Reporting To:

Prepared By:

Senior Security Analyst
SoftGen Australia Pty Ltd

Date:

Contents

Executive Summary

This document contains summary information of the results of an internal and external network vulnerability and penetration test, conducted by SoftGen between the xx and xx of January 2016 as well as a number of recommendations associated with mitigating some of the identified risks. Separate documentation has also been provided indicating the steps required to remediate systems.

It has been concluded as a result of the testing that:

- External penetration from the internet was difficult and ultimately unsuccessful
- Externally facing system security and associated encryption used by VPN and Servers should be improved
- Servers and Infrastructure patching is generally up to date and maintained
- A breach of the wireless network was achieved in approximately 45 minutes
- There are unsupported Windows XP workstations and Windows 2000/3 Servers which should be replaced or remediated using the steps outlined in the technical reports

The remedial action and recommendations are as follows:

- Address the vulnerabilities using the remediation steps provided in the associated annexes
- Improve the security of the servers with unsupported operating systems by segregating them on the network and introducing application firewall or change control systems to prevent malicious code from running
- Improve the security of the wireless network system to require authenticated access.
- Review network access requirements holistically to include access to wireless, wired and remote access from company owned and personal devices
- Improve network segregation to isolate and control access to guest, corporate, server and printer networks.
- Increase controls on Web Filtering to mitigate threats initiated from behind the firewall

Finally, the extent and results of the testing was affected by the health of the network, There is either a substantial network configuration issue or an individual network system (probably router or switch) is failing. This needs to be identified and resolved to improve performance. The pre Audit Testing was unable to provide a complete assessment on the xxxx risk picture as per the requirements of the Statement of Works. The reasons are outlined below.

The Vulnerability Assessment Test Process

The testing was performed using two laptops running Kali Linux 1.3 and Kali Linux 2.0 with Rapid7's Nexpose and Metasploit, Nmap, Airmon-NG, HashCat and Wireshark.

As per our standard security practice, and to avoid interfering with penetration testing previously run with these machines, operating systems were reinstalled from scratch

The Audit Process and Reports

The Audit objective is to identify potential system vulnerabilities and provide remediation steps to mitigate the risk to the IT environment.

This is an Executive Report, written for technical and non-technical audiences. A more detailed technical report along with the test results is attached to this report for the IT Staff. SoftGen is available for further consultation on our findings and recommendations.

This document contains confidential and propriety information which could help a hacker compromise your systems and is intended for the exclusive use of xxxxxx. Use the Penetration Test Report if you wish to pass information to third parties.

Confidentiality

The testing has been limited to the boundaries set in the proposal. During our investigation, we may have been able to access confidential material from your business and your users. No files have been opened without your permission and any information we have gained about your business will remain confidential.

External Testing

Overview

From the information provided by POC, we tested the following external IP Addresses and hosts:

- 202.9.24.128/29
- 202.9.24.160/29
- www.Sampleaw.com.au
- mail.Sampleaw.com.au

Overall the testing indicates that the ability for gain access to the network externally via the internet is difficult, with no discernible method of entry able to be established and exploited. The general remediation actions and recommendations are generally associated with improving or changing the type of encryption systems in use, and several of the recommendations could be undertaken within the scope of general maintenance activity.

The most likely method of penetration to the network will likely be associated with credentialed access through compromised usernames and passwords. There is at present no policy to control or limit what external devices can access the systems, and how the credentials are cached or stored on the system accessing via the RDWeb https://access.Samplewa.com.au

Firewall

A copy of the firewall rules was provided and reviewed, but so specific testing of the access rules or policies was performed. The vulnerability test and penetration test would suggest that the firewall is configured appropriately.

The review of the rules seems to indicate there is no restriction on traffic passing from the DMZ the LAN and trusted networks is open. Thus if an attack platform could be established on an internet facing server in the DMZ, the ability to move to nodes on the LAN trusted networks is relatively easy.

It is recommended that a review of the applied rule sets be undertaken, to ensure that restrictions are in place between Firewall Zones and VLAN's are in place and remove unnecessary or superfluous configuration.

VPN Concentrators

As a result of the testing, some changes to the configuration of the VPN tunnels are recommended, as well as the type of certificates used. The steps for remediation are set out in Annex B.

