Yonkers Public Schools
Internal / External Penetration Test

Organization:	Yonkers Public Schools
Contact Person:	Chris Carvalho
Date:	December 12th, 2023
Email:	CCarvalho@YonkersPublicSchools.org

GSA contract #47QTCA22D0030

BMB Consulting LLC / XLAHEEJELCC3 / 890Z

CISA Assessment Evaluation and Standardization (AES) Certified

GSA Schedule - 54151HACS Highly Adaptive Cybersecurity Services (HACS) Include a wide range of fields such as the seven-step Risk Management Framework services, information assurance, virus detection, zero trust architecture, network management, situational awareness and incident response, secure web hosting, backups, security services, and Security Operations Center (SOC) services. HACS vendors are cataloged under five subcategories: High-Value Asset Assessments, Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, and Penetration Testing.

Executive Summary

BMB Consulting LLC ("BMB") shall provide an Internal / External Penetration Test ("Pen Test") for Yonkers Public Schools ("Client"). This service evaluates a hacker's capabilities to compromise external network devices, systems, and services.

The assessment's objective is to provide feedback to the Client concerning its ability to preserve the Confidentiality, Integrity, Availability, and Security of the information maintained by and used by its origination. BMB will test the security controls intended to secure sensitive data.

Services Overview

This project shall include multiple pen testers for approximately three months. BMB's certified professionals have the tools, knowledge, experience, and expertise to execute this Pen Test on client-designated devices. We will Perform this Pen Test exercise with the expertise to identify, understand, and evaluate potential risks to external IP addresses, portals, and systems.

After this project, BMB will provide a Pen Test report that will include data obtained from network resources or any information regarding the vulnerabilities, exploits, or access to sensitive data. The Pen Test report will include publicly available information found.

Engagement Schedule

Pen Tests take approximately three months to complete. BMB and the Client will jointly determine the start date for the engagement within 30 days of the contract signature. The deliverable is a detailed final Pen Test report, as described above. A Business Day is local Monday through Friday, 8:00 a.m. to 5:00 p.m., excluding BMB's official holidays.

Assumptions

BMB and the Client understand that unintentional service disruption may be possible during the project as possible service disruption and destructive probing will be performed during agreed-upon and approved time frames. Although reconnaissance and information-gathering processes are traditionally less disruptive than testing, disruptions can occur anytime. BMB is not responsible for interruptions of the network services while completing the task described in this proposal and services described herein and requires the Client to maintain up-to-date system backups and a tested disaster recovery plan in case of any unforeseen system disruptions. BMB will take every precaution to limit exposure to any system downtime for the Client.

BMB and the Client understand and agree that the services provided throughout this proposal are intended to improve the Client's overall security posture. During the Pen Test, BMB will make every effort to identify all risks, at the current point in time, by unauthorized or authorized parties that may affect the environment.

Engagement Deliverables

The Pen Test report will contain documented and detailed findings from performing this contracted service and provide objective recommendations to remedy identified and anticipated vulnerabilities.

Scope

BMB shall assess the Client's security posture and identify the applications, systems, and network vulnerabilities, gaps in IT security governance, assessment of patching methodologies, current network security capabilities, and potential existing security incidents. The Pen Test and reporting will be based on NIST 800-53 (Security and Privacy Controls for Information Systems and Organizations).

This assessment will include externally accessible systems, hosts, and applications in the Client's environment. It shall consider, at a minimum, all the following to be within the scope of work:

- Identifying application, system, and network vulnerabilities and assessing their patching methodologies.
- Limited to publicly accessible hosts residing in the Client network segments deemed part of the Client's IP block. This includes underlying Network Management and out-of-band zones and segments that provide network communications and services to publicly

accessible hosts. The private addresses or servers will also be in scope, but access will be through other means.

