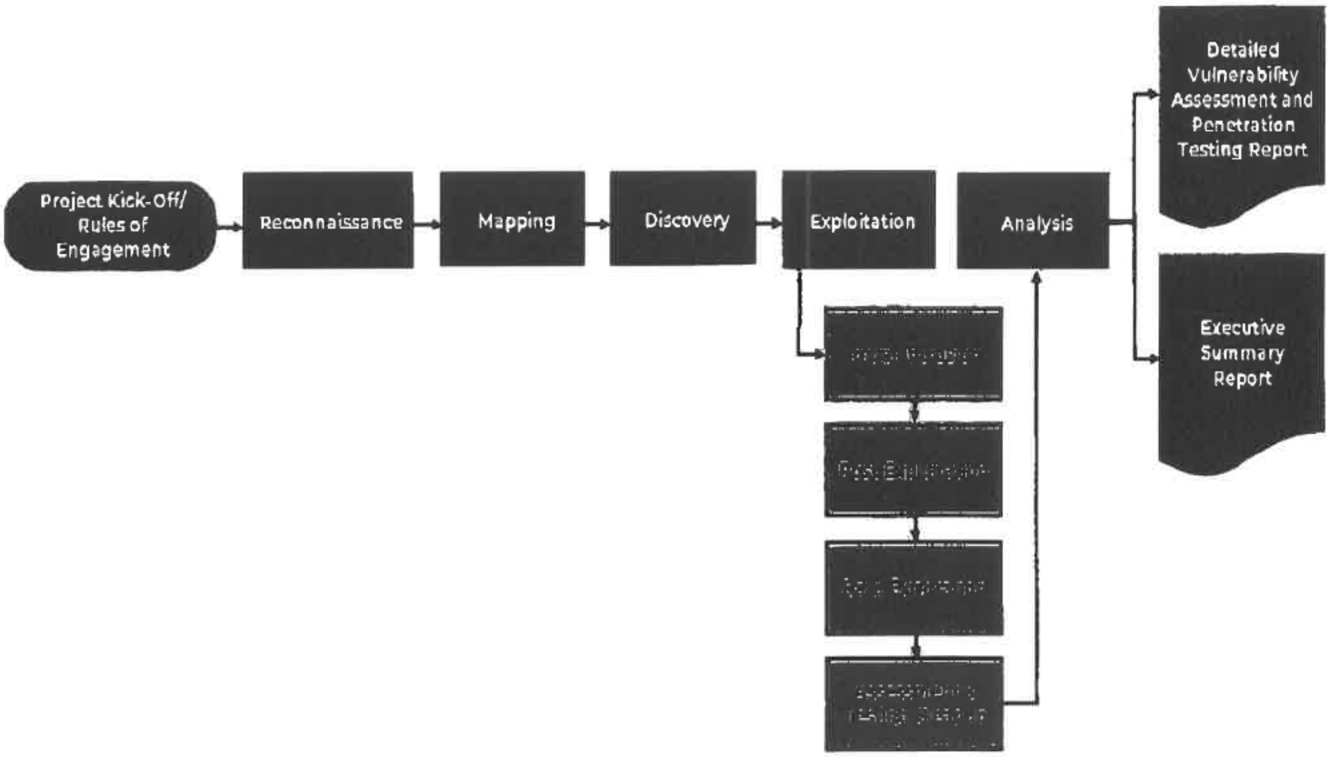
Methodology and Approach

Alliant will conduct a comprehensive cybersecurity assessment for the West Virginia Lottery, as per the requirements stated in the RFP. The assessment will include external network, website, wireless, and internal/client-side penetration testing assessments, all in accordance with the Center for Internet Security methodology and using guidelines from OWASP Top 10 Project and NIST SP 800-115 Information Security Testing and Assessment technical guide and broken into the multiple phases.

During the assessment, Alliant will use a combination of automated tools and manual techniques to identify areas of exploitable vulnerability in the Lottery's infrastructure. The goal of this assessment is to provide the Lottery with a clear understanding of its cybersecurity posture and to identify potential threats and vulnerabilities that could be exploited by attackers. Alliant will provide the Lottery with a detailed report outlining the results of the assessment and recommendations for addressing any vulnerabilities identified.

Our technical approach in the figure below outlines the tasks needed to fulfill your organization's requirements. Our proposal provides a detailed and comprehensive description of our processes, tools, and outputs.

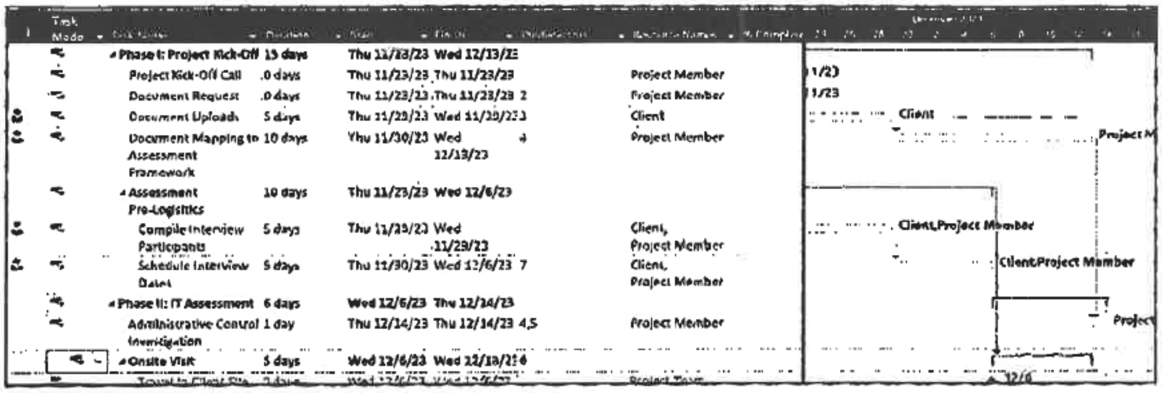
Figure 2: Penetration Test Methodology


Project Kick-Off/ Rules of Engagement
Reconnaissance
Mapping
Discovery
Exploitation
Analysis
Detailed Vulnerability Assessment and Penetration Testing Report
Executive Summary Report
Post Exploitation

Phase 1: Project Kick-Off/Rules of Engagement

At the outset of our engagement, we will arrange a project kick-off call to coordinate all the activities. Before the kick-off call, the Alliant team will define all the tasks, deadlines, dependencies, deliverables, and resource allocation in detail. These details will be presented to your team during the project kick-off call. Subsequently, a comprehensive assessment of project phases, tasks, and deadlines will be conducted to identify potential risks. The figure below is an excerpt from a sample project plan that further illustrates these details.

Figure 3: Example Project Plan



Task Mode	Task Name	Duration	Start	Finish	Predecessors	Resource Names	% Complete
	Phase I: Project Kick-Off	15 days	Thu 11/23/23	Wed 12/13/23			
	Project Kick-Off Call	0 days	Thu 11/23/23	Thu 11/23/23		Project Member	
	Document Request	0 days	Thu 11/23/23	Thu 11/23/23	2	Project Member	
	Document Uploads	5 days	Thu 11/23/23	Wed 11/29/23	3	Client	
	Document Mapping to Assessment Framework	10 days	Thu 11/30/23	Wed 12/13/23	4	Project Member	
	Assessment Pre-Logistics	10 days	Thu 11/23/23	Wed 12/6/23			
	Compile Interview Participants	5 days	Thu 11/23/23	Wed 11/29/23		Client, Project Member	
	Schedule Interview Dates	5 days	Thu 11/30/23	Wed 12/6/23	7	Client, Project Member	
	Phase II: IT Assessment	6 days	Wed 12/6/23	Thu 12/14/23			
	Administrative Control Investigation	1 day	Thu 12/14/23	Thu 12/14/23	4,5	Project Member	
	Onsite Visit	5 days	Wed 12/6/23	Wed 12/13/23	4		
	Travel to Client Site	2 days	Wed 12/6/23	Wed 12/6/23		Project Team	

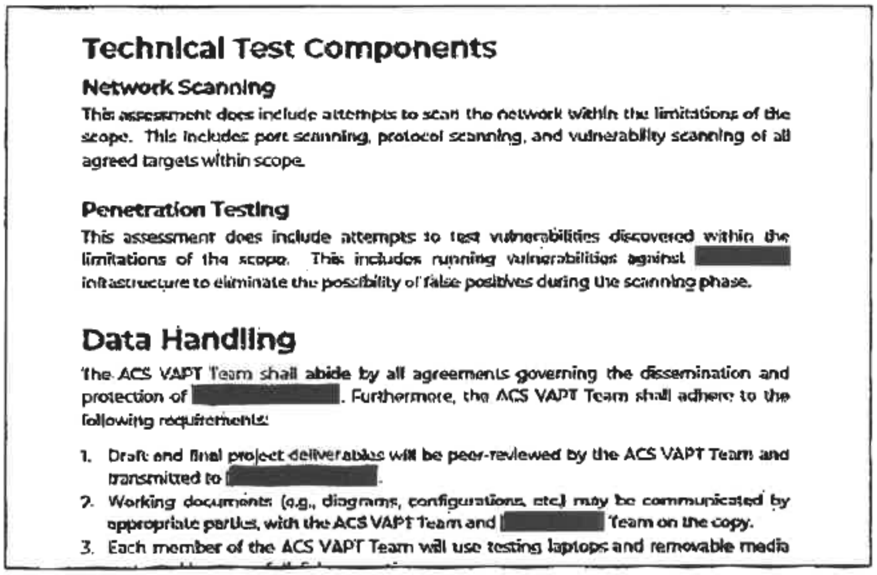
During the project kick-off meeting, Alliant will engage with your stakeholders to discuss and obtain approval for all assessment and testing techniques. Our team will propose various methods, starting with non-disruptive measures and gradually increasing the level of effort. This approach mirrors the actual behavior of malicious agents, who tend to be cautious. It is important to note that all activities will be discussed and approved before any actions are taken. We will clearly define a schedule of events and produce a Rules of Engagement document outlining the project's scope. The document will contain all the necessary parameters, including specific testing parameters, the testing team's rules, and information about testing that can help protect the client.

