Security and Vulnerability Issues in University Networks

Sanad Al Maskari, Dinesh Kumar Saini, Swati Y Raut and Lingraj A Hadimani

Abstract— **The paper deals with security architecture and its possible implementation for a campus network and vulnerability analysis. In the paper an attempt is made to identify the critical points in the campus network for identifying the possible vulnerability and attack points. Vulnerability analysis is very helpful to secure the critical information and data in the campus network and servers. An attempt is made to engineer the architecture. We identify all the possible discrete points and give the detailed specifications to implement the security measures on them.**

Index Terms **—Security, Vulnerability, Cyber hardening, University Network, Architecture.**

I. Introduction

Securing large network has been always an issue to IT managers and security analyst. There are large similarities between securing a large network and university network but each one has its own issues and challenges. Pointing fingers at students is an easy option- a large number of suspects transiting inside the network. Current education pays more attention to IT technology to improve their students learning experience. Creating a convenient and secure network system in an educational environment is a challenging task. [1]. University tends to have a weak centralize policies. This means that they have tendency toward decentralization. This could be due to the way universities have been operated long time before computer systems was born. In some universities different departments will have it is own IT department, staff and budget ,the central IT group only provide bandwidth and high level services. Having decentralized IT group raises a challenge when it comes to policy making and policy enforcement

Small IT groups tend not to focus on policy making and enforcement. It is a well known fact that rejecting restrictions has been the tendency for academic staff especially in the area of research. Such resistance makes it harder to IT departments to centralize their policy; such resistance will also affect the IT processes and procedures (patch management, configuration control, change control, change management).

It was found that most universities have a lenient IT policies and procedures. There is no written usage policy document (DO's and DON'Ts) for student and staff. [4]Students at the university are considered to pose a high security risk to the university system. Students are good in transferring viruses and other malicious programs into the network. They can act as a malicious transient point. Creating and executing a policy to eliminate the security risks in the intranet is a challenging task. [2]

II. CAMPUS SETUP VALUNEARBLE POINTS

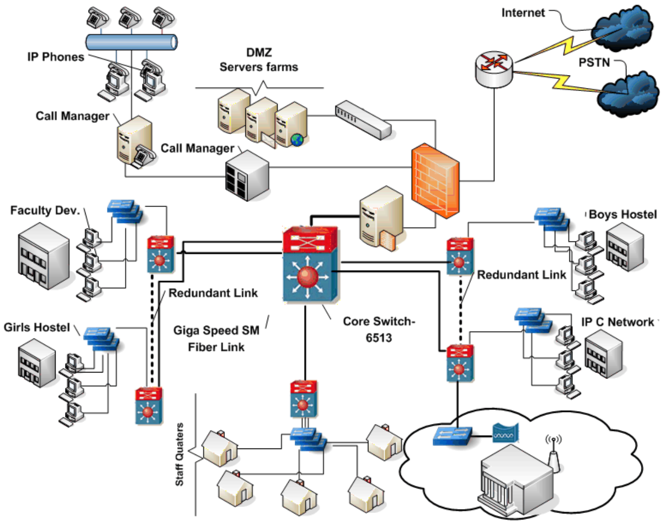

Fig.1 Sample Network setup

A. *Computer vulnerabilities*

Sample university network is given in Fig. 1, It is a fact now that computer vulnerabilities are steadily increasing since 1995 [3]. Malicious activities are still rising despite all the efforts to reduce it which includes:

- More patches and updates supplied by vendors
- Increased Public awareness and media attentions.
- Creating computer crime units.
- More tools in the security arsenal.
- The creation of Computer Crime and Intellectual Property Section by The Department of Justice.

Day by day we see incremental increase of new vulnerabilities and many patches released monthly to tackle this issue. Despite that effort thousands of systems are under the security microscope. Patching every hole in the network doesn't mean your system is secure; it takes only one hole for an attacker to bring it down.

III. NETWORK ATTACKS AND COUNTER ATTACKS STRATGIES

Host discovery

Most universities strive to create a convenient learning

Sanad Al Maskari is with Sohar University, Sohar, Sultanate of Oman (Sanad@soharuni.edu.om)
Dinesh Kumar Saini is Sohar University, Sohar, Sultanate of Oman (dinesh@soharuni.edu.om)
Swati Y Raut is with Pravara Rural Engineering, College, Ahmednagar , Maharshtra, India.(getdiya2008@gmail.com)
Lingaraj A. Hadimani is with Caledonian College of Engineering, Muscat, Sultanate of Oman (lingaraj@caledonian.edu.om

environment through IT technologies. In a university network there are many software applications, network devices, online systems and various servers running. Knowing what is inside a network is a critical security requirement. Host discovery can be used to monitor the network for any new devices, network growth and any suspicions devices. The total vulnerabilities is shown in Fig.2

