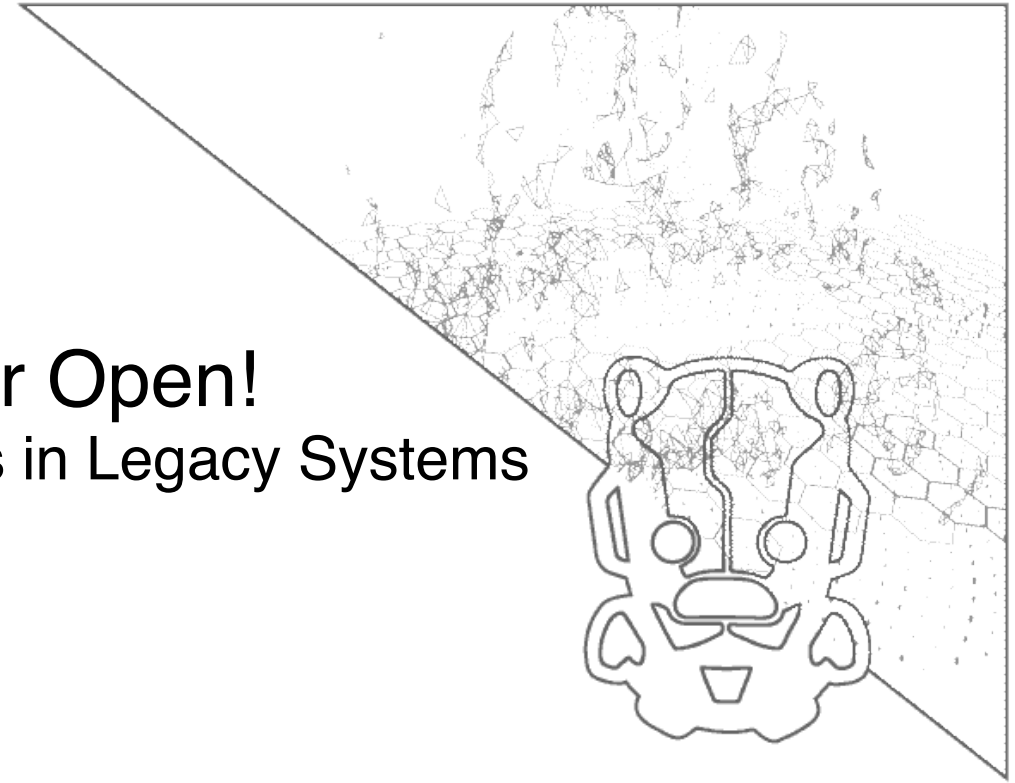
You Left The Back Door Open!

Finding Legacy Vulnerabilities in Legacy Systems



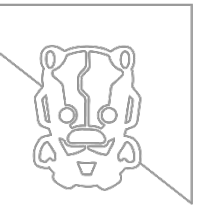
Nick Dunn

IOActive®

Standard Disclaimer

- As usual, these techniques can be used for good or evil.
- The techniques are intended for testing software, not breaking it.
- If you discover major issues in commercial software or find systems accidentally exposed to the internet, report them/fix them, play nicely, and don't go down the path of world domination (or minor theft).

Agenda

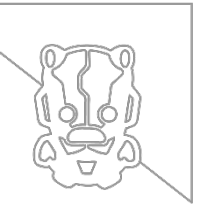


- Intro & whoami
- AS/400 overview
- AS/400 design and terminology
- Security Assessments of AS/400
  - Tools
  - Scanning and enumeration
  - Account enumeration and application landscape
- Exploiting misconfigurations and vulnerabilities
  - Privilege escalation
  - Exploiting the database and system configuration
- Mitigations and defences
- Conclusions
- Learning more
- Questions

whoami

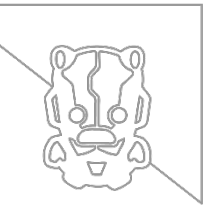
@N1ckDunn

@nickdunn@infosec.exchange

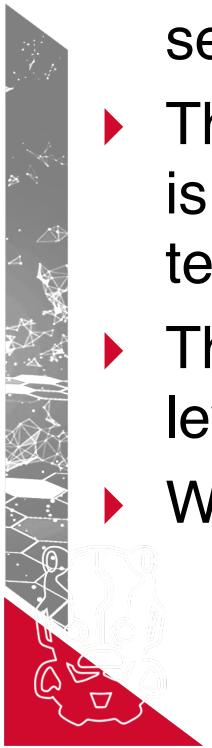


- Coming from software development and architecture
  - 6 years as software developer, architect, team lead, working in secure software for the financial sector
  - Worked as an in-house penetration tester and code reviewer in online gambling
  - Security consultancy
- Moved into security consultancy and worked on:
  - Code review
  - Penetration testing
  - Threat modelling, architecture review
  - Automating security testing with new tools, scripts, etc.
  - Security research

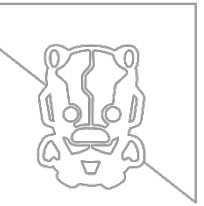
What This Talk Is (and Isn't) About



- This is a talk about the AS/400 system and how to test security of its configuration and applications.
- There will be some discussion of why the system is the way it is, and how this can affect secure configuration, and security testing.
- The talk will show how to test AS/400 systems, determine risk levels for the situation, and recommend suitable defences.
- We will not be discussing RPG or COBOL programming.



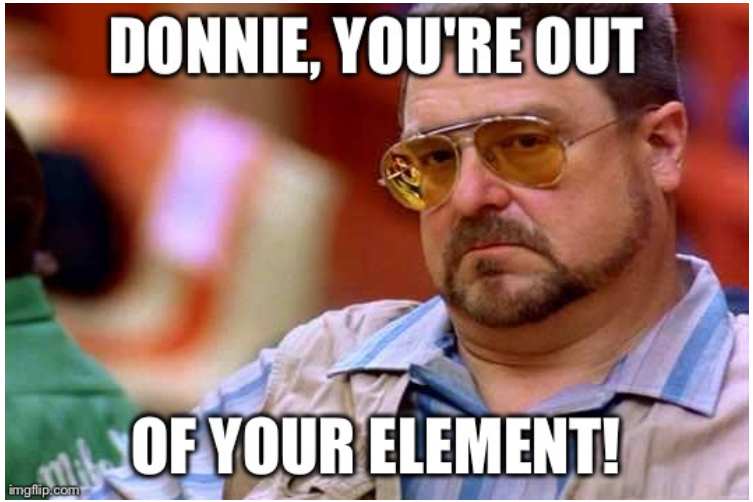
The Benefits of Testing AS/400



- AS/400 runs a very large number of services by default.
- As a result, both services and user accounts can be enumerated trivially.
- Those responsible often don’t realise how easily these systems can be hacked or how insecure the systems frequently are.
- It’s not unusual for applications handling large sums of money to be running on these systems and so securing them correctly can be very important.

Don’t be intimidated by AS/400

- The retro-cool, text-only interface might look obscure but it can be navigated without much difficulty.
- Mainframes have a reputation for being difficult or obscure, but AS/400 is reasonably easy to understand (and also doesn’t really count as a mainframe).



What is AS/400?

- IBM AS/400 has undergone multiple name changes.
- Large numbers were sold and are still in use.
- It is a ‘minicomputer’ system – in this context ‘mini’ means the size of a fridge.
- It was first developed in the late 1980s, modern and innovative (for the time), aimed at medium-sized businesses.

The Changing Names of AS/400

- Since its introduction, the system has undergone multiple name changes:
  1. AS/400
  2. iSeries
  3. System i
  4. Power Systems
- The name changes don't seem to have stopped people from referring to it as AS/400 (AS400).

Uses of AS/400

- Half a million models had been shipped by 1997.
- Typically used for ERP, supply chain management, and financial/banking applications.
- I am yet to see a company using the web server or email server (both pitched as selling points when it came out).

Design Concepts

- At one time the system was intended to provide companies with a powerful server to run back-office applications, along with email, FTP, and web server facilities.
- The original intention was to provide a unified set of core systems that was easy to manage, with a single user account to access the applications.

What Does AS/400 Look Like?

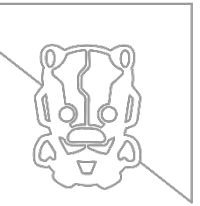
- It has a classic text-based interface, that looks like this:

```
MAIN                          IBM i Main Menu
                                                          System:
Select one of the following:

     1. User tasks
     2. Office tasks
     3. General system tasks
     4. Files, libraries, and folders
     5. Programming
     6. Communications
     7. Define or change the system
     8. Problem handling
     9. Display a menu
    10. Information Assistant options
    11. IBM i Access tasks

    90. Sign off

Selection or command
===>

F3=Exit    F4=Prompt    F9=Retrieve    F12=Cancel    F13=Information Assistant
F23=Set initial menu
(C) COPYRIGHT IBM CORP. 1980, 2009.
 ONLINE                                    M  20,7
```

An Additional Benefit of AS/400 Testing

- There is lots of coloured text on a black background so your testing will look like Hollywood movie hacking.

Why is AS/400 Still in Use?



- One very frequent question when people first see AS/400 applications in operation, is “Why hasn’t this been replaced?”
- These systems are very stable, generally perform useful or vital functions, and replacement of minicomputers or mainframes is expensive and non-trivial.