Remote Access Gateway

XXXX. use a Windows 2012 R2 RDWeb remote access gateway to establish remote desktop access to the network. The vulnerability scan testing concludes that changes to the certificates should be implemented, and disabling of certain SSL options to improve the overall security posture of the environment. All remediation steps are detailed in Annex B.

The remote access gateway only requires a username and password to gain access to the network, and there is no limit to the type of device the user may choose to gain access. The risk is that passwords may be compromised. For example, credentials may be cached on an unsecure or shared computer, or that the user may be using a common password. To mitigate the risk, Multifactor authentication for the remote access gateway and webmail portal are recommended

Website

The testing concludes that the website server has no significant vulnerabilities. The recommended remediation is similar to the VPN and Remote Access Gateway recommendations and changes to the type of certificates used on the associated servers

Internal Testing

Overview

The testing of internal systems indicated that the network and infrastructure was generally in good health. The vulnerability scanning of the servers and network devices indicated that the systems were up to date with security patches which infers that there is a regime of regular patching, or patching has recently been performed. A recent upgrade of the Remote Desktop environment to Windows 2012 R2 has likely assisted in keeping the systems up to date. The majority of the vulnerabilities that were detected could be remediated during regular maintenance activity.

Servers

The IT department is aware of a number of servers running Windows 2000 and Windows 2003, which are no longer supported by Microsoft. These system did not have a specific vulnerability scan performed against them, as they cannot be remediated. The internal penetration testing concluded that these systems could be penetrated at will, with administrator access obtained. Recommendations to protect these servers if they are still required to run legacy applications has been provided. They include, virtualising the windows servers on VMware and then protecting (ring fencing) the servers using a VMware vShield virtual appliance for each server, or a firewall product such as McAfee Change Control.

The internal servers all have a common issue, which is the need for X.509 certificates and to have SSL disabled and TLS upgraded. These are all easily dealt with and Remediation Steps have been attached. A master Certificate for the sample.com.au domain should be purchased from a Master Licenser like VeriSign (Symantec) or Thawte. Using a Certificate License Generator, the IT Department can then issue Certificates for Servers, Network Systems, Bespoke Software and Websites.

The vulnerability scans indicate servers have Server Message Block options open. These vulnerabilities can easily be closed with Group Policy Changes.

Wireless Network

Wireless network injection testing was performed on Level 28 in an attempt to gain access to the corporate network. The result of the test was that it took 45 minutes to capture the encrypted password, and 6.5 minutes to crack the encryption. While there are some remediation steps that can be undertaken to mitigate the risk associated with the wireless network (such as Radius Authentication), the ability to breach the wireless network relatively quickly highlights the holes in the physical network security, and should be reviewed more broadly in the context of network admission control for wireless, wired, and remote network access requirements.

Workstations

The majority of the workstations on the network are remote desktop clients, running Windows XP. Like the Windows 2003 and 2000 Servers, xxxx. is aware that the devices are no longer support by Microsoft and as a result they are subject to vulnerabilities for which there is no remediation steps available. The devices however by design essentially do not process or access data. So while the security of the Remote Desktop session is not using the latest encryption, the risk to XXXX is not considered high. Some recommendations have been put forward on how to further improve the security of these systems to mitigate as much as possible these systems being a point of ingress in future.

Printers and Network Hardware

Our testing revealed 177 devices internally, these are a mix of Servers, Routers, Firewalls, Printers, PC's and BYOD devices.

The PC's/Laptops are reasonably configured but are really of little consequence as Terminal Services is being used for user access. There are a few smaller issues that need addressing, however these can be remediated largely by creating Group Policy settings on the Domain Controllers.

The printers have been left fairly open, however the opportunity for an attacker to pivot from a printer into a server is not easily accomplished as the printer rights in the Active Directory make access difficult. Nevertheless, the printers should have their firmware upgraded and be placed in a separate one way VLAN or subnet that allows printing but not access.

The adoption of the Terminal Server systems has been instrumental in improving the security of all the systems at Barry. Nilsson.

Web Filtering and Malware Mitigation

The testers are aware that there is a web filtering solution that, for instance blocks executable files from being downloaded. However, the testers feel that the Web Filtering device is being underutilized or that the policies in place are more relaxed than they should be. There are Web Sites that users can access that should be denied. An effective security strategy must include controls over staff access to suspicious websites. In particular, some finance and economic sites are a problem because of the "Watering Hole" attacks that can be launched from them. Attacks are targeting specific organisations directly with these attacks.

