Preparing for Mainframe Security Vulnerabilities

SDS MAINFRAME SECURITY

Finding Awareness, Virtuality, Boundaries, and Humanity in Mainframe Security

Reg Harbeck
Chief Strategist
Mainframe Analytics, Ltd.

Approach

- Pre-Computing Security Awareness
- Security Virtualization and Virtuality
- Passive versus Active Approaches
- Mandates
- Dissolving the Boundary Between History and Real-Time
- Reaction, Alerting, Automation, and Platform Choice
- Pervasive Humanity

Pre-Computing Security Awareness

- Trust, Group Identities, Shibboleths, Rumpelstiltskin
- Armor, Walled Cities, Keeps
- Locks, Doors, Guards, Passwords
- Rules, Laws, Sanctions, Enforcers, Legal Systems
- Records: Individuals, Chronicles, Logs

"Those who cannot remember the past are condemned to repeat it."

– George Santayana

Security Virtualization and Virtuality

- Locked doors and server rooms
- Passwords and resource-attached access
- "I was just kidding" vs Military-grade security
- Rings of security?
- Separation of duties; externalization of security
- Secrets, integrity, but not trust
- SMF, SYSLOGs, other LOGs
- Three types…

Passive versus Active Approaches

- Know the past, but it's not enough
- Know patterns, but it's not enough
- Build protection, but it won't stay enough
- Look for what isn't the case, not just "eureka"
- Stay informed on issues and fixes

Mandates!

- Accounting principles
- Professional standards
- Business and stock market laws, rules
- SOX!
- PCI, HIPAA,GLBA, PIPEDA, GDPR, etc.
- Limitations: Moore's Law and Murphy's Law

Dissolving the Boundary Between History and Real-Time

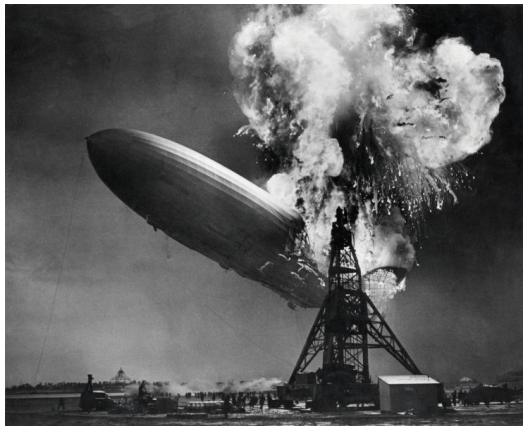
- Real-time notification of alerts
- Intelligence, pattern matching, emergent patterns: AI
- Consolidation of sources
- Selection of sources
- Dynamic adjustment, refinement, curation

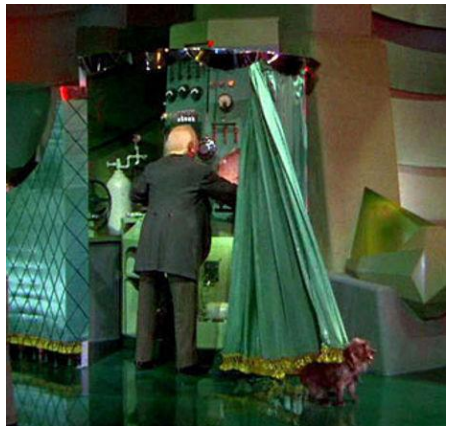
Reaction, Alerting, Automation, and Platform Choice

- "Automate as close as possible to the source" refers to keeping events, reactions, and targets close
- But with multiple platforms, the locus is the business and its people
- Synchronous, on-platform, vs asynchronous, multi-platform
- Flooding of automated actions can become DoS; likewise with alerts
- Build and respond to a four-dimensional picture
- …because it's all about…

Pervasive Humanity

Oh, the humanity!





