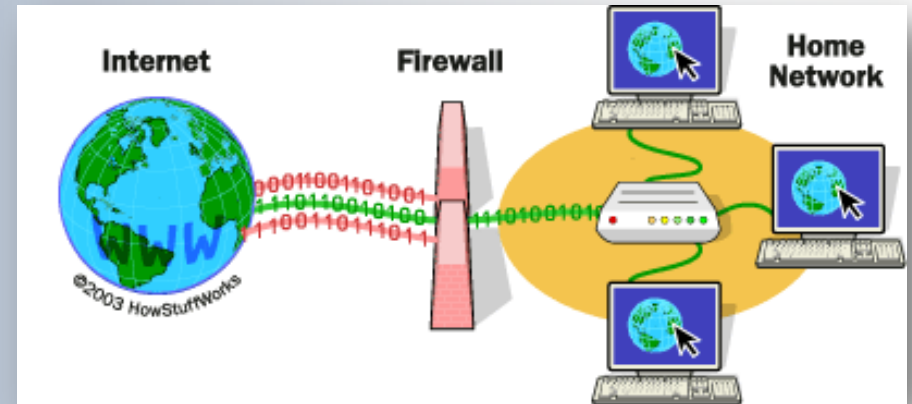


# COMP 175

## System Administration and Security



# CONTROLLED ACCESS



# Control access to system

- Access control mechanisms – application layer
  - ◆ FTP server security directives in `/etc/ftpaccess`
  - ◆ Apache server: `/etc/httpd/httpd.conf`
- Control network traffic at network layer - Firewall
  - ◆ operates at lowest level of the networking protocol stack
  - ◆ examines and discards packets from unauthorized systems before they have a chance to attack applications
- Use advanced routing techniques
  - ◆ IP masquerading “Hides” LAN clients



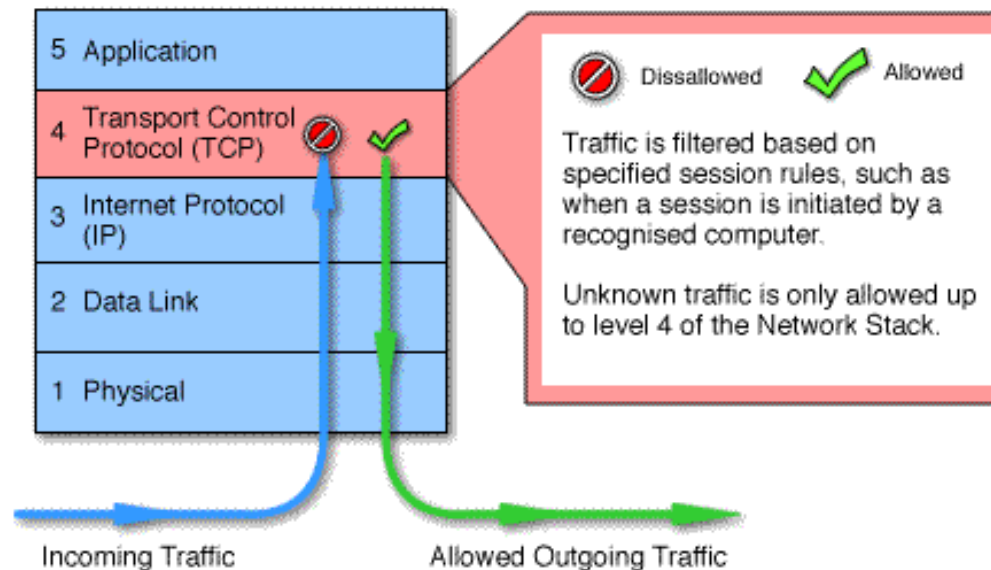
# Access control at different layers

OSI model	Security method	Internet model
Application layer	Application configuration files	Application layer
Presentation layer	xinetd.conf	
Session layer	TCP Wrappers	Transport layer
Transport layer	Proxy server	
Network layer	Packet filtering firewall	Internet layer
Data Link layer		Link layer
Physical layer	Special switching equipment	



# Firewall

- A firewall -- a packet filter
  - ◆ Access control at lower level of stack
  - ◆ Firewalls rely on rules
    - **Rules:** IP packet characteristics and action to take
- Networking stacks in Linux are contained in the kernel
  - ◆ gives Linux control over network packet management





# Firewalls

## Packet Filtering Firewalls (Stateless)

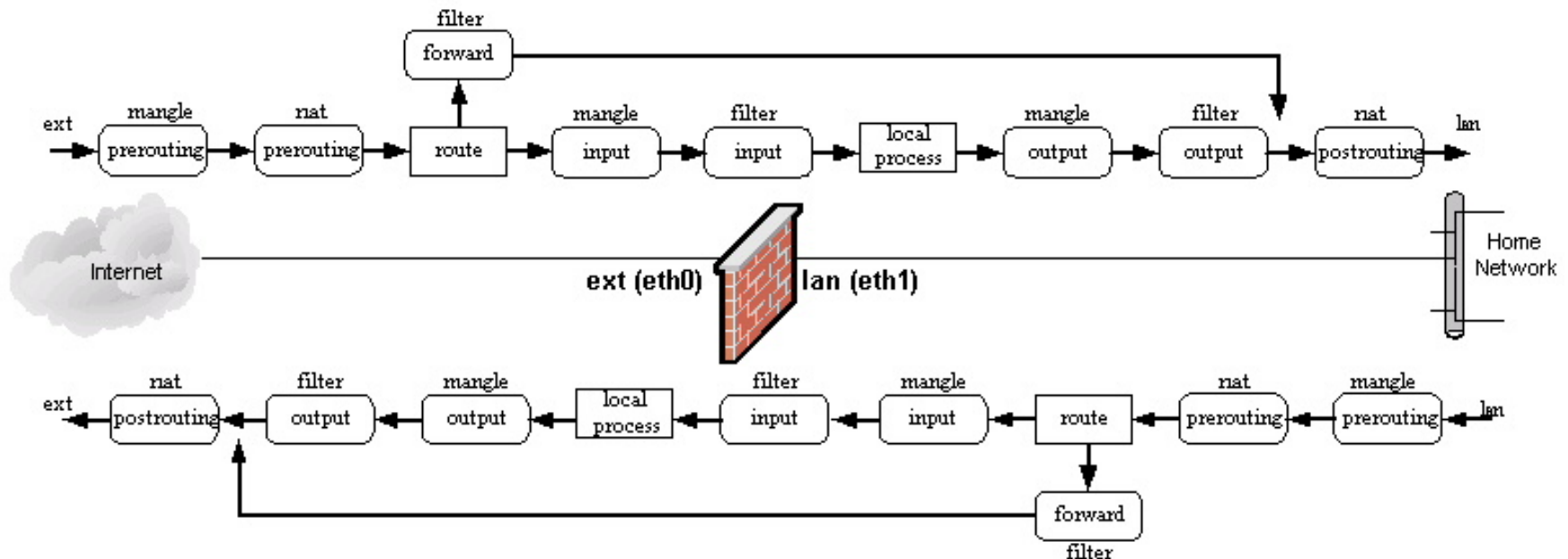
- **Simplest** type of firewall. For each packet the firewall applies its rule set to determine which packet to allow/disallow. Criteria are:
  - Source IP address
  - Destination IP address
  - TCP/UDP source port
  - TCP/UDP destination port
- Rule may be based on a single/multiple criteria. Disallowed packets may be dropped (silently discard) or rejected (discard and send "error responses" to the source).



