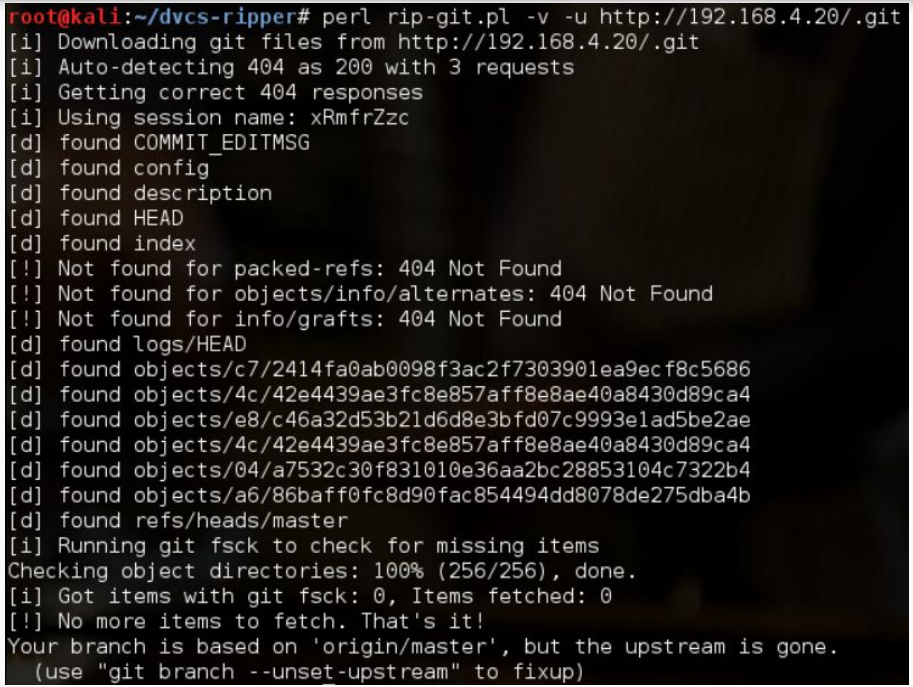
Red Team Debrief

At-Large CCDC 2016

Methodology

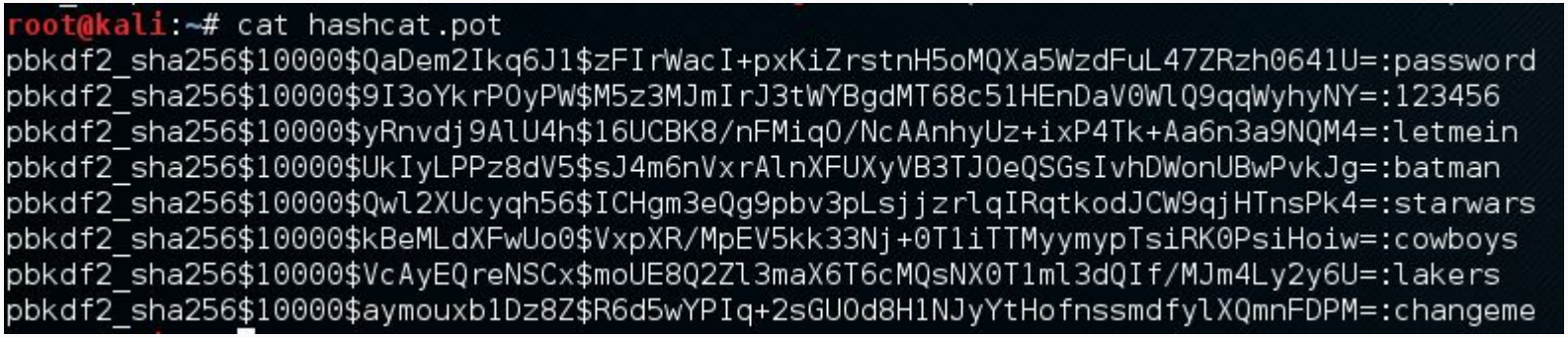
- Our aim is to find vulnerable services in the environment and replicate attacks against all blue teams in a timely manner to provide a fair and level playing field for the competition.
- Saturday we conducted reconnaissance of the environment and gained persistence.
- Sunday we ramped up our presence 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



