B"h

דו"ח מעבדה- תרחיש מס' 5

פרטים:

מגישה: רעיה חזי

תאריך: 27.12.2018

שם התרחיש: denial of service attack.

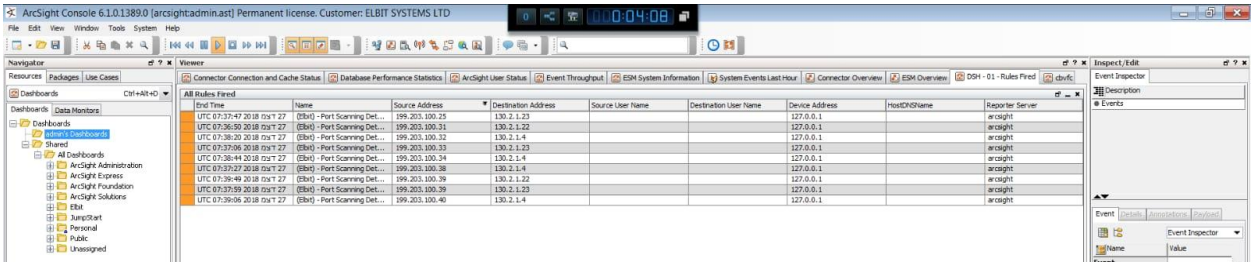
תהליך ההתקפה:

- התוקף ביצע התקפת denial of service על האתר. www.cnn.com (מנצלת פרצת אבטחה במנגנון הקמת הקשר של TCP).
- תהליך – התוקף שלח רצף של חבילות SYN לשרת שלנו, ובכך אילץ אותו לפתוח חיבורים רבים במקביל עד שלא נשארים לו עוד משאבים לקבלת חיבורים חדשים. תהליך זה גם ימנע ממשתמשים אחרים לקבל שירות, וגם הפיל את השרתים.
- SYN flood- כאשר לקוח ניגש לשרת ע"י TCP פרוטוקול, נידרש לבצע three way handshake, לפני שמידע כלשהו יועבר ביניהם. הלקוח שולח SYN packet לשרת ראשון. השרת יגיב ב- SYN request, שהיא – SYN ACK packet. ולבסוף – הלקוח יחזיר ACK packet שתאשר ששני הצדדים אישרו את החיבור. רק לאחר מכן – מידע יוכל להיות מועבר בין 2 הצדדים.

ב – SYN flood- התוקף שולח מספר רב מאוד של SYN packets לשרת, ע"י spoofed IP addresses , מה שיגרום לשרת לשלוח תשובה (syn ack) ולהשאיר את הפורט חצי-פתוח, מחכה לתגובה ממארח שלא קיים. (בהתקפה יותר פשוטה – התוקף ישתמש בחומת האש כדי לבטל SYN-ACK packets לפני שהן מגיעות אליו.) דבר זה גורם לכך שהמערכת תתקשה להתמודד עם עומס הבקשות, ולבסוף – לא תוכל לתת מידע ללקוחות אמתיים, מה שמוביל ל – מניעת שירות.