# NetFilter / IP Tables

## NetFilter

- Provides hooks inside the kernel
  - ◆ A hook connects another program at that point
- IP Tables: list of rules associated with the hooks





# Using NetFilter / IP Tables

NetFilter / IP Tables provide:

- **Stateful Packet Filtering** - act on packets based on their state
- **Packet Mangling** - Examine & alter header fields
- Logging based on the value of any header field
- Pass packets to programs for further processing outside of the Linux kernel
- Implementation of intelligent routing based on Quality of Service (QoS) features



# Stateful Firewall

- Examines **content** of packets rather than just filtering them by address
- Take into account the **state** of the connections they handle, e.g a legitimate incoming packet can be matched with the outbound request for that packet and allowed in.
- Conversely, an incoming packet masquerading as a response to a nonexistent outbound request can be blocked
- A stateful firewall would block all SYN-ACK and ACK packets that are not a legitimate part of a 3-way handshake





# Network Address Translation

- IP tables provides special routing functionality  
Network Address Translation (NAT)
- NAT alters the IP address or other header information in a packet
  - ◆ NAT 1:1 Inside/Outside address mapping
  - ◆ IP masquerading / Port Address Translation
  - ◆ One public address hides multiple private ones
  - ◆ Most uses of NAT are a form of PAT
    - Port Address Translation



# NAT pros and cons

- NAT can use one IP address for a LAN to connect to the Internet
- Behind their router, the same private IP addresses can be reused on every LAN
- A remote computer cannot connect to a client within a masqueraded LAN. The firewall effectively hides the entire LAN
- However NAT can break some network services (FTP, IRC, streaming audio) – special handling is needed to fix this



# iptables

- iptables - userspace module where sysadmin interacts to enter firewall rules into predefined tables (CLI)
- Netfilter - kernel module, built into the kernel, that actually does the filtering





# iptables

- **filter** INPUT, OUTPUT, and FORWARD tables.  
The default table, will report its contents with the iptables -L command
- **nat** Used for creating NAT tables  
PREROUTING table alters packets as soon as they enter (used when masquerading connections)  
OUTPUT table alters locally generated packets  
POSTROUTING tables alters packets before they are about to be sent on the network
- **mangle** Alters the packets – to fix up specific protocols for functionality



# iptables Config

```
#!/bin/sh
```

```
#Define interfaces:
```

```
EXTIF="eth1"
```

```
INTIF="eth0"
```

```
echo "    External Interface:  $EXTIF"
```

```
echo "    Internal Interface:  $INTIF"
```

```
$IPTABLES -P INPUT ACCEPT          (set the policy)
```

```
$IPTABLES -F INPUT                  (flush any existing rules)
```

```
$IPTABLES -P OUTPUT ACCEPT         (set the policy)
```

```
$IPTABLES -F OUTPUT                 (flush any existing rules)
```

```
$IPTABLES -P FORWARD DROP         (set the policy)
```

```
$IPTABLES -F FORWARD               (flush any existing rules)
```

```
$IPTABLES -t nat -F                (Table nat flush)
```

```
# deny incoming with private address
```

```
$IPTABLES -A INPUT -i $EXTIF -s 169.254.0.0/16 -j(ump) DROP
```

```
$IPTABLES -A INPUT -i $EXTIF -s 172.16.0.0/12 -j DROP
```

```
$IPTABLES -A INPUT -i $EXTIF -s 192.168.0.0/16 -j DROP
```



# iptables Config

# don't like - ignore

```
$IPTABLES -A INPUT -I $EXTIF -s 62.0.0.0/8 -j DROP
```

```
$IPTABLES -A INPUT -I $EXTIF -s 63.223.0.0/16 -j DROP
```

```
$IPTABLES -A INPUT -I $EXTIF -s 64.50.144.0/20 -j DROP
```

# don't like - reject - go away

```
$IPTABLES -A INPUT -i $EXTIF -s 212.0.0.0/8 -j REJECT --  
    reject-with icmp-host-unreachable
```

# Allow all connections OUT and only existing in

```
$IPTABLES -A FORWARD -i $INTIF -o $EXTIF -j ACCEPT
```

```
$IPTABLES -A FORWARD -i $EXTIF -o $INTIF -m state --state  
    ESTABLISHED,RELATED -j ACCEPT
```

# Do PAT and masq inside addresses

```
$IPTABLES -t nat -A POSTROUTING -o $EXTIF -j SNAT
```

Prevent attempts from outside establishing a connection

Allow inside to establish connection to outside – e.g. initiation



# Blocking all Incoming ICMP

# To allow POP3 traffic

```
iptables -A OUTPUT -p tcp -s 0/0 -d 0/0 --dport 110 -j  
ACCEPT
```

#Block all incoming ICMP traffic:

```
iptables -A INPUT -p icmp -s 0/0 -d 0/0 -j DROP
```

#Block ICMP traffic from 10.100.100.0/24

```
iptables -A INPUT -p icmp -s 10.100.100.0/24 -d 0/0 -j DROP
```

# rate limit by protocol to slow DoS attacks

```
iptables -A INPUT -p tcp --dport 22 --syn -m limit --limit 2/m --limit-burst  
3 -j ACCEPT
```

```
iptables -A INPUT -p tcp --dport 22 --syn -j DROP
```