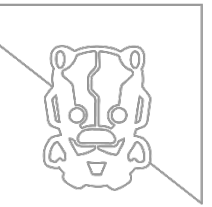
AS/400 Terminology

- Some terms may seem unfamiliar.
- Terms that do seem familiar may have a different meaning than the one you expected.

AS/400 Terminology

- OS/400 (Later renamed IBM i)
  - The AS/400 operating system. It's common for people to use ‘AS/400’ (or iSeries) to refer to both hardware and software.
- Integrated File System
  - The integrated file system (IFS) allows applications running on other file systems (PC, Linux, etc.) to access data stored on the AS/400. The IFS integrates all file systems on the AS/400 under a single interface with a single set of rules.
- Objects
  - Objects are an underlying system design concept for AS/400. Objects include data files, user profiles, job queues, message queues, print queues, compiled programs, text documents, menus, etc. Objects are categorized by type, allowing the user to specify what type of objects are required for a given task.
- Libraries
  - A library is an AS/400 object that is used to locate other AS/400 objects in the integrated database.

AS/400 Terminology



- Physical Files
  - A physical file record has a fixed set of fields. Each field can have variable lengths. The physical file record consists of field descriptions and data.
- Logical Files
  - Logical files allow a user to access data in different format from associated physical files. The logical file contains no data record, just a mapping to a data record in a physical file.
- Collections
  - A collection is a grouping of related SQL objects. This is the SQL equivalent to a Library in the native interface.
- Integrated Database
  - The AS/400 contains a relational database called DB2/400. It is literally integrated at system level. Any other databases that are used would run on top of the operating system.

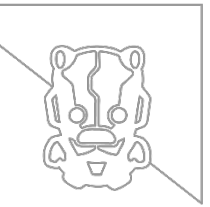
Time to Get Started

- Now that we've covered the baseline knowledge, we can start hacking…

Methodology

- The work can be done following a reasonably standard methodology:
  - Scanning & enumeration
  - Exploitation & access
  - Post-exploitation

Tool Requirements

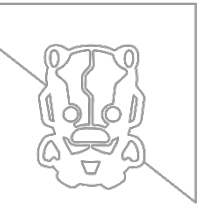


- Nmap
  - Scanning AS/400 is first step - Nmap is very helpful for service enumeration on a system that has so many services
- Nessus
  - As above Nessus provides further help with system enumeration and identifying potential issues, but caveats apply… It can return some special-case false positives, and can impact the system being scanned
- Wireshark
  - Useful for direct examination of traffic
- IBM iAccess
  - Improved access to AS/400 terminal, with GUI for filesystem and databases
  - If you are unable to obtain a copy it is possible to use telnet or this free Java 5250 terminal client: http://tn5250j.org/
- Hack400
  - The essential AS/400 test tool, useful for reviewing system configuration, username enumeration, and privilege escalation

Enumeration

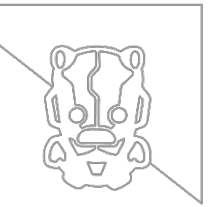
- As with any assignment, we begin with enumeration, in order to determine next steps.
- Initial Scanning and Enumeration:
  - As for any server, a configuration review can reveal lots of issues
  - Some common or useful system commands will be discussed on the following slides
  - Scanning with Nmap – in a default out-of-the-box configuration you will see a lot of open ports and see a few things that may look dubious, such as mail servers and FTP servers
  - Scanning with Nessus – you may see both real vulnerabilities and false positives highlighted in a Nessus scan of a typical machine

Nmap



- Scanning with Nmap, is a good starting point.
- A non-hardened system will usually have FTP, telnet, POP3, and multiple web servers in the scan results.
- Identifying these services will help us to determine how close the system is to its default state, and provide a list of potential ingress points.

Nmap



- The Nmap scan should cover the full port range (TCP and UDP).
- `nmap -Pn -vv -sSV -p 0-65535 -oA tcp_scan [10.1.1.1]`
- `nmap -Pn -vv -sUV -p 0-2000 -oA udp_scan [10.1.1.1]`
- These scans will typically bring back a large range of results that we'll discuss later.
- (the number of open ports may surprise someone who is used to 'normal' systems)

Nessus

- Nessus and Nmap are both useful, but be careful!!
- You may see both real vulnerabilities and false positives highlighted in a Nessus scan of a typical machine
- Important – There is a possibility of excessive resource consumption resulting from a port scan of AS/400. I have never seen this occur, but be careful and keep an eye on things

What Do I Do With the Scan Results?

- The Nmap and Nessus scans provide information on:
  - Services that can be used for username enumeration
  - Potential issues for the various services
  - A general indication of the amount of hardening that may have been carried out

Results Analysis

Scanning with Nmap, against a default out-of-the-box configuration, you will see a lot of open ports and see a few things that may look dubious, such as mail servers and FTP servers.

```
Not shown: 65490 closed tcp ports (reset)
PORT      STATE SERVICE              REASON         VERSION
21/tcp    open  ftp                  syn-ack ttl 62 IBM OS/400 FTPd
23/tcp    open  telnet               syn-ack ttl 62 IBM OS/400 telnetd
25/tcp    open  smtp                 syn-ack ttl 62 i5/OS V5R4M0 or OS/400 smtpd
80/tcp    open  http                 syn-ack ttl 62 Apache httpd
110/tcp   open  pop3                 syn-ack ttl 62 qpopper pop3d
137/tcp   open  netbios-ns?          syn-ack ttl 62
139/tcp   open  netbios-ssn?         syn-ack ttl 62
397/tcp   open  anynet-sna           syn-ack ttl 62 AnyNet SNA
427/tcp   open  svrloc?              syn-ack ttl 62
445/tcp   open  microsoft-ds         syn-ack ttl 62
446/tcp   open  drda                 syn-ack ttl 62 IBM DRDA
447/tcp   open  drda                 syn-ack ttl 62 IBM DRDA
448/tcp   open  ddm-ssl?             syn-ack ttl 62
449/tcp   open  as-servermap         syn-ack ttl 62 IBM OS/400 as-servermapd
515/tcp   open  printer              syn-ack ttl 62
657/tcp   open  rmc?                 syn-ack ttl 62
992/tcp   open  tcpwrapped           syn-ack ttl 62
1364/tcp  open  ndm-server?          syn-ack ttl 62
2001/tcp  open  http                 syn-ack ttl 62 Apache httpd
2002/tcp  open  globe?               syn-ack ttl 62
2008/tcp  open  conf?                syn-ack ttl 62
2011/tcp  open  raid-cc?             syn-ack ttl 62
2020/tcp  open  http                 syn-ack ttl 62 Apache httpd
2480/tcp  open  powerexchange?       syn-ack ttl 62
4800/tcp  open  iims?                syn-ack ttl 62
5989/tcp  open  ssl/wbem-https?      syn-ack ttl 62
5990/tcp  open  ssl/wbem-exp-https?  syn-ack ttl 62
8470/tcp  open  cisco-avp?           syn-ack ttl 62
8471/tcp  open  pim-port?            syn-ack ttl 62
8472/tcp  open  otv?                 syn-ack ttl 62
8473/tcp  open  vp2p?                syn-ack ttl 62
8474/tcp  open  noteshare?           syn-ack ttl 62
8475/tcp  open  unknown              syn-ack ttl 62
8476/tcp  open  as-signon            syn-ack ttl 62 IBM Client Tools signon
8477/tcp  open  unknown              syn-ack ttl 62
8478/tcp  open  unknown              syn-ack ttl 62
8479/tcp  open  unknown              syn-ack ttl 62
9004/tcp  open  http                 syn-ack ttl 62 Apache httpd
```

Results Analysis

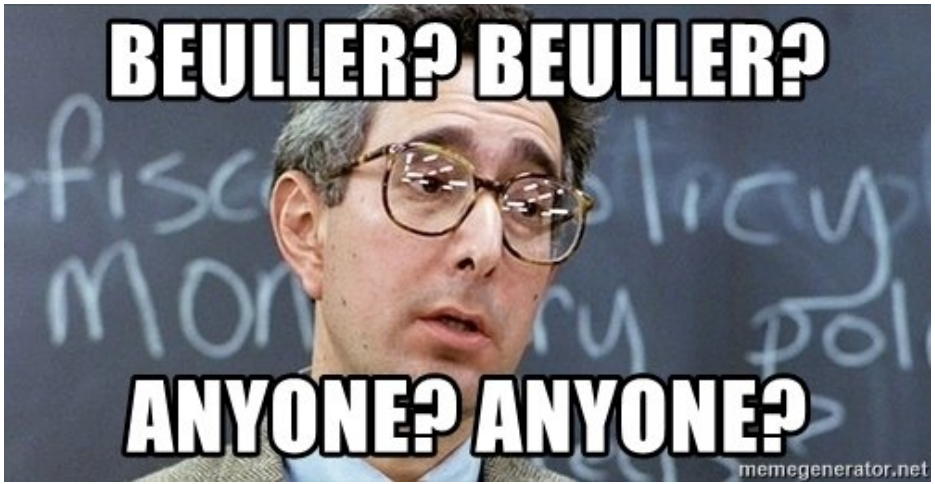
- Making sense of (and abusing) the scan results:
  - Default accounts and passwords
  - User enumeration with telnet and FTP
  - Common Services [FTP, SSH, telnet, SMTP, POP3, web servers, SMB]
  - Note that the Nessus SMB issue is a false positive – no need to worry about the non-issue as typically there will be long list of issues and fixes after these tests
  - Checking if eavesdropping is possible with Wireshark

Web Server Results

- Analysis of Nessus scan results:
  - In addition to the SMB false positive, Nessus will usually provide several other issues, mostly web server related
  - Nessus is likely to identify unsafe ciphers on any web servers on the system – the more common recommendation will usually be to switch off the web server rather than disable weak ciphers
  - Switching off the servers can be done by the sysadmin, although this should be carried out with caution – default use of the ENDTCPSVR command to shut down servers would switch off telnet and require a restart
  - Nessus may report web server vulnerabilities, based on the web server's version number. Many of these will be false positives, relating to issues that only exist for the Windows or Linux version of that server.