These are some of the aspects addressed in the Rules of Engagement agreement:

- Roles, along with contact information.
- Testing Schedule.
- Testing Restrictions.
- Confidentiality agreements.
- Handling of sensitive and critical vulnerabilities.
- In-scope targets, including IP addresses and URLs.

Developing and signing off on the Rules of Engagement document for penetration testing and vulnerability scan activities is crucial in ensuring the security of systems within the project's scope. By meticulously crafting this document, we can ensure the testing is conducted safely and controlled, minimizing the risks to your infrastructure and data. It is essential that all stakeholders participate in developing this document and that it is reviewed and signed off on by all parties before testing begins. This will help us to maintain a clear and open communication channel throughout the testing process and ensure that everyone is on the same page regarding the objectives and expectations of the testing. A snippet from our Rules of Engagement agreement is attached below:

Figure 4: Rules of Engagement Document



Technical Test Components

Network Scanning

This assessment does include attempts to scan the network within the limitations of the scope. This includes port scanning, protocol scanning, and vulnerability scanning of all agreed targets within scope.

Penetration Testing

This assessment does include attempts to test vulnerabilities discovered within the limitations of the scope. This includes running vulnerabilities against [redacted] infrastructure to eliminate the possibility of false positives during the scanning phase.

Data Handling

The ACS VAPT Team shall abide by all agreements governing the dissemination and protection of [redacted]. Furthermore, the ACS VAPT Team shall adhere to the following requirements:

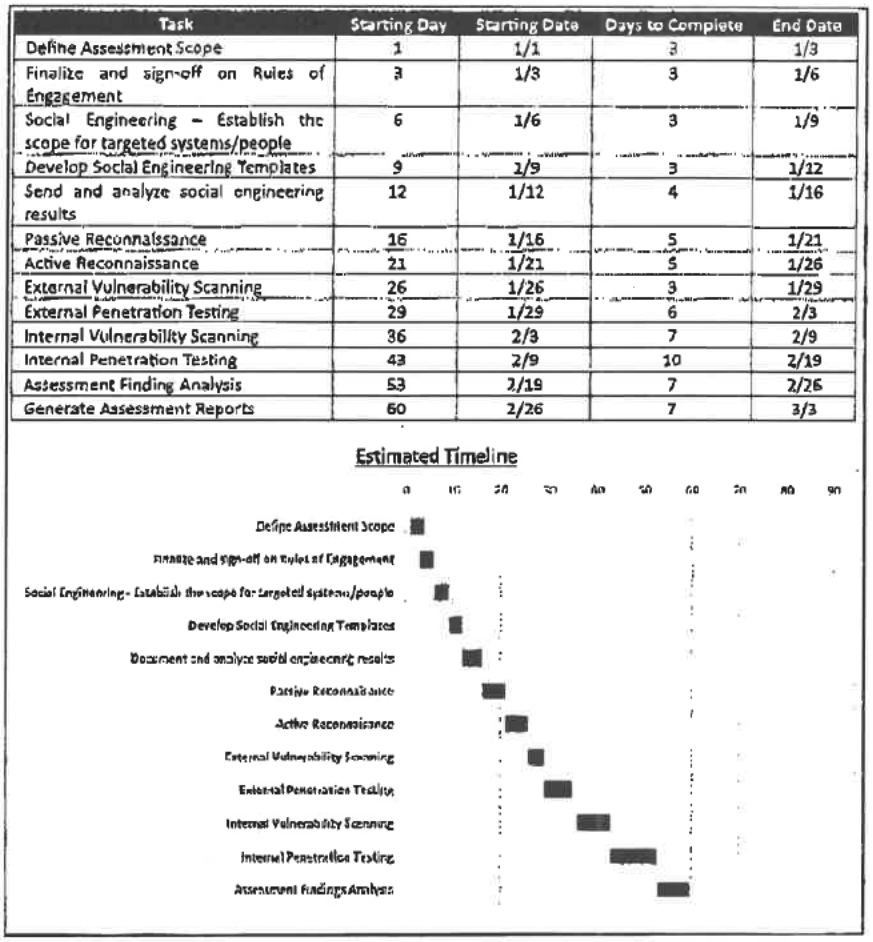
1. Draft and final project deliverables will be peer-reviewed by the ACS VAPT Team and transmitted to [redacted].
2. Working documents (e.g., diagrams, configurations, etc.) may be communicated by appropriate parties, with the ACS VAPT Team and [redacted] Team on the copy.
3. Each member of the ACS VAPT Team will use testing laptops and removable media

Throughout the engagement, the Alliant project team will deliver periodic status updates through your team's preferred communication method and regular project status emails.

At Alliant, we believe that effective project management is critical to the success of any organization. That's why we've made it our mission to provide exceptional project management services to businesses of all sizes and industries. Our project manager will provide regular updates on any developments, answer questions, and address concerns throughout the process. A project management runbook is attached in *Appendix A*.

Another way we ensure effective project management is by establishing a clear project timeline. We will establish a clear project timeline at the kick-off meeting, including specific delivery dates for each milestone. Below, we have provided a sample timeline for a penetration test for your reference.

Figure 5: Sample Timeline



Task	Starting Day	Starting Date	Days to Complete	End Date
Define Assessment Scope	1	1/1	3	1/3
Finalize and sign-off on Rules of Engagement	3	1/3	3	1/6
Social Engineering – Establish the scope for targeted systems/people	6	1/6	3	1/9
Develop Social Engineering Templates	9	1/9	3	1/12
Send and analyze social engineering results	12	1/12	4	1/16
Passive Reconnaissance	16	1/16	5	1/21
Active Reconnaissance	21	1/21	5	1/26
External Vulnerability Scanning	26	1/26	3	1/29
External Penetration Testing	29	1/29	6	2/3
Internal Vulnerability Scanning	36	2/3	7	2/9
Internal Penetration Testing	43	2/9	10	2/19
Assessment Finding Analysis	53	2/19	7	2/26
Generate Assessment Reports	60	2/26	7	3/3

Estimated Timeline
0
10
20
30
40
50
60
70
80
90
Define Assessment Scope
Finalize and sign-off on Rules of Engagement
Social Engineering - Establish the scope for targeted systems/people
Develop Social Engineering Templates
Document and analyze social engineering results
Passive Reconnaissance
Active Reconnaissance
External Vulnerability Scanning
External Penetration Testing
Internal Vulnerability Scanning
Internal Penetration Testing
Assessment Findings Analysis

Phase 2: Reconnaissance

Reconnaissance is the action taken to assess an organization's security strategy. The objective of this phase is to gather intelligence about the target network's internal systems and vulnerabilities in order to identify potential weaknesses and devise an effective penetration testing strategy.

Alliant employs various techniques to achieve its goals, including Infra Assessment and Scoping, External/Internal Scanning, Network Enumeration, OSINT, Dark web recon, banner grabbing, and OS fingerprinting. These methods assist in identifying potential entry points and assess the target system's security posture.

By utilizing automated tools, Alliant can identify and report potential security vulnerabilities in networks, hardware, software, and systems. This helps map the attack surface, discover vulnerabilities, and assess the target's security posture, allowing for a comprehensive understanding of the target environment and identification of potential weaknesses.

The reconnaissance phase of penetration testing is crucial for understanding the target's architecture, potential vulnerabilities, and attack surface. It aims to gather as much information as possible about the target system or network before launching any attacks.

During the reconnaissance phase, Alliant will gather information about the domain ownership, IP ranges, network structure, and potential vulnerabilities. This includes using OSINT gathering, constructing custom password lists, detailed DNS lookups, and collecting data from accessible network resources. Publicly available documents will be analyzed for metadata as well.

Using information gathered about the target network and its systems, we will identify vulnerabilities that can be exploited to gain unauthorized access to the network. To achieve this, several steps can be taken, including identifying software versions and configurations, anti-malware, firewall, and IDS products on the system, gathering information about the network, and verifying the ability to execute scripts or third-party programs. It is important to note that all testing should be conducted with the permission and knowledge of the client, and appropriate legal agreements should be in place before conducting any testing.

Phase 3: Mapping

During the mapping phase, our primary focus is to understand the network's architecture and topology. The objective of this phase is to identify all accessible systems, services, and potential entry points using a combination of automated tools and manual techniques for network mapping. By creating a comprehensive map of the target network's structure, we can identify potential attack vectors and entry points.