- Conducting vulnerability scanning and current patching methodology assessment for Client hosts and endpoints. Scans on servers will be performed outside of regular business hours, 6:00 p.m. to 7:00 a.m., or directed by the Client.
- Performing denial of service and potentially disrupting tests will occur during testing periods approved by both parties.
- Conducting Pen Tests for publicly accessible systems when initial vulnerability scanning identifies potential high-impact vulnerabilities.
- Conducting web application testing based on the current OWASP top 10 listings.
- If BMB testing comes across systems out of scope, the test will stop as the findings will be documented. At the time of the findings, BMB will notify the Client of the out-of-scope networks or resources.
- If the Pen Test gains access to a system, the testing should assess the attacker's ability to leverage the system to access other systems and networks.
- Web applications encountered will be tested against the technologies used. As requested, a username and password may be required to test a specific site further.
- Publicly available information or access data via the Client's IPs or sites will be discovered and used throughout the test. BMB will perform a security assessment against websites and review emails, passwords, and information on the dark web.
- BMB will review and recommend the Client incident management plan if any gaps in IT security governance are found.
- BMB will recommend best practices to secure the existing infrastructure if any vulnerabilities are found.
- Assessing existing security systems and components, including antivirus, firewalls, and network monitoring. BMB shall assess current network security capabilities and their ability to identify and potentially stop cyber-attacks, data loss, and misuse of IT resources. These network security resources include firewalls, Intrusion Prevention Systems, and endpoint security applications.
- If the Client encounters any alerts during the Pen Test, kindly document the alert and send it to BMB for review.

BMB is providing the Client with objectives and requirements for this contracted Pen Test. As part of this process, an initial discovery discussion was held to understand the environment. BMB's proposed services will evaluate the effectiveness of the Client network and application security controls and practices while evaluating risk and suggesting remediation advice for areas that require improvement. BMB brings a wealth of knowledge and experience to ensure the Client receives a holistic assessment that is thorough and, ultimately, beneficial.

BMB SOW includes the following ethical hacking verticals:

- Network Penetration Testing Internal & External
- Web Application Testing

External and Internal Penetration Testing Overview

Information security follows a continuous design, deployment, testing, and improvement cycle. Policies and guidelines, implementation processes and procedures, and testing form the basis for this process. While policies and procedures may be formalized and well-understood, process breakdowns or simple human error can lead to unknown vulnerabilities that can only be discovered through testing processes.

For information security, one of the best ways to accomplish these objectives is through a process referred to as penetration testing. A security professional employs tools and techniques real-world attackers use to test configurations and simulated steps. Leveraging their technical knowledge of architecture, operating systems, applications, and publicly available or well-known information, these experts can often crack systems and networks—revealing critical vulnerabilities within an infrastructure. BMB's experienced security team will utilize techniques and tools commonly used by attackers to exploit the in-scope Client systems. This process is known as penetration testing and goes beyond automated scanning and tools following an approach outlined in the Methodology.

Requirements and Objectives

In today's business environment, protecting information, complying with legal and regulatory requirements, and aligning with commonly accepted security best practices are integral to success and service delivery. The Client has requested a proposal from BMB to assess and document the Client's network security posture's strength versus external threats to the Client's IT environment.

Methodology

Penetration Testing follows a five-step methodology:

1. Reconnaissance
2. Scanning
3. Exploitation or Enumeration
4. Maintaining Access
5. Cleanup

Step One: Reconnaissance (Information Gathering): This phase uses public sources of information such as Google searching, public websites, OSINT and Blog communities, domain naming and registration information, and other information to determine as much information about potential targets as possible. This information is then integrated with any information provided by the Client to build as complete a picture as possible of the target systems and network.

Step Two: Scanning

Scanning is a deeper form of information gathering, using technical tools to find openings in the target and the systems in place. These openings include internet gateways, listening ports, vulnerability lists, and available systems. Vulnerability scanning is expected in this phase.

Step Three: Exploitation or Enumeration
During the enumeration phase, the tester actively tries to confirm or expand his information regarding the system. This can involve additional tools that actively attempt to map networks, systems, and configuration settings.