Username Enumeration

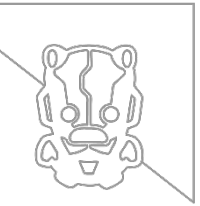
- When looking for usernames we have several things to help us.
- IBM provides a list of default usernames.
- AS/400 applications can help us to avoid randomly trying to brute-force different accounts and to avoid too much guesswork.



Username Enumeration on AS/400

- AS/400 provides each user with a single login, with the same password allowing access to the terminal, FTP, email, and the default web applications.

Default Accounts

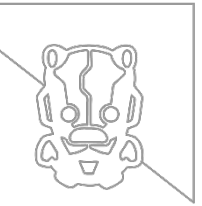


- AS/400 has a number of default accounts.
- The ANZDFTPWD (Analyze Default Password) command can be used to identify default accounts with default passwords.
- Safe Usage: `ANZDFTPWD ACTION(*NONE)`
- Unsafe Usage: `ANZDFTPWD ACTION(*PWDEXP)`
- Living on the edge: `ANZDFTPWD ACTION(*DISABLE)`

Default Accounts

- The following non-exhaustive list of AS/400 default accounts have a password that matches the username:
  - QSECOFR
  - QSYSOPR
  - QPGMR
  - QUSER
  - QSRV
  - QSRVBAS
- There are other IBM system accounts, and a number of lists are available online.

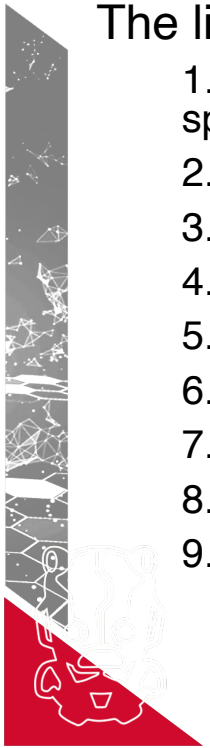
Username Enumeration (telnet, FTP and POP3)



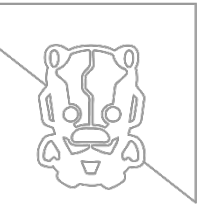
Telnet provides a variety of CPF error codes in its responses for failed logins.

The list below can be used to help with user enumeration:

1. CPF1133 – Value USER NAME is not a valid name (formatting issue such as spaces or invalid characters in the username)
2. CPF1120 – User USERNAME does not exist
3. CPF1107 – Password not correct for user profile
4. CPF1394 – User profile USERNAME cannot sign on
5. CPF1118 – No password associated with user USERNAME
6. CPF1109 – Not authorized to subsystem
7. CPF1110 – Not authorized to workstation
8. CPF1116 – Next not valid sign-on attempt varies off device
9. CPF1392 – Next not valid sign-on disables user profile



Username Enumeration (telnet, FTP and POP3)



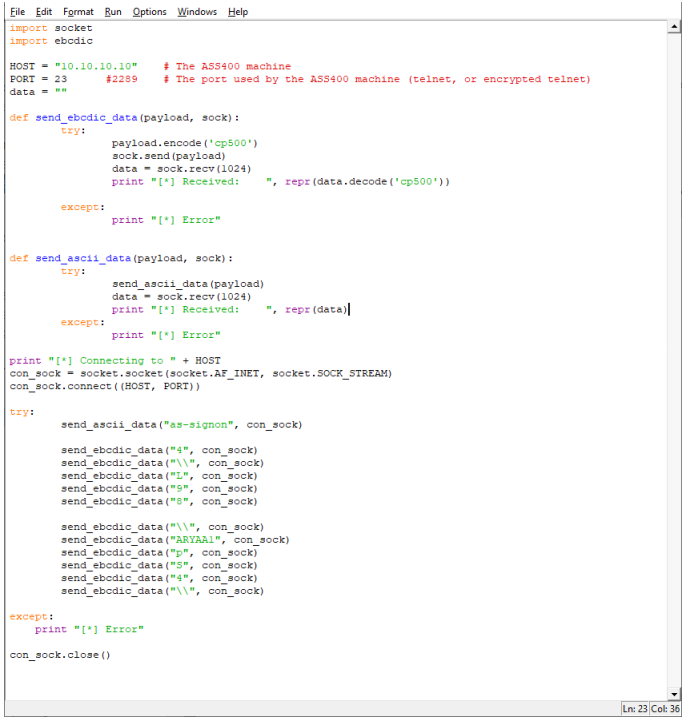
User enumeration with POP3:

```
+OK POP3 server ready
USER test
+OK POP3 server ready
PASS pass1234
-ERR Logon attempt invalid CPF2204
```

Error code CPF2204 indicates that the account does not exist

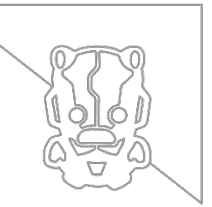
Username Enumeration (telnet, FTP and POP3)

In the absence of Hack400 (more on that later), it's possible to enumerate users with a relatively simple Python Script.



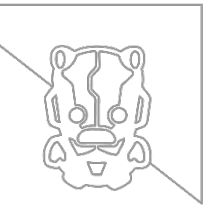
```
File  Edit  Format  Run  Options  Windows  Help
import socket
import ebcdic

HOST = "10.10.10.10"    # The AS400 machine
PORT = 23       #2289   # The port used by the AS400 machine (telnet, or encrypted telnet)
data = ""

def send_ebcdic_data(payload, sock):
        try:
                payload.encode('cp500')
                sock.send(payload)
                data = sock.recv(1024)
                print "[*] Received:    ", repr(data.decode('cp500'))

        except:
                print "[*] Error"


def send_ascii_data(payload, sock):
        try:
                send_ascii_data(payload)
                data = sock.recv(1024)
                print "[*] Received:    ", repr(data)
        except:
                print "[*] Error"

print "[*] Connecting to " + HOST
con_sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
con_sock.connect((HOST, PORT))

try:
        send_ascii_data("as-signon", con_sock)

        send_ebcdic_data("4", con_sock)
        send_ebcdic_data("\\", con_sock)
        send_ebcdic_data("L", con_sock)
        send_ebcdic_data("9", con_sock)
        send_ebcdic_data("8", con_sock)

        send_ebcdic_data("\\", con_sock)
        send_ebcdic_data("ARYAA1", con_sock)
        send_ebcdic_data("p", con_sock)
        send_ebcdic_data("5", con_sock)
        send_ebcdic_data("4", con_sock)
        send_ebcdic_data("\\", con_sock)

except:
    print "[*] Error"

con_sock.close()
```

From Enumeration to Exploitation

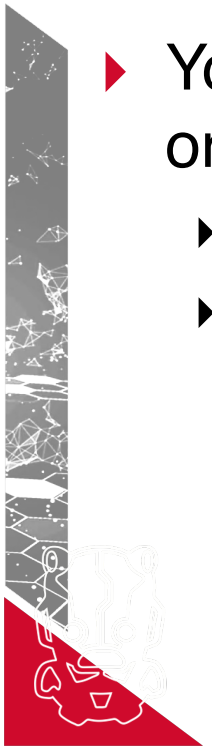


- The usernames that have been gathered can be used for brute-forcing (again with Python scripts) if you are *sure* there is no login limit.
- In the event that there is a login limit, password-guessing attacks can still be attempted within safe limits (it's not *that* unusual to find instances of username=password).