To achieve this, our team at Alliant uses various tools and techniques to map the network. Automated tools are used to quickly identify open ports, active services, and running applications. Manual techniques are also used to validate the automated tool's results and identify any potential blind spots.

The objective of this phase is to create an accurate and up-to-date map of the target network's structure. This map helps us identify potential entry points and attack vectors, which are then prioritized based on their criticality and potential impact. This comprehensive understanding of the target environment helps us design an effective penetration testing strategy and plan for subsequent phases.

During the mapping phase of a penetration test, Alliant will conduct a thorough analysis of the target systems and networks to identify potential vulnerabilities and attack vectors. This will involve the use of various tools and techniques to scan for open ports, identify the underlying operating system and software, and map out the network topology.

For example, Alliant may use ICMP sweeps, traceroutes, and port scanning to identify hosts and services on the network, as well as OS and version scanning to determine the software and their versions. Additionally, Alliant may conduct SSL/TLS analysis, virtual hosting and load balancer analysis, and web application spidering to identify vulnerabilities and attack vectors in web applications and services.

The goal of the mapping phase is to gather as much information as possible about the target systems and networks so that Alliant can identify the most effective attack vectors for exploiting any vulnerabilities that may be present. This information will be used to develop a comprehensive plan of attack for the Exploitation phase of the penetration test. By conducting a thorough network mapping exercise, our team can also provide valuable insights to our clients on how to secure their network architecture and topology against potential attacks.

Phase 4: Discovery

During the Discovery phase, our focus is on gathering information about the target organization by collecting intelligence about the target environment's infrastructure, applications, and potential vulnerabilities to inform subsequent attack strategies.

The methodology for gathering information about a target environment includes both passive and active reconnaissance techniques. Passive reconnaissance involves collecting publicly available information, such as domain names and employee details, while active reconnaissance involves probing for open ports and services. To aid in this process, various tools are utilized, including OSINT (Open Source Intelligence) tools, search engines, and network scanning tools. The objective of this reconnaissance is to gather intelligence about the target environment's infrastructure, applications, and potential vulnerabilities. This information is then used to inform subsequent attack strategies.

Alliant also enumerates live or accessible nodes using port scanning, system service identification, remote operating system fingerprint, firewall enumeration, and intrusion detection evasion. Banner grabbing and OS fingerprinting are also performed on targeted systems to remove false positives.

The Discovery phase is essential for identifying potential entry points and assessing the target system's security posture. By gathering intelligence about the target environment, we can identify potential weaknesses and devise an effective penetration testing strategy. It's important to note that all testing should be conducted with the permission and knowledge of the client, and appropriate legal agreements should be in place before conducting any testing.

During the discovery phase, we will use tools such as Nessus or Burp Suite to identify vulnerabilities in the target network or system. We'll also connect and interact with services to uncover information and validate usernames/emails using tools like Metasploit or manual enumeration techniques. Our focus will be on identifying web application-specific vulnerabilities, authentication/authorization issues/bypasses, and possible vulnerabilities affecting the provided host. Additionally, we'll enumerate services on APs, Bluetooth devices, and other RF devices to disclose any misconfigurations that may be present, helping us to identify potential attack vectors and vulnerabilities that can be exploited in the later stages of the test.

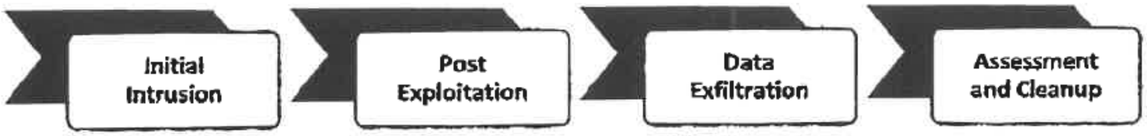
Phase 5: Exploitation

Ensuring the security of your system requires developing a comprehensive threat model. This involves thoroughly analyzing the system's assets, business processes, and human factors to identify potential threat vectors and weak points, considering the attacker's perspective so that we work in as realistic a model as possible. Our security assessment process is extremely meticulous and thorough. We take every possible measure to ensure that we simulate the actions of highly motivated bad actors who may try to gain access to your environment.

After gathering all the necessary data, we can commence the Exploitation phase. We will utilize various manual and automated tools and techniques to identify and exploit the vulnerabilities discovered in the vulnerability scan. We aim to thoroughly test the system's security and address any shortcomings before malicious actors can exploit them. It is essential to understand that this is not an exhaustive process. This is simply a pass/fail scenario. Once a vulnerability is found, we consider the environment failed.

Our four steps in this phase are intrusion, exploitation, exfiltration, exfiltration, and clean-up. Each step is planned and executed precisely to identify potential vulnerabilities in your security system.

Figure 6: Four Tasks in Penetration Testing



<u>Task 1: Initial Intrusion</u>

During the Initial Intrusion, we will leverage multiple publicly available exploit proof of concepts and payload techniques to gain the initial foothold. Some of these tools/techniques are:

- PowerShell DNS Delivery with PowerDNS.
- SharpShooter Payload Generation Framework.
- Responder.
- Gophish.
- BeEF.

- Phishing.
- Kerberos Domain Username Enumeration.
- SMB Password Guessing.
- Low Privilege Active Directory Enumeration from a non-domain Joined Host.

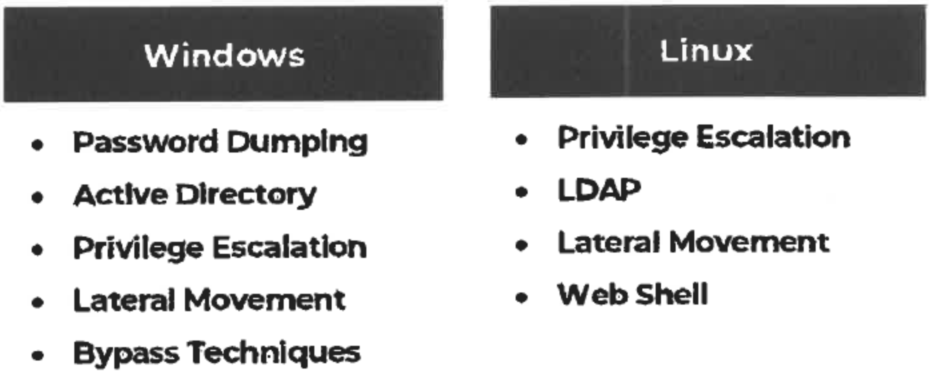
Task 2: Post-Exploitation

Post-Exploitation is done after a successful exploit or brute force attack. The Heavy load brute force or automated attacks will only be performed with prior approval by the Lottery obtained during the *Project Kick-Off.* It has two stages: maintaining access and information gathering.

- Maintaining access is crucial for continued remote access to the target system.
- Information gathering involves collecting data from the target system to refine the attack strategy and launch further attacks.

Post-Exploitation tools include command-line, network, password-cracking, and vulnerability scanners. The engagement's rules may prohibit post-exploitation techniques depending on infrastructure health or data sensitivity. There are specific methods for both Windows and Linux operating systems, as shown in the figure below.

Figure 7: Methods for Windows and Linux OS



Windows

- **Password Dumping**
- **Active Directory**
- **Privilege Escalation**
- **Lateral Movement**
- **Bypass Techniques**

Linux

- **Privilege Escalation**
- **LDAP**
- **Lateral Movement**
- **Web Shell**

Task 3: Data Exfiltration

Depending on requirements established with the organization during the kick-off, we can exfiltrate data or provide evidence to the client that data can be extracted. Our methods include DNS data exfiltration, DNS tunneling, SG1 encryption, DNSExfiltrator, DET data exfiltration toolkit, data exfiltration via formula injection, and out-of-band exploitation. We will not use any production data for this testing; instead, we will generate test data or files to document any attempts to extract data.

Figure 8: Use of Advanced Tools

Alliant Utilizes the Most Advanced Tools

Our team of experts will utilize the latest advanced tools to conduct comprehensive and detailed investigations. We regularly review and update our toolset to ensure it incorpo rates the latest technology available.

How We Do It

At Alliant, we use a range of hardware, operating systems, and applications during our assessments.

We initially follow the Grey Box Offender Model, based on the OWASP Web Security Testing Guide and NIST 800-115 methodology.

We rely on standard practices such as OWASP TOP10 and NIST CVSS for threat classification.

Task 4: Assessment and Testing Cleanup

After conducting Penetration Testing activities in your environment, our consultants will remove any tooling or infrastructure previously deployed. The tools used in the penetration test are designed to exploit system vulnerabilities for unauthorized access. Therefore, it is imperative to remove these tools to ensure system integrity and security. Leaving such tools in place that expose any potential vulnerabilities or attack vectors that will further expose an organization to risk. By documenting each step, we can ensure we clean up all accounts and tooling deployed for testing. As part of our customized approach, we thoroughly document all our considerations and actions. This documentation is a detailed record of our activities during the testing and ensures a thorough clean-up at the end of the engagement.

Phase 6: Analysis

Penetration testing, also known as pen testing or ethical hacking, is a crucial step in securing networks. It involves attempting to exploit vulnerabilities in a system to identify potential entry points for hackers. Once the testing is complete, the next crucial step is analyzing the results.

