#SHAREorg

SHARE
Technology · Connections · Results

# How to Detect Mainframe Intrusion Attempts

Paul R. Robichaux
NewEra Software, Inc.

Friday, August 10 at 9:30 – 10:30 am
Session Number 11530
Platinum 8

SHARE in Anaheim 2012

# Abstract and Speaker


- The Internet today is a complex entity comprised of diverse networks, users, and resources. Most of the users are oblivious to the design of the Internet and its components and only use the services provided by their operating system or applications. However, there is a small minority of advanced users who use their knowledge to exploit potential system vulnerabilities. With time and adequate system resources these Hackers or Crackers can compromise any information system including a zEnterprise Mainframe Complex.

- This presentation will provide insight into:

  First, the severity of the intrusion problem, the common attack points: Ports and Packets, how they are exploited by spies to reach and steal proprietary information or embed Remote Access Trojans (RATs) that can take remote control of a system and it's connected resources.

  Second, who the attackers are: Hackers, Crackers, Spies and how to detect their activities and fight back their attacks using a combination of common sense best practices and system tools.

  Third, the components of Network Policy Management and how the Policy Management Agent (PAGENT) can be used in a zEnterprise to detect and defend against a Mainframe Intrusion.

- Paul R. Robichaux is CEO of NewEra Software, Inc. He served as the Chief Financial Officer of Boole and Babbage for the ten years immediately preceding his co-founding of NewEra in 1990. He holds a BS in Accounting and a Masters in Business Administration from a Louisiana State University and is a Certified Public Accountant.

- The corporate mission of NewEra Software is to provide software solutions that help users avoid non-compliance, make corrections as needed and in doing so, continuously improve z/OS integrity.

# Continuing Education Credit

CERTIFICATE OF ATTENDANCE

Awarded to

as presented at the following
Continuing Education Course

Eligible for Continuing Professional Education Credit of One Hour

Brian Cummings, SEC Project Manager

SHARE in Anaheim
Security and Compliance Project
August 6 – 10, 2012
Anaheim, California

# Mainframe Intrusion!

*The Agenda:*

- *Looks like we're in really big trouble!*
- *Is your Mainframe Under Attack?*
  - ✓ *How do you know?*
  - ✓ *What can you do?*
- *Common Attack Techniques!*
  - ✓ *Port Scanning*
  - ✓ *Data Packet Fragmentation*
  - ✓ *Remote Access Trojans*
- *Who are they?*
  - ✓ *White Hats Vs. Black Hats*
  - ✓ *Tools of the Trade*
  - ✓ *Available Training*
- *Attack Scenario*
  - ✓ *Server Farm*
  - ✓ *The Mainframe*
- *Fighting Back – IPSec Defenses!*
  - ✓ *Scan Detection*
  - ✓ *Malformed Packets*
  - ✓ *External Security Manager*
  - ✓ *Management Policy*
- *The Policy Management Agent*
  - ✓ *Internet Key Exchange*
  - ✓ *Network Security Services*
  - ✓ *Defense Manager*
  - ✓ *Traffic Regulation Management*
- *Intrusion Detection Services (IDS)*
  - ✓ *The Agent Configuration*
  - ✓ *Policy: Rules, Actions, Reports*
  - ✓ *Securing Policies – pasearch*
  - ✓ *IDS Report Summaries*
- *Project White Paper*

# Mainframe Intrusion!

*We're all under Attack!*

"…Government, businesses and consumers are under attack. Hardly a week goes by without a report of a cyber security breach and warnings from IT security experts about the vulnerability of corporate assets ranging from intellectual property to critical nation state infrastructure assets."

*Source: CYBERSECURITY – A Financial Times Special Report – June 1, 2012*

*"…In 2011 Security Breaches Cost US Companies an Estimated $US125 Billion."*

*Source: The Ponemon Institute – www.ponemon.org – Annual Survey 2011*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > How do you know?*

- Inside the Castle, personnel that have authorized system access and necessary technical knowledge that are motivated by positive organizational goals are considered organizational assets; friendly, vetted, productive system users. On the other hand those negatively motivated to do harm are a threat to system integrity.
- Outside the Castle, all those negatively motivated and in possession of the required resources: time, technical knowledge and hardware and software tools, Hackers and Crackers, represent an equally dangerous threat to system integrity.

*Source: Phil Hopley – h2index – a UK based IT Research Firm*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > What can you do?*

- The old "medieval city" approach to IT Security just doesn't work anymore.
- Organizations believed to have adopted the best approaches have a robust security governance policy, backed up by good communications to assure ***awareness***, ***awareness*** and more ***awareness*** among everyone in their organizations.
- 97% of all Security Breaches could be avoided if organizations adopted simple, straight forward, IT Security Measures.
- IT Security should be everyone's concern, it is for certain everyone's problem!

*Source: Phil Hopley – h2index – a UK based IT Research Firm*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Techniques*

- One popular Spying Method used to identify host targets is to look for open Network Ports.
- Think of a Network Port as an entry point into the Castle. Once inside friends and enemy spies have access to your treasure!
- In a typical computer network the Port Address and an IP address are joined together to create a unique access point.
- Spies will Exploit Networks by:
  - ✓ Scanning for exposed Port defenses
  - ✓ Sending fraudulent Data Packages
  - ✓ Hiding Remote Attack Trojans (RATS)

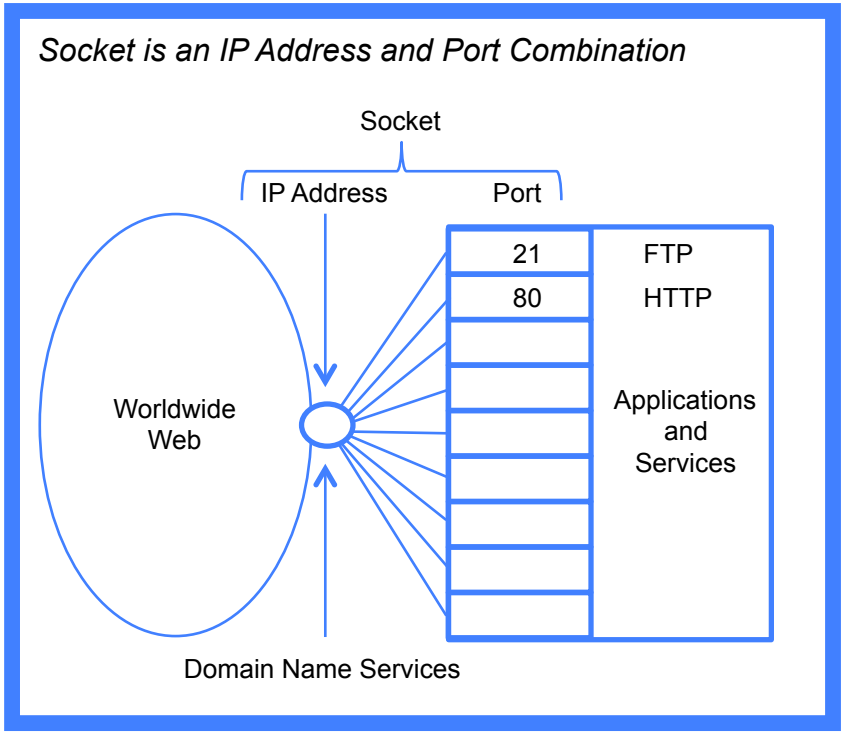
*Source: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers*

*Note - Denial-of-Service (DoS) Attacks*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Ports*

- A socket address combines an IP and port number, much like a telephone connection combines a phone number and a particular office interchange extension.
- Based on this address, internet sockets deliver incoming data packets to the appropriate application process or thread.
- Some Ports are designed specifically to "Listen" for requests such as the return of a web page to a display browser or to receive file transfers from remote users and sites.
- The open nature of such Listening Ports makes them vulnerable to network spies.




*Source: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Ports*

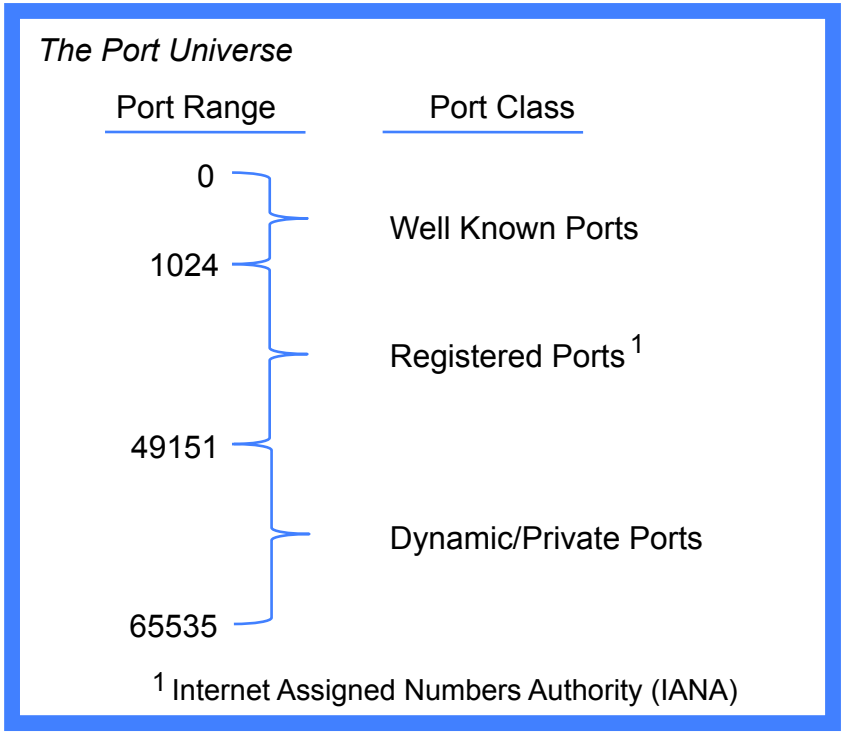
*Socket is an IP Address and Port Combination - OMVS Command - `netstat -a`*

```
MVS TCP/IP NETSTAT CS V1R13       TCPIP Name: TCPIP            18:43:55
User Id  Conn     Local Socket            Foreign Socket          State
-------  ----     ------------            --------------          -----
AXR04    00008716 192.86.33.152..1267     173.1.13.243..25        Establsh
BPXOINIT 0000000F 0.0.0.0..10007          0.0.0.0..0              Listen
FTPSERVE 0000000E 0.0.0.0..21             0.0.0.0..0              Listen
INETD1   00000012 0.0.0.0..23             0.0.0.0..0              Listen
TN3270   00008713 192.86.33.152..623      98.254.29.53..34346     Establsh
TN3270   000086CA 192.86.33.152..623      64.81.66.48..4076       Establsh
TN3270   0000000D 0.0.0.0..623            0.0.0.0..0              Listen
TN3270   000086DE 192.86.33.152..623      64.81.66.48..4089       Establsh
TN3270   000086BE 192.86.33.152..623      64.81.66.48..52802      Establsh
TN3270   000086C0 192.86.33.152..623      66.254.206.55..50373    Establsh
TN3270   000086B0 192.86.33.152..623      99.22.54.177..1045      Establsh
```

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Ports*

- Well Known Ports, port numbers in the range from 0 to 1023 are used by system processes that provide widely-used types of network services.
- Registered Ports, port numbers in the range from 1024 to 49151 are assigned by IANA[1] for specific service upon application by a requesting entity. Can be used by ordinary users and processes.
- Dynamic or Private Ports, port numbers in the range 49152–65535 cannot be registered and are used for automatic allocation of temporary ports.