Wireshark



- This is useful for inspecting network traffic.
- You may find it is useful to monitor network traffic in order to:
  - View login credentials
  - View transactions with sensitive data (e.g. financial data, personal details)

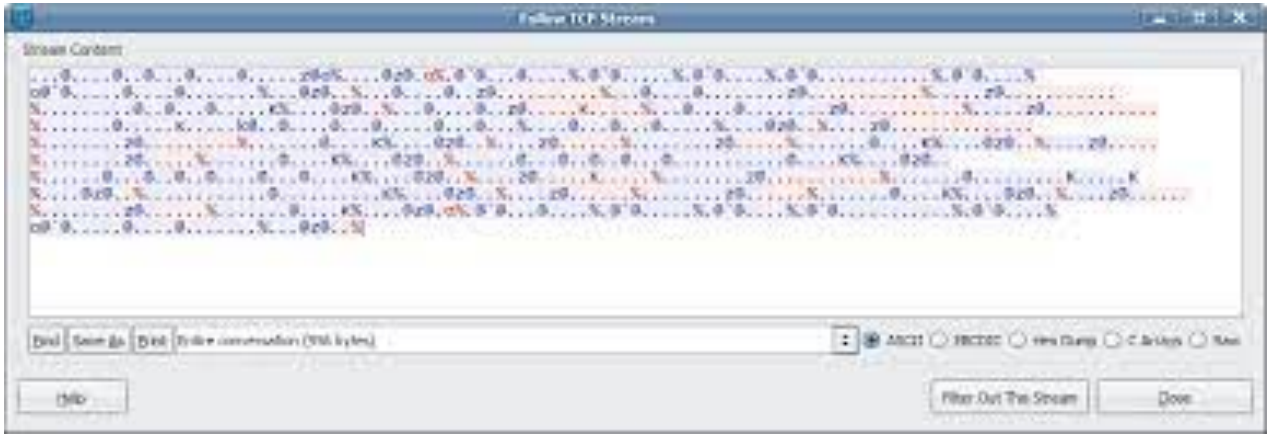


Wireshark

- At first the text may seem unreadable. It's important to note that what you're seeing may not be down to encryption as AS/400 uses EBCDIC encoding.

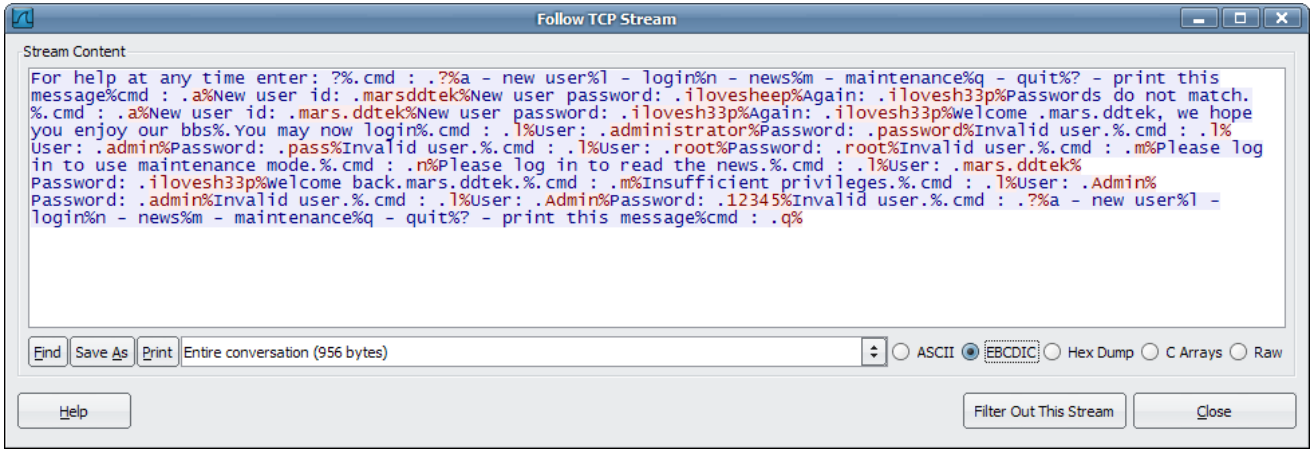
Wireshark

- With ASCII encoding the traffic might look like it's encrypted.

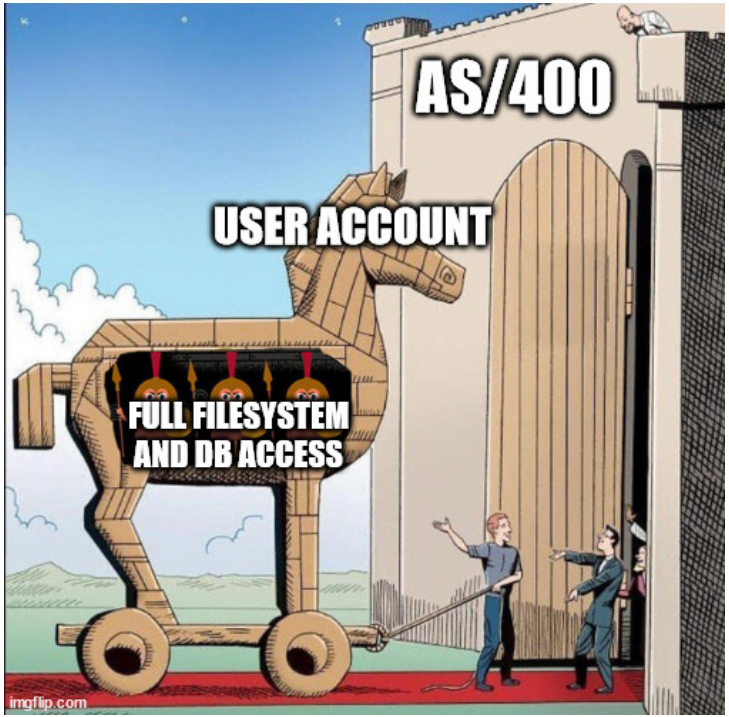


Wireshark

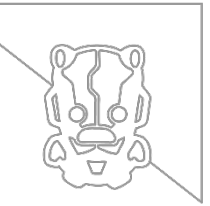
- Use EBCDIC instead of the default ASCII to check whether traffic is encrypted or not.



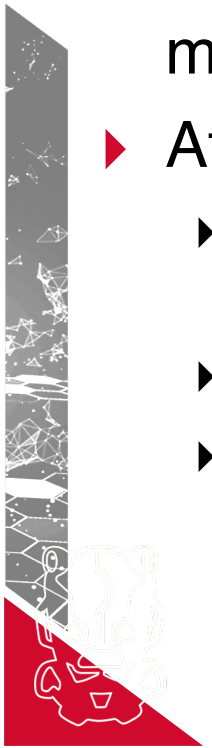
Integrated File System and the Single Login



Integrated File System

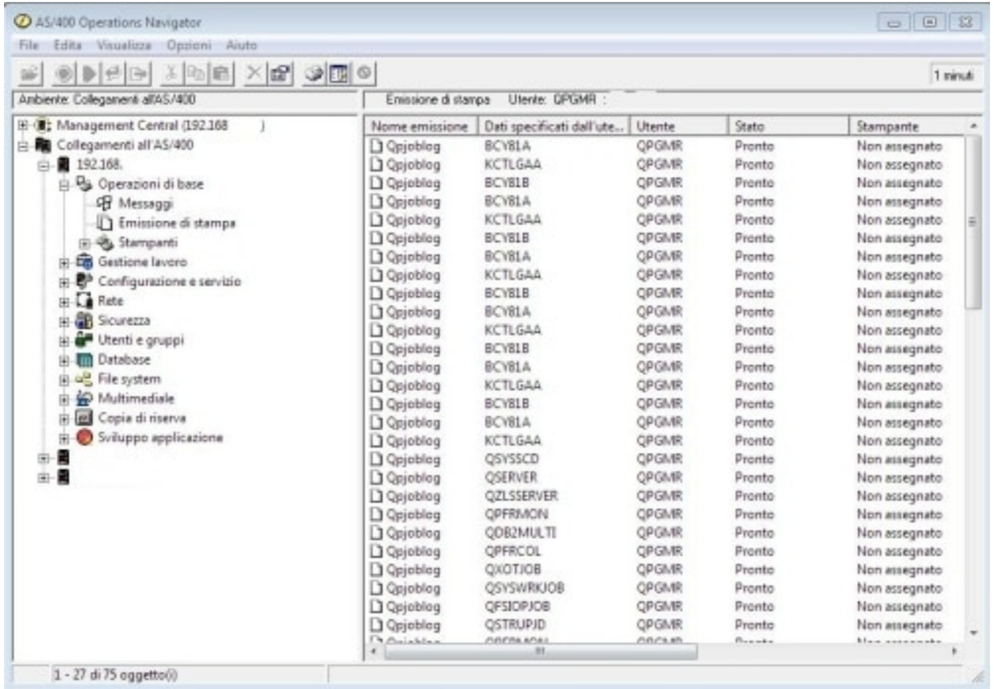


- The single login per user provided easy system management when first introduced.
- At the time of the system's design:
  - Mainframes (and minicomputers) were secured with a locked door
  - PCs were typically sold with no network card
  - Packet-sniffing tools were outside the skillset/understanding of regular users



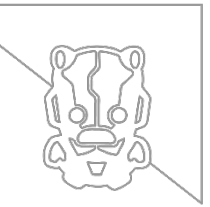
Integrated File System

- Use iAccess to browse the filesystem via the GUI.