"Technology out of control" and "The man behind the curtain"

- Humanity: the standard, the target, the meaning, the future
- The shape of things to come orbits the shape of humanity
- The choice of what matters, how to react and proact, always comes home

SDS MAINFRAME SECURITY

Improving Mainframe Security by Addressing Vulnerabilities through SIEM

Colin van der Ross
Sr. Systems Engineer
Software Diversified Services

Agenda

- 2022 Cost of a Data Breach Report - Ponemon
- What is SIEM and why should you integrate the mainframe into your SIEM strategy?
- z/OS security events you should consider sending to your SIEM

2022 Cost of a Data Breach Report: IBM & Ponemon Institute

- Average total cost of a data beach in the US is $9.44 million.
- It took an average of 277 days to identify and contain a data breach.
- Leveraging AI and automation tools saved $3.05 million per breach.
- Implementing a zero trust architecture saved $1 million per breach.
- Extended detection and response (XDR) technologies helped save an average of 29 days in breach response time.

Why integrate z/OS events into SIEM?

- Compliance requirement
  - PCI, SOX, HIPAA, GLBA, etc.
- Mainframes contain sensitive data
  - Target for hackers
  - Large corporations have 70% of data on mainframes
- z/OS is not invulnerable
- If you have a SIEM, include the mainframe!

What is SIEM? – Security Information & Event Management

- Security Management provides a holistic view of an organization's information technology security
- SIEM combines SIM (Security Information Management) and SEM (Security Event Management) functions into ONE Security Management System

Why SIEM?

- SIEM is the core of a defense in-depth strategy
- Attackers leave behind a trace – Logs
- Security events provide insight into…
  - When the event occurred?
  - Why it happened?
  - What happened?

- This portion of the presentation is about security events you may want to consider monitoring using a z/OS SIEM data collection agent.
- The suggestions are by no means exhaustive, my goal is to provide general recommendations as a foundation for a thorough security evaluation and configuration of a z/OS SIEM agent.

Mainframe Vulnerabilities

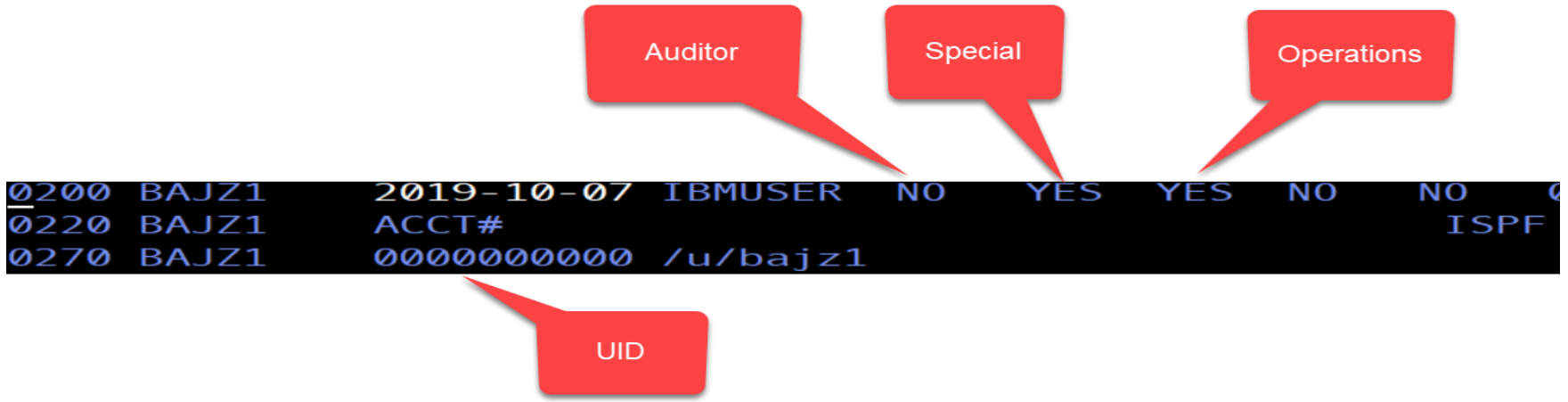
- Sharing credentials with others
- Unauthorized access to APF libraries
- RACF database improperly protected
- Excessive number of super users
- Data set profiles with UACC(READ) or higher
- Data set and resource profiles in WARN mode

