International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 1 (January-February, 2016), PP. 221-223

Network Vulnerability Assessment

Utkarshni Sharma[1], Ankita Gupta[2]
[1]Assistant professor, [2]Computer Science Engineering (IS)
PEC University, Chandigarh 3rd October, 2015 ,ssid: 15212027
utkarshni.sharma03@gmail.com

Abstract *– **Vulnerabilities are the gateways by which threats manifest.***

Network vulnerability assessment is a continuous process. It gives continuous service over months or years including intrusion detection, monitoring, components and site assessments. The assessment is on the enterprise's security policies and procedures, the National Institute of Standards and Technology, accepts Principles and Practices for Securing Information Technology Systems. There are two types of assessments, technical and non-technical. Technical assessment is used to unearth component vulnerabilities and ingress component technical security. Another performs on-site security assessment of network's support structure. Data analysis and reporting is a final step. This constituent puts together information from the site assessment and technical assessment with threat information. Advice on how to extenuate the risks are also given.

*Keywords**: Technical and non-technical vulnerability assessment, on-site security assessment.***

I. PRIMER

Today networks operate in an open environment. This connectivity on a universal scale makes them competitive and with that uncovers them to many attacks and monetary losses. Day after day more and more enterprises are losing millions through high- technology crime and IT misuse and abuse. Those crimes include financial, telecommunications fraud, and theft of proprietary information, theft of information from computer or from their components, and vandalize of data or networks.

This paper is concerned with both structured and unstructured threats. Examples of structured threats include industrial undercover activities and cyber terrorism. Structured threats have several common characteristics, most important include goals, organization, planning, time, funding, technical expertise, and tools. Structured threats normally target assets or services of value. For example, structured threats may be designed to pilfer funds, acquire subtle information, or disrupt critical services such as power generation, water management or law enforcement and safety operations. In many cases structured threats require detailed information about the network, its components, and the environment that they are attacking. This information includes network and system design and operations information that may be in the hands of employees and, in some cases, may be openly available on the Internet to outsiders.

The notorious computer virus attacks so far, Code Red and NIMDA, both within the past year, were likely products of single individuals. They caused millions in damages and disruption.

Unstructured threats are transient in nature. These threats are not organized, do not have funding, or may not involve the use of tools. A college student who tries to access a local area network out of oddity, or an employee who enters invalid data causing system failure are examples of unstructured threats. In addition to human activity, unstructured threats can originate from natural and structural sources.

II. STRATAGEM

The investigation generally tailor the breadth and depth of the network security valuation process to meet the enterprise's needs and capital profile. However the process outline is based on a repeatable, proven approach and reflects best Business Practices for information security. The process examines both hard (computers, routers, etc.) and soft (personnel, physical, environmental, etc.) architectural essentials. Modular approach gives the flexibility to perform assessments from outside or from within the enterprise, at any level of the network, and can include the use of statistical sampling modus operandi for large systems. Sampling helps reduce a client's costs and maintains a level of confidence that the assessment provides.

The process is takes place, by accumulating data and identifying the components and confines of the client's

network. No matter what the size of the assessment, need is, to bound the network and find out what is important to the client. Data collection includes an information exchange with the client. The base of assessment is on the enterprise's security policies and procedures, the National Institute of Standards and Technology's (NIST), Generally Accepts Principles and Practices for Securing Information Technology Systems, and other best practices

A. STEP 1 – DATA COLLECTION AND NETWORK IDENTIFICATION.

Before entering the step 1, need is to

i. Present general assessment options to the client and establish an indenture that describes specifically what assessments will bring about under the agreement.
ii. Provide the client a checklist or opinion poll containing information that will be needed to discuss at the pre-assessment session meeting with network administrators, network security administrator and functional area AIS managers.
iii. Shelter technical and procedural information from the client such as network diagrams, security policies and procedures, and functional descriptions of data and applications.

Work in this step is to identify and confirm network components and services, connectivity to the network (e.g., routers, modems, etc.), who is gaining access to grave sub-networks, and any unauthorized network services (e.g., employees running their own web sites). It sounds upfront, but very few enterprises have a complete understanding of their network architecture, applications, information distribution and location, who has access to network resources, and how this access is achieved.

B. Process

a. Client orientation
- Meet with client's staff (network administrators, network security administrator, and functional area MIS managers) for a pre-assessment briefing and dialogue.
- Define client's main security concerns.
- Determine if the client has a security policy, and if so, how is that policy enforced.
- Determine client's most critical systems or information, where it is located, and who has access to these systems and/or information.
- Fix client's outlooks from the assessment.
- Dispense data collection sheets.

b. Collect and analyze data.
- Collect security and network information from client staff discussions, either through site visits or via templates accessible through our secure website, or through available documentation such as network diagrams, security policy (if exists), and functional descriptions of data or applications.
- Determine the system/network architecture (physical and logical configuration) and the network connectivity.
- Collect IP addresses and subnet masks for the networks that will be part of the assessment.

c. Conduct initial inquiries and scan component services.

d. Identify network users.