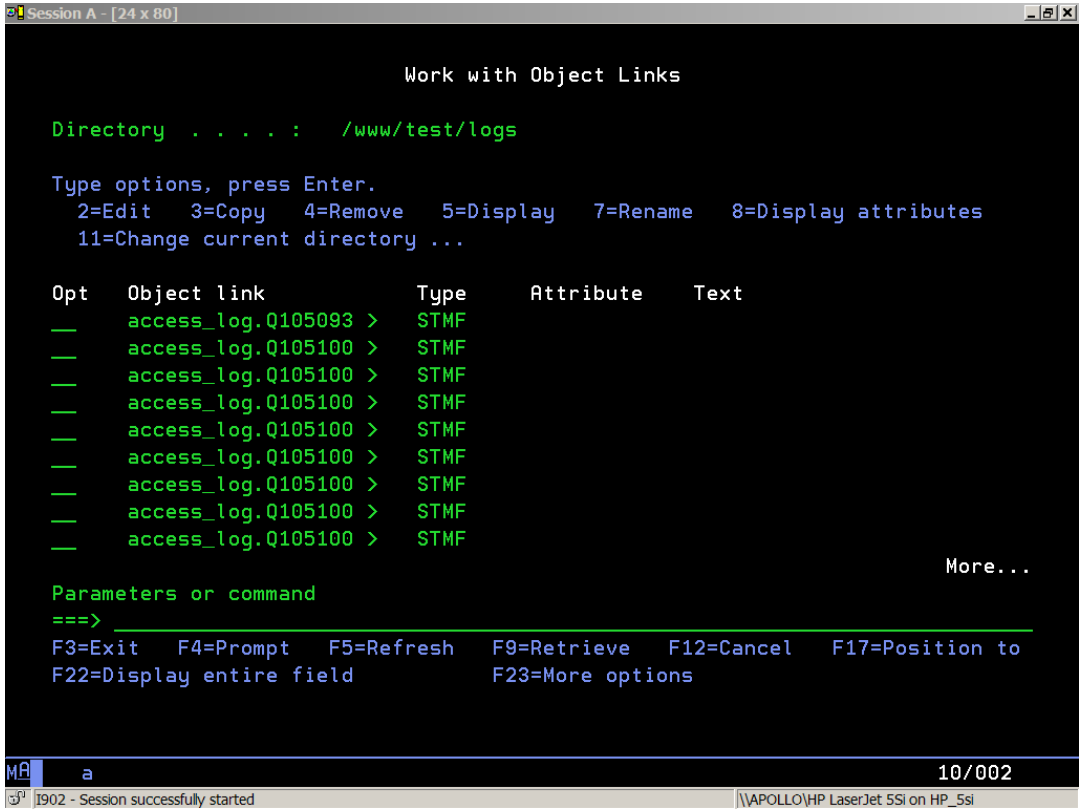
IOActive

Integrated File System

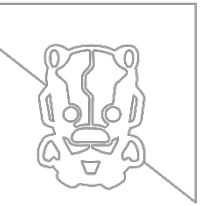


- Use the QSH command to browse the filesystem from the terminal.
- In any situation where the root folder has ‘relaxed’ permissions, all child folders will inherit these from the root.
- This is a permissive, but common, set of permissions:
  - `DTAAUT(*RWX) OBJAUT(*ALL)`
- Note that altering root permissions can break things it may be safer to assign custom settings to sensitive folders.

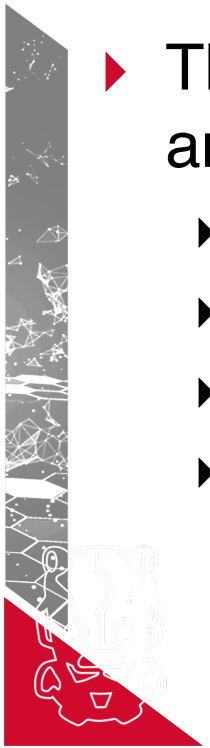
Integrated File System



Hack400

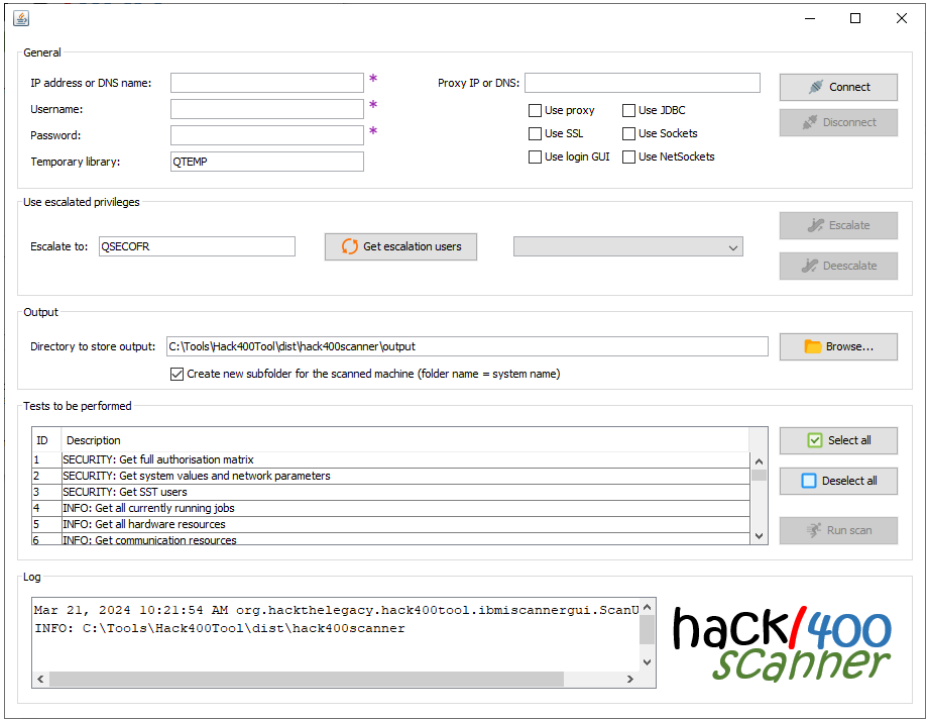


- The Rolls Royce of AS/400 testing tools.
- This tool lists weak permissions, available users, etc. and the results can be used for further mischief:
  - User enumeration
  - Privilege escalation
  - Password cracking
  - Exploiting applications



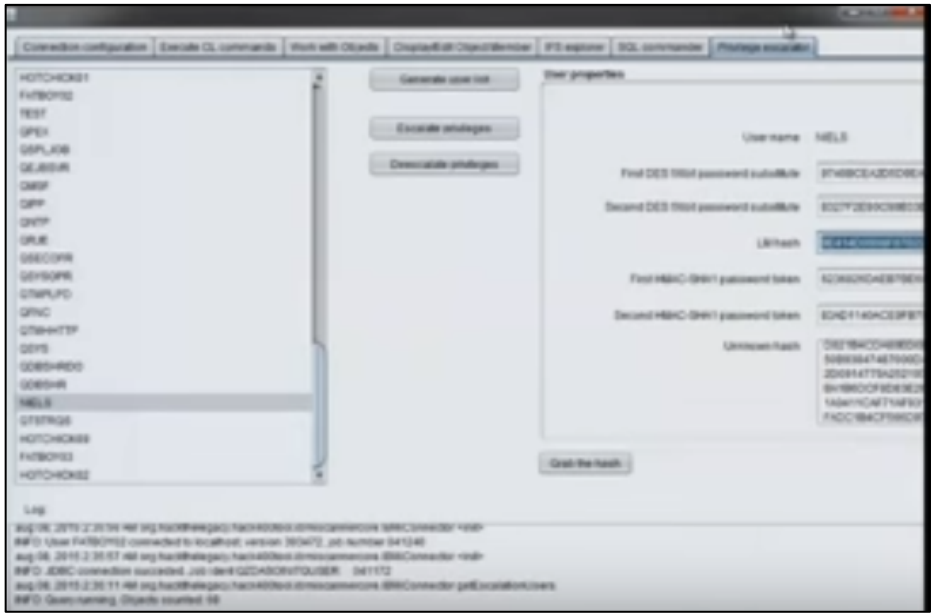
Hack400 – Username Enumeration and Privilege Escalation

- Hack400 Scanner can list users and escalate privileges



Hack400 – Username Enumeration and Privilege Escalation

- Hack400 Exploiter can grab hashes when authenticated as a user with sufficient privileges.



Hack400 – Hashes

- The hashes from Hack400 Exploiter can be useful in multiple ways:
  - Cracked hashes can be used to escalate privileges, and to investigate password hygiene (e.g. are privileged accounts all using same password, how many users have the username as a password, etc.)
  - ADSelfService Plus allows AS/400 to sync with Active Directory so the collected LM hashes may be useful in a red team exercise, or in the scope of a broader exercise, if this is allowed as part of the test exercise.