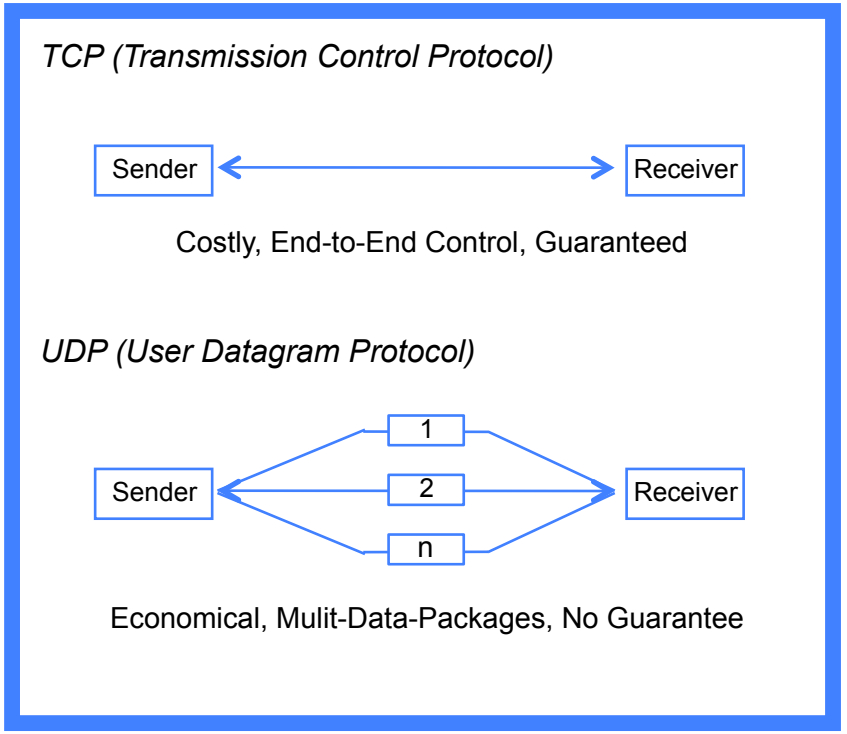



*Source: http://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Ports*

- TCP (Transmission Control Protocol) Port transmissions connect directly to the computer it's sending data to, and stay connected for the duration of the transfer. With this method, the two computers can guarantee that the data has arrived safely and correctly.
- UDP (User Datagram Protocol) Ports release data packages into the network with the hopes that they will get to the right place. This means that UDP relies on the devices in between the sending and receiving computer to get the data where it is supposed to go, no guarantee it will.




*Source: http://www.bleepingcomputer.com/tutorials/tcp-and-udp-ports-explained/*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Ports*

- Network Ports, under the control of the z/OS Communication Server, are defined to the TCP/IP Stack via a unique configuration profile.
- Identifying and documenting the types and uses of each port is an essential step towards increasing security awareness.
- A Port Scanner is often used to identify ports. Freely available Scanners Advertise:

  *"Use this tool to inspect your own computer's TCP/IP ports and see what open network ports hackers might discover on your machine."*

*z/OS Communication Server for z/OS*

<> Operator Command to Display Ports:

/Display TCPIP,,NETSTAT,PORTList

<> Port List Report returned to System Log:

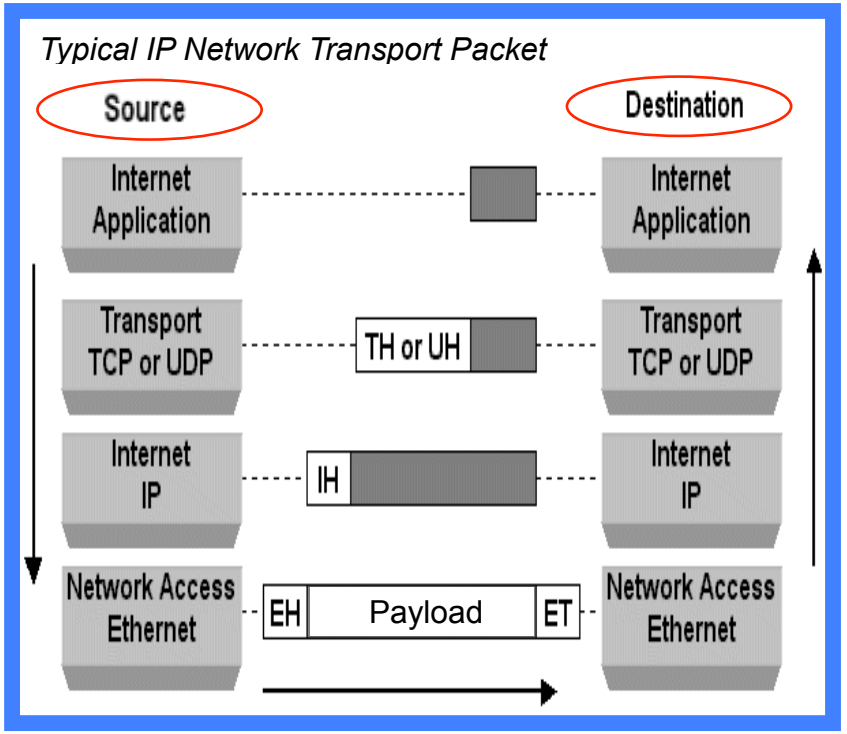
```
RESPONSE=S0W1
EZZ2500I NETSTAT CS V1R11 TCPIP 404
PORT# PROT USER     FLAGS    RANGE   MORE>
7     TCP  MISCSERV DA
9     TCP  MISCSERV DA
19    TCP  MISCSERV DA
20    TCP  OMVS     DA
21    TCP  FTPSERVE DA
19    UDP  MISCSERV DA
53    UDP  NAMESRV  DA
111   UDP  PORTMAP  DA
135   UDP  LLBD     DA
161   UDP  OSNMPD   DA
```

*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*GOOGLE: "TCP/IP Port Scanner"*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Packets*

- A packet consists of two kinds of data: Control Information and the User Payload.
- Control information provides data the network needs to deliver data, for example:
  - ✓ source and destination addresses,
  - ✓ error detection codes, checksums, and
  - ✓ sequencing information
- Typically, Control Information is found in packet headers and trailers, with payload data in between.
- A Packet is considered Malformed when it is of a non-standard size, fragmented or overlaid Packet Control Information.

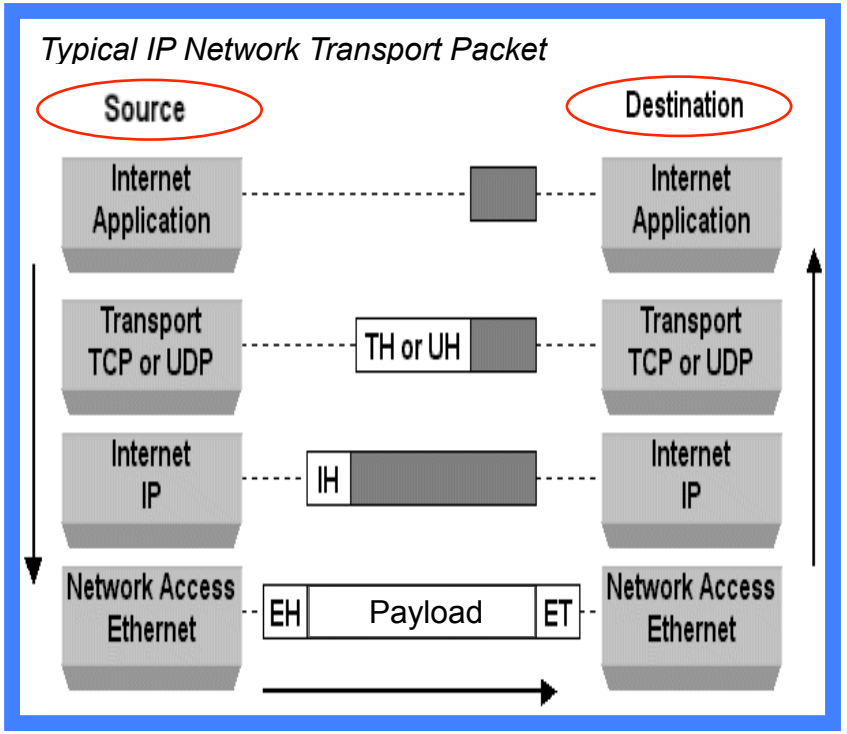



*Source: Wikipedia – From the Query "Network Packet"*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Packets*

- Intrusion Detection (IDS) Attack Policies help protect z/OS Mainframes from both known and unknown attacks and provide timely notification when attacks do occur.
- The philosophy behind IDS Attack Policies is to disallow anything that is not known and/or specifically allowed.
- Malformed Packet Policies cover many known attacks designed to cause system crashes and/or denials of IT service.
- Many malformed packet attacks use fragmentation to overlay header fields.

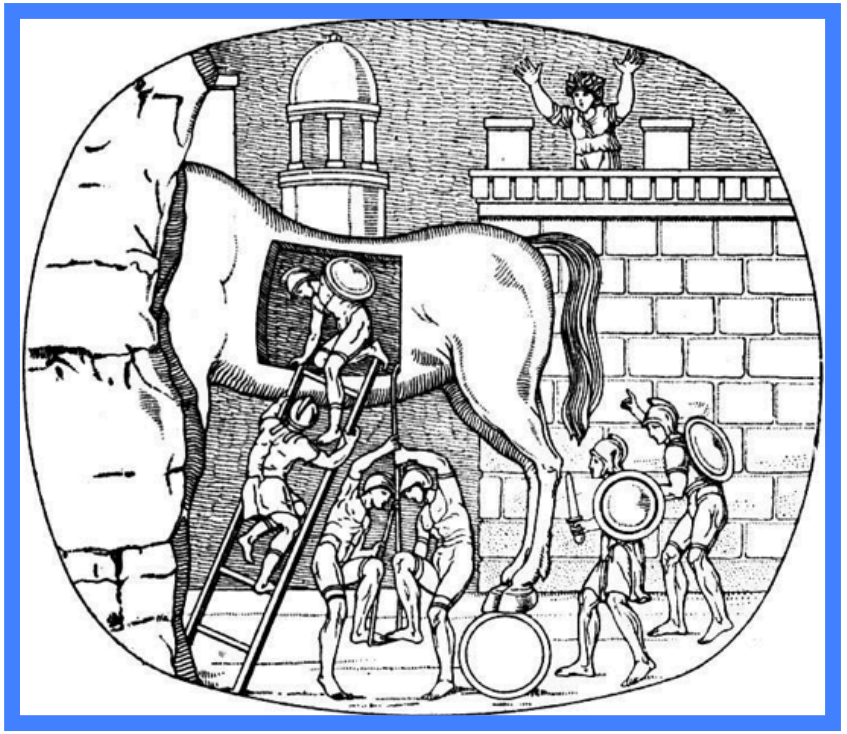



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Trojans*

- During the Trojan War Greeks presented Troy with a wooden horse containing hidden warriors. At night, they overran the city.
- Network Trojans contain malicious code inside apparently harmless programming or data that can take control to do damage.
- Trojans are classed by how they breach and damage systems. The main types are:
  - ✓ Remote Access Trojans (RATS)
  - ✓ Data Sending Trojans
  - ✓ Destructive Trojans
  - ✓ Proxy Trojans
  - ✓ FTP Trojans

