CSCI-6542 Computer Network Defense
Case Study - Penetration Test Statement of Work

Purpose

The purpose of this vulnerability assessment is to determine if Organization ABC is vulnerable to exploit from software running within the network. Specifically looking for known vulnerable software such as Windows XP, Windows 2003, or even unpatched versions of newer operating system.

While the focus of this assessment is on vulnerable software, Organization ABC is also interested in understanding other soft or non-technical vulnerabilities that could lead to their compromise. This includes social media footprint and exposed information about business processes that could potentially be leveraged by an attacker.

Assessment

The assessment of Organization ABC's security posture will be broken down into two phases. The first phase will involve determining how vulnerable they are to external attack. This portion of the assessment will be conducted with no prior knowledge of Organization ABC's network or configurations, also known as black box testing. This will involve documenting all externally facing network assists as well as any other information that could be leveraged to gain access to Organization ABC's network.

The second phase of the assessment will be conducted from within Organization ABC's network from the perspective of an employee. With a number of company laptops recently reported stolen, ABC is concerned that an attacker may try to target the organization from within their private network. While information regarding the network will be provided prior to this phase of the assessment, all aspects of the internal network derived from the assessment will be documented.

Scope

The scope of the security assessment is limited directly to Organization ABC's assets. Organization ABC does not want any partner organizations that maintain assets for them to be targeted. These third party service providers have their own security assessment procedures.

Limitations and Restrictions

While Organization ABC has specifically requested that the entirety of their network be assessed, they would like to limit vulnerability demonstrations to that of a reverse shell payload. While ABC is interested in understanding the extent of their vulnerabilities and the specific damage that each discovered vulnerability can cause, they want to minimize any interference that the assessment may cause to business operations.

Time Constraints

Organization ABC has requested that any activities that may interfere with normal network activity such as scanning or simulating attacks be conducted outside of normal business hours. As Organization ABC conducts business exclusively in the continental United States, all network scans and attack simulations will be conducted outside of the hours of 9AM to 9PM EST.

Schedule

Pre Assessment Research - Week 1 - May 4-8th 2015

- Social Media Analysis
- Open Source Analysis

Phase 1 - Week 2 - May 11-15th 2015

- Mapping of External Network Assets
- Scanning and Fingerprinting of Network Assets
- Simulated Attacks against potentially vulnerable systems

Phase 2 - Week 3 - May 18-22nd 2015

- Mapping of Internal Network Assets
- Scanning and Fingerprinting of Network Assets
- Simulated Attacks against potentially vulnerable systems

Assessment Reports & Conclusion - Week 4 - May 25-29th 2015

- Report Creation
- Present findings to network and system administrators
- Present findings to corporate IT leadership

Communication Strategy

All communications will be conducted in person with Organization ABC's representatives. No information regarding network vulnerabilities will be communicated electronically due to Organization ABC's security concerns. Organization ABC's representatives and some network administrators will be present during all phases of the assessment to ensure that any potential disruptions from network assessments are resolved quickly.

Incident Response Procedures

Any non-trivial incident that occurs during the planned assessment will result in immediate pause in assessment until the incident can be resolved. Organization ABC wants to ensure that disruption of operations is minimized during the assessment.

Tasks to be Performed

Pre Assessment Research

- Social Media Analysis
  - Any social media content that is linked to Organization ABC will be analyzed to ensure that no confidential or potentially compromising information has been revealed.
  - This includes any employee's social media accounts that are available for public consumption and clearly linked to the organization.
- Open Source Analysis
  - All open source records available referencing or citing Organization ABC will be examined for potentially compromising information.
  - Frequently some information about organizations networks can be determined through WHOIS lookups and other means. Any relevant findings will be documented and reported.

Phase 1 - External Vulnerability Assessment

- Mapping of External Network Assets
  - Any network asset discovered during the pre assessment phase would be mapped using a lightweight and unobtrusive scan from the NMAP software. Each system's results would be documented.
  - This would include public facing webservers and other domains discovered during the pre assessment research phase.
  - Each scan would be reported to Organization ABC's representatives to determine if ABC's network perimeter sensors were detecting these potentially malicious activities.
- Scanning and Fingerprinting of Network Assets

    - Systems would then be scanned using a more obtrusive tool called Nessus to determine specifically which ports and protocols that a particular machine was using. This would also attempt to resolve versions of operating systems and software running on the network.
    - Each scan would be reported to Organization ABC's representatives to determine if ABC's network perimeter sensors were detecting these potentially malicious activities.
- Attack Simulation
    - Machines that were identified to be running potentially vulnerable applications or software versions would be targeted for attack.
    - Each software and operating system would be tested against each relevant Common Vulnerability and Exposure (CVE) report.
    - Metasploit Framework will be used to test each potentially vulnerable machine, software, and protocol and the results will be documented. In cases where CVE's are too new for Metasploit Packages to exist, custom ones will be used.

