דו״ח מעבדה- תרחיש מס׳ 02

פרטים :

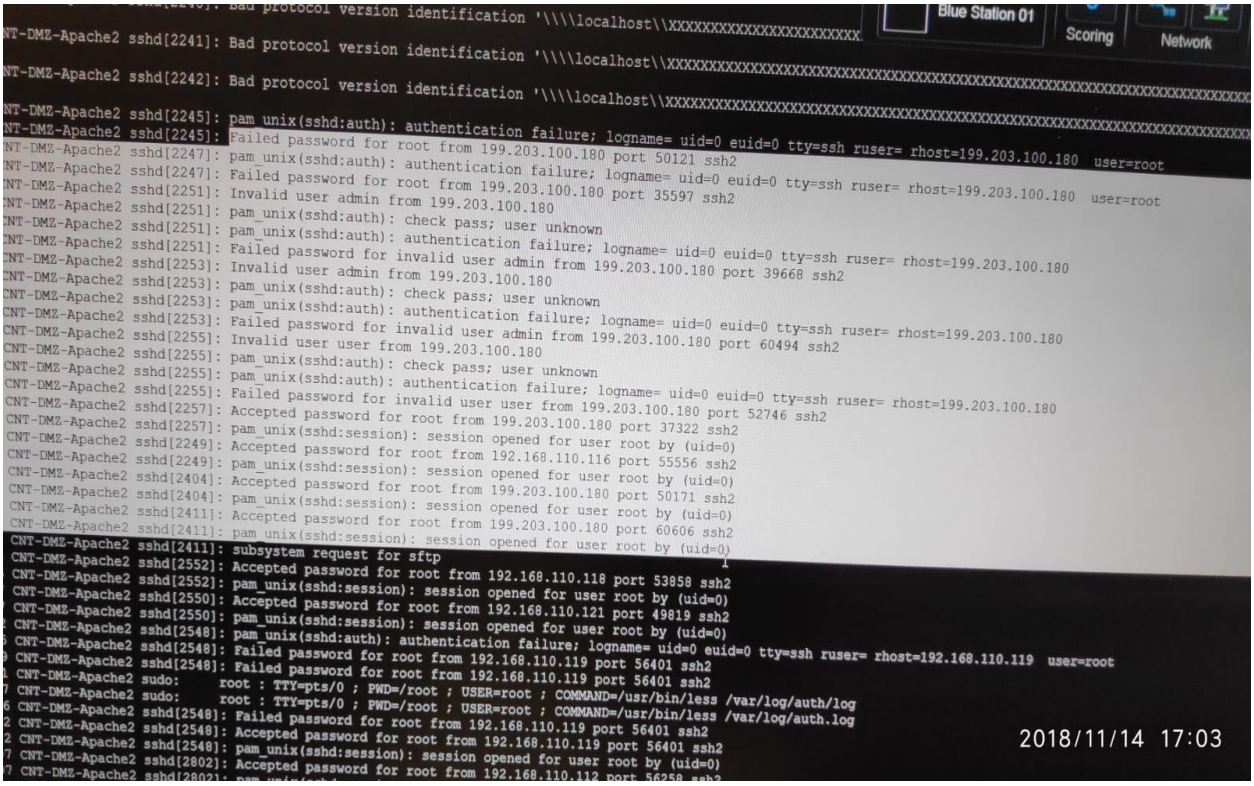
מגיש : אוראל מרדכי

תאריך : 14.11.18

שם התרחיש : Web Defacement

תהליך ההתקפה :