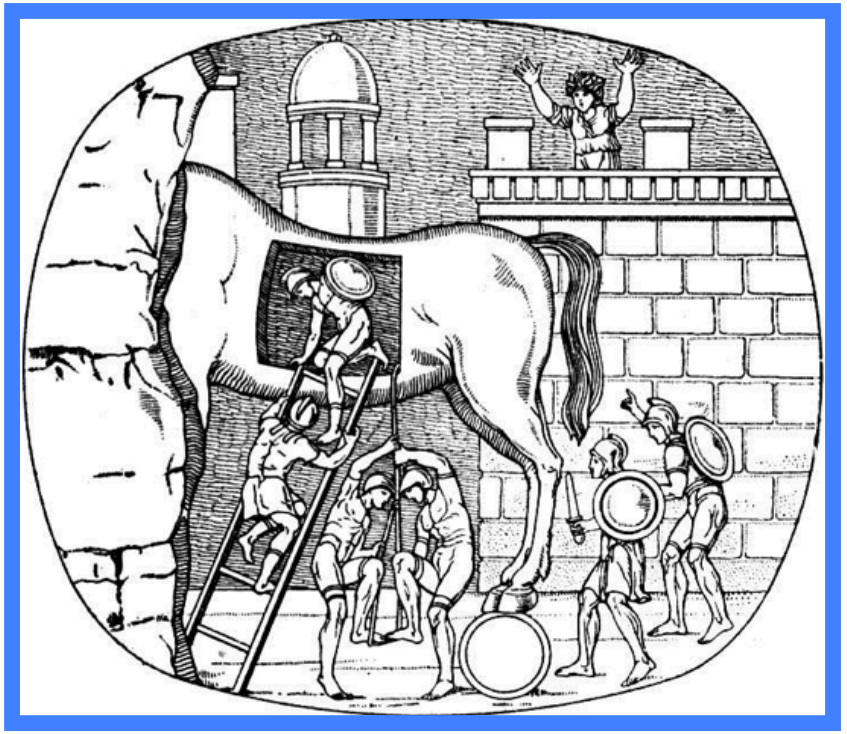


*Source: http://www.webopedia.com/TERM/T/Trojan_horse.html*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Trojans > RATs*

- RATs can be key stroke loggers and remote controllers, they can configure the IP port the RAT listens on, how the RATs execute and contact their originator.
- RATs are usually downloaded invisibly with a user-requested program -- such as a game -- or sent as an email attachment.
- Once the host system is compromised, the spy may use it to distribute RATs to other vulnerable computers and establish a botnet.
- RATs are difficult to detect because they don't show up as running programs or tasks.

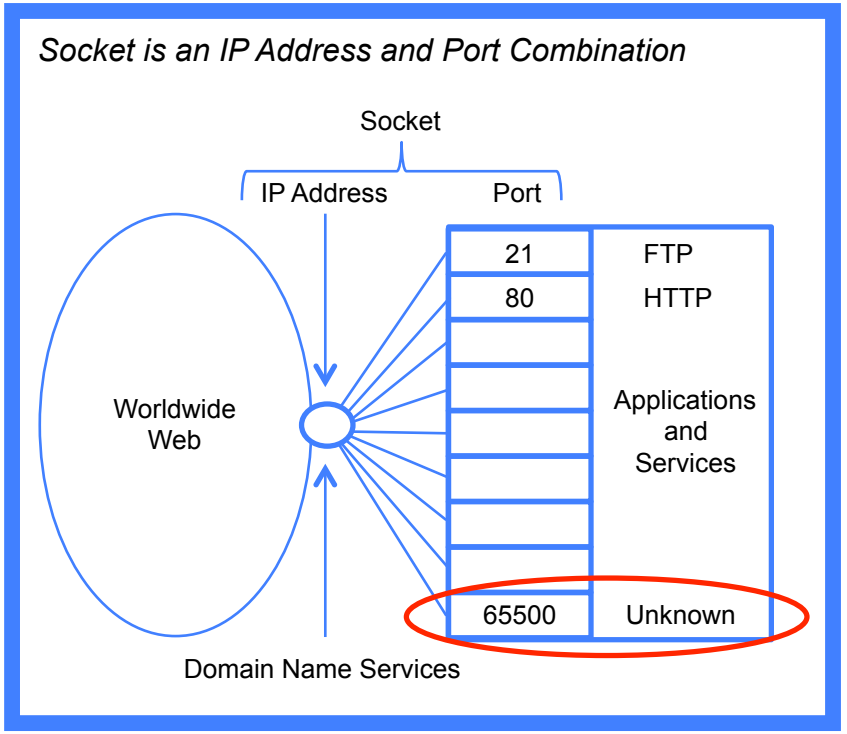


*Source: http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Trojans > Rats*

- A brute force attack is one where spies use automation to guess a valid password as quickly as possible.
- Whether or not a spy enters a system hiding in a Package Fragment or disguised behind a Valid Password the goal will be the same, take control of the system by creating an "Unknown" remotely controllable service.
- To avoid detection Hackers attempt to cover their tracks, for example, if they open an unauthorized network port they will replace system services (netstat) with their own, modified version of the service.




*Source: http://searchsecurity.techtarget.com/definition/RAT-remote-access-Trojan*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > How and Who are they?*

- Penetration tests (Pen-Tests) are a critical component to the over-arching information security (IPSec) plan protecting any organization from attack.
- Pen-tests provide valuable data on how well network and related information assets are reached and protected for intrusion.
- Pen-Testers are those that conduct Penetration Tests for the purpose of discovering and reporting weaknesses.
- Hackers, on the other hand, are those that use Penetration Tests to exploit network weaknesses for nefarious reasons.


*Source: Detection and Characterization of Port Scan Attacks – 2002*
*By Cynthia Bailey Lee, Chris Roedel, Elena Silenok*
*Computer Science & Engineering UC-San Diego*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Tools*

- Google the keywords *"Remote Access Trojan"* into your browser and the reply will be a set of links to hundreds of free RATs – the most popular being Back Orifice from Dead Cow and SubSeven.
- Google in *"Port Scanners"* and the results are similar – the most popular being nmap from nmap.org.
- Now Google in *"Free Hacker Tools"* in order to get a general idea of overall availability. The results will be on the order of 20 million hits with insecure.org topping the list of sources.

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Training*

❑ Find what you need on YouTube! Here is your Starter Set:

- ✓ *Hackers*
  A National Geographic Documentary - (46:39)
- ✓ *Introduction to Hacking*
  Eli the Computer Guy - (68:00)
- ✓ *How to Hack a Web Site*
  Dr. Susan Loneland - (43:53)
- ✓ *Anonymous, A Hackers World*
  16X9 - (20:10)
- ✓ *SubSeven Trojan Backdoor*
  Unknown - (6:57)
- ✓ *Nmap Basics and a Lot More*
  nmap.org – (9:31)

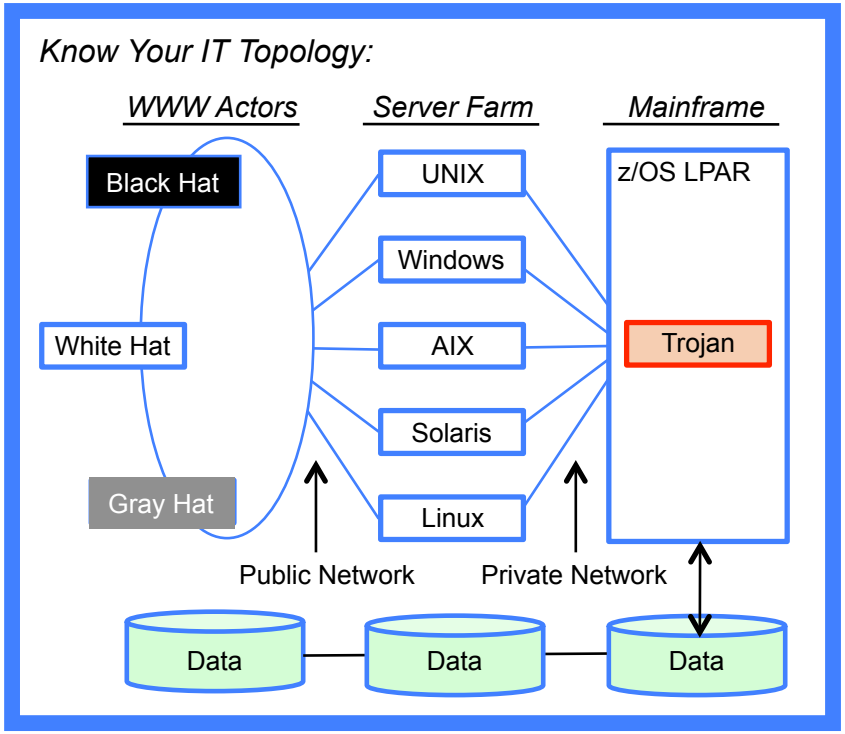
*Source: HTTP//:youtube.com*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Scenario*

- An attack against a z/OS Mainframe that is networked to a heterogeneous Server Farm could unfold as follows:

1. Scan the Server Farm for open ports
2. Send a malformed Packet to all
3. Open the packet and activate a port
4. Send a Trojan to the open server(s)
5. Begin scan for open mainframe port
6. Send malformed Packet to one
7. Open the packet and Logon
8. Begin scanning for Relevant Data
9. FTP Data to Internet Drop Box
10. Terminate and Erase Self




*Source: All that have been cited up to this point!*

*Note - Denial-of-Service (DoS) Attacks*

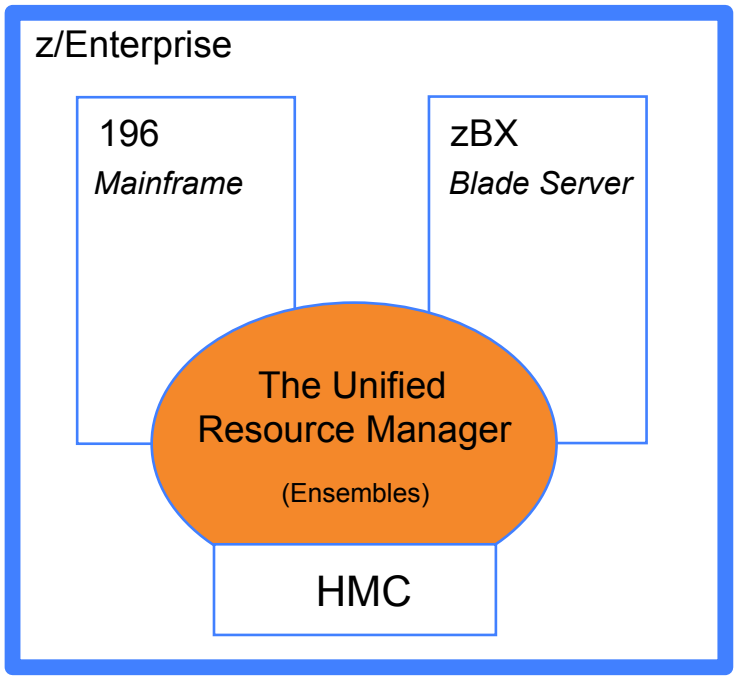
# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Attacks > Hyper-Scale*

❑ Hyper-scale servers are designed for large scale datacenter environments where parallelized workloads are prevalent. The form-factor serves the unique needs of these datacenters with streamlined system designs that focus on:

- Performance
- Energy efficiency
- Platform Density

❑ Hyper-scale servers forego the full management features and redundant hardware components found in traditional enterprise servers as these capabilities are accomplished primarily through software.