The primary goal of a penetration test is to identify weaknesses in a system that attackers could exploit. Organizations can safeguard their sensitive data and systems from cyber-attacks by detecting and addressing these vulnerabilities before malicious actors exploit them.

Penetration tests generate two main types of results: vulnerabilities and exploitation. Vulnerabilities refer to the specific weaknesses detected during the test, such as outdated software or misconfigured settings. Exploitation refers to successful attempts to access a system through the identified vulnerabilities.

Analyzing vulnerabilities is a vital step in comprehending the penetration test results. This involves categorizing each vulnerability based on its severity, impact, and likelihood of exploitation. Prioritizing remediation is crucial to tackle the most critical vulnerabilities and minimize exposure to potential attacks.

Analyzing the results of multiple penetration tests over some time can help identify patterns and recurring vulnerabilities. This can be useful in identifying areas of the system that require more attention and resources for better protection against cyber-attacks.

After analyzing the results of a penetration test, it is important to communicate the findings to relevant stakeholders within the organization. A detailed report outlining all vulnerabilities detected, their severity level, and remediation recommendations should be provided. This helps ensure that necessary actions are taken to address the identified vulnerabilities.

Phase 7: Reporting

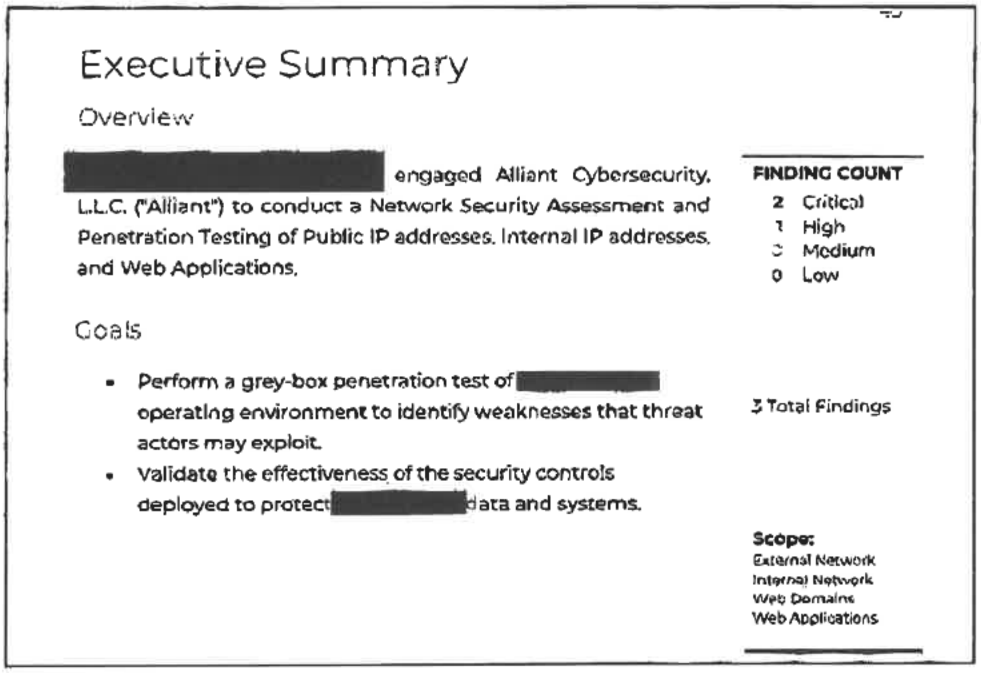
Reporting Overview

The report will consist of all the essential (Critical, High, Medium, Low) findings during the entire assessment and will include asset details, vulnerability details, risk scores, business impacts, and recommendations. The report will be based on NIST 800, OWASP Top 10 2021, and the ISO 27001 framework. Alliant will generate a report that includes a detailed description of the security risks found, their potential impact on the organization's systems, and recommendations for remediation. The reports should also provide a detailed explanation accompanied by images of how each security vulnerability was identified, with any privacy data that includes sensitive information, such as passwords or social security numbers, redacted from the reports. All reports and findings will be submitted to the organization electronically.

Executive Summary Report

The Executive Summary report will provide a comprehensive overview of the project's scope, approach, findings, and recommendations for detailed review by relevant stakeholders, presenting a summary of the project to senior management in a format that is easy to understand and useful for decision-making. The report will convey information clearly and concisely, ensuring the project and recommendations are entirely understandable. The content will include assessing and grading the current state and recommendations for an improved security posture.

Figure 9: Executive Summary from a Sample Report



Executive Summary

Overview

[redacted] engaged Alliant Cybersecurity, L.L.C. ("Alliant") to conduct a Network Security Assessment and Penetration Testing of Public IP addresses, Internal IP addresses, and Web Applications.

FINDING COUNT

2	Critical
1	High
0	Medium
0	Low

Goals

- Perform a grey-box penetration test of [redacted] operating environment to identify weaknesses that threat actors may exploit.
- Validate the effectiveness of the security controls deployed to protect [redacted] data and systems.

3 Total Findings

Scope:
External Network
Internal Network
Web Domains
Web Applications

Detailed Technical Report

The client's technical staff will receive a comprehensive report identifying strengths, security vulnerabilities, and weaknesses. Each vulnerability or weakness is assigned a risk rating based on its severity to the organization, with detailed exhibits included to provide additional context. The report also contains technical remediation steps that can be taken to address any issues and improve overall security. This vital resource will assist your technical staff in ensuring that their systems and data are secure and safe.

In addition, the report will identify the current state of the security posture, including coding standards and other security practices. Alliant will analyze and identify inefficient and suboptimal design/configuration areas, contrasting industry and vendor best practices and identifying potential threats. Based on these findings, Alliant will provide design and development optimization recommendations, application code reviews, vulnerability identification, and detailed tactical and strategic next steps. A detailed sample report has been attached in *Appendix B*.

References

Alliant has cemented its position as a leader in the cybersecurity realm, particularly in the domain of Penetration Testing. With over 22 years of dedicated service, our expertise has been honed through hands-on experience across a wide range of industries and client engagements. We have had the privilege of partnering with hundreds of clients and have conducted over 70 penetration tests, including physical security assessments, external and internal network testing, application assessments, social engineering tests, and wireless testing in just the past 4 years, offering our clients deep insights into their security posture and providing tailored solutions that fortify their defenses against evolving cyber threats.

Reference #1 – Enterprise Community Partners

Contact Name:	Craig Sweet
Contact Information:	csweet@enterprisecommunity.com

Services Provided:

Alliant worked with Enterprise Community Partners for four years and utilized advanced techniques and tools to conduct comprehensive penetration testing that emulated the tactics of potential attackers. These proactive assessments aimed to uncover system vulnerabilities before they could be exploited, providing valuable insights to strengthen the security posture of our clients.

Reference #2 – South Central Regional Medical

Contact Name:	Ralph Heath, IT Director
Contact Information:	rheath@scrm.com

Services Provided:

Alliant performed a HIPAA Risk Assessment and Penetration Test for South Central Regional Medical to identify and evaluate cybersecurity risks and vulnerabilities. We reported on our findings and provided prescriptive recommendations to improve their security posture and protect their business. During the process, our team assessed the security efficacy of the cyber risk management controls, policies, and procedures, as well as compliance with HIPAA Security Rule, external network, internal network, and web applications. We were able to identify compliance gaps, potential security exposures, and gaps in business processes.

Reference #3 – Dillon Gage

Contact Name:	Stan Shepherd
Contact Information:	(404) 668-7793, sshepherd@dillongage.com

Services Provided:

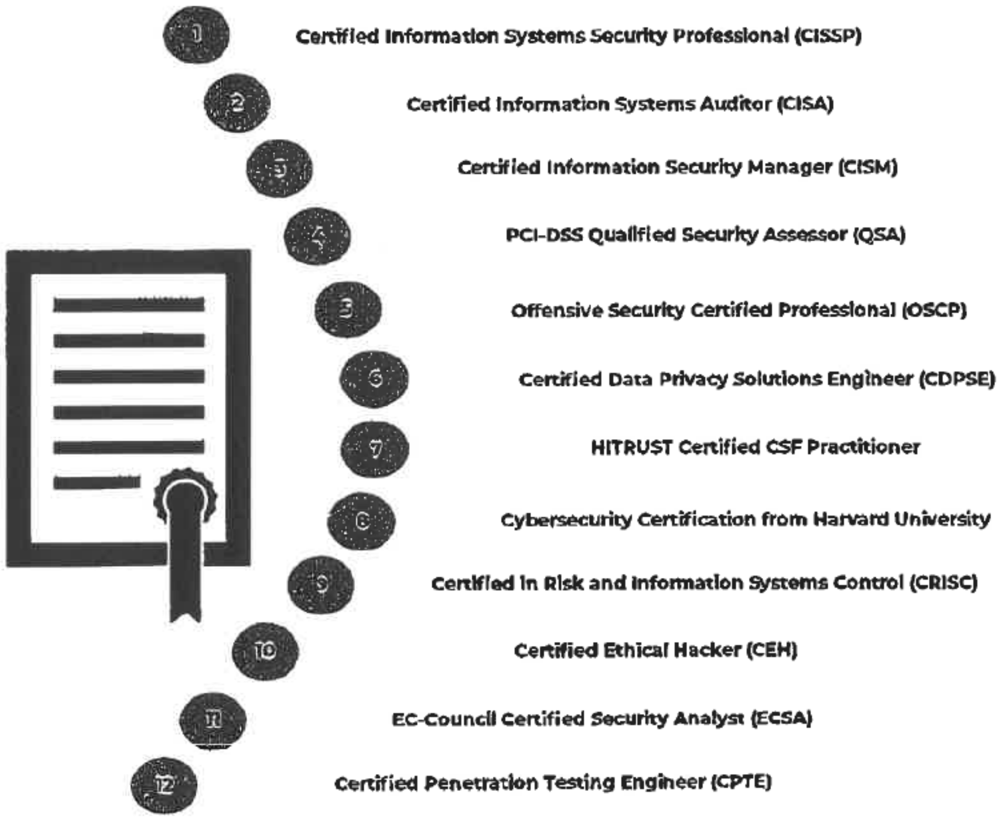
Alliant has been working with Dillon Gage for the past year, employing advanced tools and methodologies to conduct thorough penetration tests that mimic the strategies of potential attackers. These proactive assessments are aimed at identifying system vulnerabilities before they can be exploited, providing actionable intelligence for strengthening our clients' security posture.