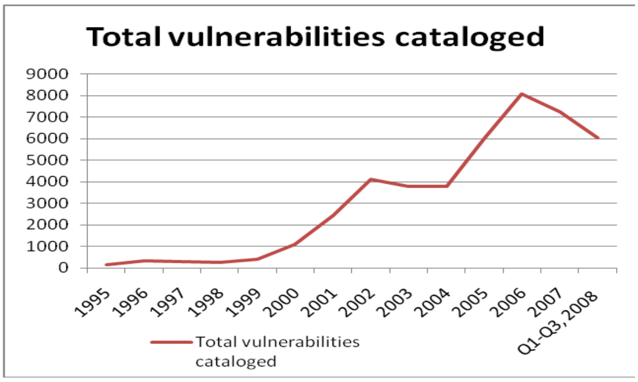

Fig. 2 Total vulnerabilities since 1995 (http://www.cert.org)

For an attacker the host discovery is a valuable tool to discover the network and select target systems to be attacked. Using single ICMP ping could be sufficient to locate hosts in the network. Scanning every port in each host can take a long time but it can reveal vital information such as what port is open in each device.

A. *OS Fingerprinting*

An attacker normally will need to know more information other than an IP address of the target machine in order to launch her/his attack. The reaction of discovering a Linux OS will be different than discovering a wireless access point, telephone PBX or a windows server. OS detection can be an effective technique to exploit vulnerabilities based on specific flaws. Also, it can be an effective way to exploit such vulnerabilities. OS detection can be used by attackers to exploits system by identifying exploits for that system version. A good example is buffer overflows vulnerability, in this vulnerability the attacker will need to generate a customized shellcode which will match OS platform and the hardware architecture.Without fingerprinting an attacker might send the wrong shellcode to the target system.

System administrators can use proactive measures to eliminate any risk by fingerprinting their own system. Determining remotely wither a given service is patched for a certain vulnerability is difficult task. To be sure that the vulnerability is real is for the administrator to exploit it. Exploiting vulnerability in a system can crash the system and cause down time and huge effort to bring it up again. OS detection can help administrators to reduce any false positive. When a vulnerability alarm issued by a system vendor an administrator can use OS fingerprinting to find out which system needs the patching before an attacker exploit the system.

Administrator can use fingerprinting to keep track of what kind of devices are running in the network. In a campus network students and staff can be malicious transient point. They can hook any device into the network which may cause security risk to the system. From a security point of view it is very critical to track and monitor all activities in the network and identify any external devices. In a campus network different sort of device could be plugged in to the network which can be very harmful. For instance students may plug their infected laptop to the private protected network which will expose the system. Employees can extend the protected network in undesirable ways. An employee can introduce a wireless access point to the network without realizing that he/she has exposed the internal network to potential nearby intruders. Using OS fingerprinting enable us to monitor the system for new devices in the network. Identifying an external device that is active for 24 hours can be considered to be a suspicious device and requires farther investigation. Finally OS detection can be used as an inventory management tool to find any devices which an accounted for.

B. *Vulnerability Scanning*

After host discovery and fingerprinting stages the attacker launches vulnerability scanning on the suspected system. The main reason for vulnerability scanning is to identify any weaknesses in the system or the network. Automated vulnerability scanners check against well know vulnerabilities identified by vendors or third parties. Vulnerabilities scanners need to be updated with most current exploits published by software vendors. Vulnerabilities scanners can cause large amount of traffic in the network and can trigger alarms in the IDS system. System administrators should have an appropriate Policy to prohibit unauthorized users in the campus network to conduct such scans.

IV. VALUNERABILITY ANALYSIS

If a set of conditions lead to the failure of authentication, access co1`ntrol, confidentiality, integrity, or availability of an information system then it is considered as vulnerability [7].

The following is a list of examples of the unauthorized or unwanted effects of vulnerability:

Executable commands without authentication

- Unauthorized access to data
- Impersonating another use or service within a system
- Becoming a cause of DoS/DDoS
- Destroying data without permission.
- The attempt to exploitation encryption system.

An organized approach to vulnerability analysis can help the organization to measure the effectiveness of their security system. Organizations must use vulnerability analysis tools to assess the organization networks and identify their current vulnerabilities before attackers and intruders can do-

Open port discovery and analysis.