Vulnerability: RACF Database Inadequately Protected

- Nefarious user, looking for a way to elevate their security level, issues RVARY command
  - Video 1

Vulnerability: RACF Database Inadequately Protected

- The command works, and the user knows the name of the primary and backup RACF databases
- Knowledge of the RACF database name allows our user to attempt to offload the database using IRRDBU00.
- The output is a flat file image of the RACF database. Using this file, the users with the SPECIAL attribute can be identified
- The passwords are not viewable but, using this information, attempts can be made to guess or crack the passwords of the users with increased authority



Vulnerability: RACF Database Inadequately Protected

- Without the SIEM agent the "unauthorized user" could go on for months unnoticed
- Even if there was no malicious intent, corrective action could be taken immediately to eliminate the vulnerability

Vulnerability: User Increasing Their Own Authority

- User with Special Authority gives themselves Operations Authority
- Perhaps there's some legitimate reason for this but Special and Operations authority on the same user ID is a "dangerous" combination
- The SIEM captures the Security Event

```
<113>Oct 03 14:10:43 SDS1 CEF:0|SDS|VSA|4.2.1|SMF80:13-00 RACF|ALTUSER|9|cat=SMF dvchost=SDS1 cs4Label=CpuSerial cs4=0003BEF72965 dst=172.22.157.10 rt=Oct 03 2022 14:1
0:43 duid=BAJZ1 dproc=BAJZ1 externalId=0187793.0 rawEvent=SMF80:13-00 RACF dpriv=CUSTOMER cs1Label=Rule cs1=BYP:Bypass Rule Checks  reason=Success EvtCd-EvtQual=13-00 s
priv=SPECIAL cs5Label=Reason1 cs5=Chg-to-class-of-prof,SETROPTS-AUDIT(cl)/Profile-chg,AUDITOR-did-SAUDIT,SPECIAL requestClientApplication=TCPS0056 DT006=RACF-Command:Kw
d=SPECIAL%%User=BCVR0   DT038=User/Group-Owner-of-Profile:CUSTOMER DT049=User-on-ACEE:ART ZEIGLER DT053=User-security-Tokens:PORTofEntry:TCPS0056,OwningUser:BAJZ1   ,O
wningGroupId:CUSTOMER
```

Recommendations

- Enable and monitor SMF type 80 security records (written every time a RACF command is executed successfully or not)
- All RACF commands should be monitored, especially those that:
  - Add new user profiles (ADDUSER)
  - Alter user profiles particularly to increase authority (ALTUSER
  - Changes to the password associated with a user profile (PASSWORD)
  - Add new data set profiles or alter existing profiles (ADDSD, ALTDSD)
  - Alter resource access lists (PERMIT)
  - Define or alter general resource profiles (RDEFINE, RALTER)
  - Change or display the status of the RACF database (RVARY)
  - Set RACF options (SETROPTS)

Vulnerability: Password Guessing

- An "unauthorized user" has learned (by offloading the RACF database, guessing, or intuiting) the IDs of privileged accounts
- User attempts to logon by guessing passwords, stopping short of the site-defined limit on invalid passwords
- Legitimate users enter invalid passwords all the time
  - But having multiple invalid attempts on 2 different user IDs from the same terminal within minutes of each other is suspicious

<113>Nov 22 11:34:51 SDS1 CEF:0|SDS|VSA|4.2.1|WTO|ICH408I|9|cat=WTO dvchost=SDS1 cs4Label=CpuSerial cs4=0003BEF72965 dst=172.22.157.10 rt=Nov 22 2022 11:34:51 duid=BCVR1 dproc=SDS1 externalId=0075380.0 reason=ICH408I cs1Label=Rule cs1=MES:ICH408I* cs2Label=message cs2=ICH408I USER(BCVR1) GROUP(CUSTOMER) NAME(COLIN VAN DER ROSS) LOGON/JOB INITIATION - INVALID PASSWORD ENTERED AT TERMINAL O31TCP18