התוקף ניסה להתחבר לשרת BBC. לשרת עשו port scanning, ולאחר שעשו port scanning לשרת זיהו אצלנו אוזן קשובה. ברגע שמצאו אצלנו אוזן קשובה התוקף התחיל לעשות brute-force attack של סיסמאות עד שפרץ את הסיסמא. התוקף ביצע החלפה של קבצי האתר BBC (מתוך תיקיית WWW תחת תיקיית האתר BBC) לקבצים זדוניים שמכילים אתר שהוא מושחט. את הקבצים של האתר האמיתי, הוא שם תחת תיקיית BBC_OLD (כי התוקף היה נחמד 😊).



```
: Bad protocol version identification '\\\\localhost\\XXXXXXXXXXXXXXXXXXXXXXX
NT-DMZ-Apache2 sshd[2241]: Bad protocol version identification '\\\\localhost\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
NT-DMZ-Apache2 sshd[2242]: Bad protocol version identification '\\\\localhost\\XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
NT-DMZ-Apache2 sshd[2245]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.180  user=root
NT-DMZ-Apache2 sshd[2245]: Failed password for root from 199.203.100.180 port 50121 ssh2
NT-DMZ-Apache2 sshd[2247]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.180  user=root
NT-DMZ-Apache2 sshd[2247]: Failed password for root from 199.203.100.180 port 35597 ssh2
NT-DMZ-Apache2 sshd[2251]: Invalid user admin from 199.203.100.180
NT-DMZ-Apache2 sshd[2251]: pam_unix(sshd:auth): check pass; user unknown
NT-DMZ-Apache2 sshd[2251]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.180
NT-DMZ-Apache2 sshd[2251]: Failed password for invalid user admin from 199.203.100.180 port 39668 ssh2
NT-DMZ-Apache2 sshd[2253]: Invalid user admin from 199.203.100.180
CNT-DMZ-Apache2 sshd[2253]: pam_unix(sshd:auth): check pass; user unknown
CNT-DMZ-Apache2 sshd[2253]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.180
CNT-DMZ-Apache2 sshd[2253]: Failed password for invalid user admin from 199.203.100.180 port 60494 ssh2
CNT-DMZ-Apache2 sshd[2255]: Invalid user user from 199.203.100.180
CNT-DMZ-Apache2 sshd[2255]: pam_unix(sshd:auth): check pass; user unknown
CNT-DMZ-Apache2 sshd[2255]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=199.203.100.180
CNT-DMZ-Apache2 sshd[2255]: Failed password for invalid user user from 199.203.100.180 port 52746 ssh2
CNT-DMZ-Apache2 sshd[2257]: Accepted password for root from 199.203.100.180 port 37322 ssh2
CNT-DMZ-Apache2 sshd[2257]: pam_unix(sshd:session): session opened for user root by (uid=0)
CNT-DMZ-Apache2 sshd[2249]: Accepted password for root from 192.168.110.116 port 55556 ssh2
CNT-DMZ-Apache2 sshd[2249]: pam_unix(sshd:session): session opened for user root by (uid=0)
CNT-DMZ-Apache2 sshd[2404]: Accepted password for root from 199.203.100.180 port 50171 ssh2
CNT-DMZ-Apache2 sshd[2404]: pam_unix(sshd:session): session opened for user root by (uid=0)
CNT-DMZ-Apache2 sshd[2411]: Accepted password for root from 199.203.100.180 port 60606 ssh2
CNT-DMZ-Apache2 sshd[2411]: pam_unix(sshd:session): session opened for user root by (uid=0)
CNT-DMZ-Apache2 sshd[2411]: subsystem request for sftp
CNT-DMZ-Apache2 sshd[2552]: Accepted password for root from 192.168.110.118 port 53858 ssh2
CNT-DMZ-Apache2 sshd[2552]: pam_unix(sshd:session): session opened for user root by (uid=0)
CNT-DMZ-Apache2 sshd[2550]: Accepted password for root from 192.168.110.121 port 49819 ssh2
CNT-DMZ-Apache2 sshd[2550]: pam_unix(sshd:session): session opened for user root by (uid=0)
CNT-DMZ-Apache2 sshd[2548]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.110.119  user=root
CNT-DMZ-Apache2 sshd[2548]: Failed password for root from 192.168.110.119 port 56401 ssh2
CNT-DMZ-Apache2 sshd[2548]: Failed password for root from 192.168.110.119 port 56401 ssh2
CNT-DMZ-Apache2 sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/less /var/log/auth/log
CNT-DMZ-Apache2 sudo:     root : TTY=pts/0 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/less /var/log/auth.log
CNT-DMZ-Apache2 sshd[2548]: Failed password for root from 192.168.110.119 port 56401 ssh2
CNT-DMZ-Apache2 sshd[2548]: Accepted password for root from 192.168.110.119 port 56401 ssh2
CNT-DMZ-Apache2 sshd[2548]: pam_unix(sshd:session): session opened for user root by (uid=0)
CNT-DMZ-Apache2 sshd[2802]: Accepted password for root from 192.168.110.112 port 56258 ssh2
```