Once active and passive information gathering is complete. Testers begin to narrow in on potential attack paths. Testers gather additional detailed information about a specific target during steps one and two. This can include an operating system or software version, allowed encryption methods, and other specific information that identifies a weakness or vulnerability and selects the appropriate exploit technique to leverage that vulnerability. During testing, it may be sufficient to identify vulnerabilities and use a limited exploit to confirm their existence. However, whether for proof or confirmation, exploits will be leveraged to gain access and show system weaknesses. BMB follows an "Error on Caution" approach to testing. It will not conduct tests or exploits to purposely take down a system or cause operational harm to a system or data.

External penetration testing applies these techniques to Internet-facing systems, where external refers to tests performed outside the organization's infrastructure. These tests target the following types of systems and services:

- Firewalls
- External Routers
- Web Servers (typically at the operating system and web server levels. Dynamic web applications are penetration tested by a comprehensive web application penetration testing approach outside the scope of a standard external penetration test unless requested)
- Domain Naming Servers (DNS)
- Remote Access
- Email Systems (Not Office 365, Gmail)
- File Transfer Servers
- Switches
- Routers
- Directory Servers (Active Directory, LDAP, LDAPS)
- Core infrastructure services (DNS, DHCP, WINS)
- File and Print Sharing Services
- Database Servers
- Internal Client-Server Applications

Step Four: Maintaining Access
Maintaining access to a target machine is commonly done by installing backdoors and planting

rootkits. This is also known as creating persistence on a target device.

Step Five: Cleanup
Covering tracks is removing all evidence that an attack ever took place. This can involve editing logs, hiding files, and de-escalating custom-privileged accounts.

Penetration Test Deliverables

Activity or Focus	Scope Requirements
Penetration Testing	Reconnaissance, Enumeration, Exploitation & Remediation Recommendations • External testing of all External and Internal assets. • During the test, the Client may provide high-value targets on which BMB can place extra effort. • BMB will follow a risk-based approach to exploit systems suspected of containing high-value information and any "Targets of Opportunity" within the project timeline allotted.

Service Deliverables

BMB will provide the following deliverables as part of this project:

Activity or Focus	Scope Requirements
Penetration Testing	**Activities:** • Conduct an internal scan of the following devices and systems based on the 20,000 workstations; there are approximately 3,000 iPads and 4,000 Chromebooks, leaving approximately 11,000 laptops and desktops. There are approximately 1000 sensors and devices. The number of printers is not determined; however, 12,000 will be the number of quoted devices. • The exploitation attempt approach will follow a schedule confirmed with the Client before testing. The internal testing phase for information gathering of the devices could take three to 4 weeks to complete.

Activity or Focus	Scope Requirements
	• Upon completion of the information-gathering phase, the devices' analysis and verifying the results of each device then create a test plan for each device, technology, OS, or group of devices. • Any Critical findings are informally communicated within 24 hours of discovery. • Perform analysis and manual testing of the scan results to confirm scan results, eliminate false positives, and describe the business risk to the Client and recommended actions.

Service Deliverables

BMB will provide the following deliverables as part of this project:

Service Level	Service Deliverables
Report	After the assessment is complete, BMB will provide the Client with a formal report that contains: • An executive summary/overview of the results of the assessment • A findings matrix summarizing items that BMB feels pose a risk to the organization and risk ratings and remediation recommendations. • Appropriate technical discussion supporting findings from the assessment
Review	A formal conference call or onsite debriefing for Client management and appropriate staff outlining the project's significant findings and recommendations. BMB participants will also be able to have interim question-and-answer conversations with the assessors regarding their findings.

Project Timelines

Internal Milestones & Deliverables	Proposed Timeline
• Network Penetration Testing – Internal • Internal Gathering • Internal Validation • Web Apps Pen Testing	Begin based on Client authorization.