In addition to the Watering Hole attacks there is the issue of malware through advertising on search and blog sites, “Malvertising” does not even need the user to click on the advertisements to be infected, if an infected ad is displayed then particular users can be infected. Malvertising is particularly effective because the site owners don’t even know that the advertisements are infected. These infections can lead to the loss of confidential information, which can lead to financial loss and impact on company reputation.

The current web filtering may not be capable of shielding against these attacks, however, a DNS Sinkhole can be created at Xxxxxxx that would shield against these events. A DNS Sinkhole can be updated several times each day from US Federal Government malware list servers.

Organisations are specifically targeted using these attacks; the URL below refers to an example of this attack: http://www.securityweek.com/chinese-attackers-hacked-forbes-website-watering-hole-attack-security-firms

Mobile Device Management

Currently, there is no device management of either company or staff owned Mobile devices. These devices, be they company owned, or personal property of the individual are granted access to the corporate network and resources. There is a risk that these unmanaged devices may be used compromise network security.

Consideration should be given to implementing a mobile security solution to control all devices attempting access to Barry. Nilsson. Systems.

In the meantime, Radius Authentication should be enabled for all Mobile Devices regardless of origin. Radius Authentication is part of Windows Server and can be implemented rapidly without additional cost.

Network Health

During the testing process it was observed that there were communication problems with external systems in particular and to a lesser degree some internal servers. This substantially impacted the amount of testing or scanning that could be performed within the time allocated

The tester used a Wireshark Protocol Analyser program to track all of the packets leaving the testing laptops as they made their way through the networks to outside systems such as https: This website lists all the latest malware and vulnerabilities and is an essential tool utilised during testing.

The results indicate that there is a significant problem with the Sample network and that it is likely being caused by an incorrectly configured switch or router or that one of these devices is failing and needs replacement.

Sample urgently needs to have a network expert with experience in Juniper switches and routers look at their configuration and utilise Wireshark to determine the cause of this problem.

Conclusions and Recommended actions

Recommended actions

We recommend the following steps:

- Follow the remediation plans listed in the attached Annexes: These remediation plans will eliminate the remaining issues with the systems.
- Network Health: Engage a Network Expert to determine the cause of the network packet loss and retransmission problems.
- Secure the Wireless Access Points: Radius Authentication should be enabled on the WAP's as this will eliminate the ability to access the internal network by attackers. It is a quick and easy solution as Radius is included as part of Microsoft Server 2008/2012 and uses existing logon credentials. The existing Meraki hardware supports extensive configuration options in this regard to segregate networks, apply policies and restrictions
- Public Wireless: Consideration should be given to carving out client use of xxxx. Wireless and establishing a standalone service for clients which uses one Wireless Access Point on Level 28 attached to its own ADSL modem. Or utilise the guest network services within the Meraki hardware
- Document Security: Digitally sign documents, and enforce change tracking. And consider the implementation of a DataRoom file sharing solution such as Citrix Sharefile to enforce restrictions and control access
- Web Filtering: Use the extended capabilities of your web filtering device and implement a DNS Sinkhole service at xxxxxx.
- Certificates: Change the types of certificates used on all servers
- Multifactor Authentication: Implement a multifactor authentication for remote access

Conclusions

Overall we find the network and infrastructure relatively free of significant vulnerabilities, and the ability to gain access to the network from the internet in the Penetration Test was difficult. The changes made by the move to Terminal Servers have served xxxxxxx. well, the security posture has the basics in place with the ability to build on the existing practices to be able to prevent and remediate vulnerabilities as they arise.

The most significant risks to xxxxxx are associated with the wireless network, simple password only access to services, and the internet filtering.

Attachments

ANNEX A

Penetration Testing Report Statement for a Third Party

ANNEX B

Internet Facing Server Report

ANNEX C

Remediation Guide

ANNEX D

Radius Implementation Guide

IF YOU WISH TO DISCUSS ANY ASPECTS OF THIS REPORT PLEASE CONTACT SOFTGEN

M: 1800 642 289
Direct: 02 9416 0416
E: sales@sgen.com.au
URL: www.softgen.net.au