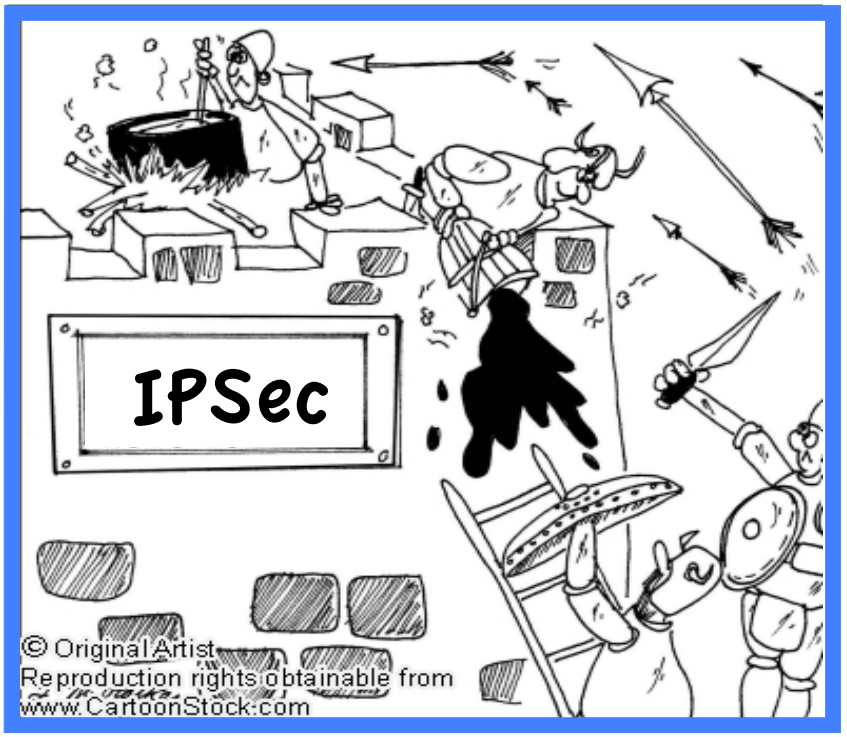



*Starting Q3 2011, IDC began to track the new form-factor called hyper-scale servers.*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Fighting Back > Ports*

- Identifying that scanning missions are underway can alert a security analyst as to what services or types of computers are being targeted for possible attack.
- Knowing what services are targeted allows an administrator to take preventative IPSec measures e.g. installing patches, fire walling services from the outside, or removing services on machines which do not need to be running on them.
- Port Scan detection counts distinct destination IPs attempting to connect to a given Port within a certain time window.

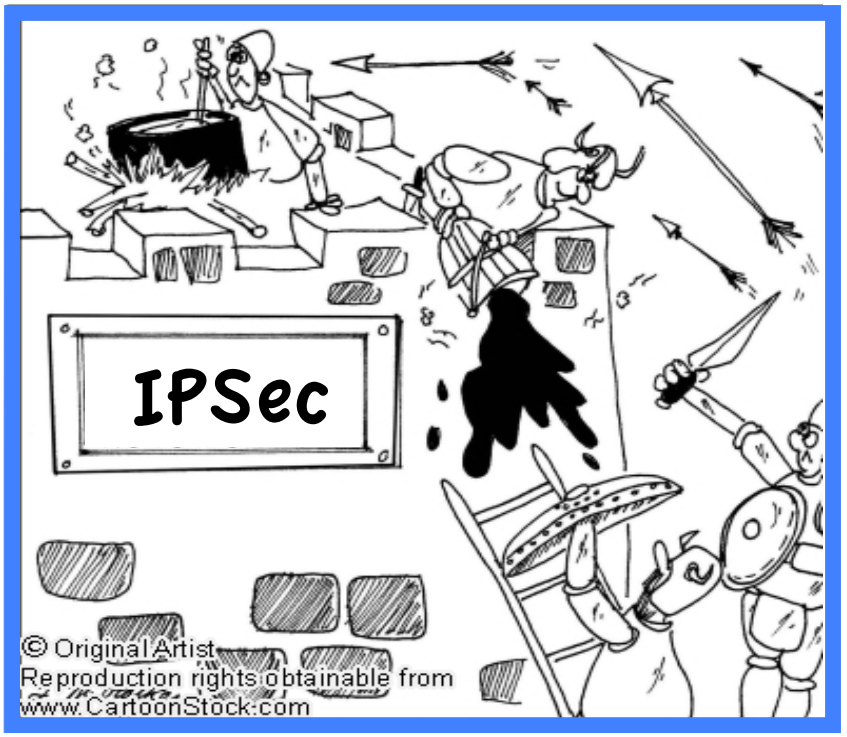



*Source: Scan Detection: A Data Mining Approach – 2006*
*By György J. Simon , Hui Xiong*
*University of Minnesota, Rutgers University*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Fighting Back > Ports*

- A number of Intrusion Detection System (IDS) methodologies have been developed to detect reconnaissance Port Scans. Most have three common weaknesses.
- Sufficiently low Scan Rate Policies lead to unacceptable false alarms as high scan activity will render the Policy useless.
- Setting a Higher threshold can leave slow and stealthy scanners undetected.
- Hiding the true identity of the attacking IP address by using IP decoys, or "zombie" computers that are under an attacker's control mask the attack's origin.

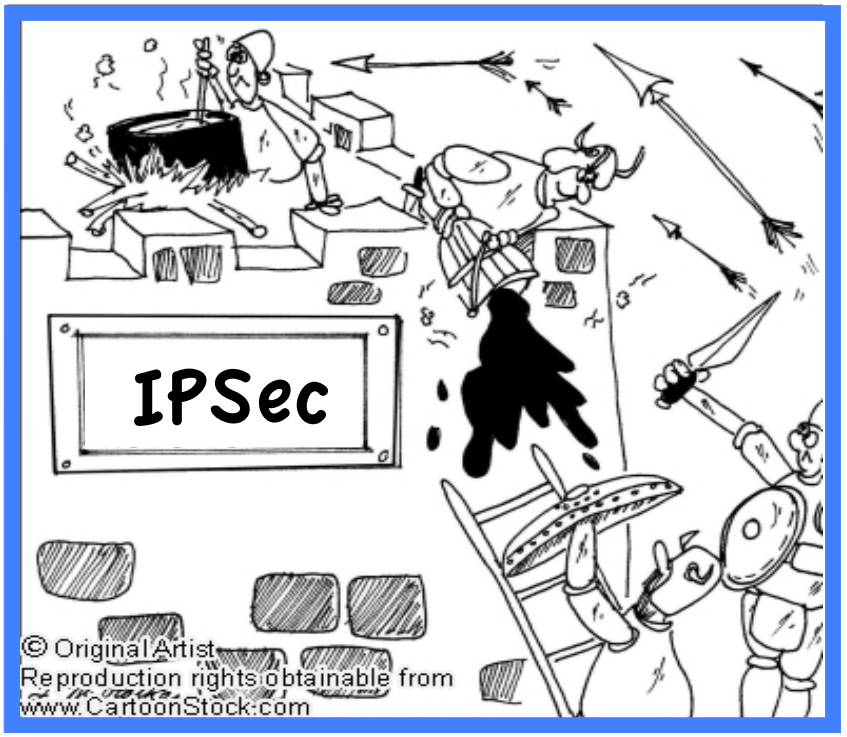



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Fighting Back > Packets*

- Malformed Packet attacks can cause IT System crashes and/or denials of IT Service.
- As packets are sent or received, they are matched to policies of the appropriate type.
- When a matching policy is found, it is implemented against the packet.
- Depending on the policy type and packet contents, this results in a variety of actions. For example a packet might be:
  - ✓ Totally discarded,
  - ✓ Processed according to its priority,
  - ✓ Have its routing changed.

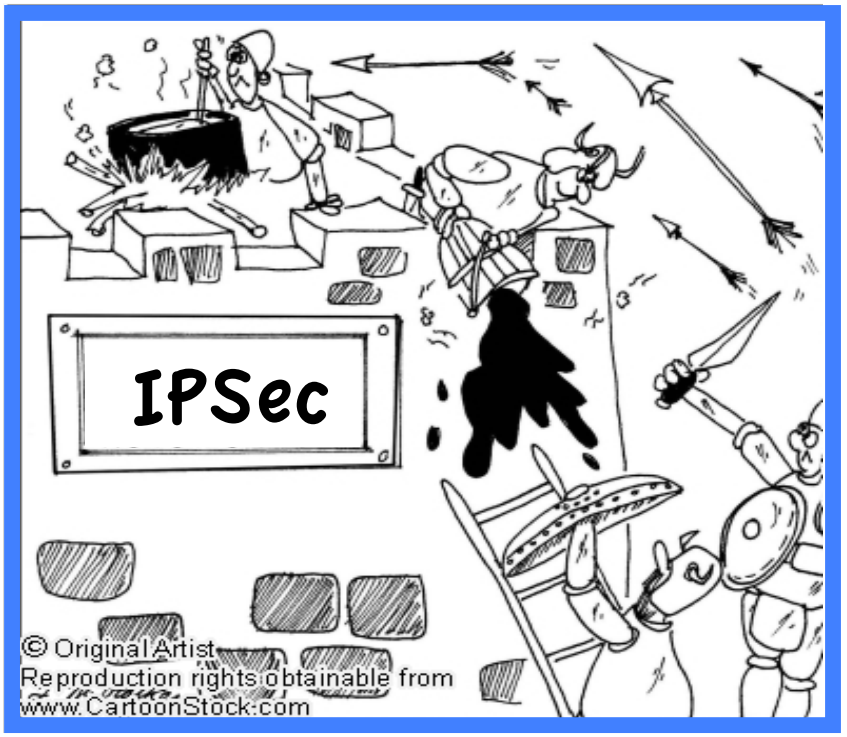



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Fighting Back > Packets*

- Malformed Packets cover many known attacks designed to cause system crashes.
- Packets that fit these descriptions should always be discarded as they rarely have legitimate source address information.
- Many malformed packet attacks use fragmentation to overlay header fields.
- The IDS fragment restriction policy will protect the network from unknown attacks by disallowing fragmentation in the first 88 bytes of any datagram.
- Fragments must be disallowed by policy.