- Active & Passive Penetration Testing
- Multiple OS scanning

A. *Common Vulnerability Analysis Tool (CVAT)*

CVAT can have the overview as shown in Figure 3. To handle different potential threats scoring, real-time attack scoring, and global scoring different vulnerable metrics can play an important role. A vulnerability metrics, with respect to CVAT, is a qualitative or quantitative measurement of critical characteristics of a given vulnerability. These metrics are grouped in to three distinct categories: base profile, intermediate, and environmental. The base profile group contains all the critical properties that remained unchanged over time. The second group consist f all characteristics of dynamic vulnerability that change over time. The environmental group focuses on vulnerability properties which are based on system implementations and user environment. The final score of CVAT represent the risk rate for a given vulnerability at a given time in a given environmental condition. [7]

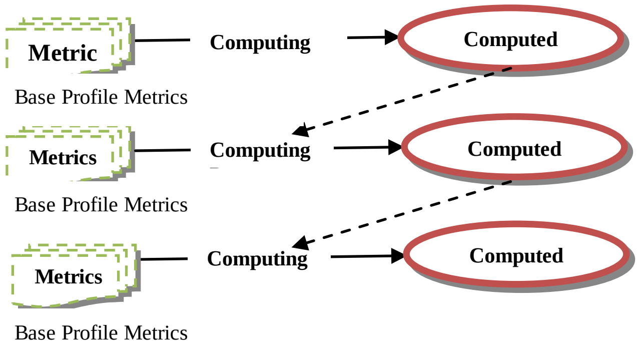

Fig. 3 Overview of CVAT

B. *Base Profile Metrics*

Once discovered and analyzed, there are certain aspects of vulnerability that remain unchanged, assuming the initial information is complete and exact. The properties of the vulnerability will remain unchanged overtime and will not change by changing the environment. The *access* and *impact* qualities are captured by the base profile metrics.

The following are the metrics used to identify if the vulnerable system is exploitable. These are of following types:

- Access Vector- identify wither the vulnerability can be exploited locally or remotely.
- Access Complexity- it measures the attack complexity in order to exploit a given vulnerability once the attacker access the system.
- Authentication- identify wither authentication is required or not to exploit the vulnerability.
- Confidentiality Impact- this metric will measure the impact of confidentiality in the exploited system
- Integrity Impact- it measure how much the integrity have been impacted on the exploited system.
- Availability Impact- in an exploited system how much the availability has been impacted.

Intermediate Metrics- consist of all characteristics of dynamic vulnerability that change over time and change as

TABLE I.
DIFFERENT VULNERABILITY METRICS

	Metrics	**Impact Factors**
Environmental Metrics	Access Vector	On the basis of locally or remotely exploited
	Access complexity	On the basis of exploitation during specialized Conditions exists or if system is always Exploitable
	Authentication	On the basis of required or not required
Intermediate Metrics	Confidentiality Impact	On the bases of level of confidentiality of the information
	Integrity Impact	On the basis of how often the integrity breaches occur
	Availability	Considering the lag or interruptions in the resource availability
	Impact Metrics	**Impact value**
Based Profile Metrics	Exploitability	On the basis of whether the exploitation code is available, Availability of proof of concept code, availability of function code , Availability of functional mobile autonomous code .
	Remediation level	On the basis of level of solution is available or not such as complete vender solution is available, an official of fix solution is available, un-official or non-vender solution is available, or no solution is available.
	Report Confidence	On the basis of degree of confidence in the presence of vulnerability such as unconfirmed different reports are there, multiple non-official sources are there, or confirmed official or vender source is there.
	Metrics	Impact Value
	Collateral Damage Potential	On the basis of the measurement of the loss in physical/property such as-no physical/property damage, system itself is damage, significant property damage, or catastrophic damage or loss.
	Target Distribution	It is based on how many system are susceptible towards the vulnerability such as no target system available, target systems are available in a small scale inside the environment, target systems are available in a medium scale inside the environment, or target systems are available in a large scale inside the environment.

the vulnerability ages. It can have following components:
Exploitability- it measure the complexity of exploitation process for the target system.

- Remediation Level- it measures the level of system recovery.
- Report Confidence- measures vulnerability credibility and degree of confidence
- Report Confidence- measures vulnerability credibility and degree of confidence

C. *Environmental Metrics-*

The environmental group focuses on vulnerability properties which are based on system implementations and user environment and vulnerabilities that are related to system distribution in a networked environment. The environmental group components are:

- Collateral Damage Potential- measure the expectable physical and logical damage to the exploited system.
- Target Distribution- measure how many systems can be infected by such vulnerability.
- Scoring- Different impact factors have been shown in the table-1 with respect to their concerned metrics. After getting the value from different metrics we can combine them for the final value to rate the risk by the vulnerability. For a given vulnerability the fundamental constituent qualities are captured and measured by the base profile metric which makes this group provide the foundation for the final score. The intermediate and environmental metrics group applies downwards and upward scoring modifiers to the base profile score.

Finally the values of all the metrics are to be combined to find out the overall risk by the vulnerability.

