**CSEC-380/597 Final**

**Winter 2021**

**Begins: Monday March 8th**

**Due: Monday 15th 5:45 pm CDT**

**Nico DeHaan Submission**

* **Network Offensive (6 pts)**
  + **Port scan –** 
    - **Import Socket and NMAP needed**
* 1) Identify open TCP ports. Found via Q1\_portscanner.py script
  + - * Answer = 21,22,80
    - 2) Identify versions of running services on the ports. Found via script servicescanner.py
      * Answer
        + OpenSSH 7.5p1 Debian 10
        + nginx 1.13.12
        + vsftpd 1.1.1
    - 3)Answer = Direct links to vulnerabilities. These were generated using a direct query with the CVE website due to the API’s either being broken or clunky. The script servicescanner.py will produce these links and a list of the CVE’s found in the output.
      * <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=nginx+1.13.12>
      * <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=OpenSSH+7.5p1+Debian+10>
      * <https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=vsftpd+1.1.1>
* **Web Offensive**
  + **SQL Injection (4 pts)**
    - Could not get this to work and spent roughly 8 hours trying. Submitted scripts anyway under blindsql.py
  + **Directory Brute Force (4 pts) - found via directorybrute.py**
    - **import requests**
    - <http://10.12.0.30/backup/flag.txt>
    - Answer = CNS{0421008445828ceb46f496700a5fa65e}
  + **Search for flag on homepage (4 pts) found via regexflag.py**
    - **import re**
    - Answer = CNS{673cc3378d0f1fbd3747d14d6b782ddb}
* **OS Offensive**
  + **SSH Brute Force (4 pts) found via sshbrute.py**
    - **import paramiko**
    - **Answer**
    - user = helpdesk
    - password = shadow
* **OS Defensive**
  + **Search for vulnerabilities (4 pts)**
    - **import OS**
    - Found using vulnscan.py
    - Output at bottom of this file
  + **Log Parser (4 pts)**
    - Ran out of time to complete.
  + **Malware test (5 pts)- found via vtscanner.py**
    - **import requests and OS**
    - Answer = File 13 is Malicious
* **Forensics** 
  + **XOR Decryption (5 pts)**
    - Spent roughly 8 hours trying to get this to work and couldn’t get there.
    - All my partial scripts and workings are under the xor.py file