<113>Nov 22 11:34:51 SDS1 CEF:0|SDS|VSA|4.2.1|SMF80:01-01 RACF|JOB-INITIATION/TSO-LOGON/TSO-LOGOFF|9|cat=SMF dvchost=SDS1 cs4Label=CpuSerial cs4=0003BEF72965 dst=172.22.157.10 rt=Nov 22 2022 11:34:51 duid=BCVR1 dproc=BCVR1 externalId=0075379.0 rawEvent=SMF80:01-01 RACF dpriv=CUSTOMER cs1Label=Rule cs1=BYP:Bypass Rule Checks reason=INVALID-PASSWORD EvtCd-EvtQual=01-01 cs2Label=descriptor cs2=VIOLATION cs5Label=Reason1 cs5=RACROUTE-REQ-VERIFY,or-initACEE-failed fileType=VIOLATIO requestClientApplication=O31TCP18 DT049=User-on-ACEE:COLIN VAN DER ROSS DT053=User-security-Tokens:PORTofEntry:O31TCP18,OwningUser:BCVR1 ,OwningGroupId:CUSTOMER

Vulnerability: Password Guessing

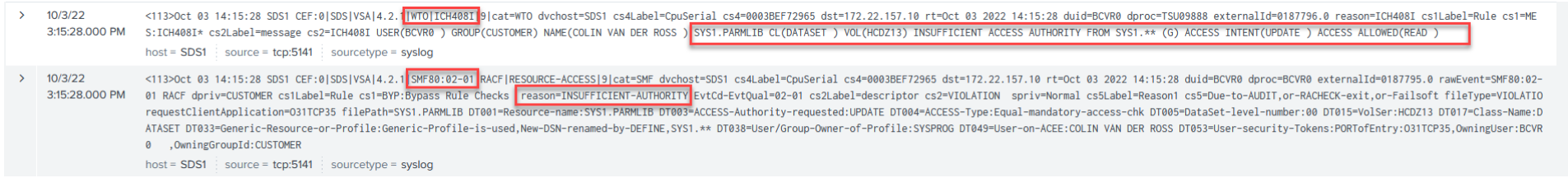
- If you not using Secure TN3270 access to your mainframe, Passwords can be sniffed using an IP Packet Trace
- Here is an example of an IP Packet Trace capturing a TSO LOGON
  - Video 2

Recommendations

- Enable and monitor SMF type 80 records that log invalid passwords
- Alternatively monitor console messages (ICH*, ACF*, TSS*) that log invalid password attempts to the system log
- Pay particular attention to attempts to access privileged user IDs and attempts to access different user IDs from the same terminal or IP address
- Implement secure TN3270 access to the mainframe

Vulnerability: Unauthorized Access to PARMLIB

- In the Security event below the user attempts to update PARMLIB



- Although update is denied, the user has read authority which allows access to a wealth of information including a list of APF authorized libraries and the program properties table that includes programs that can bypass RACF

```
 /*                    OMVS
PPT PGMNAME(BPXVCLNY)                  /* PROGRAM NAME
    CANCEL                             /* CAN BE CANCELLED (DEFAULT)
    KEY(8)                             /* PROTECTION KEY   (DEFAULT)
    NOSWAP                             /* NON-SWAPPABLE
    PRIV                               /* PRIVILEDGED
    SYST                               /* SYSTEM TASK , NOT TIMED
    NOPASS
```

Vulnerability: Unauthorized Access to APF Libraries

- User attempts to edit an APF authorized library and is denied by RACF

```
ICH408I USER(BCVR0    ) GROUP(CUSTOMER) NAME(COLIN VAN DER ROSS   ) 362
  SDSQ.VSA.LOADLIB CL(DATASET ) VOL(SDSSY1)
  INSUFFICIENT ACCESS AUTHORITY
  ACCESS INTENT(READ    )  ACCESS ALLOWED(NONE    )
```