During the penetration testing procedure, we conduct a thorough assessment of the client's network, web interfaces, applications, and other vulnerable areas to detect and expose any security flaws. The assessment results are then compiled into a detailed report, providing a comprehensive overview of the vulnerabilities identified and recommendations for remediation. Alliant's expertise in this area ensures that our clients can maintain a robust and secure IT infrastructure, protecting them against various cyber threats.

Key Personnel

We are thrilled to have the opportunity to partner with the organization to provide network penetration testing and cybersecurity assessments. Our team of highly skilled professionals brings decades of experience with Fortune 1000 companies, government entities, small to medium-sized businesses, and more in various industries. Our expertise and our constant drive to do better for our clients is what sets us apart, and we keep ourselves up to date with certifications such as:

Figure 10: Our Team Certification



1. **Certified Information Systems Security Professional (CISSP)**
2. **Certified Information Systems Auditor (CISA)**
3. **Certified Information Security Manager (CISM)**
4. **PCI-DSS Qualified Security Assessor (QSA)**
5. **Offensive Security Certified Professional (OSCP)**
6. **Certified Data Privacy Solutions Engineer (CDPSE)**
7. **HITRUST Certified CSF Practitioner**
8. **Cybersecurity Certification from Harvard University**
9. **Certified in Risk and Information Systems Control (CRISC)**
10. **Certified Ethical Hacker (CEH)**
11. **EC-Council Certified Security Analyst (ECSA)**
12. **Certified Penetration Testing Engineer (CPTE)**

We believe that the success of any penetration testing project depends on the people involved, and we are proud to have a team of dedicated and experienced personnel who will be working to make our engagement a success. Our team members have a deep understanding of the latest trends and best practices in providing the services requested, and they are equipped to manage any challenges that may arise during the engagement. We are committed to providing the highest level of service to our clients, and we look forward to working with the Lottery to ensure the security of their infrastructure.

EXPERTISE

- Cybersecurity Compliance Advisory
- Business Process and Technology Integration
- Strategic Planning
- P&L Management
- Digital Transformation
- Governance, Risk, & Compliance
- Business Continuity Planning and Advisory
- Leadership and Team Management
- Customer Relationship Management
- Corporate Social Responsibility
- Corporate Governance and Ethics

RIZWAN VIRANI

Principal, Chief Executive Officer

Our team is led by Rizwan Virani, who is responsible for creating customer experiences that surpass those of our competitors. He achieves this by utilizing data-driven insights to make informed decisions, and by collaborating closely with clients to establish key performance indicators (KPIs) that measure the success of our engagements. By continuously monitoring these KPIs and gathering customer feedback, he ensures that Alliant is meeting and exceeding customers' expectations. In addition, Rizwan is also responsible for negotiating and signing contracts, allocating internal resources to complete projects, and removing any obstacles that may arise.

EXPERIENCE

- Oversees the firm's enterprise risk management, cybersecurity, and privacy operations.
- Prepared both private and public organizations for information security and data privacy
- Provides thought leadership in the technology and security industry.
- Serves as Virtual CISO for several municipalities and other government agencies.
- Featured in several industry publications such as SC Magazine, Security Magazine, Help Net Security, etc.
- Mentors talented security professionals to contribute to the cybersecurity and technology industries and ecosystem.
- Disaster recovery planning and implementation.
- Leads strategic plans for the practice.

STEVEN HUNTER

Chief Technology Officer

EXPERTISE

- Information Technology Advisory & Implementation
- Cybersecurity Program Management
- Cybersecurity Compliance Advisory
- Identity & Access Management
- Cloud Security Management
- Risk Assessment/Management
- Governance, Risk Management, and Compliance (GRC)
- Business Continuity Planning and Implementation
- Digital Transformation

PROJECT ROLE

Steven Hunter is the Chief Technical Officer responsible for identifying cyber risks, developing cybersecurity strategies, and protecting technology assets from potential threats. He ensures that technology decisions align with business objectives and manages tech teams by providing them with the skills and resources necessary to implement digital transformation strategies. Steven also manages relationships with strategic vendors and technology partners and sets goals and KPIs based on customer input. He ensures that milestones and timelines are met to achieve successful outcomes.

EXPERIENCE

- Recognized in 2021 and 2022 as one of the 100 Best Digital Leaders in the Nation
- Provides thought leadership across informational technology domains
- Internationally published articles and discussions on information technology on various platforms and forums
- Created and delivered customized, innovative solutions for many clients and industries with Fortune 1000 companies
- Served on the Advisory Boards of Hewlett Packard and The Texas CIO Council
- Serves as a Board Member for Compudopt
- Atlas Scholar Mentor providing STEM Leadership to Houston Area Students

EXPERTISE

- Security Operations Center Management
- Risk Assessment/Management
- Governance, Risk, & Compliance
- Incident Response Management
- Identity & Access Management
- Cybersecurity Advisory & Implementation
- Cloud Security Management
- Digital Transformation
- Cybersecurity Program Management
- Cloud Infrastructure Architect

SOY JOSEPH

Director of Security Operations

Soy is a highly skilled professional responsible for ensuring that all cybersecurity measures comply with statutory and regulatory requirements related to information access, security, and privacy. In this capacity, he meticulously reviews alerts, alarms, dashboards, and reports to determine the relevance and urgency of cybersecurity threats, vulnerabilities, and incidents. To ensure a timely and accurate response to alerts, Soy implements industry-standard procedures and directs appropriate threat escalation responses, preparing clear and concise communication during major incidents. He has defined protocols and developed 'playbooks' for operational response to cyber threats, and he leads SOC staff during incident response actions. Soy is known for his exceptional ability to manage high-pressure situations with critical stakeholders, demonstrating the strong analytical skills needed to problem-solve and manage crises. He is a respected leader in his field and is committed to ensuring that his organization stays ahead of the curve in terms of cybersecurity best practices and measures.

EXPERIENCE

- Risk Assessment and Management for clients in multiple industries.
- Established and Managed Security Operations Center for clients in various domains.
- Implemented Identity and Access Management for enterprises across the nation.
- Thought leader and Advisor for Information Security.
- Technical Consulting on Authentication and Authorization strategy for on-premise and in the cloud.

EXPERTISE

- Governance, Risk Management, & Compliance (GRC)
- Cybersecurity Compliance Frameworks such as:
  - CIS
  - CSA
  - CMMC 2.0
  - CSF
  - ISO
  - NIST
  - PCI-DSS
  - HIPAA
- Information Security
- Systems Administration
- Network Security

ROY BLOOD

Senior Cybersecurity Consultant

Roy is a seasoned professional who performs security and risk assessments in a fast-paced environment. He provides timely and practical recommendations to mitigate the identified risks while adhering to industry standards such as ISO (number_1)/2, NIST, CIS, PCIDSS, SWIFT CSP, regulatory requirements like BSP circulars, and best practices. Additionally, Roy is responsible for performing maturity assessments in the fields of cyber security and information technology. He participates in discovery workshops with other consultants and key stakeholders from both the IT and other business units. Roy also presents project proposals to client project teams and other key stakeholders. As a facilitator, Roy conducts Security Training and Awareness programs for the organization, ensuring that employees are well-equipped to handle any security challenges.

EDUCATION AND EXPERIENCE

- Worked at Accenture as a Security Consulting Senior Manager for 7 years.
- Served as a HIPAA Information Security Officer at an e-commerce support company for 2 years.
- Led IT/IS team to apply NIST risk management framework and develop new systems from concept to Authority to Operate.
- Directed 14 Security Analysts to establish a Security Operations Center (SOC) for a United States DoD program.
- Established a Computer Security Incident Response Team (CSIRT) program and provided training and leadership.
- Managed corrective action and plan of action milestones in support of the site security plan.