**Vulnscan Output**

**PRETTY\_NAME="Kali GNU/Linux Rolling"**

**NAME="Kali GNU/Linux"**

**ID=kali**

**VERSION="2017.2"**

**VERSION\_ID="2017.2"**

**ID\_LIKE=debian**

**ANSI\_COLOR="1;31"**

**HOME\_URL="http://www.kali.org/"**

**SUPPORT\_URL="http://forums.kali.org/"**

**BUG\_REPORT\_URL="http://bugs.kali.org/"**

**Static hostname: kali**

**Icon name: computer-vm**

**Chassis: vm**

**Machine ID: 4f3e6024180e491a9c50121f1d53c77d**

**Boot ID: 88557157725d4aa2bccc25b7ed93c5bb**

**Virtualization: vmware**

**Operating System: Kali GNU/Linux Rolling**

**Kernel: Linux 4.12.0-kali1-amd64**

**Architecture: x86-64**

**USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND**

**root 1 0.2 0.8 154336 8172 ? Ss 14:59 0:00 /sbin/init**

**root 2 0.0 0.0 0 0 ? S 14:59 0:00 [kthreadd]**

**root 3 0.0 0.0 0 0 ? S 14:59 0:00 [kworker/0:0]**

**root 4 0.0 0.0 0 0 ? S< 14:59 0:00 [kworker/0:0H]**

**root 5 0.0 0.0 0 0 ? S 14:59 0:00 [kworker/u2:0]**

**root 6 0.0 0.0 0 0 ? S< 14:59 0:00 [mm\_percpu\_wq]**

**root 7 0.0 0.0 0 0 ? S 14:59 0:00 [ksoftirqd/0]**

**root 8 0.0 0.0 0 0 ? S 14:59 0:00 [rcu\_sched]**

**root 9 0.0 0.0 0 0 ? S 14:59 0:00 [rcu\_bh]**

**root 10 0.0 0.0 0 0 ? S 14:59 0:00 [migration/0]**

**root 11 0.0 0.0 0 0 ? S 14:59 0:00 [watchdog/0]**

**root 12 0.0 0.0 0 0 ? S 14:59 0:00 [cpuhp/0]**

**root 13 0.0 0.0 0 0 ? S 14:59 0:00 [kdevtmpfs]**

**root 14 0.0 0.0 0 0 ? S< 14:59 0:00 [netns]**

**root 15 0.0 0.0 0 0 ? S 14:59 0:00 [khungtaskd]**

**root 16 0.0 0.0 0 0 ? S 14:59 0:00 [oom\_reaper]**

**root 17 0.0 0.0 0 0 ? S< 14:59 0:00 [writeback]**

**root 18 0.0 0.0 0 0 ? S 14:59 0:00 [kcompactd0]**

**root 19 0.0 0.0 0 0 ? SN 14:59 0:00 [ksmd]**

**root 20 0.0 0.0 0 0 ? SN 14:59 0:00 [khugepaged]**

**root 21 0.0 0.0 0 0 ? S< 14:59 0:00 [crypto]**

**root 22 0.0 0.0 0 0 ? S 14:59 0:00 [kworker/0:1]**

**root 23 0.0 0.0 0 0 ? S< 14:59 0:00 [kintegrityd]**

**root 24 0.0 0.0 0 0 ? S< 14:59 0:00 [bioset]**

**root 25 0.0 0.0 0 0 ? S< 14:59 0:00 [kblockd]**

**root 26 0.0 0.0 0 0 ? S< 14:59 0:00 [edac-poller]**

**root 27 0.0 0.0 0 0 ? S< 14:59 0:00 [devfreq\_wq]**

**root 28 0.0 0.0 0 0 ? S< 14:59 0:00 [watchdogd]**

**root 29 0.0 0.0 0 0 ? S 14:59 0:00 [kauditd]**

**root 30 0.0 0.0 0 0 ? S 14:59 0:00 [kswapd0]**

**root 31 0.0 0.0 0 0 ? S< 14:59 0:00 [bioset]**

**root 45 0.0 0.0 0 0 ? S< 14:59 0:00 [kthrotld]**

**root 46 0.0 0.0 0 0 ? S< 14:59 0:00 [ipv6\_addrconf]**

**root 47 0.1 0.0 0 0 ? S 14:59 0:00 [kworker/0:2]**

**root 86 0.0 0.0 0 0 ? S< 14:59 0:00 [ata\_sff]**

**root 95 0.0 0.0 0 0 ? S 14:59 0:00 [scsi\_eh\_0]**

**root 96 0.0 0.0 0 0 ? S< 14:59 0:00 [scsi\_tmf\_0]**

**root 97 0.0 0.0 0 0 ? S 14:59 0:00 [scsi\_eh\_1]**

**root 98 0.0 0.0 0 0 ? S< 14:59 0:00 [scsi\_tmf\_1]**

**root 99 0.0 0.0 0 0 ? S 14:59 0:00 [kworker/u2:1]**

**root 100 0.0 0.0 0 0 ? S 14:59 0:00 [kworker/u2:2]**

**root 109 0.0 0.0 0 0 ? S 14:59 0:00 [kworker/u2:3]**

**root 162 0.0 0.0 0 0 ? S< 14:59 0:00 [bioset]**

**root 163 0.0 0.0 0 0 ? S< 14:59 0:00 [bioset]**

**root 165 0.0 0.0 0 0 ? S< 14:59 0:00 [kworker/0:1H]**

**root 202 0.0 0.0 0 0 ? S 14:59 0:00 [jbd2/sda1-8]**

**root 203 0.0 0.0 0 0 ? S< 14:59 0:00 [ext4-rsv-conver]**

**root 239 0.0 0.6 67920 6128 ? Ss 14:59 0:00 /lib/systemd/systemd-journald**