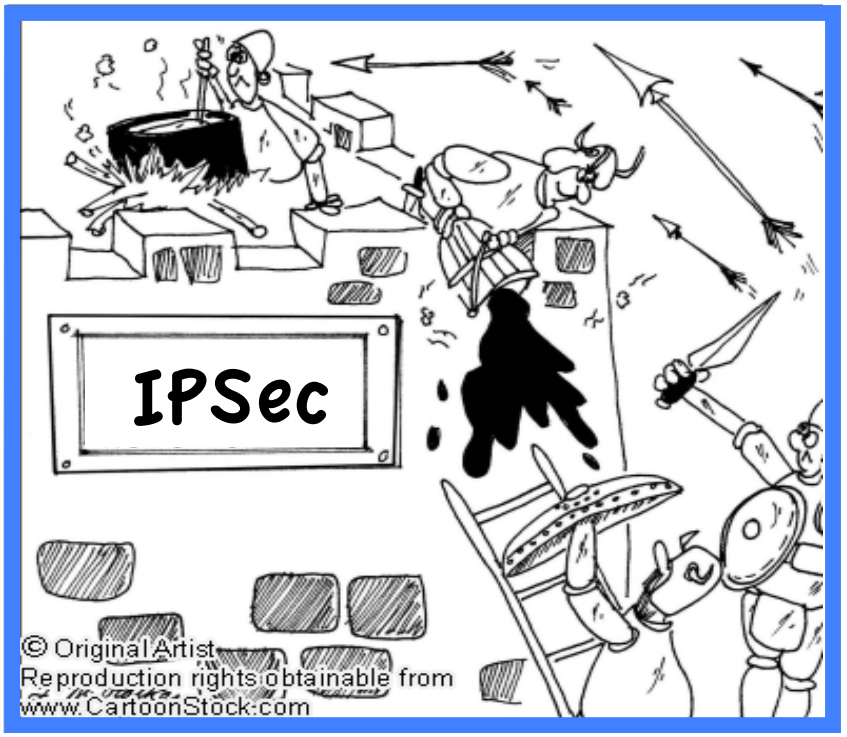



*Source: z/OS V1R13.0 Communications Server IP Configuration Guide*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Fighting Back > Trojans*

- The only way to defend yourself from a Cyber Spy is to understand the attacker and her intrusion methods in-depth.
- Turn off any network service that is not needed so that it will not become an avenue of attack.
- Keep the operating system of all servers updated to the latest release.
- Understand and use logical and physical firewalls.
- Only talk to systems you know and trust.
- Things change quickly, stay up to date.

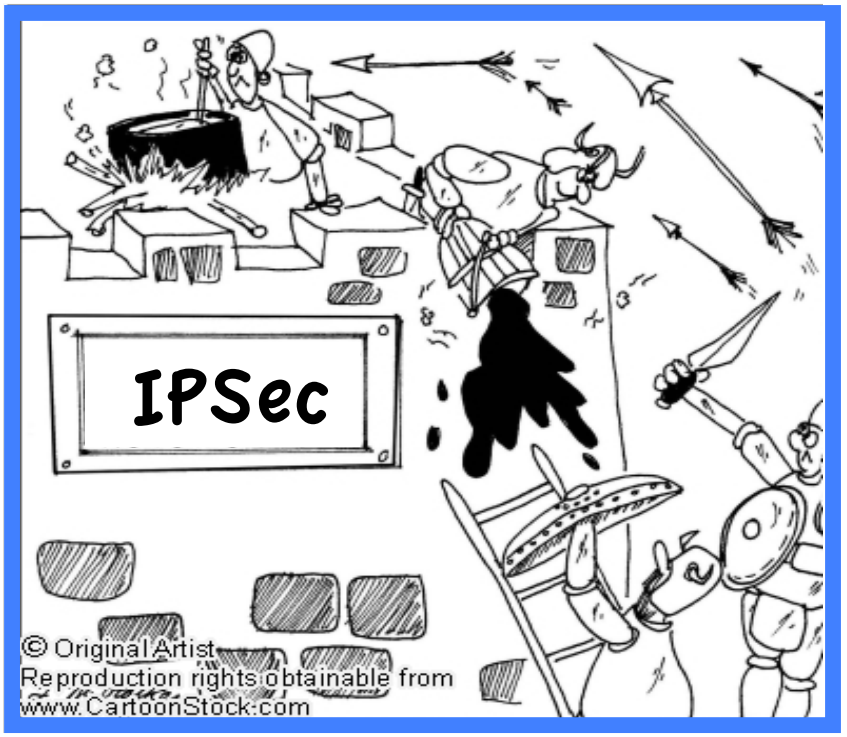



*Source: http://www.techrepublic.com/blog/security/10-security-tips-for-all-general-purpose-oses*
*http://infosec.ufl.edu/events/dlm-Cyber-Self-Defense-handout.pdf*

# Mainframe Intrusion!

*We're all under Attack! > Is your Mainframe Safe? > Fighting Back > Trojans*

- Caution Security and Systems Staff on the use of Social Networking that might reveal personal information, password selection and/or personal planning, vacations and/or sick leave.
- Limit or deny access to System Administration Functions, root authority.
- Develop unique policies for controlling the selection and enforce of Admin Passwords, "Just say no to IBMUSER".
- Restrict or deny access from unapproved Smart Phones, and other personal devices.

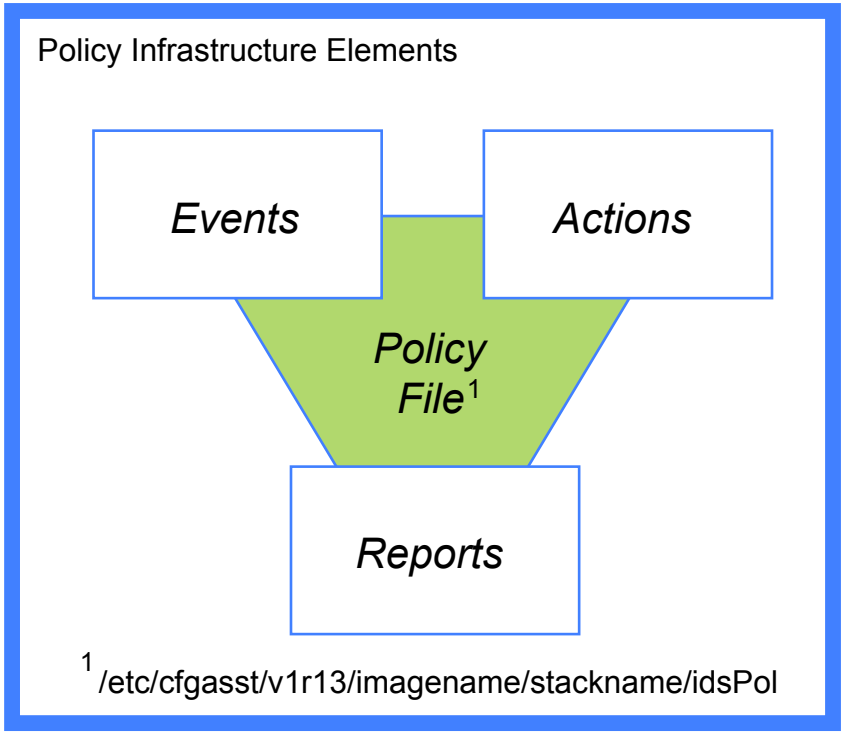



*Source: All cited up to this point*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Management Policy*

- Management Policies are a pre-defined set of network Events, corresponding reply Actions, related Notifications and Reports.
- Policy files are created and maintained using the z/OSMF Configuration Assistant, or the PC-based Configuration Assistant for the z/OS Communication Server.
- The same Policy Configuration can be applied across many multiple IP Stacks in the same underlying LPAR.
- Unique Policy Configurations can be deployed for each IP Stack in an LPAR.

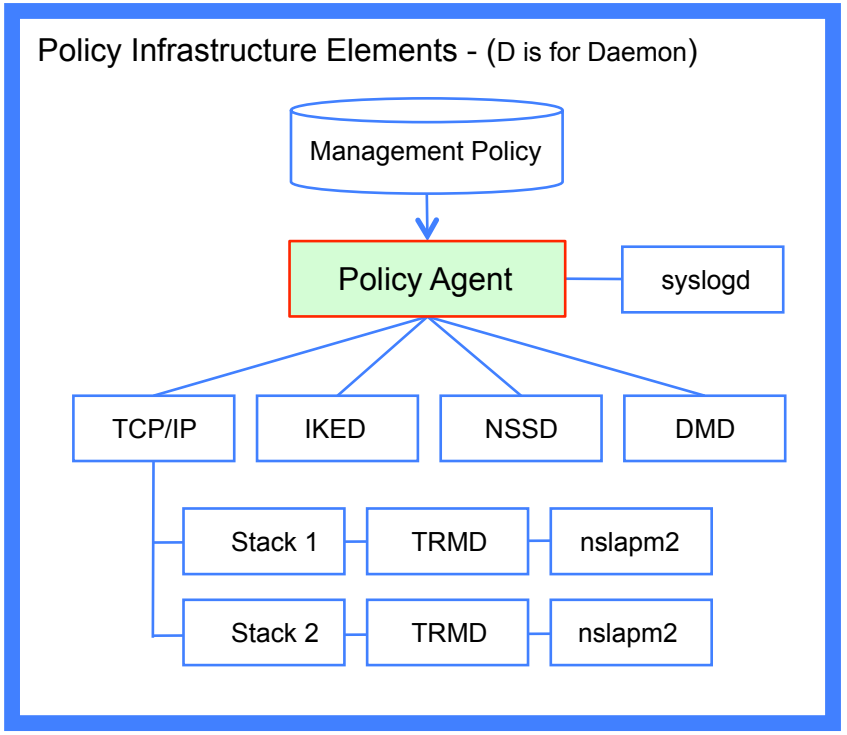



*Source: V1R13 IBM Configuration Assistant for z/OS Communications Server tool*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Enforcement*

- PAGENT, a z/OS address space, builds the Policy Infrastructure needed by the z/OS Communication Server to support Intrusion Detection Services (IDS). PAGENT acts as:
  - ✓ Policy Server executes on a single system and installs policies for others
  - ✓ Policy Client retrieves remote policies from the Policy Server.
- The Policy Infrastructure Includes:
  - ✓ Internet Key Exchange (IKED)
  - ✓ Network Security Services (NSSD)
  - ✓ Defense Manager (DMD)
  - ✓ Traffic Regulation Management (TRMD)
  - ✓ The Reporting Subagent (nslapm2)

