Top 10 IBM i Configuration Mistakes that Leave your System Vulnerable

Carol Woodbury, CISSP, CRISC, PCIP
VP, Global Security Services
Carol.Woodbury@helpsystems.com

Three Types of Hackers

- Targeted attack
- Attack of opportunity
  - Takes advantage of known vulnerabilities in applications, operating systems or protocols or servers/applications that are out-of-date (missing patches)
- Attack for ‘fun’
Type of Security Incidents

Exploiting misconfigurations

- Hacker scans for misconfigured AWS containers
  - [https://www.secureworldexpo.com/industry-news/capital-one-hacker-other-companies-indictment](https://www.secureworldexpo.com/industry-news/capital-one-hacker-other-companies-indictment)
The Insider Threat

- Inadvertent threat actors are **insiders in your company** who unwittingly compromise the environment.
- Two of the most prolific ways X-Force researchers have observed inadvertent insiders leaving organizations open to attack is by **falling for phishing scams** or social engineering, and through the improper configuration of systems, servers, and cloud environments, and by **foregoing password best practices**.

- IBM X-Force Threat Intelligence Index 2019

Who’s the Target?

**Most Frequently Targeted Industries in 2018**

<table>
<thead>
<tr>
<th>Industry</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finance and Insurance</td>
<td>13%</td>
</tr>
<tr>
<td>Transportation</td>
<td>13%</td>
</tr>
<tr>
<td>Professional Services</td>
<td>11%</td>
</tr>
<tr>
<td>Retail</td>
<td>11%</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>10%</td>
</tr>
<tr>
<td>Media</td>
<td>9%</td>
</tr>
<tr>
<td>Government</td>
<td>8%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>8%</td>
</tr>
<tr>
<td>Education</td>
<td>6%</td>
</tr>
<tr>
<td>Energy</td>
<td>5%</td>
</tr>
<tr>
<td>Healthcare</td>
<td>4%</td>
</tr>
</tbody>
</table>

Source: IBM X-Force

© HelpSystems LLC. All rights reserved.

www.helpsystems.com/professional-security-services
#1: Running at the Wrong Security Level (QSECURITY)

<table>
<thead>
<tr>
<th>QSECURITY Value</th>
<th>Total Available IBM i Security Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 50</td>
<td></td>
</tr>
<tr>
<td>Level 40</td>
<td></td>
</tr>
<tr>
<td>Level 30</td>
<td></td>
</tr>
<tr>
<td>Level 20</td>
<td></td>
</tr>
<tr>
<td>Level 10</td>
<td></td>
</tr>
</tbody>
</table>

#2: Allowing Weak Passwords

- Password composition rules aren’t set or are weak
  - Use QPWDRULES
- Users use the same password everywhere
- Users re-use passwords that have been compromised
  - User education!

Change Password

Please use 8 or more characters with a mix of letters, numbers and symbols.
#3: Running at the Wrong Password Level (QPWDLVL)

<table>
<thead>
<tr>
<th>System value</th>
<th>Description</th>
</tr>
</thead>
</table>
| 0            | Default: Character set: A-Z, 0-9, $, @, # and _
|              | Maximum length: 10 |
| 1            | Same as level 0 but gets rid of old NetServer password
|              | Safe to move if you are not using NetServer or not connecting with Windows 95, 98, ME or Windows 2000 server – end users will see no difference |
| 2            | Character set: Upper / lower case, all punctuation and special characters, numbers and spaces
|              | Maximum length: 128
|              | Keeps NetServer password, encrypts with old and new algorithms
|              | Sign on screen changed to accommodate longer password, CHGPWD and CRT/CHGUSRPRF pwd field changed |
| 3            | Same as level 2, gets rid of old encrypted password and old NetServer password
|              | Safe to move if you are not using NetServer or not connecting with Windows 95, 98, ME or Windows 2000 server – end users will see no difference |

Changes require an IPL
https://www.helpsystems.com/resources/on-demand-webinars/moving-password-level-2-or-3-and-other-password-tips-and-tricks

Passwords – Get Rid of Them!!

- Switch to use SSO (Single Sign-on)
- IBM i passwords can be eliminated because AD credentials are used for authentication

#4: Not Using 2FA (Two-Factor or Multi-Factor (MFA)) Authentication

- Authenticating with at least two of the following:
  - Something you know
  - Something you have
  - Something you are
- Required by several laws and regulations including PCI DSS

Encrypt Data in Motion

- Make sure all communications – even internal communications – are encrypted
- For internal communications
  - Use DCM (Digital Certificate Manager) to create and/or assign certificates
  - Use the Certificate Authority certificate in the deployment of Access Client Solutions (ACS)
  - Configure clients to use an encrypted session
- For guidance:
- For secure file transfer and communications outside of the organization use GoAnywhere.
#6: Using Weak Encryption (QSSL* System Values)

- **QSSLPCL** – list of SSL protocols on the system
  - *OPSYS* – list is determined by the system and can varies by release. This is the default. Or to control, specify one or more of the following:
    - *TLSV13 (V7R4)*
    - *TLSV12*
    - *TLSV11*
    - *TLSV1*
    - *SSLV3*
    - *SSLV2*

- **QSSLCSLCTL** – who controls the list specified in QSSLCSL – the system (*OPSYS - default) or user (*USRDFN)*

- **QSSLCSL** – contains list of ordered cipher suites to be used on an SSL connection. Can only be modified if QSSLCSLCTL is *USRDFN*.

