International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Network Monitoring Risk Assessment

Naman Gupta[1]; Richa Mehta[2] & Dr. Priti Puri[3]
[1,2] Symbiosis Centre for Information Technology
[3] Assistant Professor Symbiosis Centre for Information Technology Pune

ABSTRACT

Attacks on the assets of the networks have become frequent and increased from the past to present. Tools have been also made available so that a layman can also try to hamper the work and attack the loopholes. Companies are facing increased losses every year due to such kind of attacks. These kind of attacks are threat to the information's security which is considered to be the asset of any organization. The document will not only elaborate the all the vulnerabilities but will also provide the best possible security controls.

This risk assessment document will help identifying the organizations:-

- *Vulnerabilities*
- *Threats*
- *Risks*
- *Risk Likelihoods*
- *Risk Impacts*

Keywords: Vulnerabilities; Threats; Risks; Likelihoods; Impacts

NETWORK RELATED RISKS VULNERABILITIES & THREATS

RISK IDENTIFICATION

The purpose of this step is to identify the risks to the network assets. Risks occur in any system when vulnerabilities (i.e., flaws or weaknesses) in the IT system or its environment can be exploited by threats (i.e. natural, human, or environmental factors).

The process of risk identification consists of three components:

- Identification of vulnerabilities in the system and its environment.
- Identification of credible threats that could affect the system.
- Pairing of vulnerabilities with credible threats to identify risks to which the system is exposed.

After the process of risk identification is complete, likelihood and impact of risks will be considered.

1.1 Identification of Vulnerabilities

Vulnerabilities were identified and documented in below table.

1.2 Identification of Credible Threats

The purpose is to identify the credible threats to the IT system and its environment. A threat is credible if it has the potential to exploit an identified vulnerability. Threats were identified related to each vulnerability and is documented in below table.

1.3 Identification of Risks

Risks were identified for the ABC Corp by matching identified vulnerabilities with credible threats that might exploit them. This pairing of vulnerabilities with credible threats is documented in below table.

VMPS Server Configuration Attacks

Attacks on these kind of devices not only reduces the reputation of the company in front of the client but also costs them a huge loss. An attacker could assign a static IP address to their system with a locally administered MAC address to subvert this system. This system also has lots of historical MAC addresses entered into it that haven't been removed.

Overview

A VMPS server or a VLAN Management Policy Server is one of the most important asset nowadays for any company. MPS (VLAN Management Policy

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Server) is a way of assigning switch ports to specific VLANs based on MAC address of connecting device.

Threats

VLAN Query Protocol (VQP) Attack: By using VQP the attacker can easily join the VLAN, can remove the genuine MAC ID and hamper the process.

Media Access Control Attack: Most common and most important threat nowadays to any server is the MAC Attack. In this the attacker sits on a physical port and generates a vast number of MAC entries. When the CAM table fills up and has no room left, traffic without a CAM entry is sent out on all ports of the VLAN in question.

Vulnerabilities	Threats	Risks	Impacts
VMPS Servers Configuration:- An attacker could assign a static IP address to their system with a locally administered MAC address to subvert this system. This system also has lots of historical MAC addresses entered into it that haven't been removed.	VLAN Query Protocol (VQP)Attack	By using VQP the attacker can easily join the VLAN, can remove the genuine MAC ID and hamper the process.	This will lead to domino effect. Server will get flooded with vast number of MAC entries.
	Media Access Control (MAC) Attack (ref.3)	Unauthorized access or users can get access to the VMPS servers and can use the company VLAN to plant a timed bomb.	Unauthorized access may lead to loss or modification in data residing on servers. Timed bomb will lead to permanent destruction of data.

Risks

Unauthorized access or users can get access to the VMPS servers and can use the company VLAN to plant a timed logics bomb which will surely effect the company at a later stage. By using VQP the attacker can easily join the VLAN, can remove the genuine MAC ID and hamper the process. Getting access into the VLAN admin touch through the query protocol will also cause a worry line for the company.

Proxy Attacks

Overview

A traditional but a very frequently seen way of getting the work hampered is switch spoofing. Switch spoofing happens when an attacker can persuade a switch to go into trunking mode which then allows all traffic for all vlans to be seen.

Threats

In switch spoofing, in a trunking mode for switch, connected port is made visible to the attacker PC, the attacker could then see traffic for all VLANs. The most impactful threat is that A malicious host now presents itself to router 1 as another router and attempts to connect by using the appropriate tagging and trunking protocols (e.g. Multiple VLAN Registration Protocol, IEEE 802.1Q, VLAN Trunking

International Journal of Research
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Protocol) (ref. 4). If successful, then the attacker can see the traffic on all the VLANs and can contact hosts on any of the VLANs.

Risks

An unnoticeable impact of the trunking mode of the switch spoofing is that the victim is traced without his/her knowledge because of which each and every data sent or received by him is noticed and fetched. The performance also goes slow as the connection starts breaking after this.