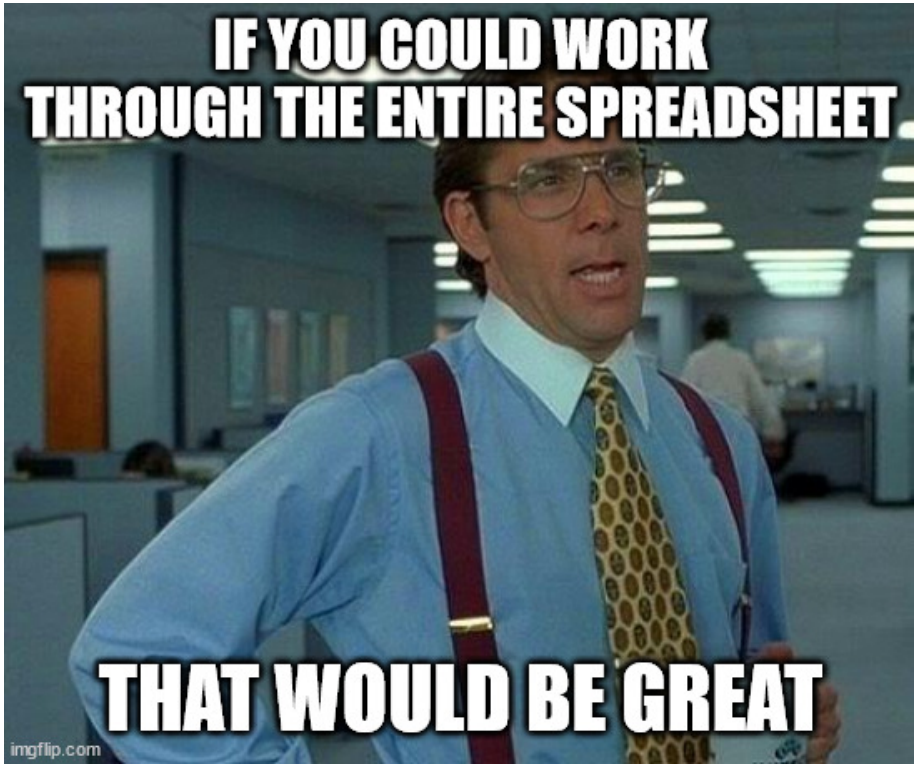
Hack400 Auditor

- Checking Configuration with Hack400

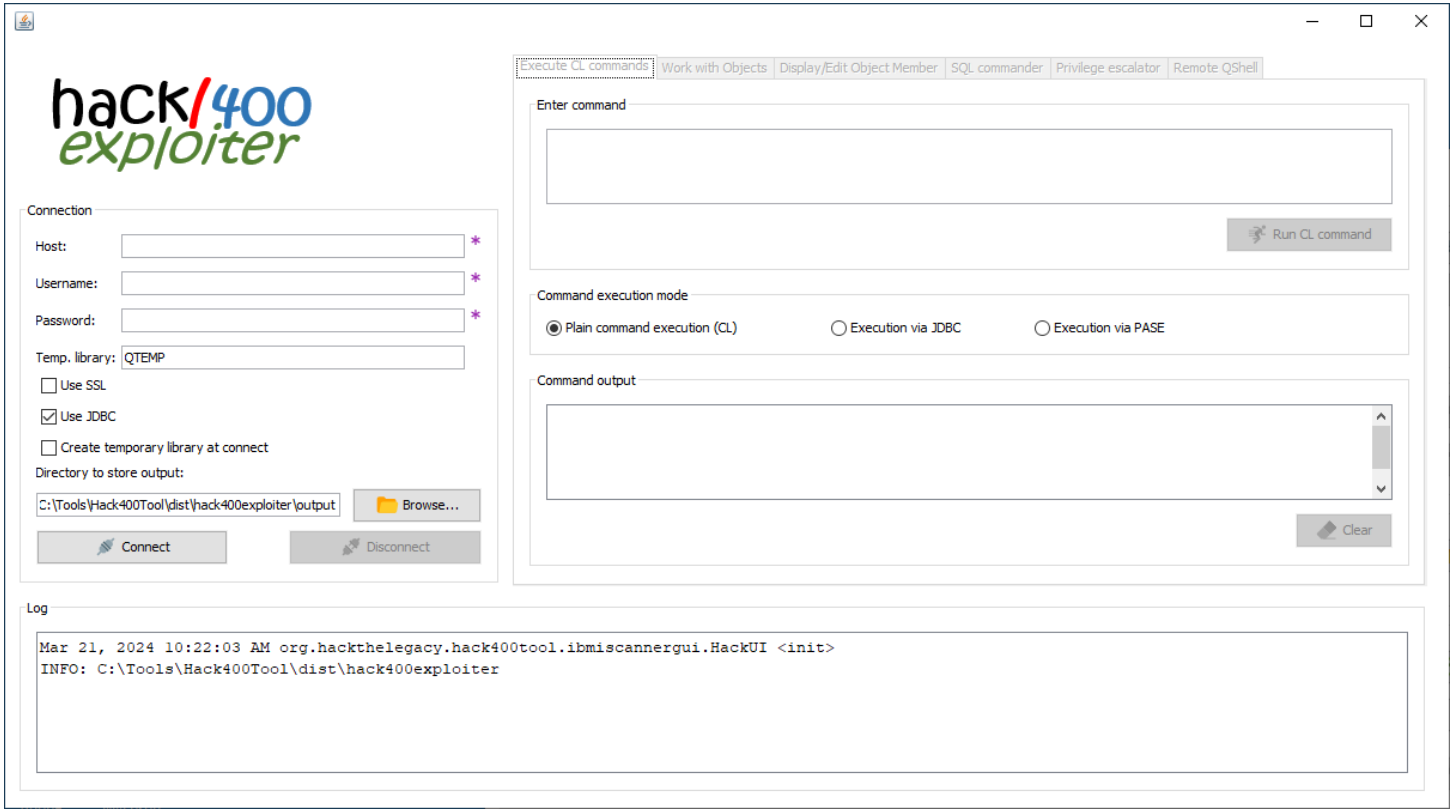
Hack400 Auditor

- The Auditor can be used if your account has sufficient privileges.
- It outputs a spreadsheet listing any unsafe settings:
  - Unlimited login attempts
  - No password complexity
  - No terminal encryption
  - etc.

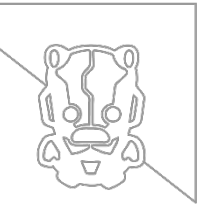
Hack400 Auditor



Exploiting Applications

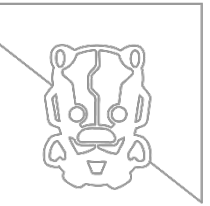


Exploiting Applications



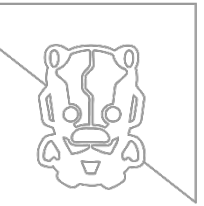
- There are a few tricks, mostly relying on the permissions set for Objects and Profiles.
- These can be explored using either Hack400 or the by accessing the AS/400 command line with iAccess or telnet.

Privilege Escalation with QSYSGETPH



- Privilege escalation can be achieved via insecure permissions on profile objects, using an attack to grant ALLOBJ permissions to any AS/400 user.
- User profiles with the *USE attribute for other accounts are able to call the QSYGETPH API without a password in order to run jobs using the identity of that user.
- In order for an account to be hijacked, one of the following conditions must be met:
  - The ‘Authority’ must be set to *USE or *ALL
  - User defined access must have an ‘X’ in the ‘*Opr*’ and ‘*Execute*’ columns

How to Find a Target



- The following command can be run from Hack400, or directly from the command line to identify profiles with a PUBLIC authority not set to EXCLUDE:
- `PRTPUBAUT OBJTYPE(*USRPRF)`
- Running this from Hack400 with a suitably privileged account, you can get your results, nicely formatted, in the same window.

How to Find a Target

- The output will be in a form resembling this example output:

Figure 1..Output of command PRTPUBAUT OBJTYPE(*USRPRF)

```
                         Publicly Authorized Objects (Full Report)                 Page     1
5761SS1 V6R1M0  080215                                              SECUREMYI  09/23/14  17:23:45 CDT
 Object type  . . . . . . . . . . :   *USRPRF
 Specified library  . . . . . . . :   QSYS

                          ASP                        Auth                    ----------Object----------
  Library     Object      Device     Owner           List    Authority  Opr  Mgt  Exist  Alter  Ref
  QSYS        ARRCFRX     *SYSBAS    ADDSECO                 *ALL       X    X    X      X      X
  QSYS        AWWGROUP    *SYSBAS    QSECOFR                 *USE       X
  QSYS        MYSECOFR    *SYSBAS    QSYS                    *ALL       X    X    X      X      X
  QSYS        RTVPGMR     *SYSBAS    MIKETL                  *ALL       X    X    X      X      X
  QSYS        QDBSHR      *SYSBAS    QSYS                    USER DEF
  QSYS        QDBSHRDO    *SYSBAS    QSYS                    USER DEF
  QSYS        QSECOFR     *SYSBAS    QSYS                    *ALL       X    X    X      X      X
  QSYS        QTMPLPD     *SYSBAS    QSYS                    USER DEF   X
  QSYS        XXXFER      *SYSBAS    QSECOFR                 *CHANGE    X
```

- Ref: https://www.securemyi.com/nl/articles/icanbeyou.html

Exploiting Applications

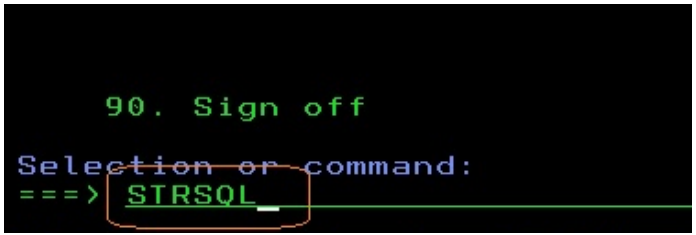
- The escalated privileges obtained in the previous step can be abused in multiple ways:
- Directly against the system:
  - Access sensitive or restricted databases
  - Obtain user hashes for cracking
  - Execute commands in the AS/400 shell
- Against Applications:
  - Different user permissions may be needed to carry out different actions in an application – for a fintech system this may allow transfer of funds, etc.

