NYS LOCAL GOVERNMENT VULNERABILITY SCANNING PROJECT

September 22, 2011

New York State Division of Homeland Security and Emergency Services

OCS

Office of Cyber Security

Executive Summary

BACKGROUND

The NYS Local Government Vulnerability Scanning Project was funded by a U.S. Department of Homeland Security State Homeland Security Program (SHSP) grant from FY 2007. The objective of the project was to perform vulnerability scans[1] of New York local governments' networks, compile scan results, and recommend mitigation methods, techniques, and procedures based on an analysis of the scan results. This effort was expected to result in a reduction of the cyber risk facing local governments.

The project consisted of network vulnerability assessments performed by the New York State Office of Cyber Security (OCS) using the QualysGuard scanning tool. The project focused on externally accessible computers and networks. While it is also important to identify and evaluate vulnerabilities in internal computers and networks, they were not within the scope of this project.

The assessments were designed to detect known vulnerabilities, as well as open ports[2] and services[3] on the participants' external networks. As the project progressed, OCS added web application scans to detect application-level vulnerabilities[4]. Both types of scans were conducted according to industry best practices. The scans were performed from February 2009 through June 2010. Results of the scans were reviewed and analyzed by a trained security analyst.

Initially the project focused on New York counties, cities, and towns, but expanded to include other local governments including police and fire departments, schools, and an airport. As a result, the final pool of participants represented a wide cross-section of local governments. Ultimately, the NYS Local Government Vulnerability Scanning Project provided a detailed view of the external security posture of 271 distinct local governments in New York.

FINDINGS

The scans resulted in the following findings:

- 2,889 confirmed vulnerabilities;
- 1,892 potential[5] vulnerabilities;

[1] A vulnerability scan is an effort to identify and prioritize weaknesses on target systems with the goal of assisting organizations by ultimately improving the security of their target systems. Vulnerability scans provide a "snapshot" of the security posture at a given point in time.

[2] A port is an application-specific or process-specific software construct serving as a communications endpoint.

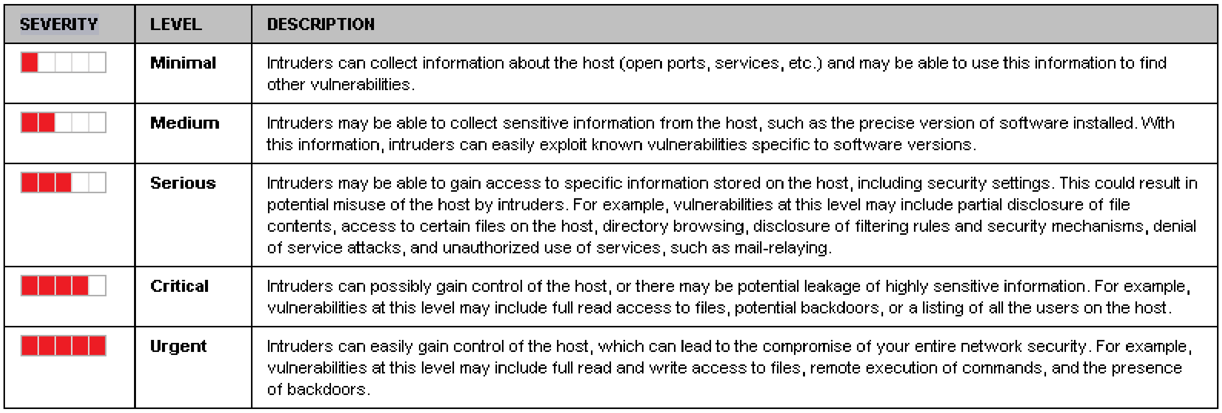
[3] Services are more commonly known for providing "business needs" such as email, web/Internet and remote access.

[4] For more information on application-level vulnerabilities see https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

[5] Potential vulnerabilities include vulnerabilities that cannot be fully confirmed. These vulnerabilities require further verification.