- The SIEM Agent captures the event and forwards it to the SIEM in real-time

<113>Oct 03 14:00:45 SDS1 CEF:0|SDS|VSA|4.2.1|WTO|ICH408I|9|cat=WTO dvchost=SDS1 cs4Label=CpuSerial cs4=0003BEF72965 dst=172.22.157.10 rt=Oct 03 2022 14:00:45 duid=BCVR0 dproc=TSU09888 externalId=0187772.0 reason=ICH408I cs1Label=Rule cs1=MES:ICH408I* cs2Label=message cs2=ICH408I USER(BCVR0) GROUP(CUSTOMER) NAME(COLIN VAN DER ROSS) SDSQ.VSA.LOADLIB CL(DATASET) VOL(SDSSY1) INSUFFICIENT ACCESS AUTHORITY ACCESS INTENT(READ) ACCESS ALLOWED(NONE)

<113>Oct 03 14:00:45 SDS1 CEF:0|SDS|VSA|4.2.1 SMF80:02-01 RACF|RESOURCE-ACCESS|9|cat=SMF dvchost=SDS1 cs4Label=CpuSerial cs4=0003BEF72965 dst=172.22.157.10 rt=Oct 03 2022 14:00:45 duid=BCVR0 dproc=BCVR0 externalId=0187771.0 rawEvent=SMF80:02-01 RACF dpriv=CUSTOMER cs1Label=Rule cs1=APF:SDSQ.VSA.LOADLIB reason=INSUFFICIENT-AUTHORITY EvtCd-EvtQual=02-01 cs2Label=descriptor cs2=VIOLATION spriv=Normal cs5Label=Reason1 cs5=Due-to-AUDIT,or-RACHECK-exit,or-Failsoft fileType=VIOLATIO requestClientApplication=O31TCP35 filePath=SDSQ.VSA.LOADLIB DT001=Resource-name:SDSQ.VSA.LOADLIB DT003=ACCESS-Authority-requested:READ DT004=ACCESS-Type DT005=DataSet-level-number:00 DT015=VolSer:SDSSY1 DT017=Class-Name:DATASET DT038=User/Group-Owner-of-Profile:IBMUSER DT049=User-on-ACEE:COLIN VAN DER ROSS DT053=User-security-Tokens:PORTofEntry:O31TCP35,OwningUser:BCVR0 ,OwningGroupId:CUSTOMER

Vulnerability: Unauthorized Access to APF Libraries

- Our unauthorized user attempts to add a dataset to APF via JCL. This time he is successful

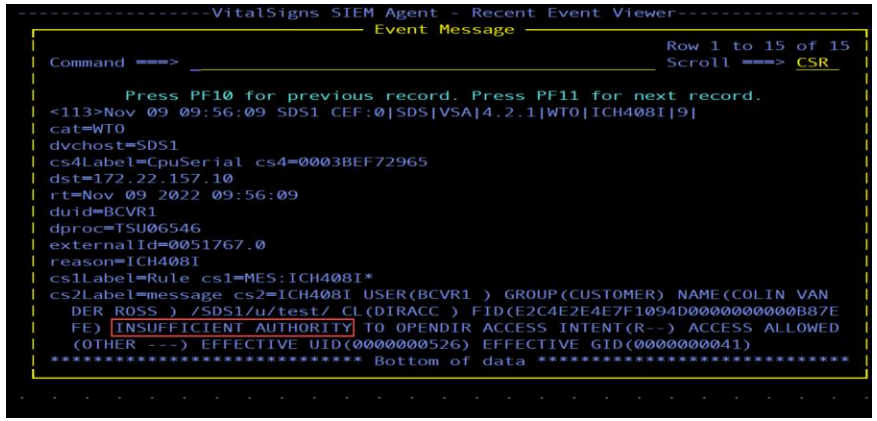
```
14:24:49.94 BCVR0     00000290  SETPROG APF,ADD,DSN=SDSQ.VSA.LOADLIB,VOL=SDSSY1
14:24:49.97 BCVR0     00000090  CSV410I DATA SET SDSQ.VSA.LOADLIB ON VOLUME SDSS
```

```
> <113>Oct 03 13:56:34 SDS1 CEF:0|SDS|VSA|4.2.1|SMF90 APFlist|Add|9|cat=SMF dvchost=SDS1 cs4Label=CpuSerial cs4=0003BEF72965 dst=172.22.157.10 rt=Oct 03 2022 13:56:34 duid=*MASTER* dproc=*MASTER* externalId=0187761.0 rawEvent=S
  MF90 APFlist cs1Label=Rule cs1=APF:* cs6Label=Function cs6=Add filePath=SDSQ.VSA.LOADLIB fileId=SDSSY1 cs3Label=Consol-Sufix cs3=01000021:** cs5Label=How cs5=UPDATE:via-SETPROG-Command|
```