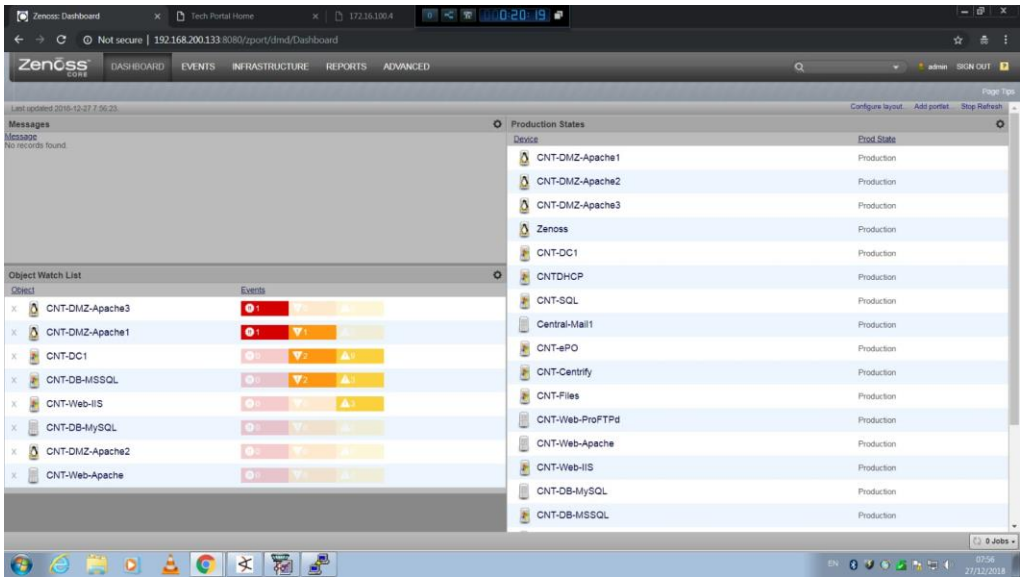
תהליך הזיהוי:

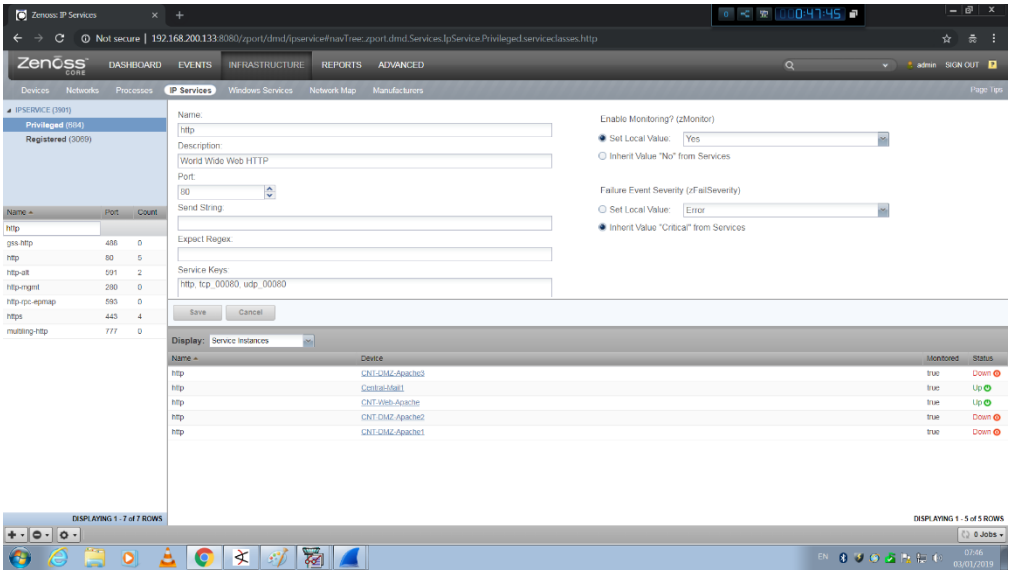
- Arcsight– התראות על port scanning- מכתובת IP- 192.203.100.193, ובנוסף- מכתובות נוספות. (כל פעם כתובת אחרת).



B"h

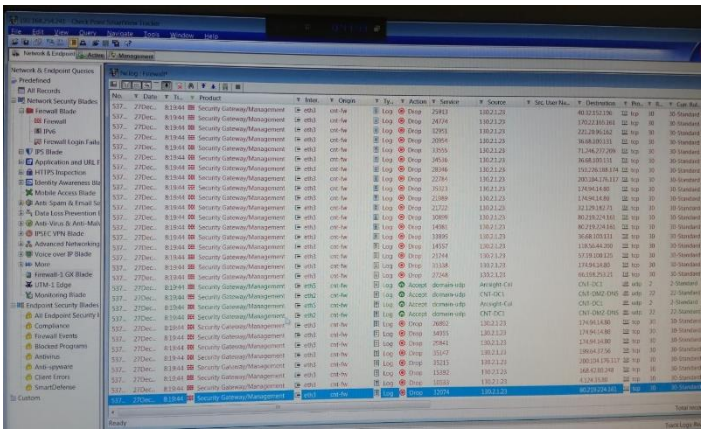
- Zenoss- התראה על apache1, apache2, apache3