Exploiting Applications

- A good understanding of the application and processes can be helpful and rewarding.
- In previous tests I've encountered situations where the amount of money that could be stolen was restricted only by the size of the input field.

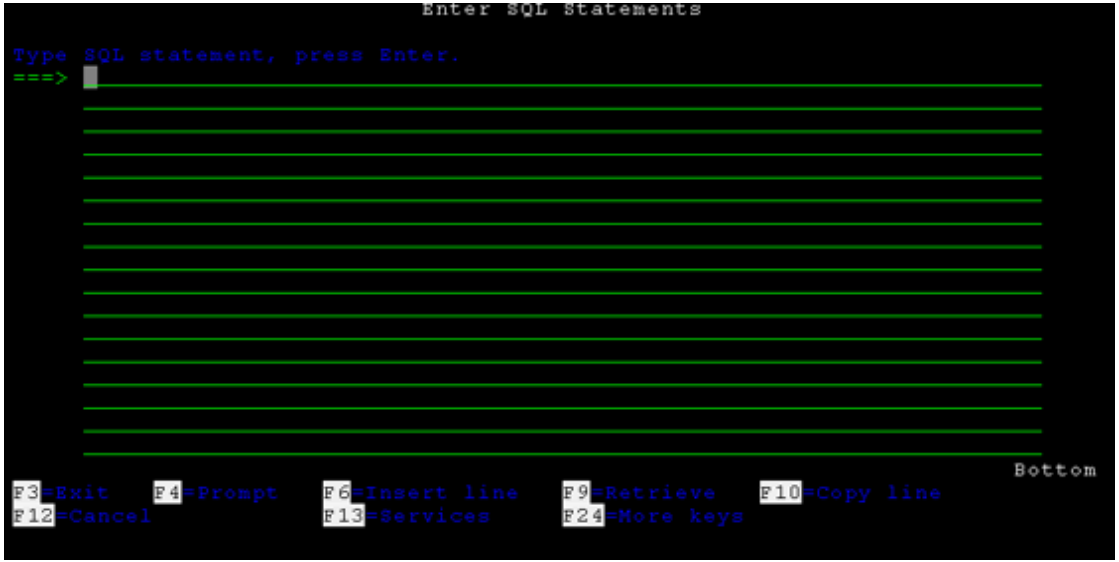
Exploiting Applications – Direct Database Queries

- Attacks can also be carried out by interacting directly with DB2.
- Use the STRSQL command to launch the interface.

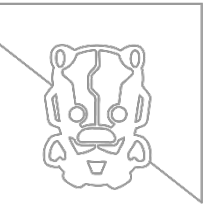


Exploiting Applications – Direct Database Queries

- With direct access to DB2, we can directly manipulate objects.
- This can free us from application-level access controls.



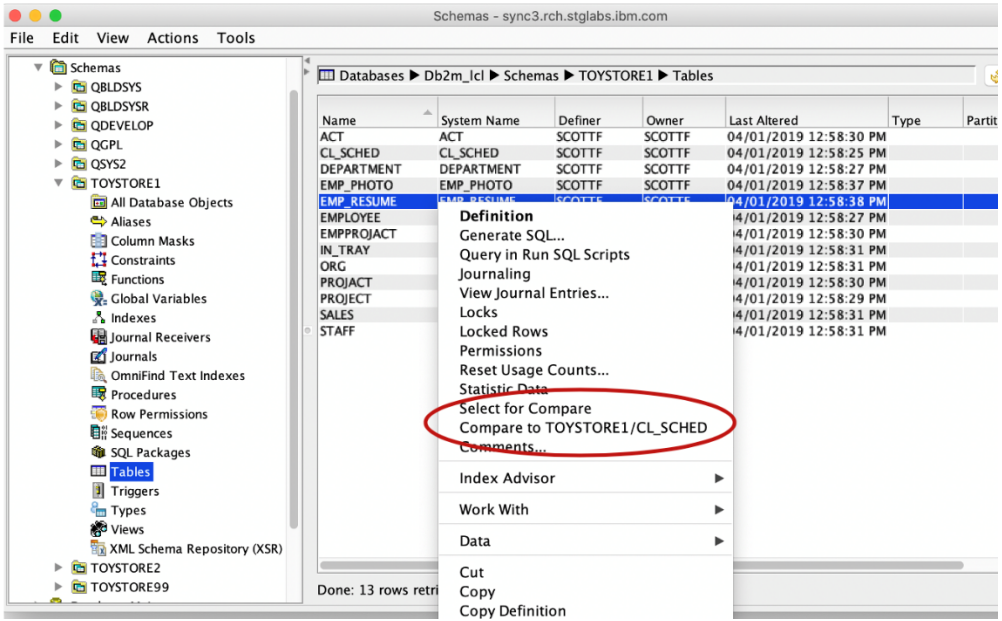
Abusing the Database



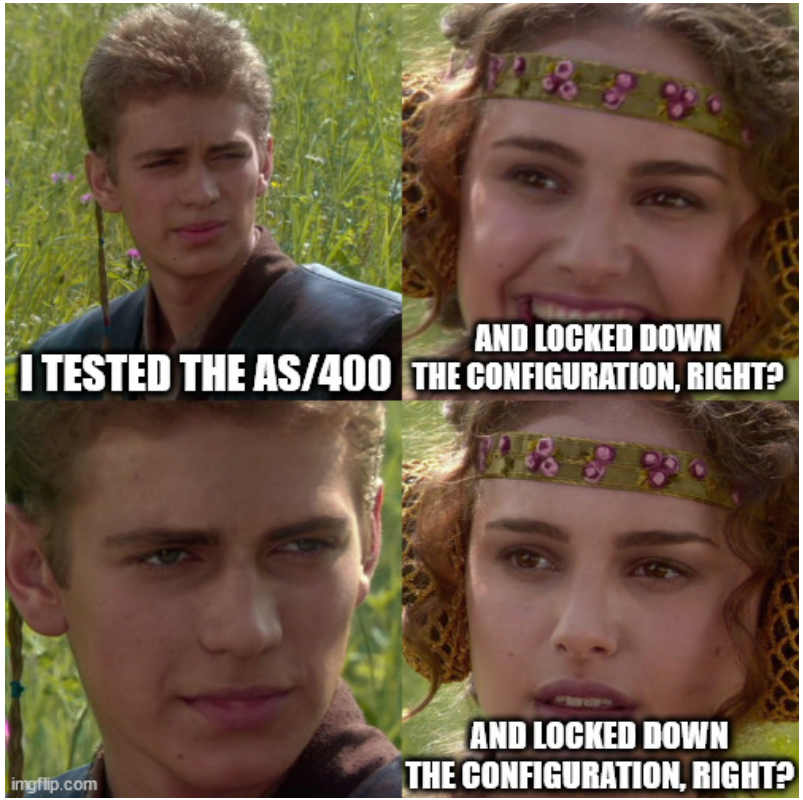
- We can use database access to find fields where passwords could be stored:
- `SELECT column_name,table_name FROM syscolumns WHERE column_name LIKE '%PWD%'`
- From these details we can obtain passwords or hashes:
- `SELECT * FROM tablename_from_results`
- Alternatively, applications may be storing sensitive data and we may be able to influence application behaviour in a similar manner to our privilege escalation example.

Navigating the Databases

- Our old friend iAccess also provides a GUI to access the databases.



Mitigation


I TESTED THE AS/400
AND LOCKED DOWN THE CONFIGURATION, RIGHT?
AND LOCKED DOWN THE CONFIGURATION, RIGHT?
imgflip.com

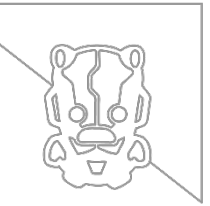
Mitigation

- Terminal encryption
- User Accounts:
  - Legacy accounts
  - Default accounts
  - Weak passwords
- Privilege Escalation
  - Object permissions
  - Database permissions
- Unused Services:
  - FTP
  - Web server
  - Email server
- Application Controls
  - Restricting database permissions
  - Segregating development and production

Terminal Encryption

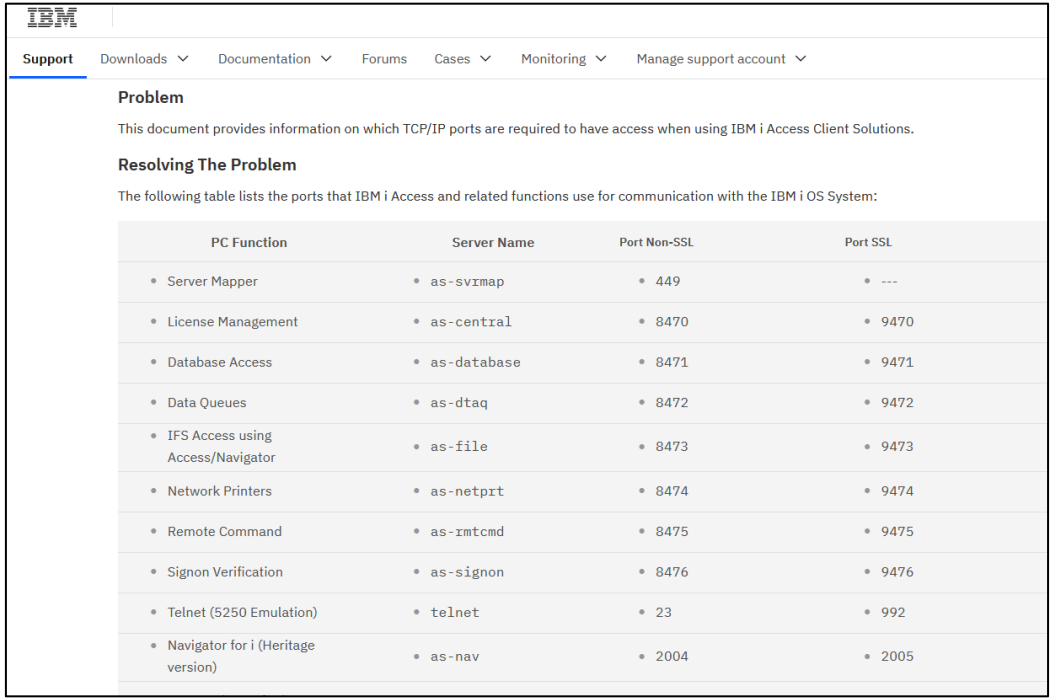
- Terminal encryption can be enabled and uses TCP port 992.
- It offers effective protection from packet sniffing for these systems.
- As a caveat, it's important to test all of these fixes in development, prior to production implementation.