EXPERTISE

- Vulnerability Management Program
- Cybersecurity Compliance Frameworks such as:
  - NIST
  - ISO (27001/27017/27018)
  - SOC2
  - GDPR
  - Secure Controls Framework
  - OWASP
  - FAIR Methodology
  - FedRamp,
  - CMMC
  - PCI
  - HIPAA
- Secure Cloud Architecture (AWS, GCP, and Azure), Windows/Mac/Linux Operating Systems

VISHAL REDDY

Senior Cybersecurity Consultant

Vishal is a cybersecurity consultant with practical experience across the Information Security field, including GRC, endpoint, network, data, product, and application security. He has a proven record of providing solutions for complex technical environments and organizational systems by leveraging key security frameworks and compliance standards. Highly skilled at developing comprehensive project plans and managing program resources to ensure projects are completed on time and within budgetary limits, Vishal has been a successful client resource as well as a valuable team member.

EXPERIENCE

- Conduct risk and compliance assessments for clients against industry frameworks.
- Analyze network architecture and digital infrastructure to identify opportunities for improvement.
- Provide recommendations on industry-specific regulatory compliance controls.
- Evaluate and develop security program policies and procedures.
- Conduct penetration testing of client operating environments to identify weaknesses and report on security control efficacy.
- Support clients in the implementation and maintenance of technology solutions.
- Bachelor of Science in Computer and Information Systems, Security and Information Assurance

ROHIT GHOSH

Senior Penetration Tester

Rohit is a Senior Penetration Tester, Certified Ethical Hacker (CEH) and Certified Hacking Forensic Investigator (CHFI) with years of experience in Vulnerability Assessments, Penetration Testing, Network Security, Data Recovery, Malware Analysis, Threat Prevention, and Cryptography.. His experience working with clients on their unique security challenges has allowed him to develop a results-driven approach to cybersecurity. Rohit has also been involved in developing and implementing comprehensive security policies and procedures for his clients, ensuring that they are compliant with industry regulations and standards.

EXPERIENCE

- Focus on identifying vulnerabilities of technology infrastructure for corporate clients. Experienced penetration tester and project manager tasked with evaluating security postures
- Provide incident response services, remediation plans, risk analysis, and recommendations.
- Advise on all aspects of security across multiple industries, primarily agriculture, manufacturing, construction, engineering, and government contracting.
- Conducted comprehensive penetration testing activities on complex enterprise systems, identifying and addressing critical vulnerabilities and providing actionable recommendations to enhance security posture.
- Developed and implemented custom methodologies and tools for performing penetration testing.

EXPERTISE

- Penetration Testing
- Network Security Assessment
- Web Application Security testing as per CERT-IN & OWASP
- Android Application Security testing
- Malware Analysis
- Reverse Engineering
- Government Risk and Compliance
- Vulnerability Management Program
- Security Operations

EXPERTISE

- NIST 800-171 controls and compliance
- ISO 27001 controls and compliance
- CMMC 2.0 controls and compliance
- CIS controls and compliance
- Project Management
- Governance, Risk Management, & Compliance (GRC)
- Cybersecurity Compliance and Audits

KARUNA SHIPPER

Project Manager

Karuna Shipper is an experienced cybersecurity professional specializing in governance, risk management, and compliance. She excels in assessing IT and cybersecurity controls against industry-specific frameworks such as NIST 800-171, ISO, CMMC 2.0, and CIS. With her expertise in conducting security assessments, risk assessments, and vulnerability assessments, Karuna can determine regulatory compliance standards for clients. She has a proven track record of working with current threat actor capabilities, tactics, and techniques using frameworks such as the MITRE ATT&CK Framework. As a Project Manager at Alliant Cybersecurity, Karuna is responsible for developing project plans and providing status presentations for client communication and service.

EXPERIENCE

- Karuna previously worked on a team sponsored by the Joint Chiefs of Staff J8 and the National Security Agency on an information campaign project
- She has advised numerous clients outside of projects on several major cybersecurity compliance frameworks.
- Karuna has managed projects for several service lines, such as Vulnerability Management, Penetration Tests, Cybersecurity Risk Reviews, and compliance readiness assessments.
- Bachelors of Arts and Sciences in International Affairs and Arabic

Appendix A: Project Management Runbook

To ensure the success of our engagement, we require a project management methodology that follows a systematic approach. This involves a few critical components: planning, organizing, risk assessment, communication, and reporting.

The project manager will play a key role in defining the scope of the test, the systems and networks to be tested, and the testing methodology to be employed. This information will then be captured in a project plan that outlines the project's objectives, timelines, resources, and expected outcomes. The project plan will also include a comprehensive project schedule, including tasks, milestones, and testing phases.

Effective communication and reporting are essential for successful project management in our engagement. The project manager will establish clear communication channels with all stakeholders, including the penetration testing team, IT team, and senior management. Furthermore, the project manager will establish a reporting framework outlining progress, issues, and risks. This framework will include regular progress reports, status updates, and a final report summarizing the test results and providing recommendations for remediation.

Table 1: Penetration Testing Project Management Runbook

Penetration Testing Project Management Runbook	
1. Understand Project Requirements.	a. Elicitation with stakeholders. b. Define penetration testing methodology (grey-box or black-box testing). c. Define penetration testing targets (e.g., full scope, targeted, etc.). d. Define project deadline.
2. Send Rules of Engagement	a. External scope. b. Internal scope. c. Web applications.
3. Receive Rules of Engagement.	
4. Validate Rules of Engagement and Scope.	
5. Create a Project Plan.	a. Assign project resources. b. Understand resource availability. c. Develop project milestones. d. Create a project timeline (based on resource availability and milestones).

Penetration Testing Project Management Runbook	
6. Create a communication plan.	a. Document project stakeholders. b. Identify communication methods. c. Define communication frequency. d. Define communication material (e.g., status emails, situation reports, etc.).
7. Conduct Discovery and Reconnaissance.	a. Open-Source Intelligence. b. Social engineering (if applicable) c. External discovery scans (if applicable). d. Web application discovery scans (if applicable). e. Internal discovery scans (if applicable). f. Plan exploit strategy.
8. Penetration Test	a. Threat modeling. b. External penetration test (if applicable). c. Web application penetration test (if applicable). d. Internal penetration test (if applicable). e. Penetration test post-mortem.
9. Reporting (Deliverables).	a. Penetration testing report. b. Executive summary.
10. Peer Review of Draft Deliverables.	
11. Quality assurance of draft deliverables.	
12. Schedule Executive Debrief.	
13. Conduct Executive Debrief.	a. Deliver final deliverables.

Appendix B: Sample Penetration Testing Report

For the Lottery, a report will be created that presents the findings and recommendations to the organization's stakeholders clearly and concisely. The report will begin by summarizing the project objectives and methodology for gathering and analyzing the data. The summary will be followed by the findings, highlighting key insights and trends from the analysis.

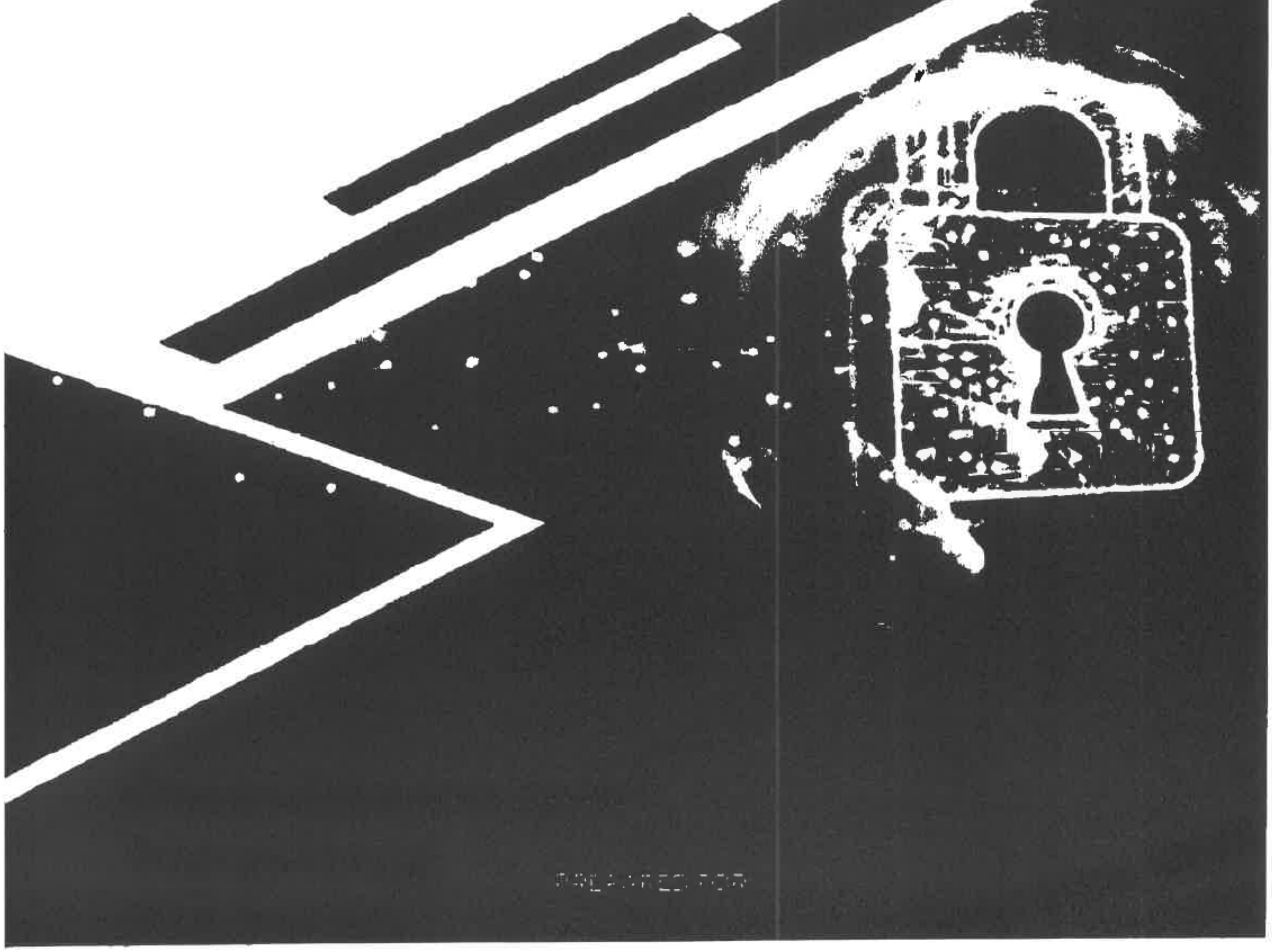
Following the presentation of the findings, the report will provide recommendations for the Lottery to consider. These recommendations will be based on the analysis and designed to help the State achieve its objectives. The report will conclude by outlining the next steps and offering the possibility of a full presentation to the selection committee, should they desire it. Overall, the report will be designed to be easily digestible and provide clear guidance to the organization's stakeholders on how to move forward.