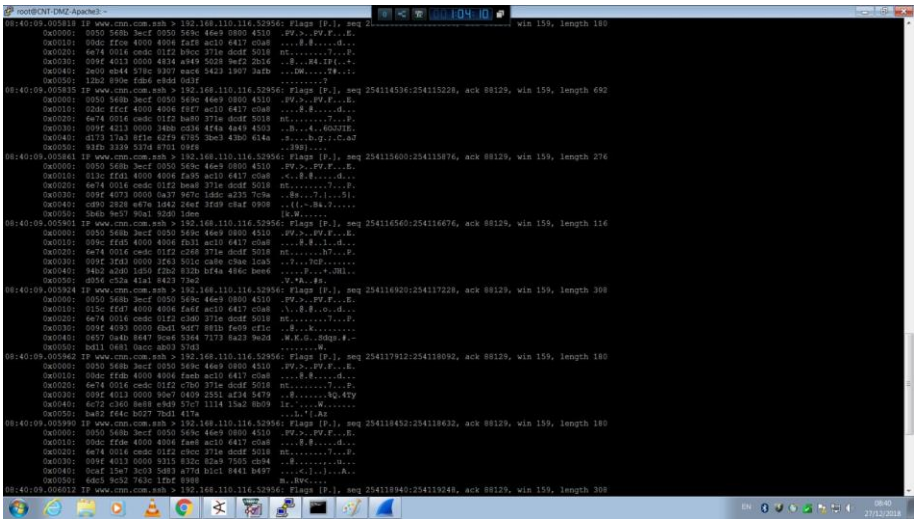
תהליך הגנה:

- חסימת כתובת IP- 192.203.100.193 בחומת האש. (פנימה והחוצה – 2 חוקים נפרדים)
- בדיקה בחומת האש – יש המון התראות של "drop" מכיוון שחסמנו את כתובת התוקף.

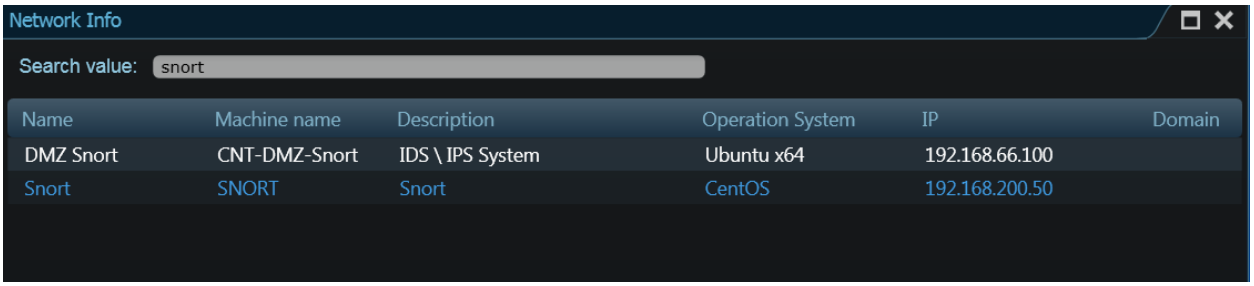


- בדיקה בלוגים של האתר. הדבר הבולט ביותר שמביא לגילוי סוג הפריצה הוא – "possible SYN flood". מפה אנו מבינים שההתקפה היא DOS.