## Protocols by Release

<table>
<thead>
<tr>
<th>OS Release</th>
<th>SSLv2</th>
<th>SSLv3</th>
<th>TLS1.0</th>
<th>TLS1.1</th>
<th>TLS1.2</th>
<th>TLS1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>V5R4</td>
<td>A</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V6R1</td>
<td>A</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V7R1</td>
<td>A</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>V7R1 w/TR6</td>
<td>A</td>
<td>X</td>
<td>X</td>
<td>A</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>V7R2</td>
<td>A</td>
<td>A</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>V7R3</td>
<td>A</td>
<td>A</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>V7R4</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

X = Enabled by default  
A = Available but not by default  
Blank = Not available
Weak Protocols and Ciphers – as of April 2019

- Protocols: SSLv2, SSLv3, TLS1.0 and TLS1.1
- Ciphers:
  * RSA_RC4_128_SHA
  * RSA_RC4_128_MD5
  * RSA_NULL_MD5
  * RSA_NULL_SHA
  * RSA_NULL_SHA256
  * RSA_DES_CBC_SHA
  * RSA_EXPORT_RC4_40_MD5
  * RSA_EXPORT_RC2_CBC_40_MD5
  * RSA_RC2_CBC_128_MD5
  * RSA_DES_CBC_MD5
  * RSA_3DES_EDE_CBC_SHA
  * ECDHE_ECDSA_NULL_SHA
  * ECDHE_RSA_NULL_SHA
  * ECDHE_RSA_NULL_SHA256
  * ECDHE_RSA_3DES_EDE_CBC_SHA
  * ECDHE_ECDSA_3DES_EDE_CBC_SHA

http://www-01.ibm.com/support/docview.wss?uid=nas8N1020876

Why the Emphasis on Encryption and 2FA?

- According to a 2017 Black Hat Hacker Survey by Thycotic, encryption and 2FA were the most difficult to get through
Coffee with Carol Webinars

- Making the Move from SSL to TLS

- Configuring ACS to use SSL/TLS

User Profiles

UP NEXT
#7: Not Reviewing User Profiles

- Group assignments need to be reviewed periodically (e.g., quarterly)
  - DSPUSRPRF USRPRF(QPGMR) TYPE(*GRPMBR)
  - DSPAUTUSR SEQ(*GRPPRF)
- Special authorities
  - Start creating new profiles with only the special authorities required to do their jobs
  - PRTUSRPRF
  - DSPUSRPRF USRPRF(*ALL) OUTPUT(*OUTFILE) OUTFILE(MY_LIB/PROFILES)
  - QSYS2.USER_INFO view
- Limited capability setting
  - Most users should be LMTCPB(*YES)
#8: Leaving Inactive Profiles on the System

- Inactive
  - Look at the Last used date (not the Last signon date!)
  - GO SECTOOLS, options 2-4

Profile Clean-up Hints

- If PASSWORD(*NONE) then set PWDEXPIV to *SYSVAL
- If profile is only used for batch processing it doesn’t need a password and can be set to STATUS(*DISABLED)
- You can’t delete (the system will prevent the deletion of) a
  - Group profile that has members
  - Profile that owns objects
Protecting Data

- Determine value of data to the organization
- Determine cost of that data being altered, unavailable, lost or stolen

- What and how many levels of defense do you need to put in place to reduce the risk to an acceptable level?

- Value of the data to the organization is often ignored!
Security Must be More than Menu ‘Security’

- Users downloading to an Excel spreadsheet
- JDBC connections to WebSphere applications
- FTP to banks, payroll processors, trading partners
- Developers updating data
- Users running SQL or Queries
- DDM
- Administrators and Analysts with legitimate command line access

#9: Not Implementing Multiple Layers of Defense (Defense in Depth)

- Exit Points
- Object Level Security
- Field Encryption
- Data
Secure the Data

- Start by considering how the data should be secured
  - For Integrity -> *PUBLIC(*USE)
  - For Confidentiality -> *PUBLIC(*EXCLUDE)

- Implement object level security to protect the data from unauthorized access
  - Determine how to secure the data without breaking other applications

#10: Not Reviewing Authorization Lists

- Review (at least quarterly), profiles authorized to authorization lists
  - DSPAUTL
  - QSYS2.AUTHORIZATION_LIST_USER_INFO

- May also want to review objects secured by the list
  - DSPAUTOBJ
  - QSYS2.AUTHORIZATION_LIST_INFO