**root 248 0.0 0.5 45912 5264 ? Ss 14:59 0:00 /lib/systemd/systemd-udevd**

**root 288 0.0 0.0 0 0 ? S< 14:59 0:00 [nfit]**

**systemd+ 305 0.0 0.4 147524 5044 ? Ssl 14:59 0:00 /lib/systemd/systemd-timesyncd**

**root 311 0.0 0.0 0 0 ? S< 14:59 0:00 [ttm\_swap]**

**root 349 0.0 0.5 65680 5792 ? Ss 14:59 0:00 /lib/systemd/systemd-logind**

**root 355 0.0 0.8 427232 9176 ? Ssl 14:59 0:00 /usr/sbin/ModemManager**

**root 359 0.0 0.6 285920 6664 ? Ssl 14:59 0:00 /usr/lib/accountsservice/accounts-daemon**

**root 364 0.0 0.0 4528 776 ? Ss 14:59 0:00 /usr/sbin/anacron -dsq**

**root 366 0.0 0.3 250284 3688 ? Ssl 14:59 0:00 /usr/sbin/rsyslogd -n**

**message+ 368 0.0 0.4 47444 4100 ? Ss 14:59 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation**

**root 411 0.0 1.4 380988 14628 ? Ssl 14:59 0:00 /usr/sbin/NetworkManager --no-daemon**

**root 412 0.0 0.2 29864 2940 ? Ss 14:59 0:00 /usr/sbin/cron -f**

**root 425 0.0 0.6 288440 6384 ? Ssl 14:59 0:00 /usr/lib/policykit-1/polkitd --no-debug**

**root 576 0.0 3.5 301136 36472 ? Ss 14:59 0:00 php-fpm: master process (/etc/php/7.1/fpm/php-fpm.conf)**

**root 579 0.0 0.2 28532 2868 ? Ss 14:59 0:00 /usr/sbin/vsftpd /etc/vsftpd.conf**

**root 580 0.0 0.3 74048 3396 tty1 Ss 14:59 0:00 /bin/login --**

**root 583 0.0 0.5 72116 5596 ? Ss 14:59 0:00 /usr/sbin/sshd -D**

**root 587 0.0 0.0 32556 840 ? Ss 14:59 0:00 nginx: master process /usr/sbin/nginx -g daemon on; master\_process on;**

**www-data 590 0.0 0.2 32940 2728 ? S 14:59 0:00 nginx: worker process**

**www-data 591 0.0 0.2 32940 2728 ? S 14:59 0:00 nginx: worker process**

**www-data 592 0.0 0.2 32940 2728 ? S 14:59 0:00 nginx: worker process**

**www-data 593 0.0 0.2 32940 2728 ? S 14:59 0:00 nginx: worker process**

**www-data 602 0.0 0.6 301136 6704 ? S 14:59 0:00 php-fpm: pool www**

**www-data 603 0.0 0.6 301136 6704 ? S 14:59 0:00 php-fpm: pool www**

**root 616 0.0 0.3 20116 3640 ? S 14:59 0:00 /bin/bash /usr/bin/mysqld\_safe**

**mysql 760 0.1 7.4 656304 76476 ? Sl 14:59 0:00 /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/x86\_64-linux-gnu/mariadb18/plugin --user=mysql --skip-log-error --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/mysqld/mysqld.sock --port=3306**

**root 761 0.0 0.1 29284 1540 ? S 14:59 0:00 logger -t mysqld -p daemon error**

**root 868 0.0 0.6 105616 7004 ? Ss 15:02 0:00 sshd: helpdesk [priv]**

**helpdesk 870 0.0 0.7 80224 7352 ? Ss 15:02 0:00 /lib/systemd/systemd --user**

**helpdesk 871 0.0 0.1 186044 1960 ? S 15:02 0:00 (sd-pam)**

**helpdesk 881 0.0 0.4 105616 4316 ? S 15:02 0:00 sshd: helpdesk@notty**

**helpdesk 882 0.0 0.1 12804 1956 ? Ss 15:02 0:00 /usr/lib/openssh/sftp-server**

**root 883 0.0 0.6 105616 6984 ? Ss 15:02 0:00 sshd: helpdesk [priv]**

**helpdesk 887 0.0 0.4 105616 4532 ? S 15:02 0:00 sshd: helpdesk@notty**

**helpdesk 888 0.0 0.1 12804 1872 ? Ss 15:02 0:00 /usr/lib/openssh/sftp-server**

**helpdesk 891 0.1 0.5 21416 5120 tty1 S 15:03 0:00 -bash**

**helpdesk 903 0.0 0.6 22668 6896 tty1 S+ 15:04 0:00 python osdefvulnscan.py**

**root 910 0.0 0.2 56952 2944 ? Ss 15:04 0:00 /lib/systemd/systemd-hostnamed**

**helpdesk 913 0.0 0.0 4396 840 tty1 S+ 15:04 0:00 sh -c ps aux**

**helpdesk 914 0.0 0.3 40528 3320 tty1 R+ 15:04 0:00 ps aux**