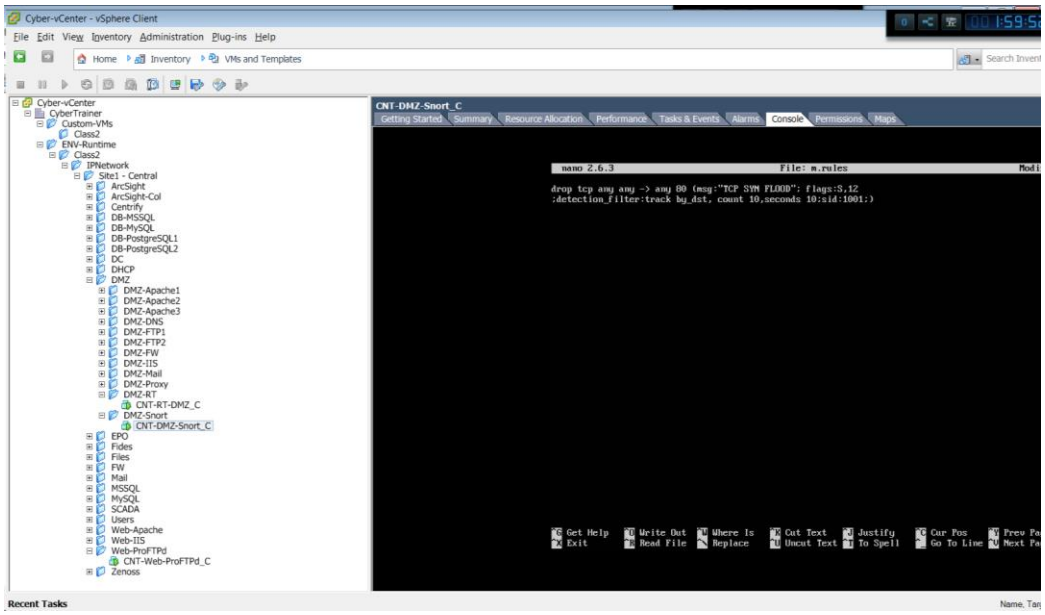
- פקודת tcpdomp- תראה את כל הבקשות של ACK שהתוקף שלח לאתר.



- כניסה לשרת snort : בשרת זה ניתן לראות את הפקאטות שעוברות ברשת, ולחוקק חוקים. שם משתמש : snort. סיסמא : P@ssw0rd



- הפקודה שתחוקק חוק שיוריד את זמן ההמתנה של השרת לתשובה מהלקוח. חוסמים בפורט 80. (ע"י any-any שירוץ ראשון).



תהליך הגנה מונעת :

יש מספר אפשרויות למניעת התקפה כזו :

- הגדלת רוחב -הפס. (בעיקר בשביל התקפות פשוטות. כל רוחב פס ניתן לעבור עם כמות מתאימה של משאבים).
- הקטנת זמן ההמתנה של השרת ללקוח. (כמו מה שעשינו – ב snort).
- שימוש בחומרה או תוכנה שמעבירה קודם את הבקשות לאזור אחר, בודקת את חשיבותם ואת רמת הסיכון שלהם (אם קיימת). מסננת את הבקשות, ורק אז מעבירה אותם לשרת המבוקש.

הפרצות באבטחת הארגון

- אי מוכנות מבחינת הארגון להתקפה כזו. (מהבחינות שצוינו לעיל).

כלים שפיתחנו

--

אופן עבודת הצוות

לא הייתה יותר מידי עבודת צוות..

חסרים/קשיים

כמה נקודות חשובות:

- DOS- denial of service. One computer's attack. (easy to block the router, and finish the attack)
- DDOS – distributed denial of service. Many computers, use many ip's and many routers. Very hard to block.
- Tracert- פקודה זו תראה את הנתיב שתעבור פקאטה מראוטר אחד על ליעד הסופי.
- Snort – מערכת למניעת חדירות. מנתחת תעבורה בזמן אמת ומדווחת על פעולות חשודות. בעלת 3 מצבים עיקריים:
  1. Sniffer- האזנה אחר תעבורת הרשת.
  2. Packet logger- תיעוד תעבורת הרשת לזיהוי וטיפול בבעיות שונות.
  3. Network intrusion detection system- מערכת לאיתור חדירות רשת. כאן ניתן לנתח פעולות לפי הכללים שהוגדרו ע"י admin.