- Now that the unauthorized user has discovered this “back door” he is free to add unauthorized modules to the APF library
- Any additions to APF should be investigated & escalated immediately

Vulnerability: Unauthorized Access to UNIX files

- Our unauthorized user attempts to add a UNIX file but is denied



- Attempts to alter authority using the SU command but is denied and captured by the SIEM Agent

Recommendations

- Enable and monitor type 80 SMF records which can be written for unsuccessful UNIX file access
- Enable and monitor type 80 SMF records which can be written for UNIX command attempts including
  - Check-ACCESS-to-DIRECTORY
  - Check-ACCESS-to-FILE
  - CHAUDIT (Change audit options)
  - KILL
  - SETEGID (Change effective GID)
  - SETEUID (Change effective UID)
  - SETGID (Change of GID)
  - SETUID (Change of UID)
- Enable SMF 109 records (Syslogd)

Vulnerability: Submitting JCL using FTP

- Unauthorized user logs in using FTP
- Then changes file type to JCL

```
 230 BCVR1 is logged on.  Working directory is "BCVR1.".
 Command:
site file=jes
 >>> SITE file=jes
 200 SITE command was accepted
 Command:
put 'bcvr1.colin.jcl(vipsamp)'
 >>> SITE VARrecfm LRECL=80 RECFM=VB BLKSIZE=27920
 200 SITE command was accepted
 >>> PORT 10,31,0,1,68,244
 200 Port request OK.
 >>> STOR 'bcvr1.colin.jcl(vipsamp)'
 ***
```