Switch Spoofing

Overview

A traditional but a very frequently seen way of getting the work hampered is switch spoofing. Switch spoofing happens when an attacker can persuade a switch to go into trunking mode which then allows all traffic for all vlans to be seen. This would happen if a trunk port was set to auto and the attacker sent spoofed DTP (Dynamic Trunking Protocol) frames or connected a rogue switch to the switch port.

Threats

In switch spoofing, in a trunking mode for switch, connected port is made visible to the attacker PC, the attacker could then see traffic for all VLANs. The most impactful threat is that A malicious host now presents itself to router 1 as another router and attempts to connect by using the appropriate tagging and trunking protocols (e.g. Multiple VLAN Registration Protocol, IEEE 802.1Q, VLAN Trunking Protocol). If successful, then the attacker can see the traffic on all the VLANs and can contact hosts on any of the VLANs.

Risks

An unnoticeable impact of the trunking mode of the switch spoofing is that the victim is traced without his/her knowledge because of which each and every data sent or received by him is noticed and fetched. The performance also goes slow as the connection starts breaking after this.

Outdated Virus Definition Attack

Overview

Not updating viruses, ignoring the virus update notification or using an outdated version of the virus seems to be a very small issue but the impact of such small cases can lead to a drastic situation. Patches with the latest safety measures can help the organization to safeguard itself from the intrusion.

Threat

If a system is not updated to the latest technology than an unauthorized breach may happen which can allow a faulty user to access the internal organization. This may put the reputation of the company at stake. Even a single system can cause a risk to the whole organization.

Risks

The outdated virus definition slows down the system performance of the system which hampers the process of an organization. Users using old versions can be attacked more frequently in the components like e-mail, program files, and data files.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 08, August 2015
Available at http://internationaljournalofresearch.org

Vulnerabilities	Threats	Risks	Control Recommendations
Virus definition and other updates: - Using old and outdated technologies and not updating to the newest ones in case of malwares and viruses.	If a system is not updated to the latest technology than an unauthorized breach may happen which can allow a faulty user to access the internal organization.	Slows down the system performance Users using old versions can be attacked more frequently.	Run virus scan software periodically. Keep software security patches updated. Only allow approved software to be run on your computer systems. Limit services on all servers and workstations to the minimum required.

RECOMMENDATIONS & CONTROLS

The purpose of this step is to recommend additional actions required to respond to the identified risks, as appropriate to the agency's operations. The goal of the recommended risk response is to reduce the residual risk to the system and its data to an acceptable level. The
following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks: Legislation and regulation

- Organizational policy
- Operational impact
- Safety and reliability
- Effectiveness of recommended options (e.g., system compatibility)

RISK NO.	RISK	CONTROLS	RECOMMENDATIONS
1.1	**Media Access Control (MAC) Attack**	MAC address spoofing can be mitigated through **port security**. This allows you to specify MAC addresses for each port or to learn a certain number of MAC add per port. Upon detection of invalid MAC the switch can be configured to block the offending mac	Channel Gateway X
1.2	**VLAN Query Protocol (VQP) Attack**	By using a dedicated VLAN ID for all trunk ports it can be controlled. (ref .2)	Dedicated VLAN ID

2	**DOS Attack**	Blocking the Attack with Packet Filters on the Router.	Firewall
3	**Data centre**	• Including both logical (authorization, authentication, encryption and passwords) and physical (restricted access and locks on server, storage and networking cabinets) security. • Limit entry points. • Use plenty of cameras. • Make fire doors exit only.	2-factor authentication
4	**Virus definition and other updates**	• Use of malware removal software. • Restrict pop-up ads • Know what you are installing.	○ Vulnerability Scanners ○ Software Security Patches Update
5	**Switch Spoofing**	• Use authentication based on key exchange between the machines on your network. E.g. - IPsec. • Implement filtering of both inbound and outbound traffic.	ACL - Access Control List is maintained.
		•	
6	**Virus Patches**	• Run virus scan software periodically. • Keep software security patches updated. • Only allow approved software to be run on your computer systems.	○ Licensed Software. ○ OS and programs up to date

CONCLUSIONS

By this paper, it is clearly stated that what are the vulnerabilities, threats and risks associated with the network assets of an organization. A few controls and recommendations have also been suggested which will

definitely help the organization to mitigate all the risks.

PROFILE

Prof. Dr. Priti Puri

Dr. Priti Puri is a Doctorate in Computer Science from Kurukshetra University and has an MTech degree in Computer Science from Kurukshetra University. She has over 8 years of experience including academics, research and as a Patent Analyst for Microsoft. She has published and presented many research papers at various refereed/indexed International journals and Conferences.

REFERENCES

[1.] **Security Technology White Paper** http://www.utopiatechnology.co.uk/UserFiles/Docs/Huawei/Switching/Whitepapers/Security%20Technology%20White%20Paper.pdf

[2.] **Dynamic VLAN'S** http://www.firewall.cx/networking-topics/vlan-networks/designing-vlans/217-dynamic-vlans.html

[3.] **MACFlooding** https://en.wikipedia.org/wiki/MAC_flooding

[4.] **Configuring Dynamic VLAN Membership with VMPS** http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst4000/8-2glx/configuration/guide/confg/vmps.pdf