B”h

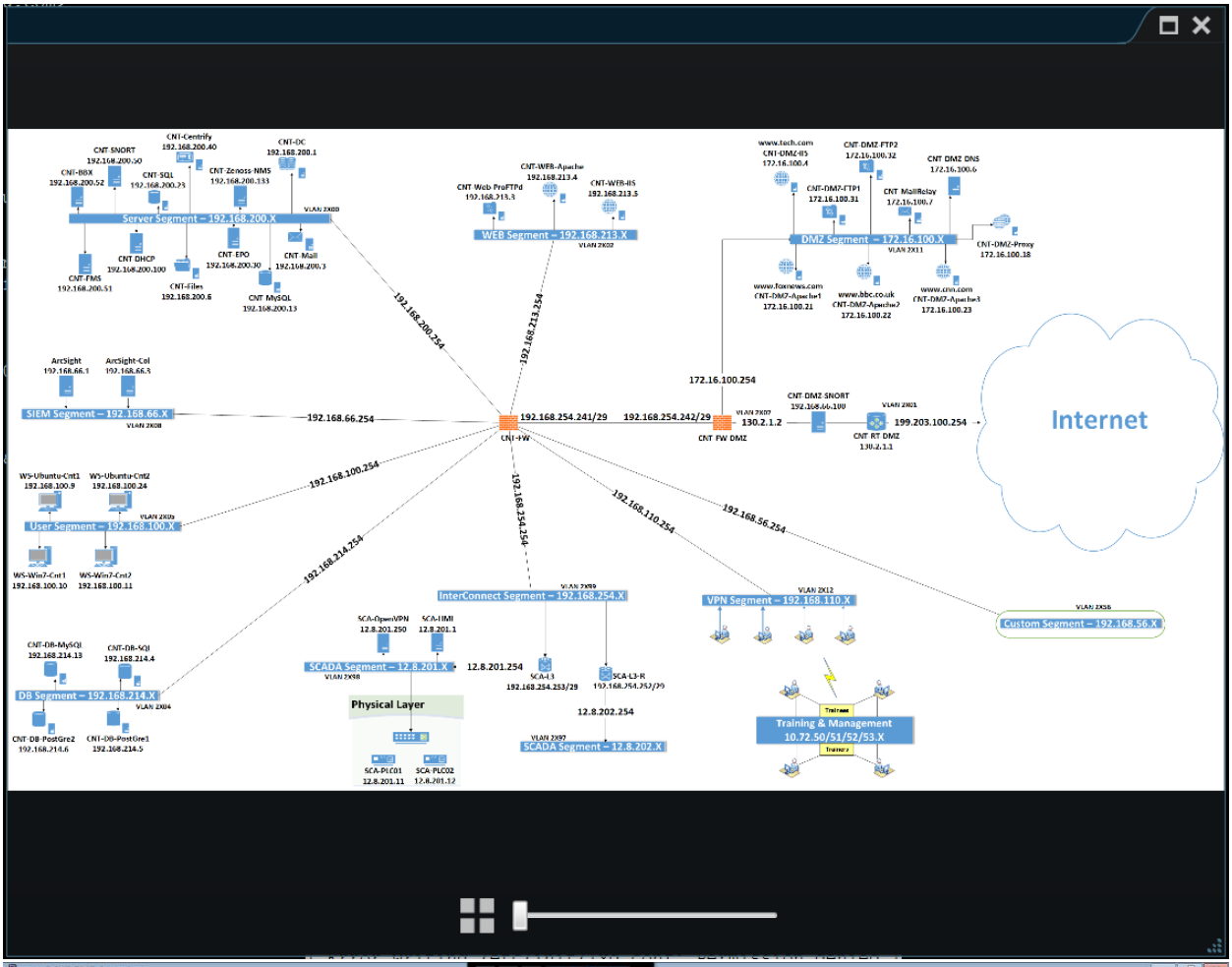
```
snort@CNT-DMZ-Snort:/var/log$ dir
alternatives.log    auth.log       auth.log.3.gz  btmp          dpkg.log       faillog    kern.log.1     lastlog  syslog       syslog.3.gz  syslog.6.gz          vmware-vmsvc.log
alternatives.log.1  auth.log.1     auth.log.4.gz  btmp.1        dpkg.log.1     installer  kern.log.2.gz  lxd      syslog.1     syslog.4.gz  syslog.7.gz          wtmp
apt                 auth.log.2.gz  bootstrap.log  dist-upgrade  dpkg.log.2.gz  kern.log   kern.log.3.gz  snort    syslog.2.gz  syslog.5.gz  unattended-upgrades  wtmp.1
snort@CNT-DMZ-Snort:/var/log$ cd snort
snort@CNT-DMZ-Snort:/var/log/snort$ dir
alert                  snort_ens160:ens192.pid.lck  snort.log.1546502710  snort.log.1546502801  snort.log.1546502884  snort.log.1546502974  snort.log.1546503057  snort.log.154650314
snort_ens160:ens192.pid  snort.log                  snort.log.1546502759  snort.log.1546502842  snort.log.1546502930  snort.log.1546503014  snort.log.1546503101
snort@CNT-DMZ-Snort:/var/log/snort$
```

```
snort@CNT-DMZ-Snort:/var$ cd ..
snort@CNT-DMZ-Snort:/$ cd etc/
snort@CNT-DMZ-Snort:/etc$ ls
acpi                  console-setup        environment  hosts.deny       locale.alias    mke2fs.conf       perl                    rc3.d          ssh            update-manager
adduser.conf          cron.d               ethertypes   init             locale.gen      modprobe.d        pm                      resolvconf     ssl            update-motd.d
alternatives          cron.daily           fonts        init.d           localtime       modules           polkit-1                resolv.conf    subgid         update-notifier
apm                   cron.hourly          fstab        initramfs-tools  logcheck        modules-load.d    pollinate               rmt            subgid-        vim
apparmor              cron.monthly         fuse.conf    inputrc          login.defs      mtab              popularity-contest.conf rpc            subuid         vmware-tools
apparmor.d            crontab              gai.conf     iproute2         logrotate.conf  nanorc            ppp                     rsyslog.conf   subuid-        vtrgb
apport                cron.weekly          groff        iscsi            logrotate.d     netplan           profile                 rsyslog.d      sudoers        wgetrc
apt                   crypttab             group        issue            lsb-release     network           profile.d               screenrc       sudoers.d      X11
at.deny               dbus-1               group-       issue.net        ltrace.conf     networks          protocols               securetty      sysctl.conf    xdg