Service Encryption



- IBM provides details on encrypting the other services.
- Note that for each service a different port exists for the encrypted version, which may impact dependent systems.

Service Encryption



IBM

Support | Downloads | Documentation | Forums | Cases | Monitoring | Manage support account

Problem

This document provides information on which TCP/IP ports are required to have access when using IBM i Access Client Solutions.

Resolving The Problem

The following table lists the ports that IBM i Access and related functions use for communication with the IBM i OS System:

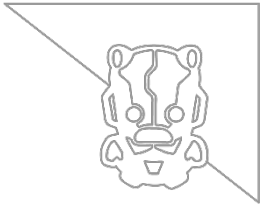
PC Function	Server Name	Port Non-SSL	Port SSL
Server Mapper	as-svrmap	449	---
License Management	as-central	8470	9470
Database Access	as-database	8471	9471
Data Queues	as-dtaq	8472	9472
IFS Access using Access/Navigator	as-file	8473	9473
Network Printers	as-netprt	8474	9474
Remote Command	as-rmtcmd	8475	9475
Signon Verification	as-signon	8476	9476
Telnet (5250 Emulation)	telnet	23	992
Navigator for i (Heritage version)	as-nav	2004	2005

Ref: https://www.ibm.com/support/pages/tcpip-ports-required-ibm-i-access-and-related-functions

User Accounts and Passwords

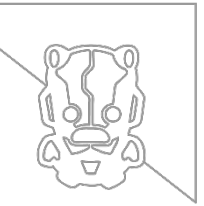
- Always enforce password complexity and limit failed logins!

User Accounts and Passwords



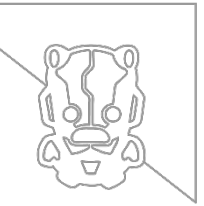
- Enforcing password complexity
  - QPWDRULES can be used to enforce mixed case, minimum length, etc.
- Limiting failed logins
  - Use QMAXSIGN to set a value between 1 and 25
  - *NOMAX indicates an unlimited amount
- Deactivate default accounts where possible, change the password where required

Unused Services

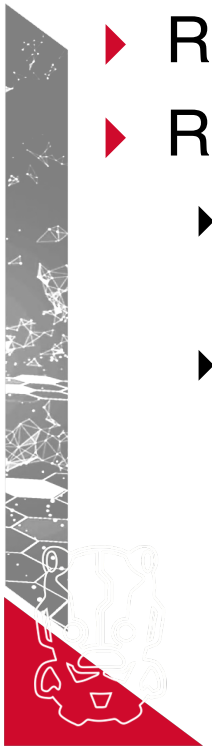


- Investigate whether the services are being used and can be safely switched off:
  - FTP
  - Email
  - Web servers
- Switching off the webservers and other services can be done by the sysadmin.
- This should be carried out with extreme caution – default use of the ENDTCPSVR command to shut down servers would switch off telnet and require a restart.

Privilege Escalation and Application Controls



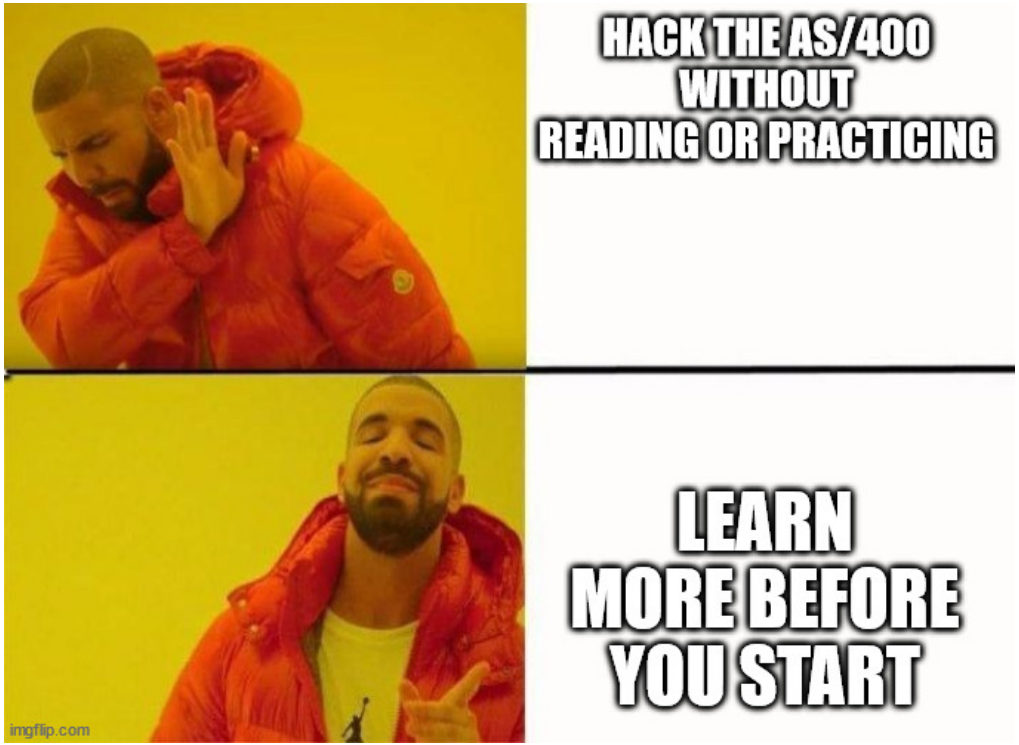
- Review database permissions.
- Restrict command line access for regular users.
- Review user profiles:
  - Ensure the *USE attribute for accounts able to call QSYGETPH API is not enabled without a valid reason
  - ‘Authority’ should not be set to *USE or *ALL, where possible



Conclusion

- AS/400 is a stable and powerful system, with a long history.
- It was designed in the days when the need for network access was enough to protect a system.
- In its default state it is vulnerable to multiple attack techniques and tools.
- A typical test can result in successful account hijack, and privilege escalation issues.

How to Learn More



Practice

- The following site offers an opportunity to practice AS/400 skills:
  - https://pub400.com/
- As this is a web-based system, you won't be able to try out any scanning, or probing of exposed services.
- It's provided as a free service to help people learn – play nicely and don't try to hack it!

References

AS400 for Pen Testers (BlackHat Europe 2006)

https://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Carmel/bh-eu-06-Carmel.pdf

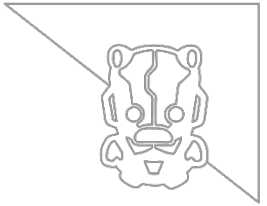
Auditing AS400

https://curbstone.com/iblog/66-beginner-s-guide-auditing-ibm-i-as-400-operating-system

IBM AS400 Security Reference

https://www.ibm.com/support/knowledgecenter/ssw_i5_54/books/sc415302.pdf

References (continued)



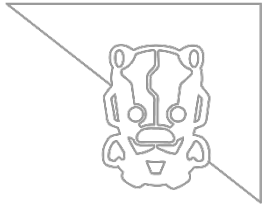
Python Script to Test for AS400 Default Credentials
https://milo2012.wordpress.com/2014/12/07/test-as400-for-default-credentials/

IBM Default Passwords
https://www.ibm.com/support/knowledgecenter/en/SSHLNR_8.1.3/com.ibm.pm.doc/install/admin_passwords_default.htm

SMB Null Session on AS400
http://www-01.ibm.com/support/docview.wss?uid=nas8N1016497

Hack400
https://github.com/hackthelegacy/hack400tool

References (continued)



IBM i for Hackers

https://silentsignal.github.io/BelowMI/

IBM AS/400 Architecture

https://code400.com/forum/forum/iseries-programming-languages/freshers/151778-as400-memory-and-architecture-for-beginners

IBM AS/400 Technical Introduction

https://treasures.scss.tcd.ie/hardware/TCD-SCSS-T.20121208.068/IBM-AS400-technical-introduction.pdf

The IBM Call Stack

https://www.ibm.com/docs/en/i/7.4?topic=overview-call-stack

Any Questions?

Thank You!