A sample report is attached below. Please note that it is customized per our client's needs and has been redacted to maintain confidentiality. The report we prepare for you will be modified to fit the entity's requirements.

[remainder of the page intentionally left blank]

ALLIANT

Penetration Testing Report



PREPARED FOR

Executive Summary

Overview

[redacted] engaged Alliant Cybersecurity, L.L.C. ("Alliant") to conduct a Network Security Assessment and Penetration Testing of Public IP addresses, Internal IP addresses, and Web Applications.

FINDING COUNT

2	Critical
1	High
0	Medium
0	Low

Goals

- Perform a grey-box penetration test of [redacted] operating environment to identify weaknesses that threat actors may exploit.
- Validate the effectiveness of the security controls deployed to protect [redacted] data and systems.

3 Total Findings

Scope:
External Network
Internal Network
Web Domains
Web Applications

Summary

The operating environment is affected by multiple critical- and high-risk vulnerabilities that resulted in the compromise of several hosts and credentials.

A vulnerable version of OpenSSL was identified and leveraged to simulate a man-in-the-middle attack that would allow a threat actor to decrypt and thus collect and modify traffic between the[redacted]nd server.

Weak Intelligent Platform Management Interface (IPMI) configuration was identified and leveraged to compromise passwords and bypass authentication.

DATES

Kick Off
01/02/2023

Active Testing
01/05/2023 -
02/26/2023

Report Delivery
03/08/2023

Assessment Report

Identified Issues

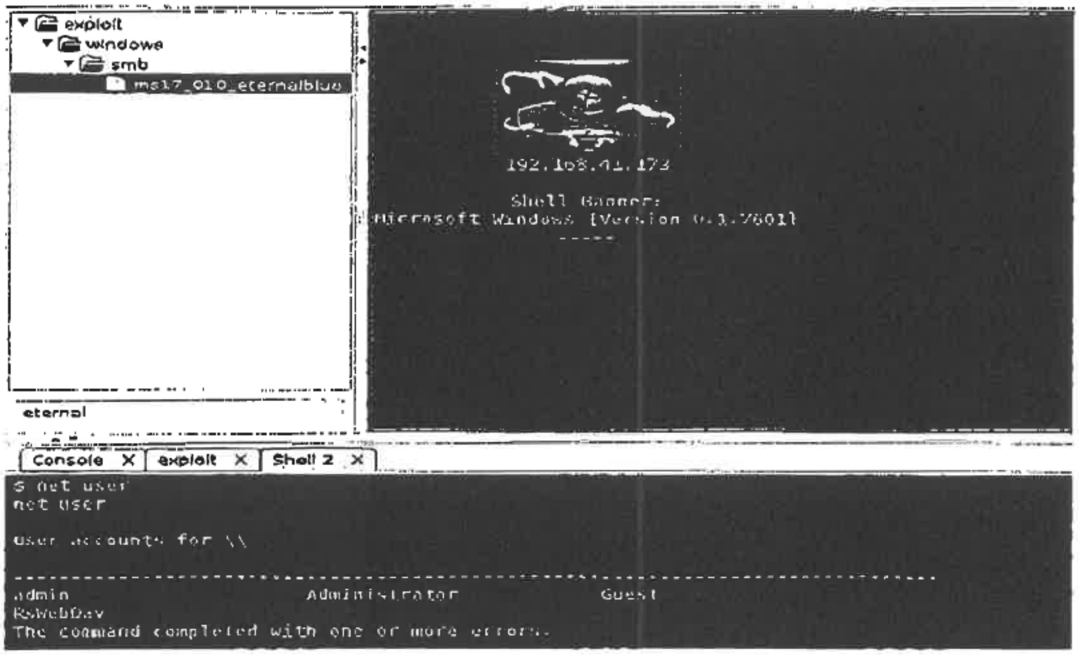
1. Remote Code Execution

Definition

Remote code execution (RCE) attacks occur when vulnerabilities are identified in targeted systems that allow threat actors to execute malicious code remotely, and systems and data may be compromised without the need for any physical access to the environment. RCE attacks allow threat actors a critical entry point into targeted environments.

Details

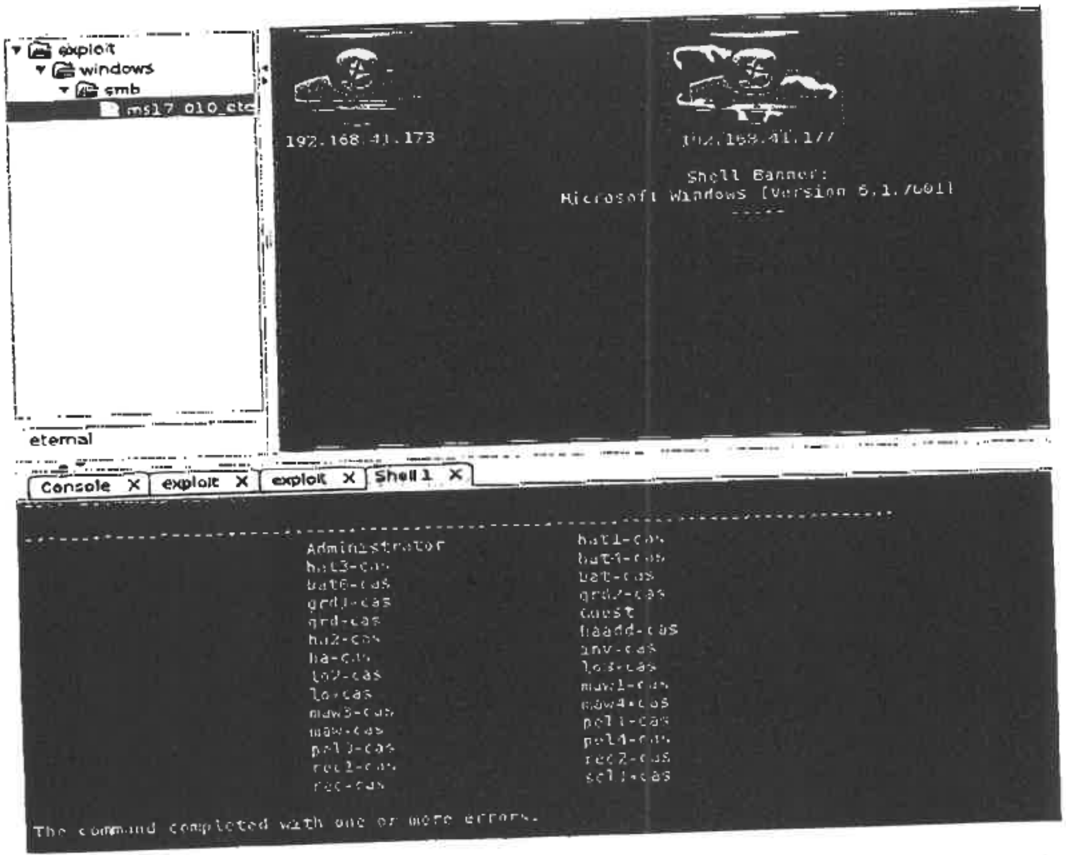
The assessment team identified a vulnerable version of Microsoft Server Message Block and successfully gained the ability to execute code on the affected host remotely. Once compromised, the affected server allowed our team to move laterally within the target environment and dump user credentials from another host.



```
192.168.41.173

Shell Banner:
Microsoft Windows [Version 6.1.7601]
-----
```

```
$ net user
net user

User accounts for \\

-------------------------------------------------------------------------------
admin                    Administrator            Guest
RsWebDav
The command completed with one or more errors.
```

Figure 1 depicts the successful compromise of the affected system



```
192.168.41.173                    192.168.41.177

                                   Shell Banner:
                         Microsoft Windows [Version 6.1.7601]
                                      -----
```

```
-------------------------------------------------------------------------------
                    Administrator            hat1-cas
                    hat3-cas                 hat4-cas
                    bat6-cas                 bat-cas
                    grd1-cas                 grd2-cas
                    grd-cas                  Guest
                    ha2-cas                  haadd-cas
                    ha-cas                   inv-cas
                    lo2-cas                  lo3-cas
                    lo-cas                   maw1-cas
                    maw3-cas                 maw4-cas
                    maw-cas                  pel1-cas
                    pel3-cas                 pel4-cas
                    rec1-cas                 rec2-cas
                    rec-cas                  sel1-cas

The command completed with one or more errors.
```

Figure 2 shows the assessment team successfully compromising another host

Affected Hosts

255.255.255.1
255.255.255.3

Recommendations

It is strongly recommended that [redacted] apply related patches provided by Microsoft that correct how SMB handles specially crafted requests.