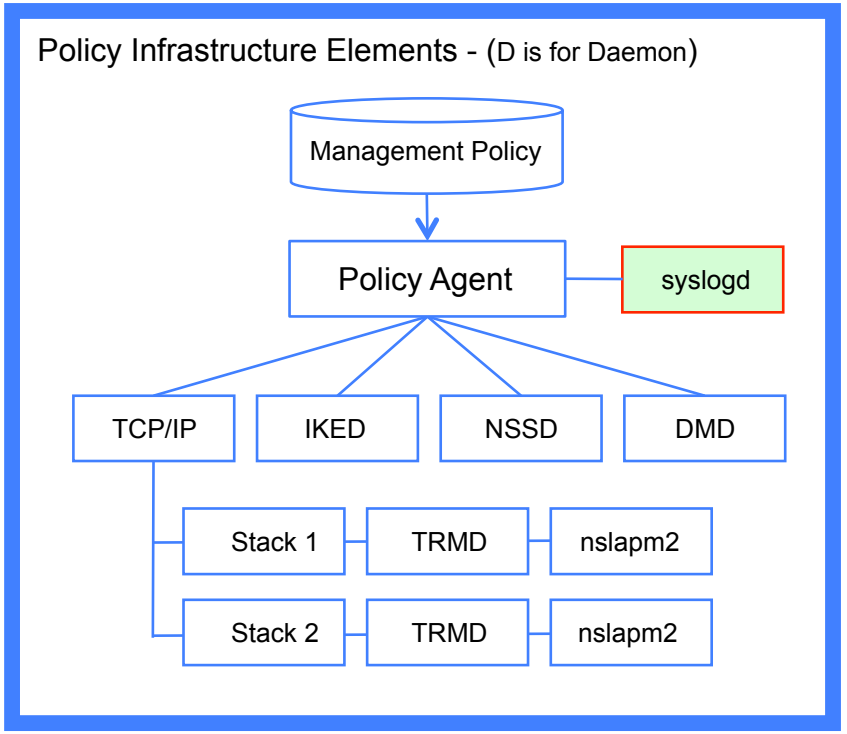



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy daemons > Syslogd*

- The central message logging facility for all z/OS UNIX® applications is the syslog deamon, syslogd.
- This deamon is not specific to the policy infrastructure, but the policy infrastructure does depend on the availability of syslogd to provide the central logging facility needed for maintaining an audit trail of policy events.
- If the syslog deamon is not available all policy event messages will be lost.
- One syslog daemon is needed for each Policy Managed LPAR in a Sysplex.

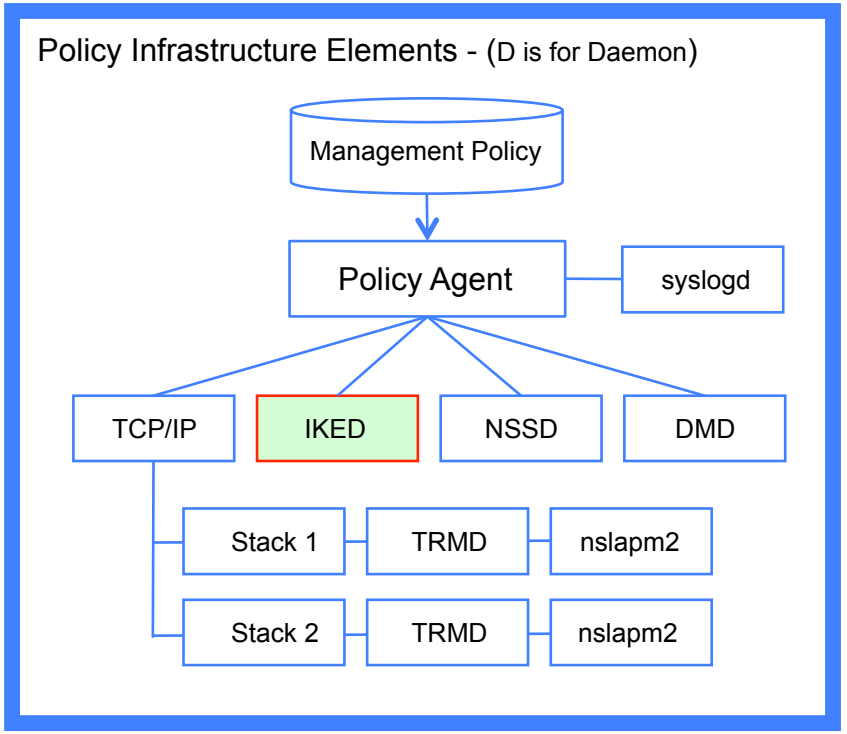



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy daemons > IKED*

- The Internet Key Exchange daemon (IKED) employs the IPSec standard used to ensure the security for Virtual Private Network (VPN). It does this by automatically negotiating and authenticating Security Associations (SA).
- Security Associations (SA) are security policies defined for communication between two or more entities where the relationship between the entities is represented by a key.
- IKED ensures secure communication without the need for pre-configuration.
- If IKED is required start one per LPAR.

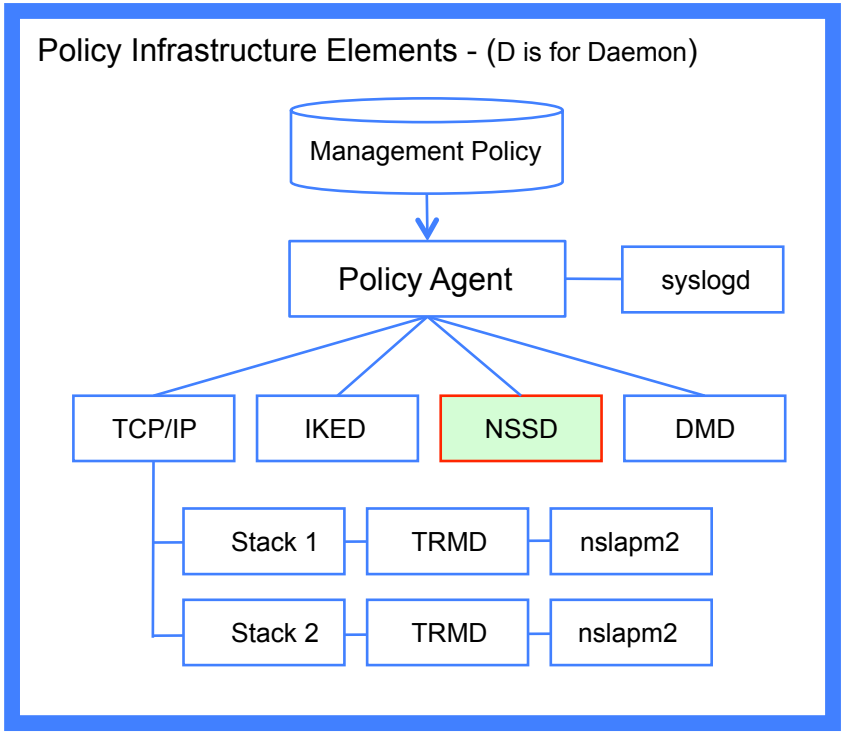



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy daemons > NSSD*

- The Network Security Services daemon (NSSD), an element of the overall z/OS networking policy infrastructure, provides IPSec Certificate and Remote Management Services and XML Appliance SAF access, certificate, and private key service.
- NSSD is the Central Certificate and Key Server for z/OS and the Network Security Server for non-z/OS platforms.
- NSSD can be used independently from any z/OS policies.
- One NSSD is required within a Sysplex.

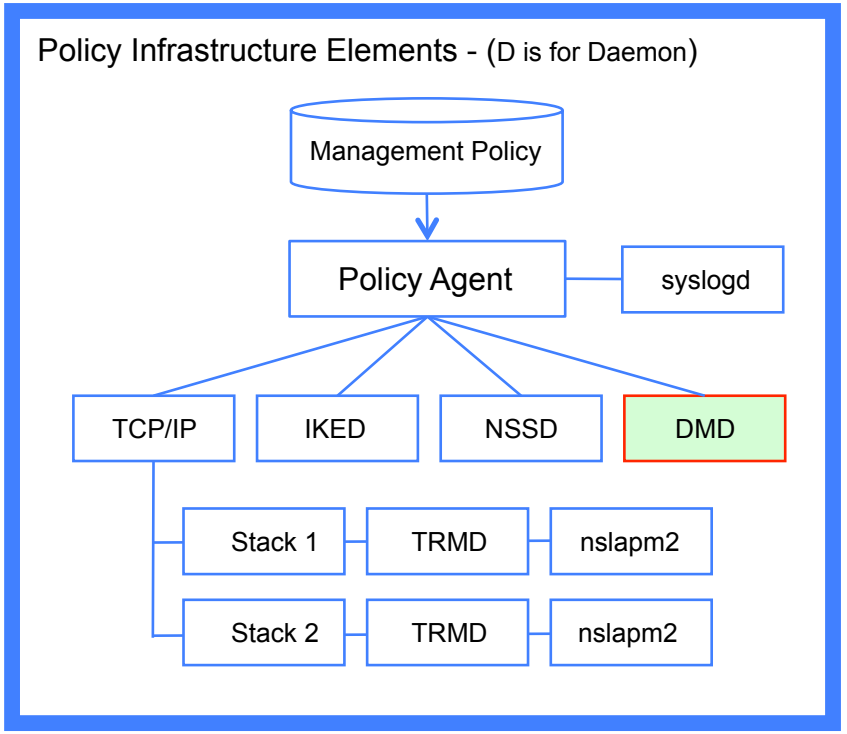



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy daemons > DMD*

- The Defense Manager daemon (DMD) provides short-term defensive filtering.
- DMD filters are typically installed by a network specialist for a limited duration (for example, 30 minutes) to block specific attacks and/or a pattern of attacks that are not otherwise defined to network defenses.
- DMD filters can be used without defining the more permanent, IPSec defensive IDS policies but typically both DMD and IPSec filter policies are required and used.
- One DMD is needed per LPAR.

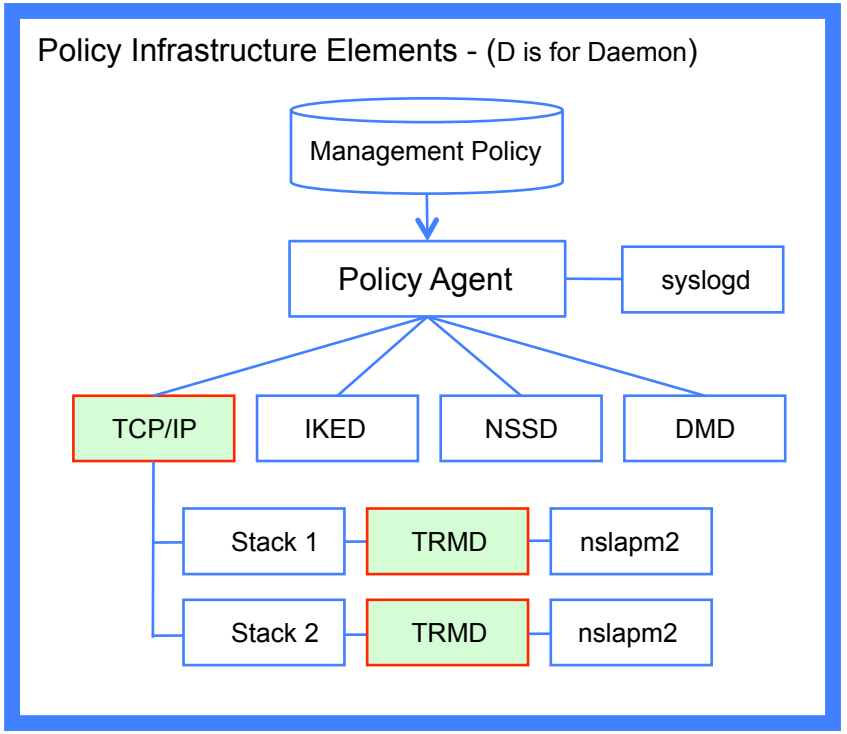



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy daemons > TRMD*

- The Traffic Regulation Management daemon (TRMD) formats and sends policy-related messages to syslogd.
- TRMD is used with:
  - ✓ Traffic Regulation (TR),
  - ✓ Intrusion Detection Services (IDS) and
  - ✓ IP Security (IPSec)
- The Traffic Regulation Management (TRM) is incorporated into the Intrusion Detection Services (IDS).
- One TRMD is needed for each TCP/IP stack in an LPAR.