Can log - detail or summary

Can generate reports

**Policy produced rules to implement on firewall**

*Now – for some other security mechanisms...*



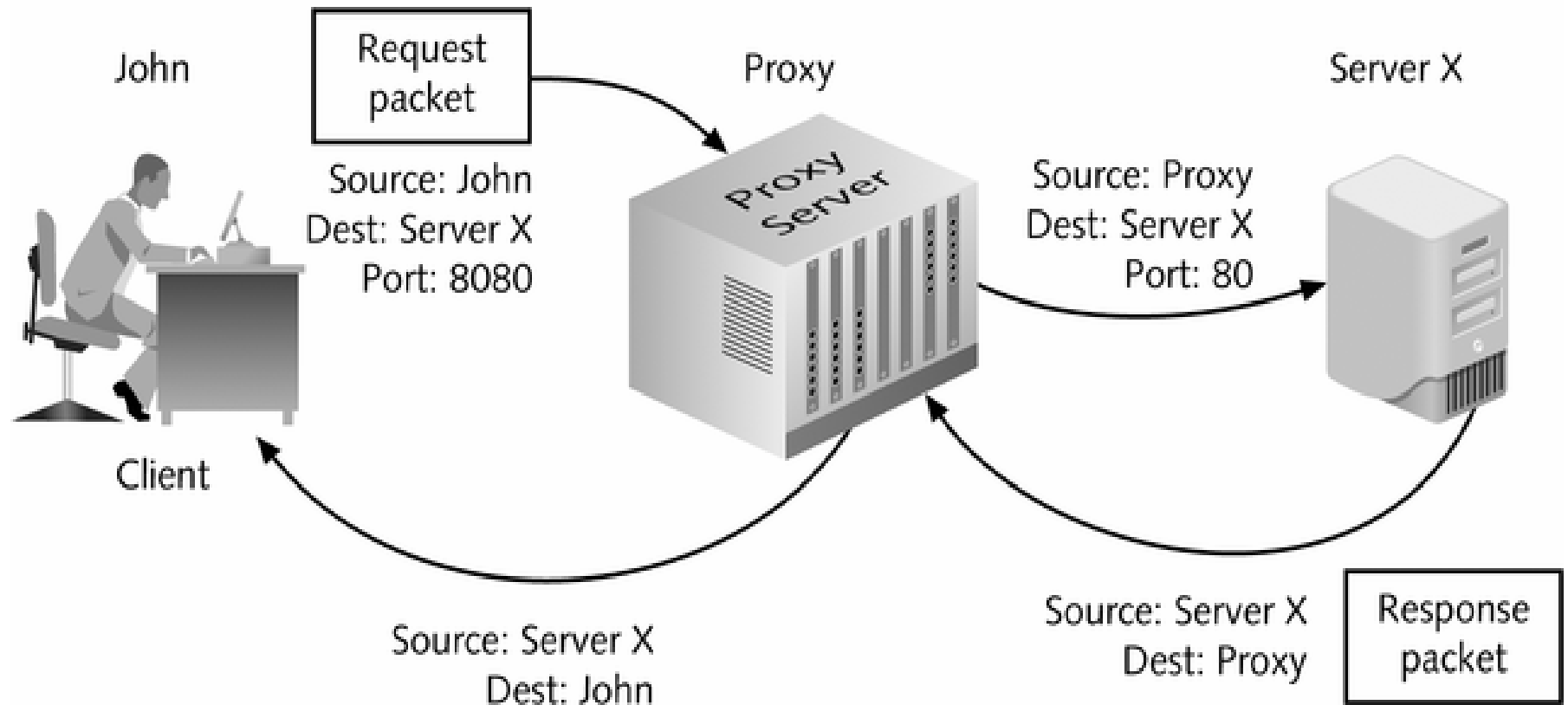
# Proxy Server

- Proxy server is very similar to IP masquerading, but the proxy works at the application level, not the IP level ("Squid" is a proxy server in Linux)
  - ◆ Must configure each client on the LAN to use special port for the proxy (vs. default port)
  - ◆ Clients use 8080/8008 instead of port 80
  - ◆ One proxy per application
- A proxy server provides security against outside attacks by insulating clients, or permits inside users to bypass internal controls (web filtering)





# Proxy server





# Encrypting Network Traffic

- The firewall restricts network traffic.
- PAT isolates clients in a LAN from the Internet
- However, the contents of packets in the LAN or through Internet are visible to everyone
  - ◆ With network analysis tool (a sniffer) hackers can view the packets
  - ◆ Prevention: encrypting the packets.
  - ◆ Some solutions:
    - Secure shell (SSH) (~~Telnet~~)
    - IPSec

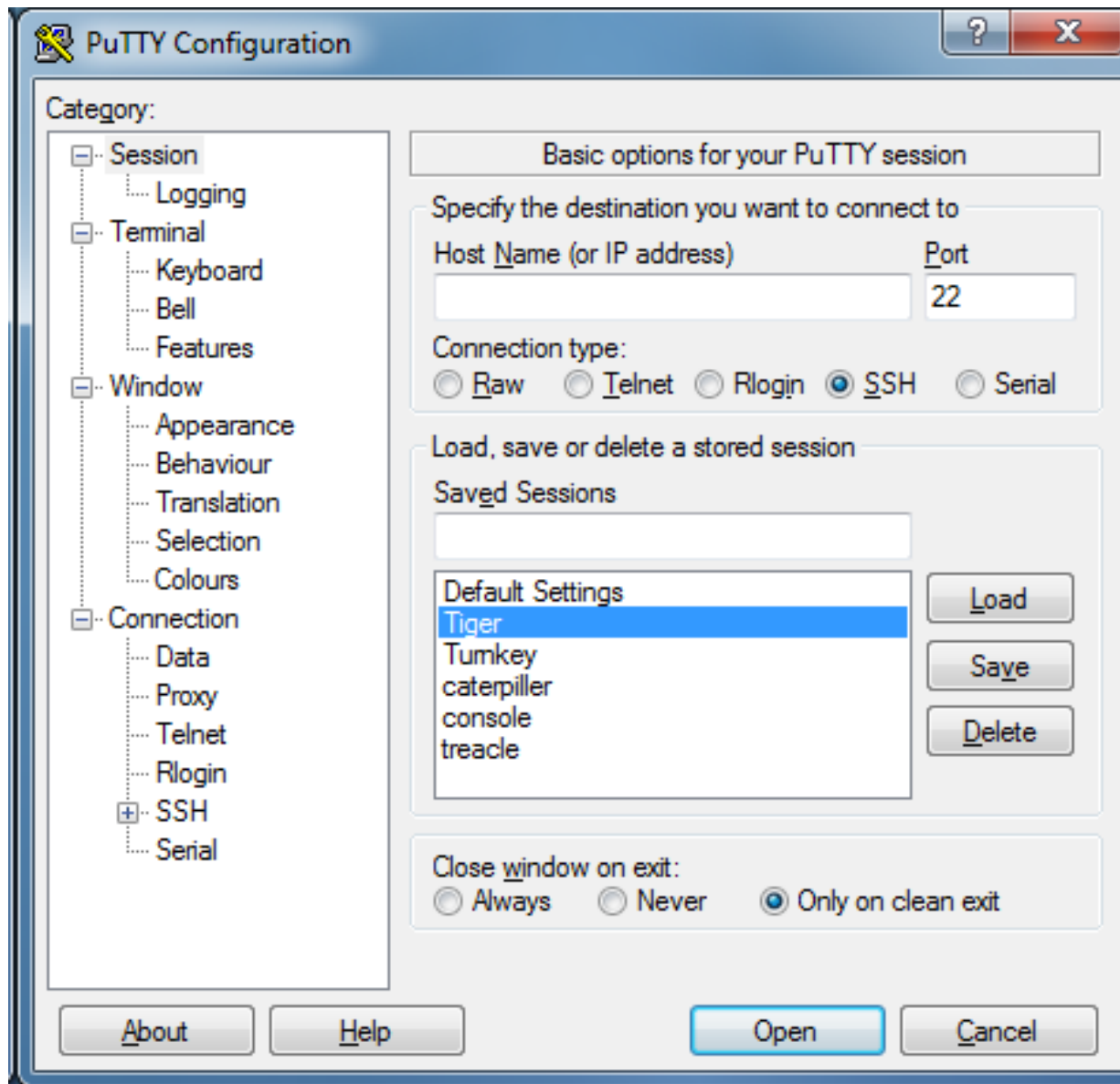


# The Secure Shell (SSH)

- Secure Shell (SSH) client-server program
  - ◆ ssh client program
  - ◆ sshd server program
- Replaces Telnet and rlogin for better security
- SSH - exchange asymmetric keys to establish the identity of a user requesting a connection
- Pass a symmetric session key securely
- Encrypt all subsequent traffic by symmetric session key