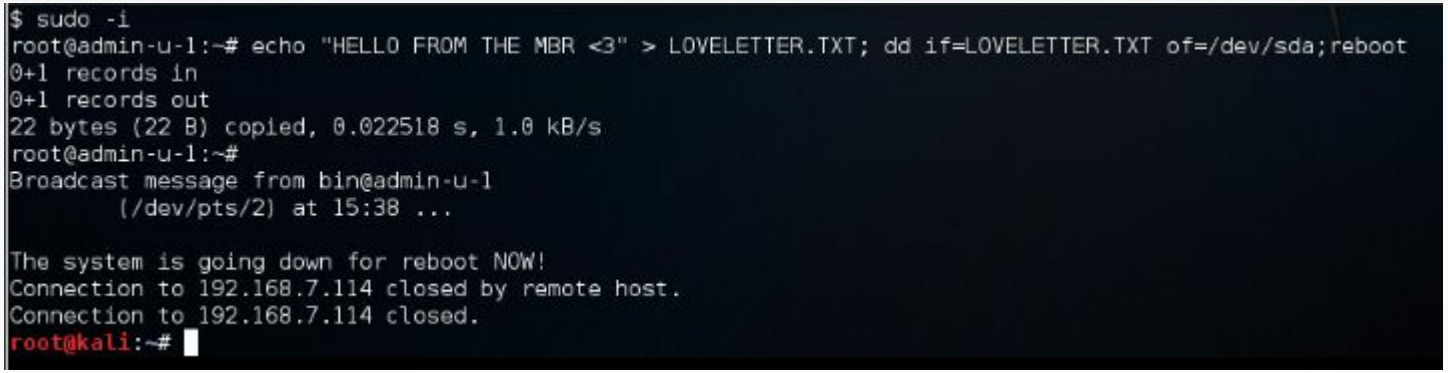
Exposed Git directories on 192.168.4.20 and 192.168.4.21

Successful Attacks



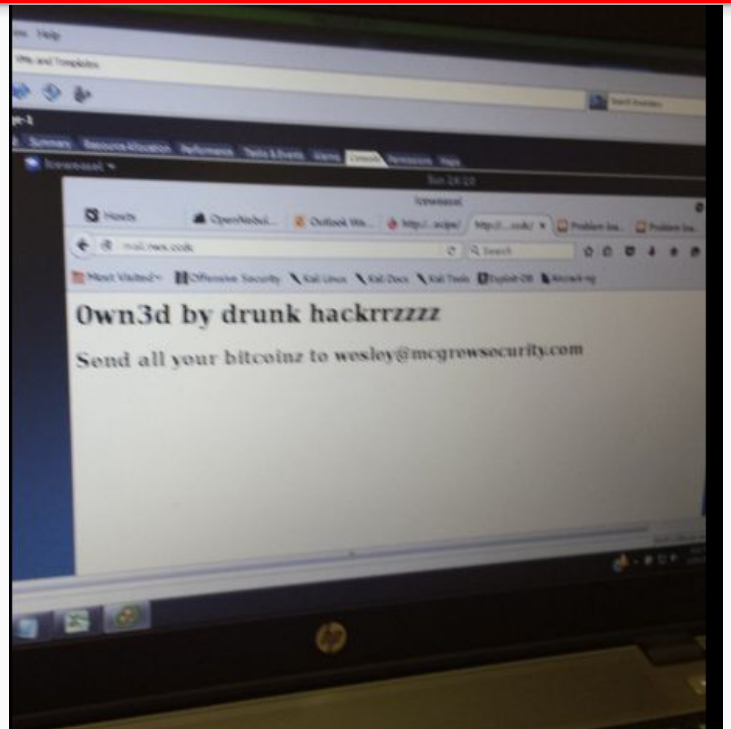
Cracked weak password hashes from Django database dump retrieved with default/weak credentials.

Successful Attacks



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!