Reference

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0146

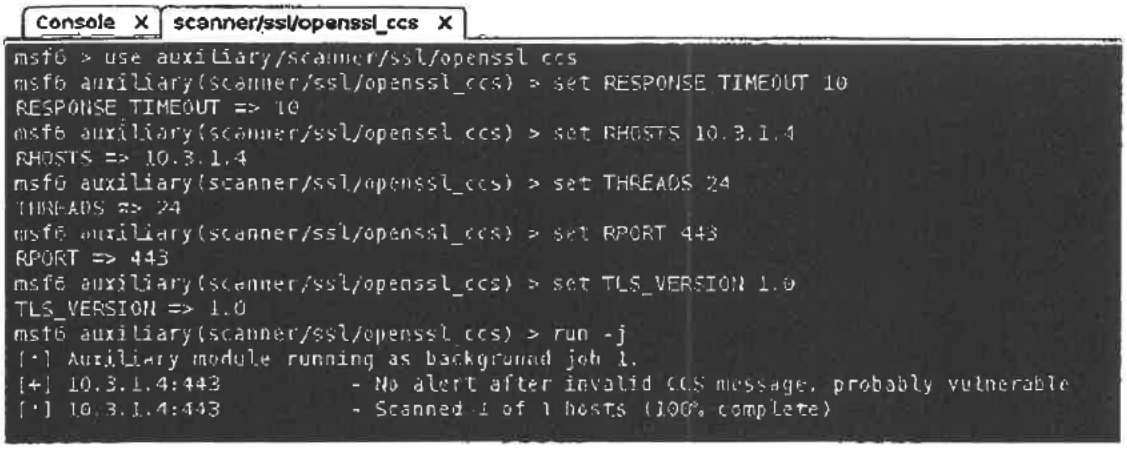
2. Man in the Middle (MITM)

Definition

Man-in-the-middle attacks allow threat actors to intercept the communications between two parties without being detected. Once a session is hijacked, threat actors can monitor all communications, collect data, and even modify packets to affect the integrity of any data shared within the compromised session.

Details

A vulnerable version of OpenSSL was identified and successfully leveraged by the assessment team to hijack a session and perform a Man-in-the-middle attack. The outdated version of OpenSSL does not properly process 'ChangeCipherSpec' messages and threat actors can trigger the use of a zero-length master key. The weak key allows for the easy hijacking of the resulting communication session.



```
msf6 > use auxiliary/scanner/ssl/openssl_ccs
msf6 auxiliary(scanner/ssl/openssl_ccs) > set RESPONSE_TIMEOUT 10
RESPONSE_TIMEOUT => 10
msf6 auxiliary(scanner/ssl/openssl_ccs) > set RHOSTS 10.3.1.4
RHOSTS => 10.3.1.4
msf6 auxiliary(scanner/ssl/openssl_ccs) > set THREADS 24
THREADS => 24
msf6 auxiliary(scanner/ssl/openssl_ccs) > set RPORT 443
RPORT => 443
msf6 auxiliary(scanner/ssl/openssl_ccs) > set TLS_VERSION 1.0
TLS_VERSION => 1.0
msf6 auxiliary(scanner/ssl/openssl_ccs) > run -j
[*] Auxiliary module running as background job 1.
[+] 10.3.1.4:443          - No alert after invalid CCS message, probably vulnerable
[*] 10.3.1.4:443          - Scanned 1 of 1 hosts (100% complete)
```

Figure 3 shows the successful hijacking of a communication session

Affected Hosts

[redacted]

Recommendation

REDACTED should immediately patch the affected versions of OpenSSL with the latest patches provided by the vendor.

Reference

https://access.redhat.com/security/cve/cve-2014-0224

3. Weak Intelligent Platform Management Interface (IPMI) Configuration

Definition

Intelligent Platform Management Interface (IPMI) provides IT personnel the ability to monitor and manage infrastructure remotely through an out of band interface. Weak IPMI configuration allows threat actors to compromise the confidentiality and integrity of affected hosts.

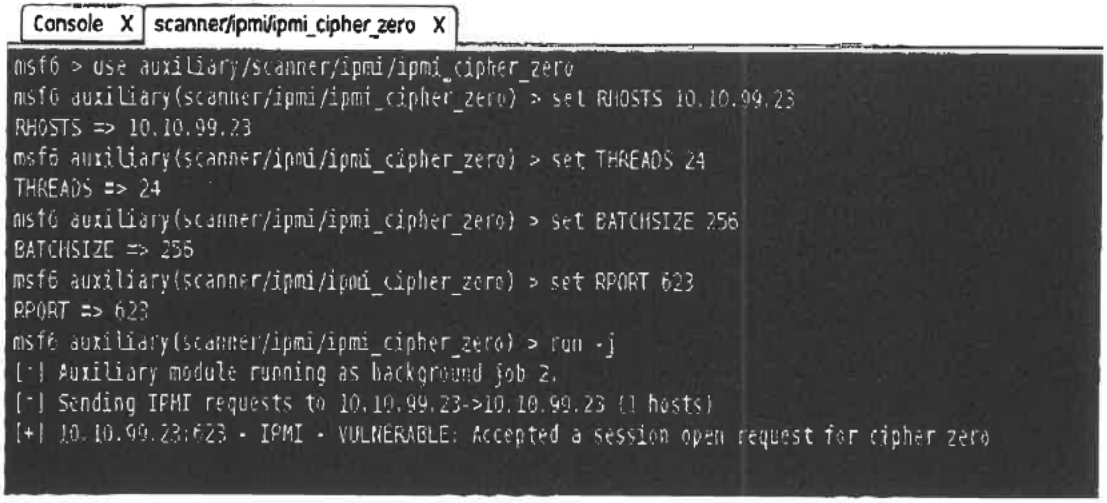
Details

The assessment team identified a weakness in the deployed IPMI configuration that allowed for both the disclosure of passwords and the bypassing of any authentication mechanisms. The assessment team was able to successfully obtain password hashes and gain access to the affected hosts. The IMPI configuration also has 'Cipher Suite Zero' enabled which permits administrator access without a password.

- Disabling IPMI over LAN
- Using strong and complex passwords to limit the ability of threat actors to compromise credentials
- Configuring Access Control both at the network level and system level to limit the exposure of the attack surface to potential threat actors

Reference

HP Support
IPMI v2.0 Password Hash disclosure
CVE-2013-4786



```
msf6 > use auxiliary/scanner/ipmi/ipmi_cipher_zero
msf6 auxiliary(scanner/ipmi/ipmi_cipher_zero) > set RHOSTS 10.10.99.23
RHOSTS => 10.10.99.23
msf6 auxiliary(scanner/ipmi/ipmi_cipher_zero) > set THREADS 24
THREADS => 24
msf6 auxiliary(scanner/ipmi/ipmi_cipher_zero) > set BATCHSIZE 256
BATCHSIZE => 256
msf6 auxiliary(scanner/ipmi/ipmi_cipher_zero) > set RPORT 623
RPORT => 623
msf6 auxiliary(scanner/ipmi/ipmi_cipher_zero) > run -j
[*] Auxiliary module running as background job 2.
[*] Sending IPMI requests to 10.10.99.23->10.10.99.23 (1 hosts)
[+] 10.10.99.23:623 - IPMI - VULNERABLE: Accepted a session open request for cipher zero
```

Figure 5 shows the successful authentication to the affected hosts

Affected Hosts

[redacted]

Recommendation

Workarounds need to be configured, as there are no patches to mitigate this vulnerability. REDACTED can deploy the following controls to secure access to IPMI:

EXHIBIT A - Pricing Page

Item #	Section	Description of Service	*Estimated Number of Assesments*	Unit Cost per Assesment & Reports	Extended Amount
1	4.1	External Network Penetration Testing	8	$ 93.03 -	$ 744.20 -
2	4.2	Website Penetration Testing	8	$ 2,261.36 -	$ 18,090.90 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 5,270.74 -	$ 42,165.90 -
4	4.4	Wireless Penetration Testing	8	$ 1,400 -	$ 11,200 -
				TOTAL BID AMOUNT	$ 72,201 -

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	Alliant Cybersecurity
Vendor Address:	3009 Post Oak Blvd, Suite 1500, Houston, TX 77056
Email Address:	rizwan.virani@alliantcybersecurity.com
Phone Number:	(713) 877-9600
Fax Number:	(713) 877-9657
Signature and Date:	Rizwan Virani 3/25/24