

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# **Real World Security Practices**

**By: Thomas Donnelly**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# What is security?



**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# Security is:

- **Ensuring information is only seen by its intended viewers**
- **Protecting infrastructure from unauthorized use**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# Simple ways to protect yourself and your company

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# End User Security



AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# End users and their workstations are a tricky animal to protect

- Many facets to protect
  - Software exploits (PDFs anyone?)
  - End user software installs
  - Data leaks
- End users resistant to security and change
  - Maintaining a balance of security and productivity is a challenge

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# How can I protect my end users? (and me from them!)

- Antivirus if you are using a Windows environment
- Use secure browsers
- End user training
- Don't give end users administrative privileges unless they absolutely need them.
- Enforce good passwords.
- Proper network design (foreshadowing...)

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# Let's touch a little extra on passwords



Today's access password is "bellyrub".

ICANHASCHEEZBURGER.COM

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# What makes a good password

- **Easy to remember**
- **UPPER, lower, numbers, and special characters**
- **Atleast 8 characters**
- **Don't use the same password everywhere**
  - **Have a “junk” password**
- **If you must write them down, use a password manager such as KeePass**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

## **Tricks for creating secure easy to remember passwords**

- **Pick something you like, a soda, candy bar, football team, etc.**
- **Replace some letters with numbers, add some special characters where they make sense to you**
- **Tada new password!**
- **Example: \$t33l3r\$ would be considered a secure password and easy to remember if you like the steelers**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**Ok so I did what you said,  
and my end users still got  
hacked and now they are  
distrupting the whole  
office.**

**It happens, and that  
brings us to:**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# Network Security



**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# What does network security do for me?

- It is strictly a layer of security.
- It is NOT security in and of itself.
  - You should never have something relying completely on network security for its protection.
- Proper design can slow down, minimize, and often completely prevent exploits of your infrastructure.
- It can help narrow down where an incident occurred.
- This should be your first line of defense.
- Best way to stop worms.

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# What does network security consist of?

- This is where a lot of the buzzwords come in. Some popular ones are: Firewalls, Access Lists, RADIUS/802.1X, VLANs, the list goes on.
- Simply put, it is a way of controlling connections. Allow people who are supposed to get to a end point to get there, only on the services they are allowed. Deny everyone else.
- Also many network security devices will take proactive action to stop an exploit if it sees one occurring.

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# **What are some common network security practices?**

- **Segment each department into their own vlan.**
- **Only allow access to required ports.**
- **Segment servers of the same type into an appropriate vlan**
- **Use intelligent firewalls**
- **Use SSL or IPSEC VPNs for remote access and connectivity to remote sites.**
- **Be careful with IPv6, NAT is no longer a security feature.**
- **Set up and IDS/IPS to stop attacks in their tracks.**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**Ok, so you said network  
security isn't an only layer,  
what else do I do?**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# Server Security



**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# **Servers are secure out of the box, why do I need to protect them more?**

**Wrong. Most operating systems are very insecure out of the box. They have services running that don't need to be. Insecure remote login settings. Sometimes kernel level insecurities are enabled by default, the list goes on. Fact is most operating systems need some TLC before they are considered secure.**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# **How do I make my servers more secure then?**

**Thankfully there are some easy steps to reduce many of the potential exploits.**

- First off disable remote root/administrator logins. These are the first usernames a hacker will try.**
- If using Linux, enforce public/private key logins for internal servers.**
  - This probably isn't possible with hosting servers due to the additional configuration needed by the end user.**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- **Enable a host based firewall.**
- **Turn off services you don't need.**
- **ENFORCE SECURE PASSWORDS**
- **Don't give people access who don't need access.**
- **Don't give people root access unless it is absolutely 100% mission critical that they have root access.**
- **Remember that when you give someone ssh/remote desktop access to a server, they are behind the firewall protecting that server.**
- **Use hosts.allow on company servers to restrict ssh access**
- **Use an antivirus solution, especially on Windows servers**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# Next up: Common Sense, with a little bit of paranoia.



AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**Remember, there are  
people out there trying to  
do bad things to you.**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**The most successful attacks are ones directed against people.**

**This is commonly referred to as  
Social Engineering**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**Social engineering  
is nothing more  
than lying to get  
what you want.**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**Phone calls, fake  
web pages,  
costumes, these are  
all tools for social  
engineering**

AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# Ok so how do I stop them?

- Physical security
- Least privilege access rights
- End user training
- Don't trust anyone unless you know them and they are physically in front of you.
- Have proper procedures in place for lost credentials.

AUTOMATION

BOOTCAMP!

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

**So I did all of this and I  
STILL got hacked.**



AUTOMATION

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# **Guess what, as said before, it happens.**

Some times there just isn't anything you can do. There is a zero day exploit in a service you must provide and someone takes advantage of it. The recent X86\_64 Linux exploit is a good showing of this. This is why we have multiple layers of security.

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# **So what do I do now that I have been hacked?**

- **Have a procedure already in place.**
- **End users should immediately notify IT and their manager if they think they may have been hacked.**
  - **No repercussions should be taken on the end users. The goal is to get them to tell IT as fast as possible, if they are scared, they may not speak until it is too late.**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

- **Disconnect the machine from the network immediately to minimize the damage caused.**
- **Don't power the machine down for many reasons. It is much easier to see where the exploit originated from and what has happened. Also, depending on what has been done, it may not boot back up.**
- **Have IT go through and determine the cause of the exploit and a solution. Put that plan into action.**
- **If the exploit is large scale or of highly sensitive data, you may want to contact the FBI.**

**AUTOMATION**

**BOOTCAMP!**

cPanel Conference '10

OCTOBER 4TH-6TH, 2010

# **So I'm secure now right?**

**With enough precaution, best practices, and paranoia, you should be fairly safe. Like mentioned before, there is always a chance. This presentation just scratches the surface of cyber security. Hopefully it scares you a little and inspires you to help make the internet a safer place.**



OCTOBER 4TH-6TH, 2010

# Thank you!

**Contact:**  
**Thomas Donnelly**  
**thomas@cpanel.net**