bash.bashrc           debconf.conf         grub.d       kernel           lvm             newt              python3                 security       sysctl.d       xml
bash_completion       debian_version       gshadow      kernel-img.conf  machine-id      nsswitch.conf     python3.5               selinux        systemd        zsh_command_not_found
bash_completion.d     default              gshadow-     ldap             magic           opt               rc0.d                   services       terminfo
bindresvport.blacklist deluser.conf        gss          ld.so.cache      magic.mime      os-release        rc1.d                   sgml           timezone
binfmt.d              depmod.d             hdparm.conf  ld.so.conf       mailcap         overlayroot.conf  rc2.d                   shadow         tmpfiles.d
byobu                 dhcp                 host.conf    ld.so.conf.d     mailcap.order   pam.conf          rc3.d                   shadow-        ucf.conf
ca-certificates       dnsmasq.d            hostname     legal            manpath.config  pam.d             rc4.d                   shells         udev
ca-certificates.conf  dnsmasq.d-available  hosts        libaudit.conf    mdadm           passwd            rc5.d                   ske1           ufw
calendar              dpkg                 hosts.allow  libnl-3          mime.types      passwd-           rc6.d                   sos.conf       updatedb.conf
snort@CNT-DMZ-Snort:/etc$ cd snort
-bash: cd: snort: No such file or directory
snort@CNT-DMZ-Snort:/etc$ cd timezone
-bash: cd: timezone: Not a directory
snort@CNT-DMZ-Snort:/etc$ cat timezone
UTC
snort@CNT-DMZ-Snort:/etc$ sysctl net.inet.tcp
sysctl: cannot stat /proc/sys/net/inet/tcp: No such file or directory
snort@CNT-DMZ-Snort:/etc$ cat sysctl.d
cat: sysctl.d: Is a directory
snort@CNT-DMZ-Snort:/etc$ cd sysctl.d
snort@CNT-DMZ-Snort:/etc/sysctl.d$ ls
10-console-messages.conf  10-kernel-hardening.conf   10-magic-sysrq.conf       10-ptrace.conf    99-sysctl.conf
10-ipv6-privacy.conf      10-link-restrictions.conf  10-network-security.conf  10-zeropage.conf  README
snort@CNT-DMZ-Snort:/etc/sysctl.d$ cat 10-network-security.conf

# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks.
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1

# Turn on SYN-flood protections.  Starting with 2.6.26, there is no loss
# of TCP functionality/features under normal conditions.  When flood
# protections kick in under high unanswered-SYN load, the system
# should remain more stable, with a trade off of some loss of TCP
# functionality/features (e.g. TCP Window scaling).
net.ipv4.tcp_syncookies=1
snort@CNT-DMZ-Snort:/etc/sysctl.d$ nano 10-network-security.conf
snort@CNT-DMZ-Snort:/etc/sysctl.d$ nano 99-sysctl.conf
```