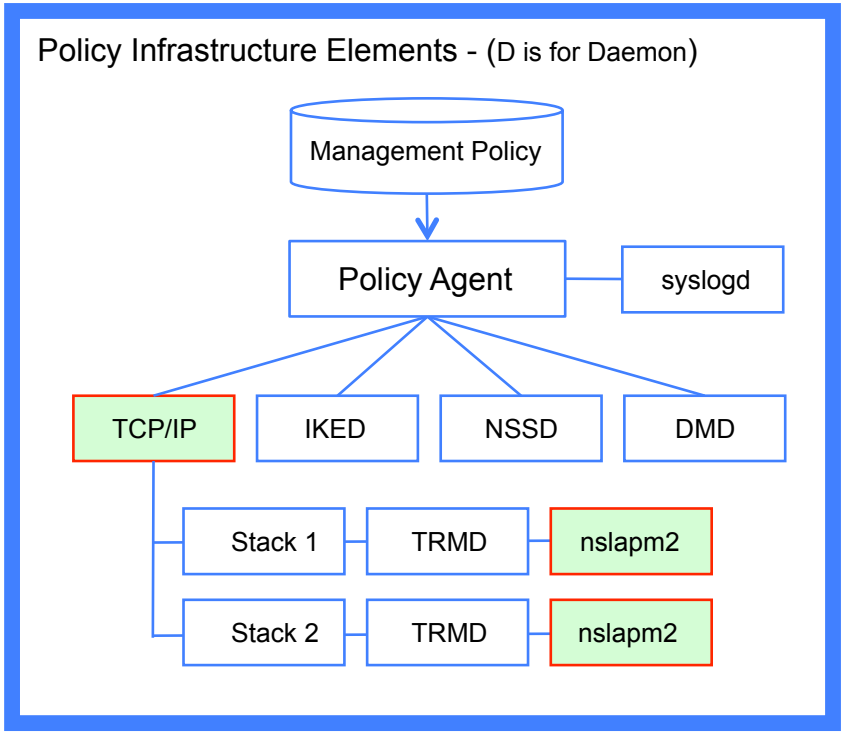



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy daemons > nslapm2*

- nslapm2 is an Simple Network Management Protocol (SNMP) subagent that provides information about defined network service policies and performance data used by network applications through Management Information Base (MIB) variables.
- These Quality of Service (QoS) metrics are retrieved by the nslapm2 subagent and monitored for any possible deviation from defined Network Policies.
- One nslapm2 subagent is needed for each TCP/IP stack in an LPAR.

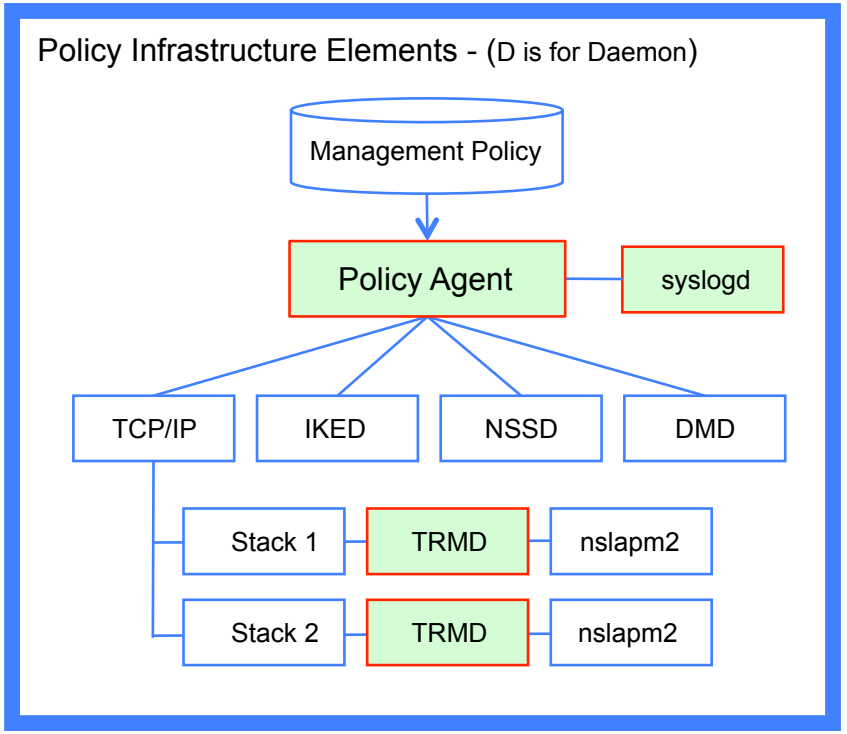



*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > Activating IDS*

- IDS detects/reports network intrusion events. IDS policy regulates the types of events detected and reported. IDS policy may be defined for scans, attacks and traffic regulation for both TCP and UDP ports.
- To deploy Intrusion Detection Services (IDS) in a z/OS Environment the following components of the Policy Infrastructure must be present:
  - ✓ PAGENT (for each LPAR)
  - ✓ Syslogd (for each LPAR)
  - ✓ TRMD (for each TCP/IP Stack)




*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > Start-Up*

- PAGENT has it own configuration file. Typically the file name contains both the name of the Image Name and the name of the TCP/IP Stack. For Example:

  /etc/cfgasst/v1r13/*imagename*/*stackname*/idsPol

- When the Policy Agent is started it reads this configuration file and starts all defined Policy Applications (AppName) for each TCP/IP Stack named (TcpImageName).

- Either z/OSMF Configuration Assistant, or the PC-based V1R13 IBM Configuration Assistant for z/OS Communications Server tool can be used to create the file.

*The PAGENT Configuration File*

```
AutoMonitorParms
{
 MonitorInterval 10
 RetryLimitCount 5
 RetryLimitPeriod 600
}
AutoMonitorApps
{
 AppName TRMD
 {
  TcpImageName TCPIP
  {
   Procname POLPROC
   Jobname TRMD
  }
 }
}
```

*Source: A NewEra White Paper – The IDS Policy Management Project*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > daemon Status*

- The Intrusion Detection Services policy is installed into the stack automatically by the Policy Agent (PAGENT).
- After the policy is installed, IDS detects, processes, and reports on events as requested by the policy.
- TRMD, part of IDS, handles reporting IDS statistics and events to syslogd.
- Problems might occur in:
  - ✓ Policy installation
  - ✓ Output to syslogd or the console,
  - ✓ TRMD initialization

*Are the PAGENT daemons Running?*

<> Operator Command to Display Ports:

```
/F PAGENT,MON,DISPLAY
```

<> PAGENT daemon Operational Status:

| APPLICATION | MONITORED | JOBNAME | STATUS |
|---|---|---|---|
| DMD | NO | N/A | N/A |
| IKED | NO | N/A | N/A |
| NSSD | NO | N/A | N/A |
| SYSLOGD | NO | N/A | N/A |
| TRMD | YES | TRMD | ACTIVE |

<> TRMD might fail because:

1. OMVS segment was not defined for the TRMD ID.
2. The TCP/IP stack is not up.

*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > Defensive Rules*

- Attack rules are a set of conditions that predefine what constitutes an attack.
- The Policy Agent defends against:
  - ✓ *Malformed Packet*
  - ✓ *Flood*
  - ✓ *ICMP Redirect*
  - ✓ *IP Fragment*
  - ✓ *IP Protocol*
  - ✓ *Outbound Raw Restrictions*

*Intrusion Detection Rules - DataHiding*

```
#-----------------------------------
# Attack - IDSRule
#-----------------------------------
IDSRule                      DataHiding
{
  ConditionType              Attack
  IDSAttackCondition
  {
    AttackType               DATA_HIDING
    OptionPadChk             Enable
    IcmpEmbedPktChk          Enable
  }
  IDSActionRef               DataHiding
}
```

*Source: z/OS V1R13.0 Communications Server IP Configuration Guide*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > Defensive Actions*

- Actions associated with an Attack Rule define reporting and logging options for a detected attack.
- The Policy Agents will disallow:
  - ✓ ICMP redirect receipts
  - ✓ Fragmentation within first 88 bytes
  - ✓ IP protocols except ICMP, TCP and UDP
  - ✓ Outbound packets using RAW sockets
- A single reusable attack action is defined and shared among all the attack rules.

*Intrusion Detection Actions – DataHiding*

```
#-----------------------------------
# Attack - IDSAction
#-----------------------------------
IDSAction                    DataHiding
{
  ActionType                 Attack nodiscard
  IDSReportSet
  {
    TypeActions              LOG
    LoggingLevel             4
    TypeActions              STATISTICS
    StatType                 Normal
    StatInterval             60
  }
}
```

*Source: z/OS V1R13.0 Communications Server IP Configuration Guide*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > Reporting*

- A Report Set can be associated with defined actions. Report can include:
  - ✓ Type of Action
  - ✓ Statistics Interval
  - ✓ Logging Level
  - ✓ Trace Data
  - ✓ Record Size
- If a packet meets a policy rule's condition during its validity period, the report specified in the policy is produced.