• Exploitation Testing • Exploit Validation		
	Phase 1 – Internal Penetration Test BMB will set specific assessment, testing & deliverable dates, review information on the infrastructure required for testing, and exchange contact information.	Week 1
	Phase 2 – Network Devices and Systems Scanning Perform scanning with several tools to validate the findings of the devices and systems. Verify all subnets are scanned with an NUC placed onsite by BMB.	Week 2 through Week 6
	Phase 3 – Manual Validation of Device & Systems Analyze a system to determine the technologies, ports and services, and OS and firmware versions. Create a map and attack plan for the testing phase.	Week 6 through Week 9
	Phase 4 – Testing of Device & Systems Create a strategic attack and testing plan for each device. Specific attacks and tests may be service-disrupting and must be scheduled with the Client. BMB will test each system with a found vulnerability.	Week 9 through Week 12
	Phase 5 – Report of Findings Create a strategic attack and testing plan for each device. Specific attacks and tests may be service-disrupting and must be scheduled with the Client. BMB will test each system with a found vulnerability.	Week 12 through Week 16

Rules of Engagement

BMB will perform a Penetration Test on the assets established or systems owned and operated by the Client.

The Client authorizes BMB to perform the tests on the following dates only, as given by the Client.

BMB and the Client will communicate via mobile phone numbers and email addresses to reach each other during the tests. Both parties guarantee that these numbers will, during the tests, only be used for communication with the other party.

The Client can request BMB to stop the tests promptly during the tests.

BMB guarantees that it will perform all tests responsibly and professionally. BMB will follow the sector's best practices and use its best endeavor to change or amend any applications, data, programs, or components of the Client's network or computer system (including hardware and

software).

BMB does not offer any implied or express guarantees. The results deem that the Client's network is secure from every form of attack. Security is an evolution of changes.

As a result, the Client guarantees that it has the legal right to subject the designated computer system to the security mentioned above Penetration Test. If it is not the computer system owner, it has obtained such a request from its legal owner.

The Client will not hold BMB liable for any indirect, punitive, special, incidental, or consequential damage (including but not limited to loss of business, revenue, profits, use, data, or another economic advantage); however, it arises, whether for breach or in tort, even if BMB has been previously advised of the possibility of such damage.

The Client is solely responsible for adequate protection and backup of data and equipment used to connect with the tests and will not claim BMB for lost data, re-run time, inaccurate output work delays, or lost profits from the tests.

BMB will not divulge any information disclosed between parties about the tests. All results are confidential and will be treated as such.

Confidential information can be used for the tests. Where disclosure to a third party is essential, the party wishing to disclose the information shall obtain prior written authorization from the other party.

All confidential material will be destroyed immediately after the tests. The information is not necessary for drafting the test reports. BMB will destroy any data related to the test thirty days after the report is delivered to the Client.

The Client should respond in a typical fashion to any detections or alerts generated during the tests. Conditions including firewall logs, IPS or IDS systems, AV alerts, etc., as it would do in an absolute security situation, not to distort the test results. However, the Client agrees not to notify the legal or public authorities of this penetration.

This agreement and appendixes constitute the entire agreement between parties related to the tests. No change, alterations, or modifications shall be valid unless in writing, dated, and signed by both parties.

Permission to Test (Required by Authorized Personnel)

Please sign below acknowledging that BMB has permission to test Client systems and does not hold BMB liable for unforeseen testing outcomes. This testing could lead to system instability. The tester will acknowledge all due care not to crash systems. Since testing can lead to instability, the Client shall not hold the tester liable for any system instability or crashes. Below

must be signed by an authorized C Level executive.

Pricing

Information Security Services	Flat Rates
Penetration Test Engagement (External)	$12,250.00
Penetration Test Engagement (Internal)	$42,700.00
Report Draft & Final	Included

Execution of Statement of Work

Company Name: Yonkers Public Schools
Address: One Larkin Center
City, State & Zip: Yonkers, NY 10701
Executed By:
Date:
PO Number (If Required):