#11: Not Reviewing Adopted Authority

- Not dangerous as long as it’s used wisely
- Need process in place to review programs that adopt – especially an *ALLOBJ profile

Caution!
- Programs that put up a command line
  - Set Use adopted authority to *NO and User profile to *USER
- Menu options that call an IBM command – WRKSPPLF, WRKQRY, STRSQL
  - Put them into a CL program and set to USEADPAUT(*NO) USRPRF(*USER)
- PRTADPOBJ (Print Adopting Objects) to monitor/review

#11 – Not Reviewing Adopted Authority

- Not dangerous as long as it’s used wisely
- Need process in place to review programs that adopt – especially an *ALLOBJ profile

Be wary of:
- Programs that put up a command line (set Use adopted authority to *NO and User profile to *USER)
- Menu options that call an IBM command – WRKSPPLF, WRKQRY, STRSQL (may been to add them to a CL program and set that program to be USEADPAUT(*NO) USRPRF(*USER))
- PRTADPOBJ

Use Policy Minder to establish a baseline and identify programs that adopt
#12: Configuring DDM to Connect without a Password

- Most DDM servers do not require a password on the connection
- ADDSVRAUTE (Add Server Authentication Entry) allows you to add an entry to connect as another (more powerful) user

- If you can’t change the DDM server configuration:
  - Secure the ADDSVRAUTE, SBMRMTCMD and CRTDDMF commands
  - Use Exit Point Manager to block access to unauthorized users
#13: Sharing root (‘/’)

Remove read/write shares – especially to ‘/root’

Removing Shares

- Select the share
- Use the Actions dropdown to choose Properties
- Click on Sessions
#14: Leaving Root at the Default *PUBLIC Authority

- Reduce the *PUBLIC authority of ‘/’ from
  - DTAAUT(*RWX) OBJAUT(*ALL) to
  - DTAAUT(*RX) OBJAUT(*NONE)

- Review the CO and DO audit journal entries prior to making any changes to make sure you accommodate objects being created into (CO) / deleted out of (DO) ‘/root’
#15: Hoarding!

- Inactive profiles
- De-commissioned servers
- Archived data past retention schedule
- Copies made prior to updating a database
  - filenameX, filenameOld, filename2, filenameCopy
- File shares
- Past versions of vendor products
- Vendor products no longer in use

#16: Not Saving and/or Not Verifying your Save Media

- How often are you saving security data (SAVSECDTA)?
  - User profiles
  - Private authorities
  - Authorization lists

- Note: Reducing the private authorities on your system reduces the SAVSECDTA and RSTAUT times

- Note: No one should have *SAVSYS special authority except Administrators and Operators
  - Can always save / restore what you own or have authority too

- Your ability to recover from malware infecting IBM i may depend on how good your back-ups are
#17: Not Staying Current!

- OS level
  - Many security enhancements – including protocols and cipher suites that may be needed for compliance - aren’t available in lower releases.
  - V7R1 out of support as of April 30, 2018

- Technology Refresh

- PTFs (especially for Java, OpenSource, etc)
  - Use the SYSTOOLS.GROUP_PTF_CURRENCY

- Sign up for email alerts

- iAccess (out of service as of April 30, 2019) -> Access Client Solutions

## Start Somewhere – Even if It’s a Small Step!
HelpSystems’ Professional Security Services

- **Managed Security Services**: Bridge the gap between auditors and IT staff by enlisting experts to monitor your IBM i security and prepare in-depth reports every month.
- **Single Sign On Managed Services**: Help implement and maintain Single Sign On, eliminating up to 80 percent of password management costs.
- **Risk Assessment**: Uncover your system’s security vulnerabilities and prepare a detailed report filled with expert findings and recommendations.
- **Penetration Testing**: Test your security defenses through penetration testing—ethical hacking required by auditors that highlights the danger of security vulnerabilities.
- **Architecture**: Close security gaps with a re-architected application security scheme designed by IBM experts to meet your unique needs.
- **Remediation**: Implement your new security architecture and ensure IT staff has the knowledge to maintain the new security scheme.

HelpSystems’ Solution-based Approach

- **Compliance Reporting**: Compliance Monitor for IBM i
- **Privileged Access Management**: Authority Broker for IBM i
- **Self-Service Password Reset**: Password Self Help for IBM i
- **Database Monitoring**: Database Monitor for IBM i
- **User Provisioning**: Identity Manager for IBM i
- **Multi-Factor Authentication**: Multi-Factor Authentication, SecurID Agent for IBM i
- **Native Encryption**: Encryption for IBM i
- **Perimeter Access Control**: Exit Point Manager for IBM i
- **Command Monitoring**: Command Security for IBM i
- **Automated Risk Audit**: Risk Assessor for IBM i
- **Security Information and Event Management**: SIEM Agent for IBM i, Event Manager
- **Native Virus Protection**: Antivirus for IBM i
- **InfoSec Policy Control**: Policy Minder for IBM i
- **Secure Managed File Transfer**: GoAnywhere

www.helpsystems.com/professional-security-services