# putty





# OpenSSH

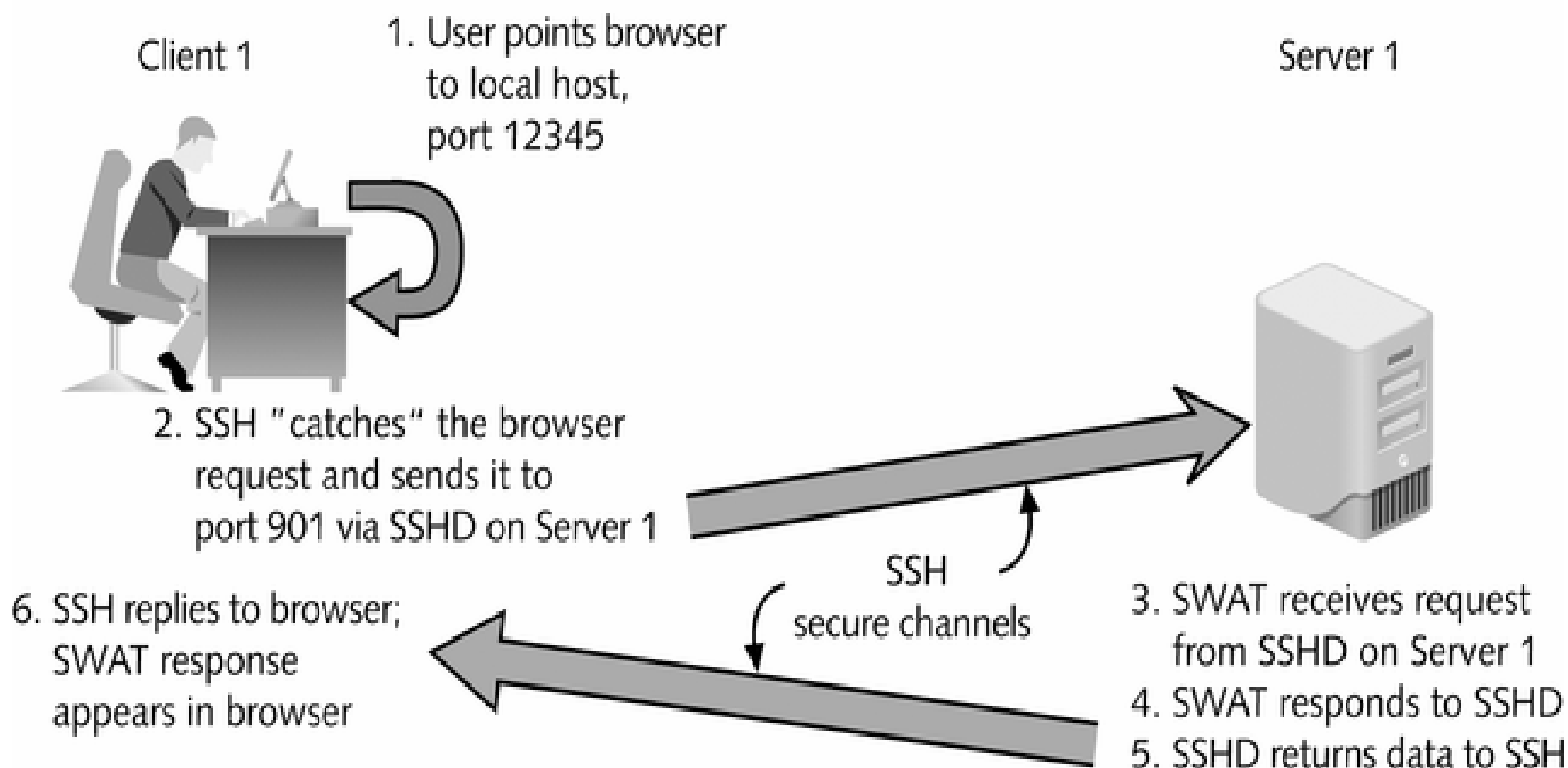
- OpenSSH implementation – cross platform
- SSH connections use port 22 by default
- To check the status of the sshd daemon
  - `$/etc/rc.d/init.d/sshd status`
- Ensure no firewall is blocking traffic on port 22
- SSH2 - more robust authentication process
- supports strong encryption of all network traffic, such as AES (128-, 192-, or 256-bit), Blowfish, CAST128
- SSH port forwarding can tunnel an insecure protocol inside a secure protocol



# Port forwarding in SSH

A system administrator wants to use SWAT to manage many Samba servers on a large LAN from a single system client1.

- However, using in SWAT in a browser, none of the traffic (including the password you must enter) is encrypted.





# Firewall Myths

The firewall will protect us

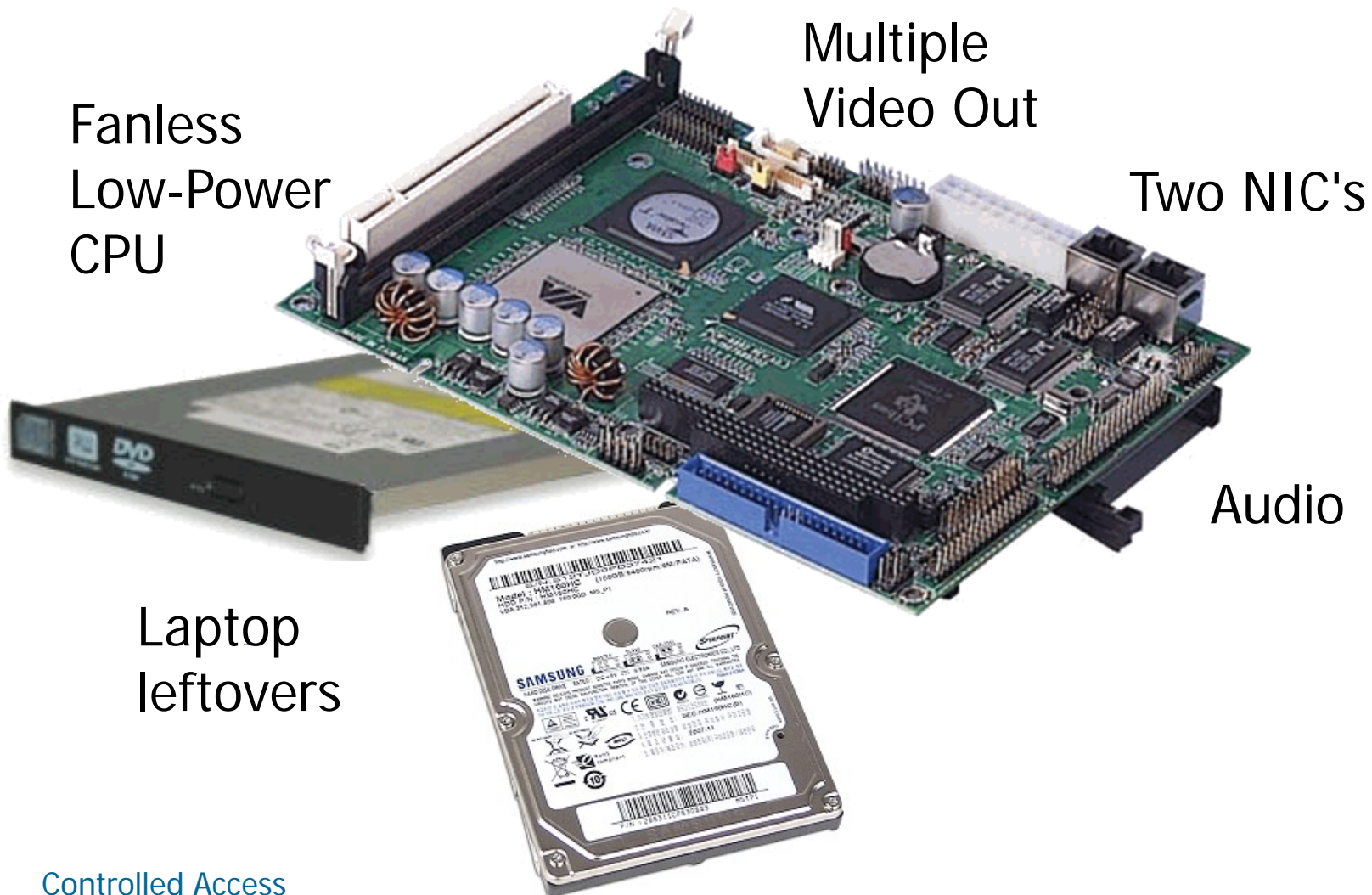
- Any open port is a hole
- Port 80 is a massive opening
- Developers know that port 80 is open
  - ◆ Remote PC applications
  - ◆ Peer to peer applications
  - ◆ Streaming media
- Bad guys know that port 80 is open too...





