10.11.1.71
Alpha

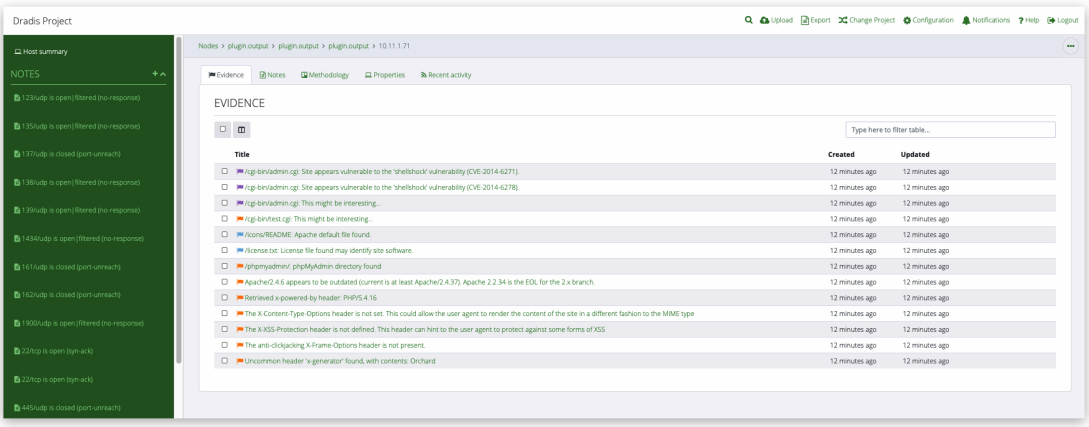
- **Recon**
  - Enum
    - Port Scanning

      This is the essential part of penetration. Find out what is available and how you could punch through it with minimum ease. DO NOT SKIP STEPS. DO NOT PASS GO. SEARCH ***ALL*** THE VERSIONS WITH `searchsploit` (or google -> `site:exploit-db.com APP VERSION`)

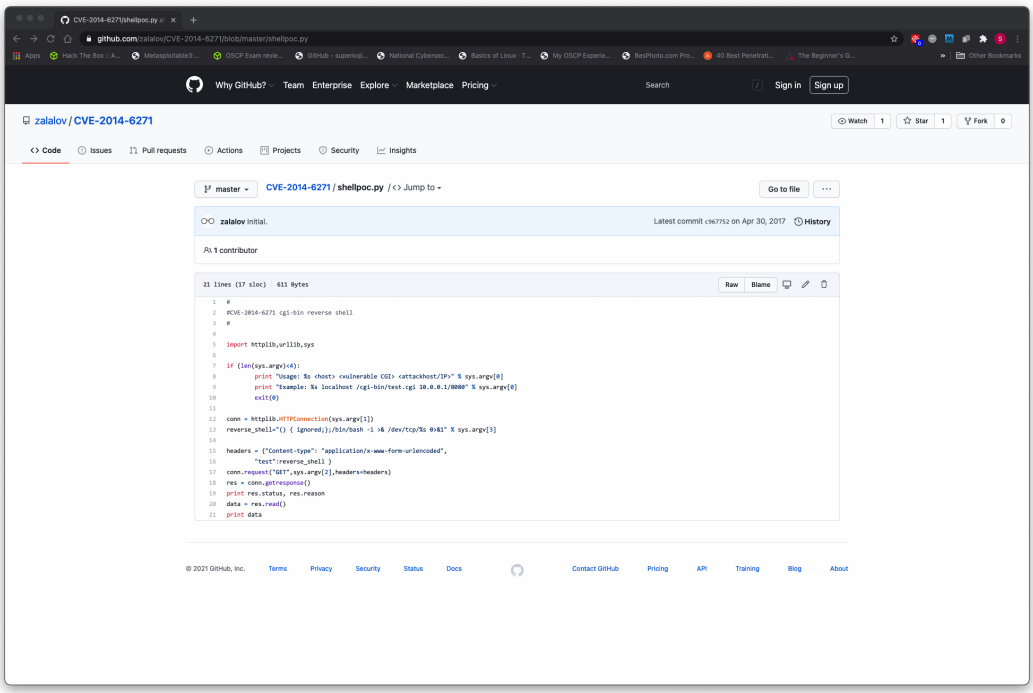
      - HTTP - 80, 8080, 8000

        ``` curl -i ${IP}/robots.txt ``` Note down Server and other module versions. searchsploit them ALL. Visit all URLs from robots.txt. ``` nikto -host $IP ``` ``` gobuster -u http://$IP -w /usr/share/seclists/Discovery/Web_Content/Top1000-RobotsDisallowed.txt gobuster -u http://$IP -w /usr/share/seclists/Discovery/Web_Content/common.txt ``` if nothing, find more web word lists. *Browse the site* but keep an eye on the burp window / source code / cookies etc. Things to be on look for:

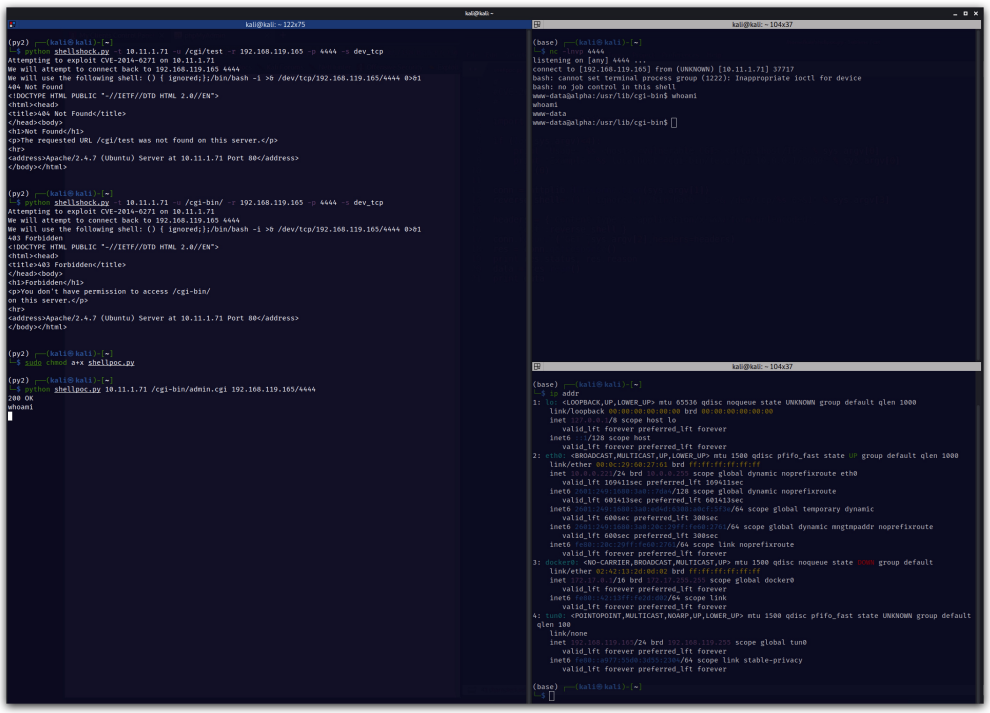
        - PHP/CGI Vulns


        ```

- cgi Shellshock Vuln



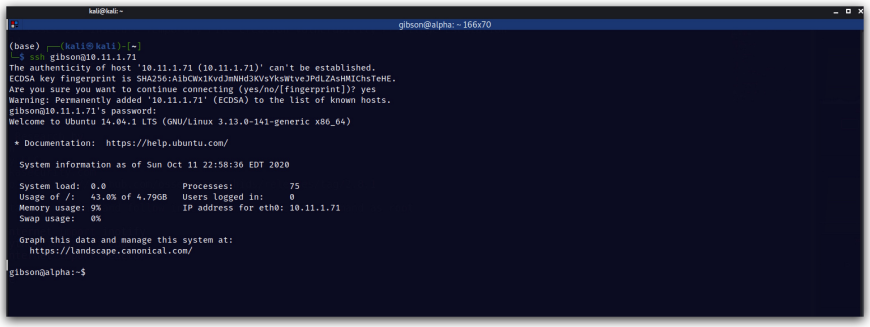
- CVE-2014-6271
  Shellshock



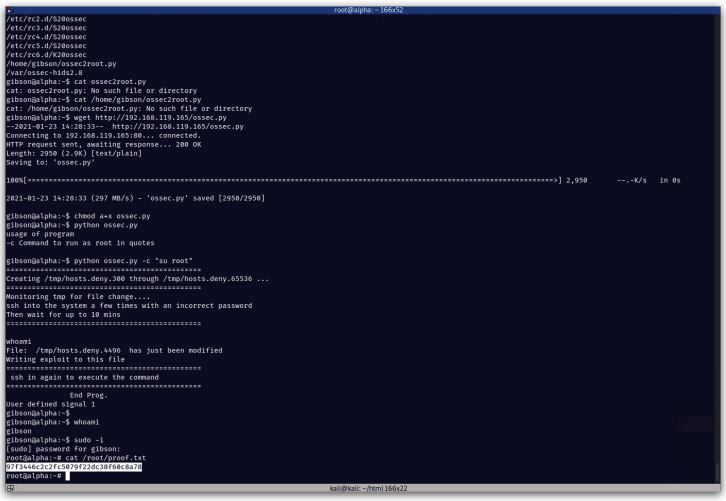
- Privilege Escalation
- Linpeas.sh

  found user gibson pw zaq1xsw2cde3

- ssh as user gibson



- Exploiting SUID Executables
- SUID Commands
- su -i
- proof.txt



- SSH - 22

Limited Shells

- python -c 'import pty; pty.spawn("/bin/sh")'