snort@CNT-DMZ-Snort: /etc/sysctl.d

```
snort@CNT-DMZ-Snort:/etc/sysctl.d$ grep iRl "timeout" /etc
grep: timeout: No such file or directory
grep: /etc: Is a directory
snort@CNT-DMZ-Snort:/etc/sysctl.d$ grep -rnw '/etc' -e 'timeout'
grep: /etc/at.deny: Permission denied
grep: /etc/sudoers: Permission denied
grep: /etc/sudoers.d/README: Permission denied
/etc/init/lxd.conf:7:kill timeout 60
/etc/init/lxd.conf:19:    /usr/bin/lxd waitready --timeout=600
/etc/init/ureadahead.conf:18:kill timeout 180
/etc/network/if-pre-up.d/ifenslave:17:          echo "Waiting for bonding kernel module to be ready (will timeout after 5s)"
/etc/network/if-pre-up.d/ifenslave:246: echo "Waiting for a slave to join $BOND_MASTER (will timeout after 60s)"
/etc/grub.d/30_os-prober:36:if [ "\${timeout}" = 0 ]; then
/etc/grub.d/30_os-prober:37:  set timeout=10
/etc/grub.d/00_header:333:  set timeout=${GRUB_RECORDFAIL_TIMEOUT:-30}
/etc/grub.d/00_header:337:      timeout="${2}"
/etc/grub.d/00_header:342:      timeout="${1}"
/etc/grub.d/00_header:354:      # No hidden timeout, so treat as GRUB_TIMEOUT_STYLE=menu
/etc/grub.d/00_header:355:      timeout="${2}"
/etc/grub.d/00_header:361:    set timeout=${timeout}
/etc/grub.d/00_header:365:  # Fallback normal timeout code in case the timeout_style feature is
/etc/grub.d/00_header:368:    set timeout=${timeout}
/etc/grub.d/00_header:372:  # Fallback hidden-timeout code in case the timeout_style feature is
/etc/grub.d/00_header:374:  elif sleep${verbose} --interruptible ${timeout} ; then
/etc/grub.d/00_header:375:    set timeout=0
grep: /etc/security/opasswd: Permission denied
/etc/hdparm.conf:64:# -S standby (spindown) timeout for the drive
/etc/overlayroot.conf:29:#      * timeout: default: 0
/etc/overlayroot.conf:37:#      overlayroot=device:dev=/dev/sdb,timeout=180
/etc/overlayroot.conf:38:#      overlayroot=device:dev=LABEL=my-flashdrive,timeout=180
/etc/overlayroot.conf:59:#      * timeout: default: 0
/etc/overlayroot.conf:66:#      crypt:mapname=mapper,pass=foo,fstype=ext3,mkfs=1,dev=/dev/disk/by-label/my-jumpdrive,timeout=120
/etc/init.d/mdadm-waitidle:40:      # mdadm --wait-clean has a short internal timeout
/etc/init.d/lxd:39:            ${DAEMON} waitready --timeout=600
/etc/init.d/udev:204:   log_action_end_msg 0 'timeout'
grep: /etc/passwd-: Permission denied
grep: /etc/ssh/ssh_host_ed25519_key: Permission denied
grep: /etc/ssh/ssh_host_rsa_key: Permission denied
grep: /etc/ssh/ssh_host_ecdsa_key: Permission denied
grep: /etc/shadow: Permission denied
grep: /etc/shadow-: Permission denied
grep: /etc/subuid-: Permission denied
grep: /etc/group-: Permission denied
/etc/apparmor.d/usr.lib.snapd.snap-confine:267:        # This is the SIGALRM that we send and receive if a timeout expires
grep: /etc/apparmor.d/cache/usr.bin.lxc-start: Permission denied
grep: /etc/apparmor.d/cache/lxc-containers: Permission denied
grep: /etc/apparmor.d/cache/usr.lib.snapd.snap-confine: Permission denied
grep: /etc/apparmor.d/cache/sbin.dhclient: Permission denied
grep: /etc/apparmor.d/cache/usr.sbin.tcpdump: Permission denied
grep: /etc/ufw/user.rules: Permission denied
```