# Add Hardware

Linux-based expandable custom firewall with audible warnings? Serial outputs for relay driven alerts?



Fanless  
Low-Power  
CPU

Multiple  
Video Out

Two NIC's

Audio

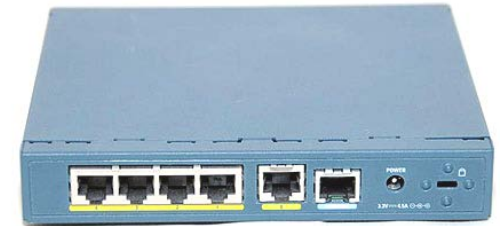
Laptop  
leftovers





# Buy Hardware

- Cisco ASA 5505 \$100-\$350
- Cisco Pix 501 \$40-50
- Juniper Netscreen \$350
- Fortinet Fortigate





# Features Vary

- VPN Connectivity (remote access)
- Intrusion Prevention System (IPS)
- Antivirus filtering
- Email filtering
- Web filtering
- Wireless support
- Web application security
- Logging
- Reporting



# December 2012

- Nov. 26 - Apple QuickTime for Windows
- Versions prior to 7.7.3 contain multiple vulnerabilities that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code on a targeted system.
- Proof-of-concept code that exploits a vulnerability with CVE ID 2012-3752 is available as part of the Metasploit framework.



- 03 – Google Chrome (W M L)
- Google Chrome versions prior to 23.0.1271.95 for Mac, Windows, and Linux contain multiple vulnerabilities that could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on a targeted system.
- Incorrect file path handling and use-after-free vulnerabilities
- An unauthenticated, remote attacker could exploit these vulnerabilities by convincing a user to view a malicious web page that contains crafted data. Successful exploitation could allow the attacker to execute arbitrary code on the system with the privileges of the user or cause a DoS condition on the affected system.
- Administrators are advised to apply the appropriate updates.
- Users are advised not to open e-mail messages from suspicious or unrecognized sources. If users cannot verify that links or attachments included in e-mail messages are safe, they are advised not to open them



# December 2012

- December – ongoing
- Deluge of fake package delivery confirmation emails containing a malicious attachment.
- FedEx and USPS invoice, label, document, etc.
  - ◆ 56kB to 323kB
- Similar fake BBB Complaint email
- Similar fake personal picture attachment

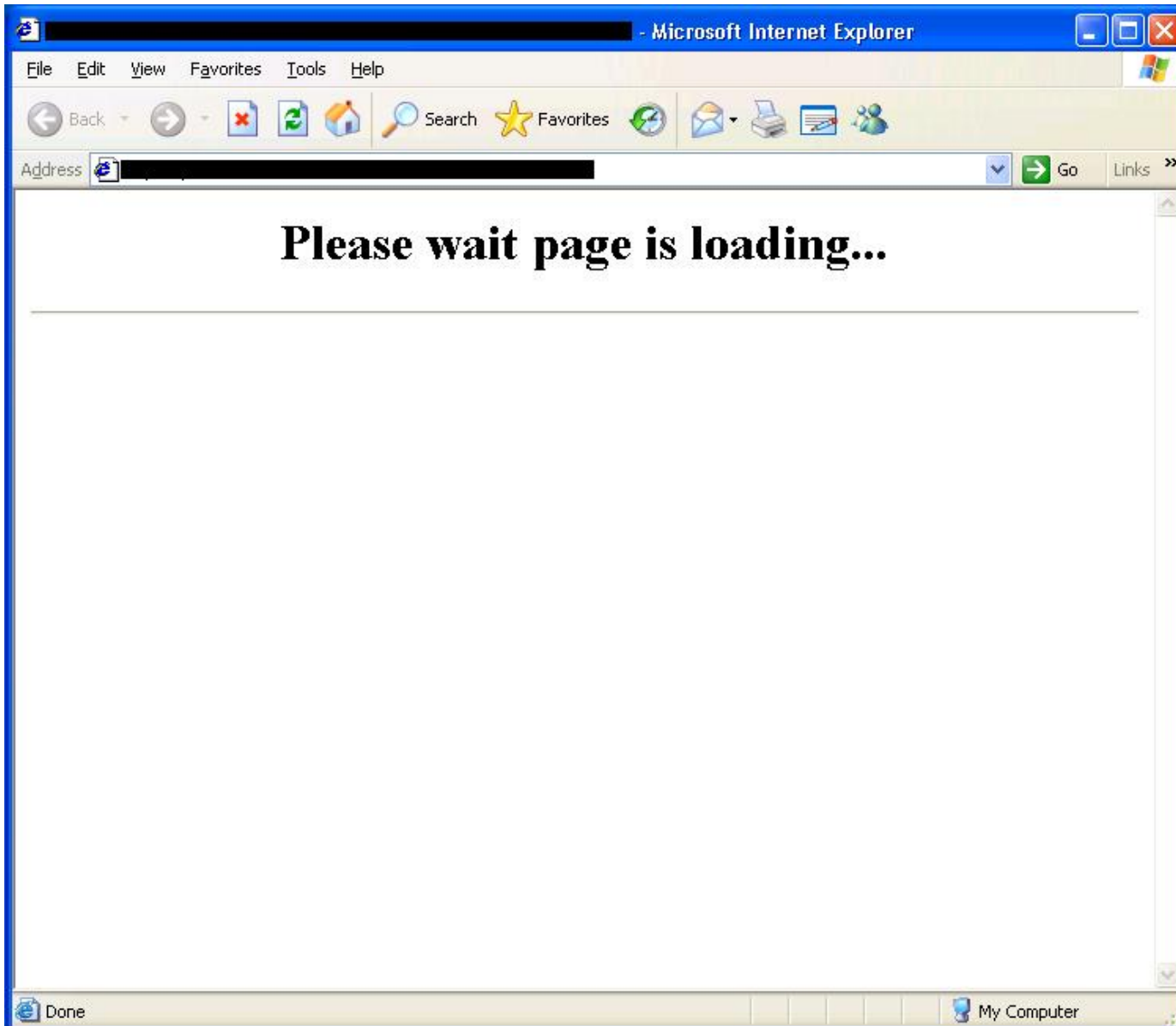


# Java Zero-Day

- Oracle Java SE contains multiple vulnerabilities that could allow an unauthenticated, remote attacker to bypass security restrictions, access sensitive information, execute arbitrary code, or cause a DoS condition on a targeted system.
- Reports indicate these vulnerabilities are being exploited successfully in the wild.