Phase 2 - Internal Vulnerability Assessment

- Mapping of Internal Network Assets
    - All possible network addresses operating on the internal corporate network will be scanned to ensure that Organization ABC's network map is accurate and that there are no rogue network assets. In large organizations like ABC, it is possible for network operators to set up rogue machines without detection; this practice is referred to as Shadow IT and is a critical security concern for ABC.
    - Each scan would be coordinated with Organization ABC's representatives to determine if internal network sensors are operating as intended.
- Scanning and Fingerprinting of Network Assets
    - Systems would then be scanned using a more obtrusive tool called Nessus to determine specifically which ports and protocols that a particular machine was using. This would also attempt to resolve versions of operating systems and software running on the network.
- Attack Simulation
    - Machines that were identified to be running potentially vulnerable applications or software versions would be targeted for attack.
    - Each software and operating system would be tested against each relevant Common Vulnerability and Exposure (CVE) report.
    - Metasploit Framework will be used to test each potentially vulnerable machine, software, and protocol and the results will be documented. In cases where CVE's are too new for Metasploit Packages to exist, custom ones will be used.

Assessment Reports & Conclusion

- Report Creation
  - Upon conclusion of the network vulnerability assessments, reports will be created summarizing each potentially vulnerable system and all other findings.
- Presentation of findings to Organization ABC's administrators
  - Findings will be presented to Organization ABC's administrators as well as recommendations on how to resolve any issues that were discovered.
- Presentation to IT Leadership
  - Findings will be presented to IT Leadership with a focus on organizational impact of vulnerabilities as well as cost assessment for remediation.
  - Any organization wide changes or policy recommendations to improve Organization ABC's security posture would also be presented at this time.

Deliverables

Organization ABC has requested that all findings be compiled into three reports focusing on each phase of the network assessment as well as a report detailing potential mitigation strategies for any discovered issues.

- External Vulnerabilities & Social/Open Source Risk Assessment
  - This report would detail all information discovered during the pre assessment phase as well as any vulnerability identified with externally facing network assets.
- Internal Vulnerabilities & Insider Risk Assessment
  - This report will detail all information discovered during the internal network security assessment. This would also detail potential risk from insider threats or attacks launched from a privileged network perspective.
- Threat Mitigation & Risk Reduction Recommendations
  - This report would detail any potential mitigation techniques, or additional sensors, firewalls, and security appliances required to reduce Organization ABC's over all risk profile. This would include recommendations regarding policy additions and modifications that would serve to improve ABC's security posture.

Sensitive Data Handling Procedures

During the course of Organization ABC's security assessment, sensitive data will be obtained, compiled and handled. While measures will be taken to minimize exposure of sensitive data, it is inevitable that this type of data will be in play. A number of measures will be taken to ensure that this data is not compromised.

All data relating to Organization ABC's network, organization, business processes and internal activities will be contained on devices provided for the network assessment. All devices will implement secure drive encryption and security measures that meet all modern standards.

None of Organization ABC's data collected or provided will be transmitted electronically due to the sensitivity of the data being collected. No third party cloud providers or service providers will be used in any way to minimize potential data leakage.

Upon completion of work all drives will be securely wiped upon completion of the assessment to ensure that data is not misplaced post assessment.

Required Manpower

Due to the requirements provided by Organization ABC this assessment will require the following personnel

Personnel Type	Number of Personnel
Social Media Analyst	1
Open Source Analyst	1
Linux Security Expert	2
Windows Security Expert	2
Network Security Analyst	2
IT Policy Expert	1

Budget and Expenses

Hardware

Item	**Required Number**	**Cost**
Laptop	9	1500 x 9 = $13,500
External Storage Drive (1TB)	3	75 x 3 = $225
Organization ABC Devices	6	N/A

Licenses & Subscriptions

Software	**Required Licenses**	**Cost**
Nessus Vulnerability Scanner	6	6 x 2,190 = $13,140
Metasploit Express	6	6 x 5000 = $30,000

Personnel Costs

Personnel Type	Number of Personnel	Cost Per Hour	Total Hour	Total Cost
Social Media Analyst	1	$100	80	$8000
Open Source Analyst	1	$100	80	$8000
Linux Expert	2	$175	120	$42,000
Windows Expert	2	$150	120	$36,000
Network Expert	2	$200	120	$48000
Policy Expert	1	$125	80	$8000

Total Cost of Materials: $56,865
Total Cost of Labor: $150,000
Total Cost: $206,685

Payment Terms

Payment for materials will be provided up front as they are required for the security assessment of Organization ABC. In addition, 1/4th ($37,500) of the labor costs will be provided up front. Upon completion of each additional phase (Internal, External, and Conclusion) 1/4th of the labor costs will be paid.