*Intrusion Detection Actions – DataHiding*

```
#-----------------------------------
# IDSReportSet
#-----------------------------------
IDSReportSet                ExceptStatReport
{
  TypeActions               Log
  TypeActions               Statistics
  LoggingLevel              1
  StatType                  Exception
  TraceData                 RecordSize
  TraceRecordSize           200
}
```

*Source: z/OS V1R13.0 Communications Server IP Configuration Guide*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > pasearch*

- The pasearch command can be used to obtain details of the management policies on your system. This is a sensitive command and needs to be protected.
- The profile to protect pasearch, defined in the SERVAUTH class is:

  EZB.PAGENT.sysname.tcpprocname.*

Where:

- EZB Constant
- PAGENT Constant for this resource type
- sysname The system name
- tcpprocname The TCP/IP proc name
- * For all policy type options

*Securing Access to Policy Files:*

```
TCP/IP pasearch CS V1R13 Image Name: TCPIPD
Date: 08/03/2011 Time: 08:26:39
TTLS Instance Id: 1312374380
  policyRule: Default_FTP-Server~1
  Rule Type: TTLS
  Version: 3 Status: Active
  Weight: 255 ForLoadDist: False
  Priority: 255 Sequence Actions: Don't Care
  No. Policy Action: 3
  policyAction: gAct1~FTP-Server
   ActionType: TTLS Group
   Action Sequence: 0
  policyAction: eAct1~FTP-Server
   ActionType: TTLS Environment
   Action Sequence: 0
 policyAction: cAct1~FTP-Server
   ActionType: TTLS Connection
   Action Sequence: 0
```

*Source: z/OS V1R13.0 Communications Server IP Configuration Guide*
*Volume 4 Security and Policy-Based Networking*

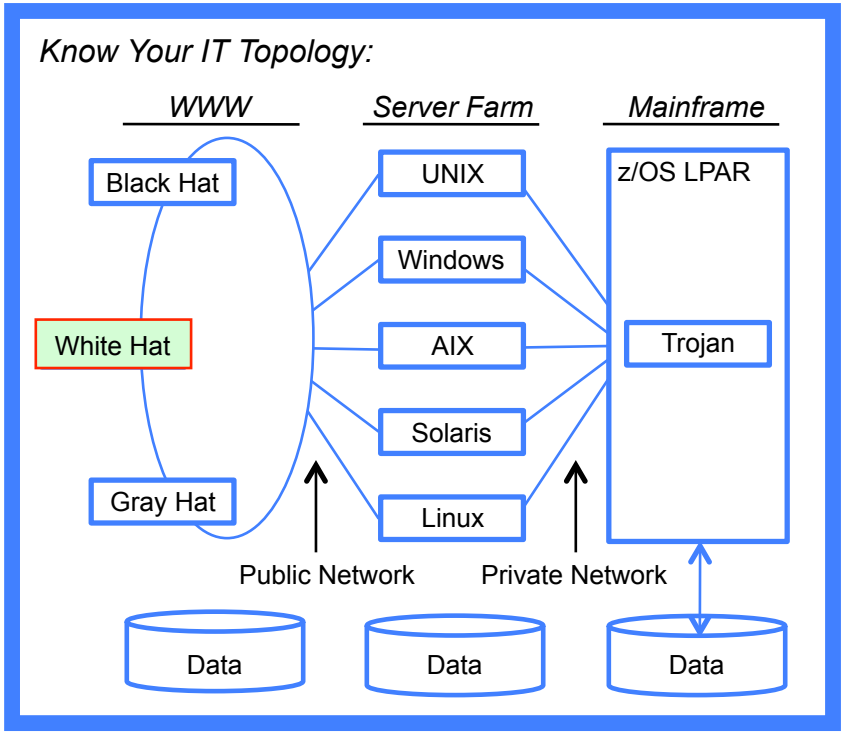
# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > IDS Testing*

- You can test IDS Policy efficacy using a PC-based network penetration testing tool (Advanced Port Scanner V1.3) against the z/OS ports.
- Such a test will likely trigger system messages similar to the following:

```
EZZ8761I IDS EVENT DETECTED 638
EZZ8730I STACK TCPIP
EZZ8762I EVENT TYPE: FAST SCAN DETECTED
EZZ8766I IDS RULE ScanGlobal
EZZ8767I IDS ACTION ScanGlobalAction
```

- These messages can be detected and spawn notification to security staff.




*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > IDS Summary*

❑ There are 16 specific areas of network vulnerability that can be monitored using PAGENT and reported on using NETSTAT Operator Commands:

- SCAN Detection
- Malformed Packets
- Restrict Outbound
- Restrict Protocol
- Restrict IP Option
- Restrict Redirect
- Restrict Fragment
- UDP Perpetual Echo
- Floods
- Data Hiding
- TCP Queue Size
- Global TCP Stall
- EE LDLC Check
- EE Malformed Packet
- EE Port Check
- EE XID Flood

*Checking Intrusion Detection Status:*

<> Operator Command to Display Ports:

```
/Display TCPIP,,NETSTAT,IDS
```

<> Intrusion Detection Services Summary:

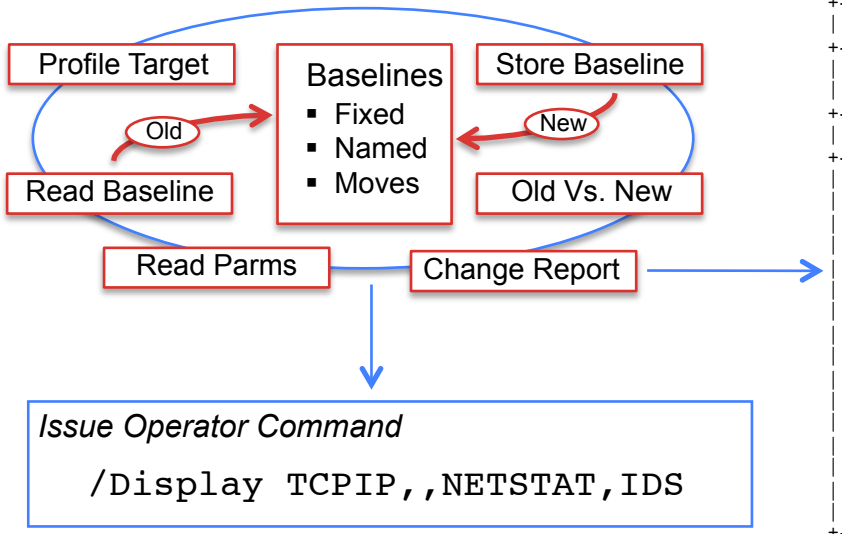
```
SCAN DETECTION:
  GLOBRULENAME: SCANGLOBAL
  ICMPRULENAME: ICMP~1
  TOTDETECTED:  0        DETCURRPLC: 0
  DETCURRINT:   0        INTERVAL:   30
  SRCIPSTRKD:   4        STRGLEV:    00000M
ATTACK DETECTION:
  MALFORMED PACKETS
    PLCRULENAME: MALFORMEDPACKET
    TOTDETECTED: 0        DETCURRPLC: 0
    DETCURRINT:  0        INTERVAL:   60
  OUTBOUND RAW RESTRICTIONS
    PLCRULENAME: OUTBOUNDRAW
```

*Source: IBM z/OS V1R13 CS TCP/IP Implementation – March 2012*
*Volume 4 - Security and Policy-Based Networking*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > IDS Baseline*

*Building an Intrusion Detection Services Baseline and Change Report*




```
+-------------------------------------------------------------------+
|          Recent Trends in Intrusion Detection Reporting           |
+---------------------+---------------------------------------------+
|     SMFID:S0W1      | INTRUSION DETECTION HISTORY AND TRENDS      |
+---------------------+-----+-----+-----+-----+-----+-----+-----+
|        DATES        |07/01|06/29|--/--|--/--|--/--|--/--|--/--|
|        TIMES        |18:39|18:38|--:--|--:--|--:--|--:--|--:--|
+---------------------+-----+-----+-----+-----+-----+-----+-----+
|        TOTAL        | 002 | 003 | 000 | 000 | 000 | 000 | 000 |
+---policy_elements---+-----+-----+-----+-----+-----+-----+-----+
|  SCAN Detection     | --C | --C | --- | --- | --- | --- | --- |
|  Malformed Packets  | --- | --- | --- | --- | --- | --- | --- |
|  Restrict Outbound  | --- | --- | --- | --- | --- | --- | --- |
|  Restrict Protocol  | --- | --- | --- | --- | --- | --- | --- |
|  Restrict IP Option | --- | --- | --- | --- | --- | --- | --- |
|  Restrict Redirect  | --- | --- | --- | --- | --- | --- | --- |
|  Restrict Fragment  | --- | --- | --- | --- | --- | --- | --- |
|  UDP Perpetual Echo | --- | --- | --- | --- | --- | --- | --- |
|  Floods             | --C | --- | --- | --- | --- | --- | --- |
|  Data Hiding        | --- | --C | --- | --- | --- | --- | --- |
|  TCP Queue Size     | --- | --- | --- | --- | --- | --- | --- |
|  Global TCP Stall   | --- | --- | --- | --- | --- | --- | --- |
|  EE LDLC Check      | --- | --- | --- | --- | --- | --- | --- |
|  EE Malformed Packet| --- | --- | --- | --- | --- | --- | --- |
|  EE Port Check      | --- | --- | --- | --- | --- | --- | --- |
|  EE XID Flood       | --- | --- | --- | --- | --- | --- | --- |
+---------------------+-----+-----+-----+-----+-----+-----+-----+
```

# Mainframe Intrusion!

*The Agenda:*

- *Looks like we're in really big trouble!*
- *Is your Mainframe Under Attack?*
  - ✓ *How do you know?*
  - ✓ *What can you do?*
- *Common Attack Techniques!*
  - ✓ *Port Scanning*
  - ✓ *Data Packet Fragmentation*
  - ✓ *Remote Access Trojans*
- *Who are they?*
  - ✓ *White Hats Vs. Black Hats*
  - ✓ *Tools of the Trade*
  - ✓ *Available Training*
- *Attack Scenario*
  - ✓ *Server Farm*
  - ✓ *The Mainframe*
- *Fighting Back – IPSec Defenses!*
  - ✓ *Scan Detection*
  - ✓ *Malformed Packets*
  - ✓ *External Security Manager*
  - ✓ *Management Policy*
- *The Policy Management Agent*
  - ✓ *Internet Key Exchange*
  - ✓ *Network Security Services*
  - ✓ *Defense Manager*
  - ✓ *Traffic Regulation Management*
- *Intrusion Detection Services (IDS)*
  - ✓ *The Agent Configuration*
  - ✓ *Policy: Rules, Actions, Reports*
  - ✓ *Securing Policies – pasearch*
  - ✓ *IDS Report Summaries*
- *Project White Paper*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Report > Cyber Crimes*

- Management has the obligation to put in place and enforce *Best Practices* that:
  - ✓ With Respect to Employees
    1. Educate
    2. Equip
    3. Empower
  - ✓ With Respect to Stakeholders
    1. Disclose Material Attacks
    2. Potential Damages
    3. Damage Mitigation
    4. Corrective Actions
  - ✓ With Respect to Law Enforcement
    1. Report, Cooperate
    2. Prosecute Offenders

*Source:http://www.thenewstribune.com/2012/06/29/2198831/cybercrime-disclosures-scarce.html*

# Mainframe Intrusion!

*Is your Mainframe Safe? – Fighting Back > Policy Agent > White Paper*

- This "White Paper" describes in detail the mechanism for defining policy metrics which in turn are used to monitor and defend network operation from spies and intruders.

The Intrusion Detection Service (IDS) Policy Management Project

A NewEra Software, Inc. White Paper
July-August, 2012

Table of Contents:

# Continuing Education Credit

CERTIFICATE OF ATTENDANCE

Awarded to

as presented at the following
Continuing Education Course

Eligible for Continuing Professional Education Credit of One Hour

Brian Cummings, SEC Project Manager

SHARE in Anaheim
Security and Compliance Project
August 6 – 10, 2012
Anaheim, California

# That's it folks, all done!

*Session Evaluation - Session Number - 11530*

How to Detect Mainframe Intrusion Attempts

Paul R. Robichaux
NewEra Software, Inc.
prr@newera.com

SHARE.org/AnaheimEval


Visit www.SHARE-SEC.com for more information on the SHARE Security & Compliance Project