# Not Good





# December 2012

- JRE Exploits exist for current patch level
- Blacole (Blackhole) exploit kit used for driveby
  - ◆ Probes computer to determine what software you have installed, then selects (from its pool of vulnerabilities) appropriate exploit to use to gain access to the computer
- ...\\AppData\\LocalLow\\Sun\\Java\\Deployment\\cache\\...
- Trojan:JS/Medfos.A - targeted Firefox extensions
- Trojan:JS/Medfos.B
- ...\\AppData\\Local\\\*.crx files (multiple) container
- ...\\AppData\\Local\\\*.js files (multiple) file
- Redirected browser
- Rogue:Win32/Winwebsec - fake antivirus product

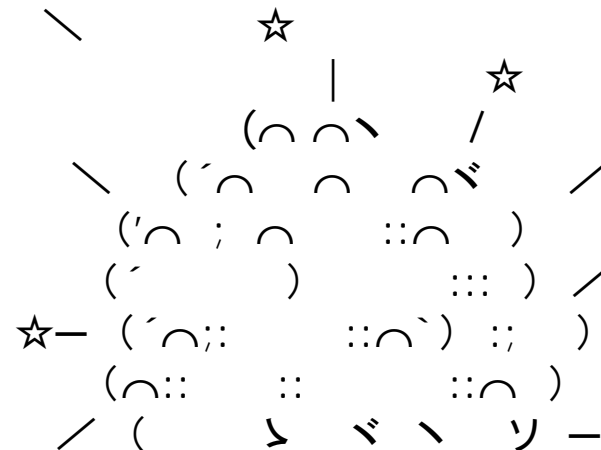




# Exploit

## Impaired MS Security Essentials

- Used to assist Security Essentials in the recovery
  - ◆ MS Sysinternals
    - Process Explorer
    - Process Monitor
    - Autoruns
  - ◆ Regedit
- HxD Hex file editor





# Blackhole Exploit Kit


 **Blackhole<sup>β</sup>**

STATISTICS | THREADS | FILES | SECURITY | PREFERENCES

[Logout](#)

Adv: Selling Iframe traffic in a huge amount JID#1: buldozer790@jabber.ru icq#1: 609347060 JID#2: technicalsupport911@jabber.org icq#2: 622729573  
Adv: IFrameShop.net - comfortable buying\selling iframe traffic with no limits. 256 countries. 24/7. Loads from 8%. Tell password "blackhole" and get +5% to the first order.

Start date:  End date:  [Apply](#) Autoupdate interval: 10 sec.

 **Blackhole<sup>β</sup>**

STATISTICS | THREADS | FILES | SECURITY | PREFERENCES

[Logout](#)

Adv: [Crypt.im](#) - crypt of iframe/javascript code.

Start date:  End date:  [Apply](#) Autoupdate interval: 10 sec.

**STATISTIC**

**TOTAL INFO**

216725 HITED ☐ 126661 HOSTS ☐ 21728 LOADS ☒ **17.16%** LOADS

**TODAY INFO**

10780 HITED ☐ 9530 HOSTS ☐ 1363 LOADS ☒ **14.31%** LOADS

**EXPLOITS**

	LOADS	% ↑
Java Rhino >	18146	82.56
PDF LIBTIFF >	3298	15.00
PDF ALL >	388	1.77
FLASH >	71	0.32
HCP >	29	0.13
MDAC >	26	0.12
Java OBE >	22	0.10

**OS**

	HITS	HOSTS	LOADS ↑	%
Windows 7	127535	75991	11474	15.10
Windows XP	46507	27240	5359	19.69
Windows Vista	41640	24676	4012	10.01

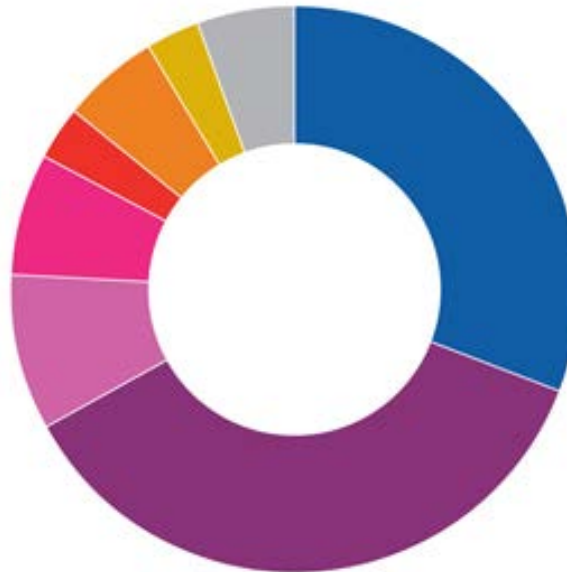
**BROWSERS ↓**

	HITS	HOSTS	LOADS	%
Chrome >	76	38	2	5.26
Firefox >	75892	47407	9603	20.26
MSIE >	138692	79587	12056	15.15



# Threat Vector Market Share

How web threats spread



- Drive-by redirect (Blackhole) 31%
- Drive-by redirect (not Blackhole) 36%
- Payload (fake antivirus) 9%
- Exploit site (Blackhole) 7%
- Exploit site (not Blackhole) 3%
- Fake antivirus 5.5%
- Search engine poisoning 3%
- Other 5.5%

Percent of malware detections in the past six months

Source: SophosLabs



# Since Ukraine: Busy

**CERTS**

Search CERTS

Arranged By: Date | Newest on top

**Today**

- US-CERT 10:03 AM  
Threat Actors Exploitin...

**Last Week**

- US-CERT Thu 8/11  
CISA Adds Two Known ...
- US-CERT Thu 8/11**  
**#StopRansomware: Ze...**
- US-CERT Thu 8/11  
Cisco Releases Security ...
- US-CERT Wed 8/10  
Palo Alto Networks Rel...
- US-CERT Tue 8/9**  
Vulnerability Summary ...
- US-CERT Tue 8/9  
Adobe Releases Securit...
- US-CERT Tue 8/9**  
Microsoft Releases Aug...
- US-CERT Tue 8/9**  
VMware Releases Secur...