B”h


Server Segment – 192.168.200.X
WEB Segment – 192.168.213.X
DMZ Segment – 172.16.100.X
SIEM Segment – 192.168.66.X
User Segment – 192.168.100.X
DB Segment – 192.168.214.X
InterConnect Segment – 192.168.254.X
SCADA Segment – 12.8.201.X
SCADA Segment – 12.8.202.X
VPN Segment – 192.168.110.X
Custom Segment – 192.168.56.X
Training & Management
10.72.50/51/52/53.X
Physical Layer
Internet
192.168.200.254
192.168.213.254
192.168.66.254
192.168.100.254
192.168.214.254
192.168.254.254
192.168.110.254
192.168.56.254
192.168.254.241/29
192.168.254.242/29
172.16.100.254
130.2.1.2
199.203.100.254
12.8.201.254
12.8.202.254


snort@CNT-DMZ-Snort: /etc
snort@CNT-DMZ-Snort:/var/log/snort$ cat snort.log
snort@CNT-DMZ-Snort:/var/log/snort$ ls
snort@CNT-DMZ-Snort:/var/log/snort$ cd ..
snort@CNT-DMZ-Snort:/var/log$ l
snort@CNT-DMZ-Snort:/var/log$ snort -vde
Running in packet dump mode
--== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
Acquiring network traffic from "ens160".
ERROR: Can't start DAQ (-1) - socket: Operation not permitted!
Fatal Error, Quitting..
snort@CNT-DMZ-Snort:/var/log$ cd ..
snort@CNT-DMZ-Snort:/var$ ls
snort@CNT-DMZ-Snort:/var$ cd ..
snort@CNT-DMZ-Snort:/$ cd etc/
snort@CNT-DMZ-Snort:/etc$ ls
snort@CNT-DMZ-Snort:/etc$ cd snort
-bash: cd: snort: No such file or directory
snort@CNT-DMZ-Snort:/etc$