D. *Bandwidth anomaly analysis*

One of the important methods to detect any Trojan, bots or clever user activities is bandwidth anomalies monitoring. [8] Users can move data intentionally and unintentionally in and out of the network by using propriety and advanced information transfer methods this can be identified by analyzing incoming/outgoing network traffic such as local host counts, Busiest Local machines, Remote Host Counts, and Busiest Remote Machines.

E. *Reconfiguration features*

As soon as the analyzed information is available the cyber defense system should having the capabilities to hardening the available tools such as intrusion detectors, firewalls, anti-malicious software, etc. These reconfiguration features are of following types:

- Reconfiguration of different tools on the network
- Information based reconfiguration
- Behaviors based reconfiguration

F. *Data Visualization.*

To analyze the results of analysis of network traffic, computer system or a particular personnel's behavior it is necessary to represent the results is some graphical or easily understandable manner. It can be based on following types:

- User friendly data visualization
- Retrieval based on user requirements

G. *Data Archival*

From the existing logs the data can be archived for following reasons:

- Statistical visualization at a later date
- Forensic evidence procurement

All the above discussed measures for the secured University Intranet architecture can be represented in the accumulated form according to the Figure 4. It clearly mentioned the various discrete points and measures to be taken over there.

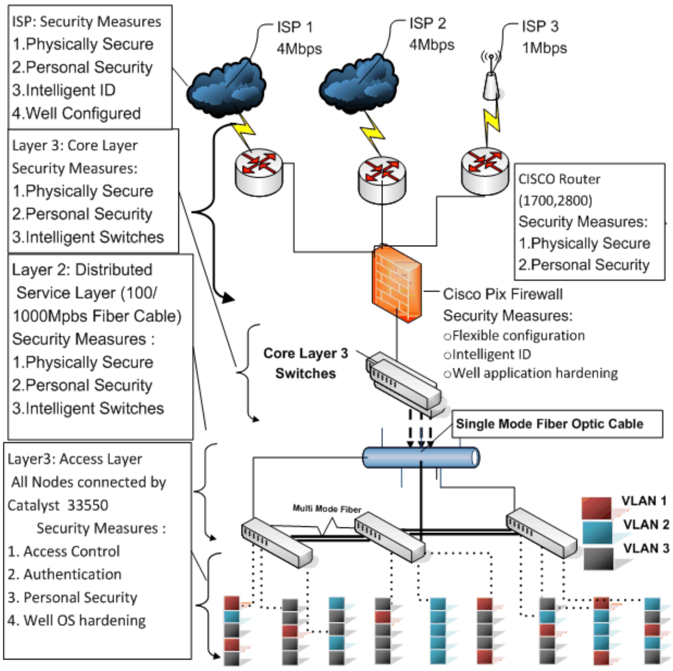

Fig. 4 Universities Secure Architecture

V. CONCLUSION

In the paper vulnerability is studied in detail and the possible attacks are considered in the campus network. Architecture for security measures and possible setup is proposed in the network. CVAT is used to handle different potential threats scoring, real-time attack scoring, and global scoring. Different vulnerable metrics are also used to collect information about the vulnerability. A vulnerability metrics, with respect to CVAT, is a qualitative or quantitative measurement of critical characteristics of a given vulnerability.

REFERENCES

[1] Cuihong, W. The problems in campus network information security and its solutions. in Industrial and Information Systems (IIS), 2010 2nd International Conference on. 2010.

[2] Zhu, J. and L. Liu. University network security risk assessment based On fuzzy analytic hierarchy process. in Computer Application and System Modeling (ICCASM), 2010 International Conference on. 2010.

[3] CERT. *CERT Statistics*. 2009 [cited 2010 4-8-2010]; Available from: http://www.cert.org/stats/cert_stats.html#vuls.

[4] Al-Akhras, M.A. *Wireless Network Security Implementation in Universities*. in *Information and Communication Technologies, 2006. ICTTA '06. 2nd*. 2006.

[5] S. Aughton, "Phishing Vulnerability Identified in Mozilla," PC Pro. 14 June 2004. Retrieved from: http ://www. pcpro. Co .uk / ? http : //www .pcpro.co.uk/news/news_story.php?id =58926

[6] Hemraj Saini and Dinesh Saini, "Malicious Objects Dynamics in the Presence of Anti Malicious Software", European Journal of Scientific Research, Vol.18 No.3 (2007), pp.354-359

[7] D. Liddle, Trojan: Remotely Operated Vehicle, IEEE Journal of Oceanin Engineering, Vol. OE-11, No. 3, 1986, pp. 364-372.

[8] Hemraj Saini and Dinesh Saini, "Proactive cyber Defense and Reconfigurable Framework of Cyber Security", International Review on Computer and Software, Vol.-2, Issue-2, 2007, pp.89-97