**Two Weeks Ago**

- US-CERT 8/4/2022  
CISA Adds One Known ...
- US-CERT 8/4/2022  
AA22-216A: 2021 Top M...
- CISA 8/4/2022**  
Cisco Releases Security ...
- CISA 8/4/2022  
F5 Releases Security Up...
- CISA 8/3/2022  
VMware Releases Secur...
- US-CERT 8/2/2022  
Vulnerability Summary ...

## #StopRansomware: Zeppelin Ransomware

US-CERT [US-CERT@messages.cisa.gov]

Sent: Thu 8/11/2022 12:08 PM

To: mmaxwell@treacle.com



You are subscribed to Cybersecurity Advisories for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

### #StopRansomware: Zeppelin Ransomware

08/11/2022 10:03 AM EDT

Original release date: August 11, 2022

CISA and the Federal Bureau of Investigation (FBI) have released a joint Cybersecurity Advisory (CSA), [#StopRansomware: Zeppelin Ransomware](#), to provide information on Zeppelin Ransomware. Actors use Zeppelin Ransomware, a ransomware-as-a-service (RaaS), against a wide range of businesses and critical infrastructure organizations to encrypt victims' files for financial gain.

CISA encourages organizations to review [#StopRansomware: Zeppelin Ransomware](#) for more information. Additionally, see [StopRansomware.gov](#) for guidance on ransomware protection, detection, and response.

This product is provided subject to this [Notification](#) and this [Privacy & Use](#) policy.

Having trouble viewing this message? [View it as a webpage.](#)

You are subscribed to updates from the [Cybersecurity and Infrastructure Security Agency](#) (CISA)

[Manage Subscriptions](#) | [Privacy Policy](#) | [Help](#)



# One Approach

- <http://www.spi.dod.mil/lipose.htm>

Lightweight Portable Security (LPS) creates a secure end node from trusted media on almost any Intel-based computer (PC or Mac). LPS boots a thin Linux operating system from a CD or USB flash stick without mounting a local hard drive. Administrator privileges are not required; nothing is installed. The LPS family was created to address particular use cases: LPS-Public is a safer, general-purpose solution for using web-based applications.

185MB and 400MB (includes Libre/Adobe) versions



# Other Approaches

- Linux Live CD, DVD, USB stick
  - ◆ CrunchBang
  - ◆ Puppy
  - ◆ NimbleX
  - ◆ Slax
- Thin client hardware
- Kiosk distributions
  - ◆ Webconverger
  - ◆ Porteus





# Geopolitical

- Syria's Internet Goes Dark
- On Nov. 27, 2012, all Internet traffic from Syria to the rest of the world abruptly stopped. Mobile phone services were cut in key areas where anti-Assad forces are strong; the government blamed rebel forces for the outages. All 84 of Syria's IP blocks were unreachable starting on Thursday, any working IP blocks were hosted overseas. According to analysis by content delivery network CloudFlare, the Internet outage was probably achieved through updates in edge router configurations, rather than physical cable cuts.