Vulnerability: Submitting JCL using FTP

- The batch job fails because the attempt to circumvent security did not work

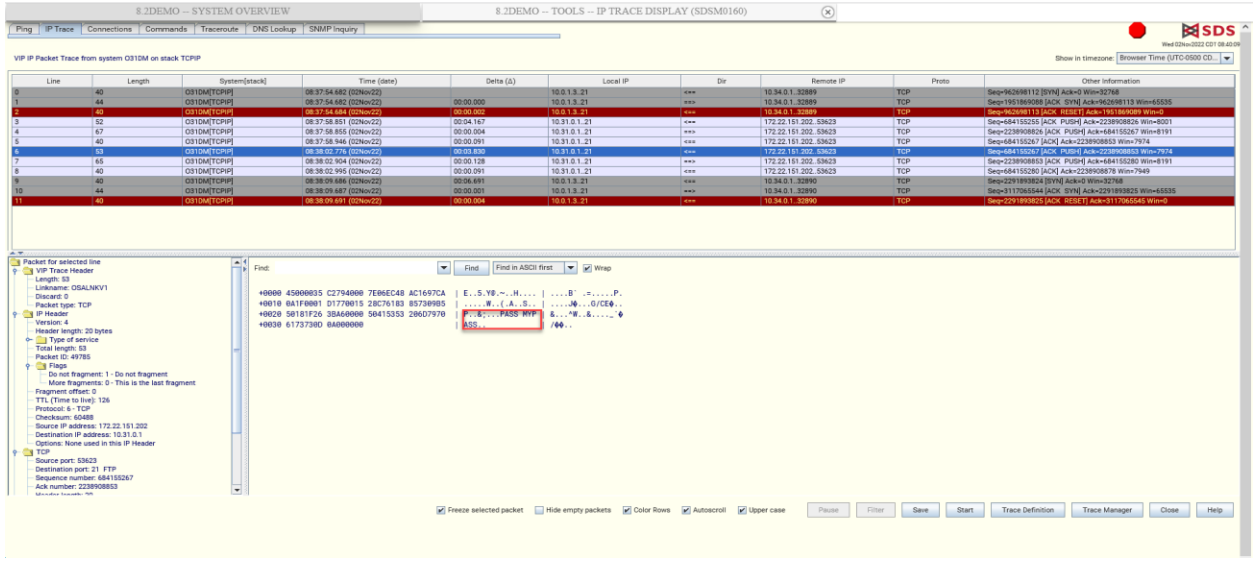
<113>Oct 13 10:56:59 SDS1 CEF:0|SDS|VSA|4.2.1|SMF80:02-01 RACF|RESOURCE-ACCESS|9|cat=SMF dvchost=SDS1 cs4Label=CpuSerial cs4=0003BEF72965 dst=172.22.157.10 rt=Oct 13 2022 10:56:59 duid=BCVR1 dproc=BCVR1 externalId=0000008.0 rawEvent=SMF80:02-01 RACF dpriv=CUSTOMER cs1Label=Rule cs1=BYP:Bypass Rule Checks reason=INSUFFICIENT-AUTHORITY EvtCd-EvtQual=02-01 cs2Label=descriptor cs2=VIOLATION spriv=Normal cs5Label=Reason1 cs5=Due-to-AUDIT,or-RACHECK-exit,or-Failsoft fileType=VIOLATIO requestClientApplication=AC169D0A filePath=SFM_SS.PORT DT001=Resource-name:SFM_SS.PORT DT003=ACCESS-Authority-requested:READ DT004=ACCESS-Type DT005=DataSet-level-number:00 DT017=Class-Name:XFACILIT DT033=Generic-Resource-or-Profile:Generic-Profile-is-used,New-DSN-renamed-by-DEFINE,SFM_SS.* DT038=User/Group-Owner-of-Profile:BAJZ1 DT049=User-on-ACEE:COLIN VAN DER ROSS DT053=User-security-Tokens:PORTofEntry:AC169D0A,OwningUser:BCVR1 ,OwningGroupId:CUSTOMER

Vulnerability: FTP Visibility

- What files are being sent to and from the mainframe?
- Are those users authorized to download & upload those files?
- READ access on a file will allow a user to download a file from the mainframe
- Subsequent dissemination of the files & information is out of your control

Vulnerability: FTP Visibility

- If you are not using Secure FTP (SFTP, FTPs, etc.), passwords and data can be "sniffed" using an IP packet trace. Are those users authorized to download & upload those files?



Recommendations

- Enable and monitor type 119 SMF records, which can be written for FTP and Telnet activity
- Monitor for increases in activity that are outside the norm and access from unexpected locations
- Evaluate FTP usage at your site
  - Intranet
  - Data that is of low importance
  - Any data that is being sent outside of your company firewall using FTP is a red flag
- Migrate to a secure form of FTP

Summary

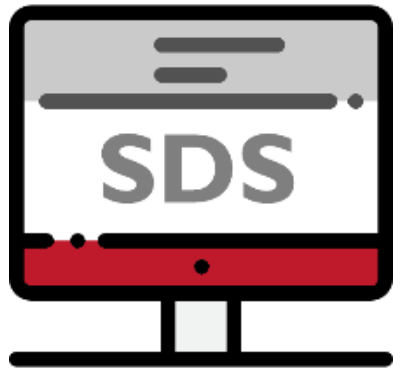
- Mainframes can be hacked
- Take stock of your organization's current situation
  - Do you have a SIEM in place?
  - Are z/OS event logs being sent to the SIEM?
  - How are you handling important WTORs and SMF records?
- Identify weaknesses and aim to improve
- We are here to help. Contact SDS for additional information on VSA and the visibility it provides

SDS MAINFRAME SECURITY

Would you like additional information?

info@sdsusa.com

(800) 443-6183
(763) 571-9000



www.sdsusa.com