To help identify network, monitoring devices were installed on critical subnet which tried to determine who is accessing the network.

e. Examine and analyze the data collected and prepare the Network Survey Report.

f. Prepare a custom-made, detailed technical security assessment plan with the customer.

C. STEP 2 – TECHNICAL SECUTIRY VALUATION

This phase is the heart of network vulnerability assessment.

During the valuation, exhaustive searches are conducted to find security flaws in network components. The internal assessment, performed at the client's side, included blend of commercially available tools, registered tools and procedures loaded on explicitly configured assessment terminals.

Vulnerability assessment govern that someone can remotely exploit vulnerabilities in the network and its components by using the target's exterior connectivity. These tools are not resident on the target and are run remotely. These tools detect vulnerabilities that attackers exploit. Checklists and manual methods are used to cover new vulnerabilities available from a diversity of information sources that continuously observe that are not covered by automated toolset. This offers client with an assessment alongside the recent threats and vulnerabilities in the industry.

D. Route

- Assess single subnet, make a report and moves on to next subnet.

a. Choice modules to gauge.

b. Run susceptibility detection tools counter to subnets and critical components.

c. Path policy implementation assessments of components.

d. Evaluate reports and run additional trials to detect vulnerabilities the tool does not detect.

e. provide overall Technical Assessment reports to client.

E. STEP 3 – SITE VALUATION

This footstep of site assessment, valuation of, on-site calculations of network's operative situation, security background and management is conducted. Site valuations gage security of the network support systems at each site by inspecting and measuring an organization's structure. This also includes a scrutiny of practices and events applied within, to ensure obtainability, protection, and integrity of network's constituents or the network's processes, data, and products.

This assessment may be conducted at several levels depending on the needs of the client. Habitually bad felonies or social engineering attacks without client agreement are not performed. However, under the suitable conditions, physical protections can be tested and social engineering attacks can be performed that stab to gain passwords or other delicate information from users. These tests often divulge physical and procedural vulnerability.

F. Route

- Access a single site, generate its report and then move to next site for valuation.

a. Place visit with the client and start the collection of the data.

b. Demeanor assessment and prepare drafts.

c. Examine personnel on the site.

d. complete the final report by evaluating the results.

G. STEP 4 – NETWORK SECURITY ASSESSMENT AND VERDICT.

This phase reports the merged security assessment findings. Also this report will find the solutions to mitigate the

information security risks. For all the segments briefing will be done at the macro level.

Gears

Protocol analyzers and applications are crucial test components for network valuation and troubleshooting. These tools not only analyze the packets sent through different protocols, but also produce statistical analysis of data traffic. Other tools have the capability to generate network traffic for testing purposes. Many analyzers have the capability to record faulty packets and fragments which help point to sources of network faults. The powerful analyzers combine dedicated hardware with high- routine analytical software, often based on an expert system.

- **Areas Gauged**

Classically, network valuation measures and analyzes routine of the following:

Network strategies – switches, routers, hubs. Includes bulk issues relating CPU, memory, buffer, link/media operation, and amount.

Applications – e-mail, audio, FTP, Telnet, etc. Application reference point information consists mostly of bandwidth.

H. Route

e. **Evaluate results from site and technical assessments.**
f. **Regulate major findings and generate a summary.**
g. **Spawn a list of commendations and supporting basis.**
h. **Guard the report and findings.**

III. YIELD

On the completion of the network vulnerability assessment, the client/customer receives following:

- Review of existing network infrastructure and issues in that.
- Analysis and results based on tests by tools.

•advise for mitigation.

- Statistical reports.
- Network assessment diagrams.

Results and suggestions from the network vulnerability assessment enable the customer to develop a meticulous understanding of their current network proficiencies and determine if the network supports their technical direction for implementation.

IV. CONCLUSION

Network vulnerability assessment not only secures our system or network from being compromised through the intruders), it plays a vital role in planning new network implementations and for troubleshooting existing ones. Through this investigation one can monitor both technical and non-technical areas and helps to extenuate the risks, causing threats.

REFERENCES

[1] Penetration testing limits http://www.penetration.com/blog/penetration-testing/limitations-of-penetration-testing/,2008.

[2] Audit your website security with web vulnerability scanner, http://www.acunetix.com/vulnerability-scanner/.

[3] Vulnerability assessment and penetration testing, http://www.aretecon.com/aretesoftwares/vapt.html.

[4] http://www.netragard.com/penetration-testing.

[5] https://www.sans.org/penetration-testing-assessing-security.

[6] nterscience.in/IJCCT_Vol3Iss6-7-8/71-74.pdf.

[7] Insider Threat Vulnerability Assessment, http://www.cert.org/insiderthreat/insider-threat-vulnerability-assessor- itva-certificate.cfm.

[8] Vulnerability assessment, https://www.purdue.edu/.../VulnerabilityAssessmentBestPractices.ppt.

[9] 10 step security and vulnerability assessment plan.

http://www.itbusinessedge.com/slideshows/show.aspx?c=82760.