# Anonymous Responds



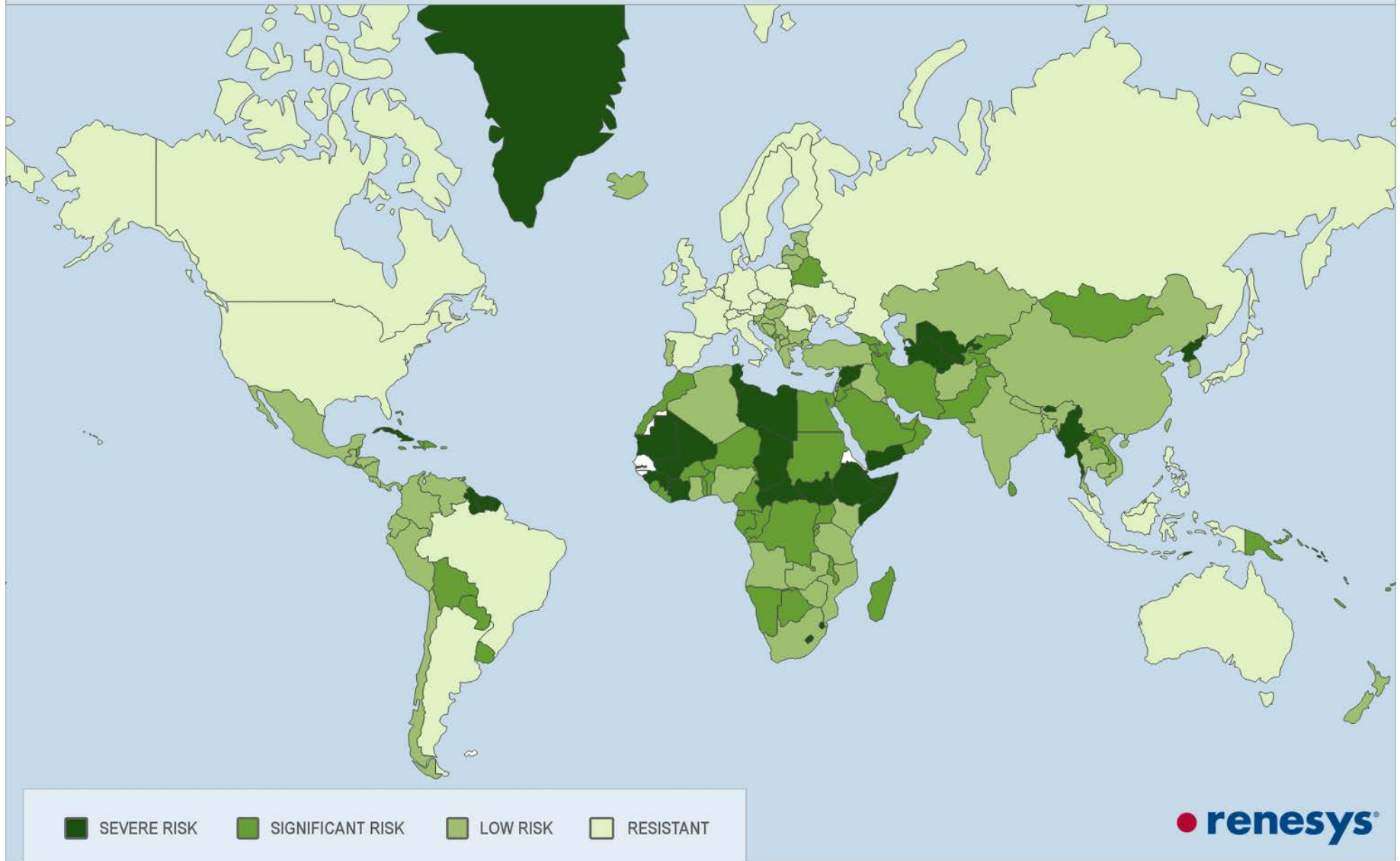




# 61 Most At Risk

## Countries w/ 1 or 2 Internet providers

Risk of Internet Disconnection - November 2012





# Safe Shopping

- <http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1104963>

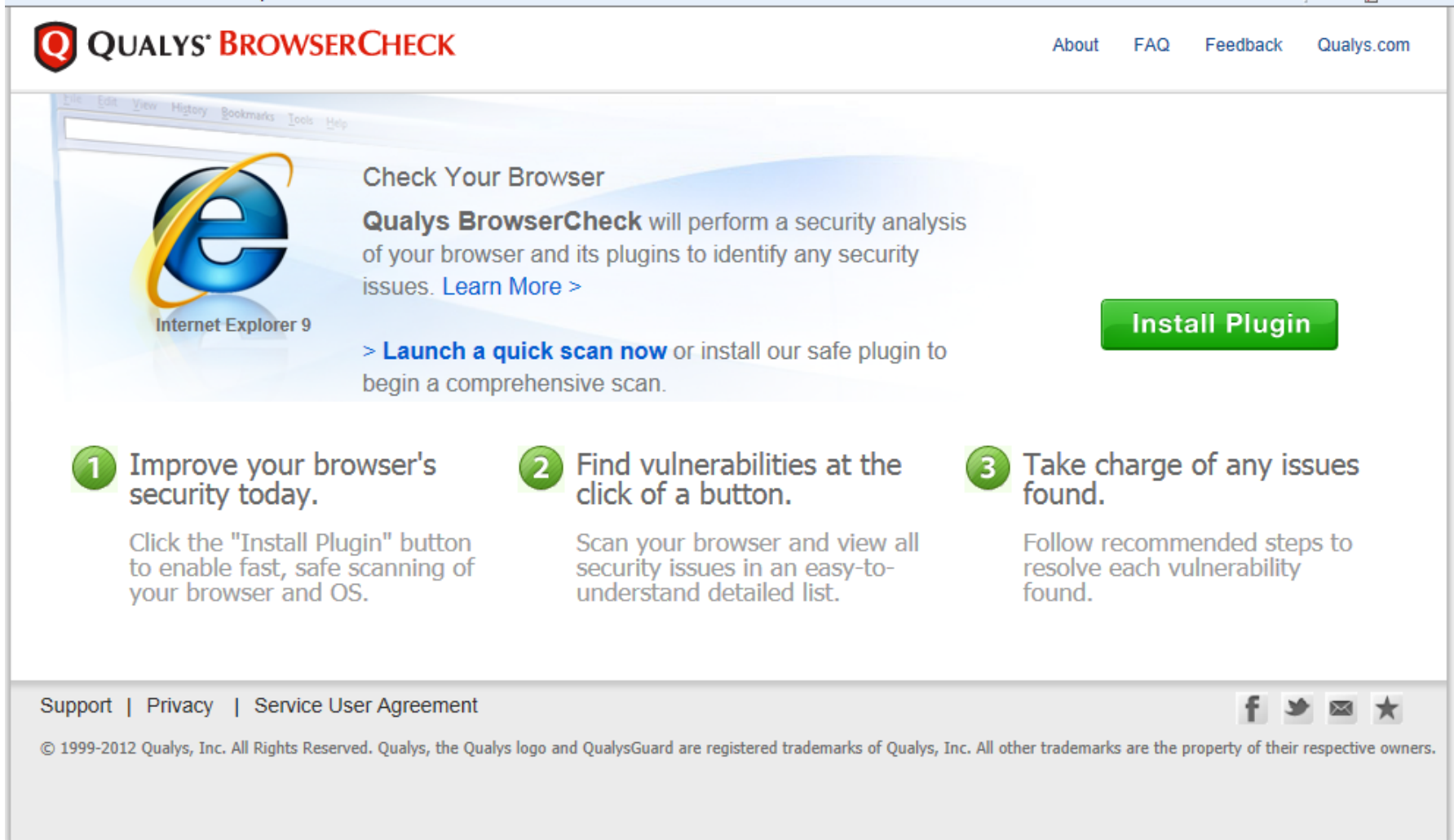
## Smartphone Security

- Automatically lock to the login screen after a couple of minutes of being idle
- Configured to use PIN or passcode for access
- Connect to Wi-Fi hotspots manually
- Have a mobile security suite installed



# Qualys Browser Check

- <https://browsercheck.qualys.com/>



The screenshot shows the Qualys BrowserCheck website. At the top, there's a navigation bar with the Qualys logo and the text "QUALYS BROWSERCHECK". To the right are links for "About", "FAQ", "Feedback", and "Qualys.com". Below the navigation bar, the main content area features a large graphic of the Internet Explorer 9 logo. To the right of the logo, the text reads: "Check Your Browser", "Qualys BrowserCheck will perform a security analysis of your browser and its plugins to identify any security issues. [Learn More >](#)", and a green button labeled "Install Plugin". Below this, there are three numbered steps: 1. Improve your browser's security today. (Click the "Install Plugin" button to enable fast, safe scanning of your browser and OS.) 2. Find vulnerabilities at the click of a button. (Scan your browser and view all security issues in an easy-to-understand detailed list.) 3. Take charge of any issues found. (Follow recommended steps to resolve each vulnerability found.) At the bottom, there's a footer with links for "Support", "Privacy", and "Service User Agreement", social media icons for Facebook, Twitter, and Email, and a star icon. Below these is a copyright notice: "© 1999-2012 Qualys, Inc. All Rights Reserved. Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners."

QUALYS BROWSERCHECK

About FAQ Feedback Qualys.com

Internet Explorer 9

Check Your Browser

Qualys BrowserCheck will perform a security analysis of your browser and its plugins to identify any security issues. [Learn More >](#)

[Install Plugin](#)

> [Launch a quick scan now](#) or install our safe plugin to begin a comprehensive scan.

- 1 Improve your browser's security today.  
Click the "Install Plugin" button to enable fast, safe scanning of your browser and OS.
- 2 Find vulnerabilities at the click of a button.  
Scan your browser and view all security issues in an easy-to-understand detailed list.
- 3 Take charge of any issues found.  
Follow recommended steps to resolve each vulnerability found.

Support | Privacy | Service User Agreement

© 1999-2012 Qualys, Inc. All Rights Reserved. Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

# Results



Browser Check Complete

## 3 Security Issues Detected

Follow the recommended actions in the results below to get software updates and resolve security issues.

[Re-Scan](#)

### Qualys® BrowserCheck Results



**Adobe Reader**  
10.0

Insecure Version

[Fix It](#)



**Java Plugin**  
1.7.0.7

Insecure Version

[Fix It](#)



**QuickTime Plug-in**  
7.7.2

Insecure Version

[Fix It](#)



**SilverLight**  
4.1.10329

Update Available



**Adobe Flash**  
11.5.502.110

Up To Date

### BrowserCheck Business Edition

Automatically track whether all your PCs are keeping up-to-date.  
FREE.



[Need Help?](#)

[Send us your feedback](#)

[Tell a friend](#)



# Seasonal Greetings

```
better !pout !cry  
better watchout  
lpr why  
santa claus < north pole > town
```

```
cat /etc/passwd > list  
ncheck list  
ncheck list  
cat list | grep naughty > nogiftlist  
cat list | grep nice > giftlist  
santa claus < north pole > town
```

```
who | grep sleeping  
who | grep awake  
who | grep bad || good  
for (goodness sake) {  
    be good  
}
```





# Remember

- A firewall implements policy
- Firewalls can be:
  - ◆ Stateless
  - ◆ Statefull
  - ◆ Application