- an average of 6 total vulnerabilities per scanned host[6];
- 60 (2%) of the vulnerabilities were rated at a critical level (see chart below), meaning exploitation could result in complete system compromise;
- 44.8% of all hosts on participants' networks had a serious (level 3 or higher) vulnerability. At least one host with a serious vulnerability was present on every participant's network;
- 30% of all vulnerabilities were attributed to web server software;
- 31.67% of vulnerabilities were due to insecure remote access implementations (the largest percentage of the critical vulnerabilities);
- 24% of local governments use a remote access method that has been known to be vulnerable for over ten years; and
- configuration issues and the use of outdated technologies (software/hardware) were determined to be the root cause of the vulnerabilities on most participants' networks.

Vulnerability Severity Levels



SEVERITY	LEVEL	DESCRIPTION
🟥⬜⬜⬜⬜	**Minimal**	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
🟥🟥⬜⬜⬜	**Medium**	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
🟥🟥🟥⬜⬜	**Serious**	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
🟥🟥🟥🟥⬜	**Critical**	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
🟥🟥🟥🟥🟥	**Urgent**	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

OCS offered participants the opportunity to have multiple scans performed in an effort to evaluate remediation efforts and detect any new vulnerability that might have been introduced. Not all of the original participants opted for a recurring scan schedule. For the 198 participants receiving follow-up scans, 30.7% of all vulnerabilities were remediated on their networks. These participants also remediated 60% of the most serious (level 4 and 5) confirmed vulnerabilities.

The report findings conclude that local governments can improve their cyber security posture with a few modifications and enhancements to current processes and/or configurations. These include:

- upgrading all end-of-life systems which are no longer supported to eliminate inherent security vulnerabilities;
- following a defined patch management[7] policy;
- eliminating insecure remote access configurations to enhance perimeter security;
- continuing periodic scanning as a part of its cyber security strategy; and

[6] A host is a system or computer that contains business and/or operational software and/or data.
[7] Patching is a process by which vulnerabilities are mitigated through regular scheduled updates to software.

- following security best practices.

As a result of the scanning process, OCS was able to aggregate the IP address spaces of the local governments. This aggregation allowed OCS to create and maintain a database inventory of addresses, owners, and owner contact information. The inventory enabled OCS to implement a no-cost custom alerting service to the local governments. Upon receipt of reports of malicious or suspicious activity from trusted third party sources, OCS is now able to check the IP address inventory against the suspicious activity source and notify local governments of a potential breaches in a timely fashion.

This project improved capabilities of both OCS and the participating local governments by:

- providing the local governments with increased awareness of security issues;
- helping local governments confirm and understand their vulnerability exposure;
- helping local governments remediate discovered vulnerabilities;
- increasing OCS's intelligence gathering capabilities; and
- improving communication between the State and locals, thereby enabling:
    - data integration with several of OCS's existing services that allowed OCS to notify participants of problems discovered by Managed Security Services and Global Threat Monitoring Services ; and
    - improved situational awareness.

Although the project has concluded, vulnerability scanning is still being delivered at no cost to the local governments and OCS plans to continue as long as funding allows.

Conclusion

Vulnerability assessments are a vital part of any information security program. Such assessments provide a high value service at a low cost. By systematically identifying and remediating vulnerabilities, an organization significantly reduces its exposure to exploits and attacks.

Lessons Learned and Recommendations

More needs to be done to educate local government about the importance of cyber security. With constrained financial resources, limited funding has been an impediment to securing the information assets of these governments. Through this project, we have found some governments that did not have any staff charged with security responsibility. We also found a wide range of aptitudes and skills related to information security within local government. Some participants were able to respond quickly to evaluate and remediate a discovered vulnerability, while others struggled to comprehend the scope of the vulnerabilities and the steps necessary to secure their networks.

The following recommendations for local governments have been derived directly from the project's findings:

- Provide more education to staff regarding the importance of information security.
- Identify a person responsible for information security regardless of the size of the organization.

- Follow best practices for building and hardening systems when deploying new systems to help alleviate configuration issues.
- Replace end-of-life and other outdated technologies.
- Keep software licenses up-to-date, thereby maintaining access to critical system patches that address current vulnerabilities.
- Have a defined patch management policy to properly secure systems.
- Improve the selection of services and software. Since many local governments rely on third party hosting for information technology needs, care must be taken in selecting those providers.
- Include security requirements in contractual agreements for third-party hosting of information technology.
- Include vulnerability assessments as part of its information security program.