2018/11/14 17:03

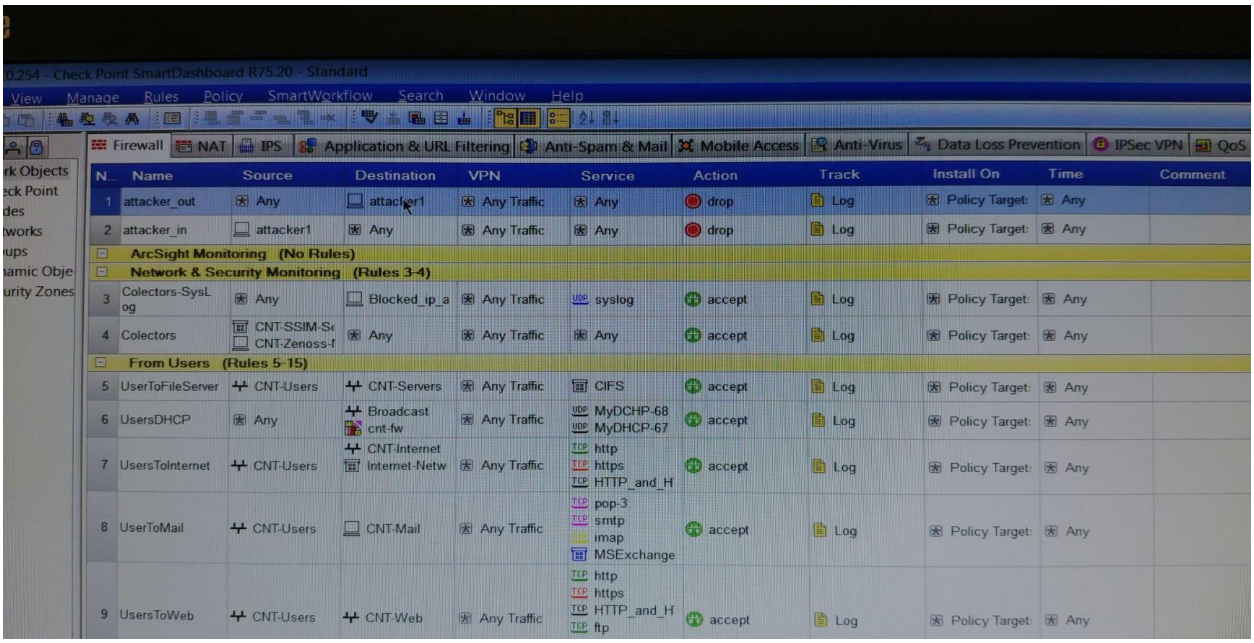
תהליך הזיהוי:

בתחילת התרחיש התקבלה התראה מה – ArcSight, שהודיעה לנו כי מתבצע על השרת Port Scanning ונעשה ביצוע של מספר ניסיונות התחברות מרובים. בנוסף לכך, לאחר שנראה לנו חשוד העניין התחלנו לעבור על אתרי האינטרנט כדי לראות אם יתבצע תקיפה על אחד מהאתרים שבשרת וגילינו כי האתר של BBC הושחט ובמקום זאת הופיע תמונה שהתוקף השתיל באתר. כאשר נכנסו ל browser של Chrome ולחצנו על F12 היה ניתן לראות את השם של התמונה שהשתמש התוקף לאתר שהשחיט ואז היה לנו כיוון לחפש את התמונה בקבצים של השרת. לאחר שעברנו על התיקיות בשרת ראינו כי בתיקיית WWW יש 2 תיקיות תחת השם BBC ו-BBC_OLD, ובתיקיית BBC מצאנו את כל הקבצים שהתוקף השתיל לנו באתר.

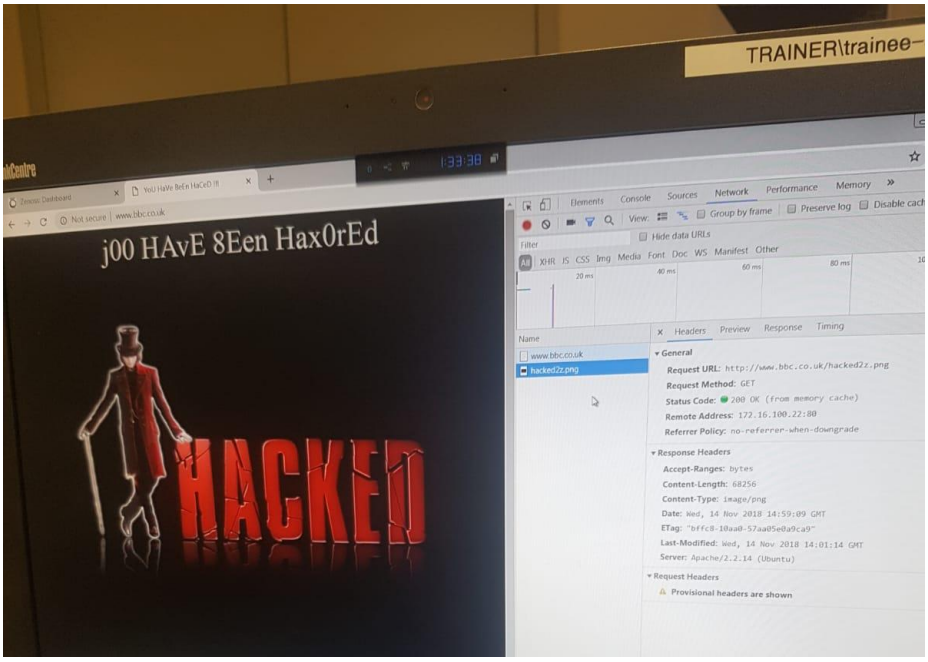
תהליך הגנה:

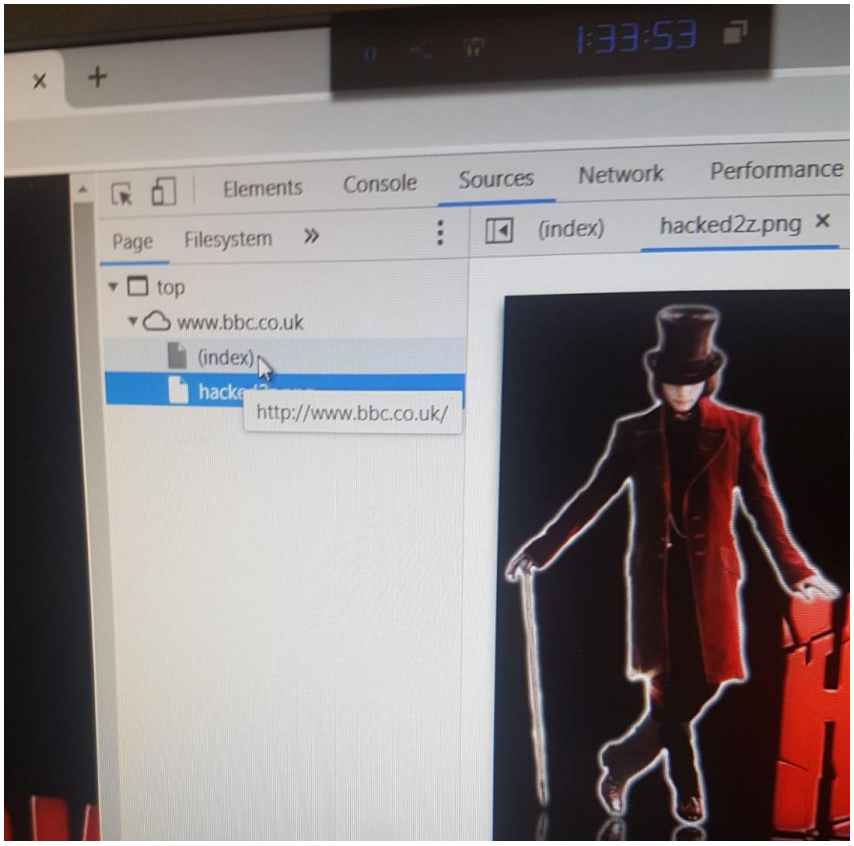
חסמנו את דרכי הכניסה והיציאה של התוקף (כתובת התוקף: 199.203.100.180) באמצעות ה firewall. הפלנו את השרת Apache2 על מנת שאנשים אחרים לא יחשפו לאתר ויראו כי פרצו לנו אותו. בחיפוש אחר הפירורים שהתוקף השאיר מצאנו בדפדפן Chrome ע"י F12 אתר השם של התמונה שעזר לנו להבין איפה יושב התמונה, באיזה תיקייה. ולאחר שעברנו על התיקיות בשרת ראינו כי בתיקיית WWW תחת תיקיית BBC הקבצים של האתר שונו.

כאן חוקקנו חוק שחוסם מהתוקף גישה להיכנס/לצאת מהשרת:



כאן באמצעות הדפדפן של כרום ראינו את הנתיב של התמונה ובכך ידענו מה אנחנו מחפשים :





תהליך הגנה מונעת :

חוץ מהורדת שרת אפצ׳י וחסימה של דרכי הכניסה והיציאה של התוקף מהשרת לא בוצע תהליך מניעתי.

הפרצות באבטחת הארגון

סיסמא חלשה, אחד מהפורטים של השרת היה פתוח.

כלים שפיתחנו

אין

אופן עבודת הצוות

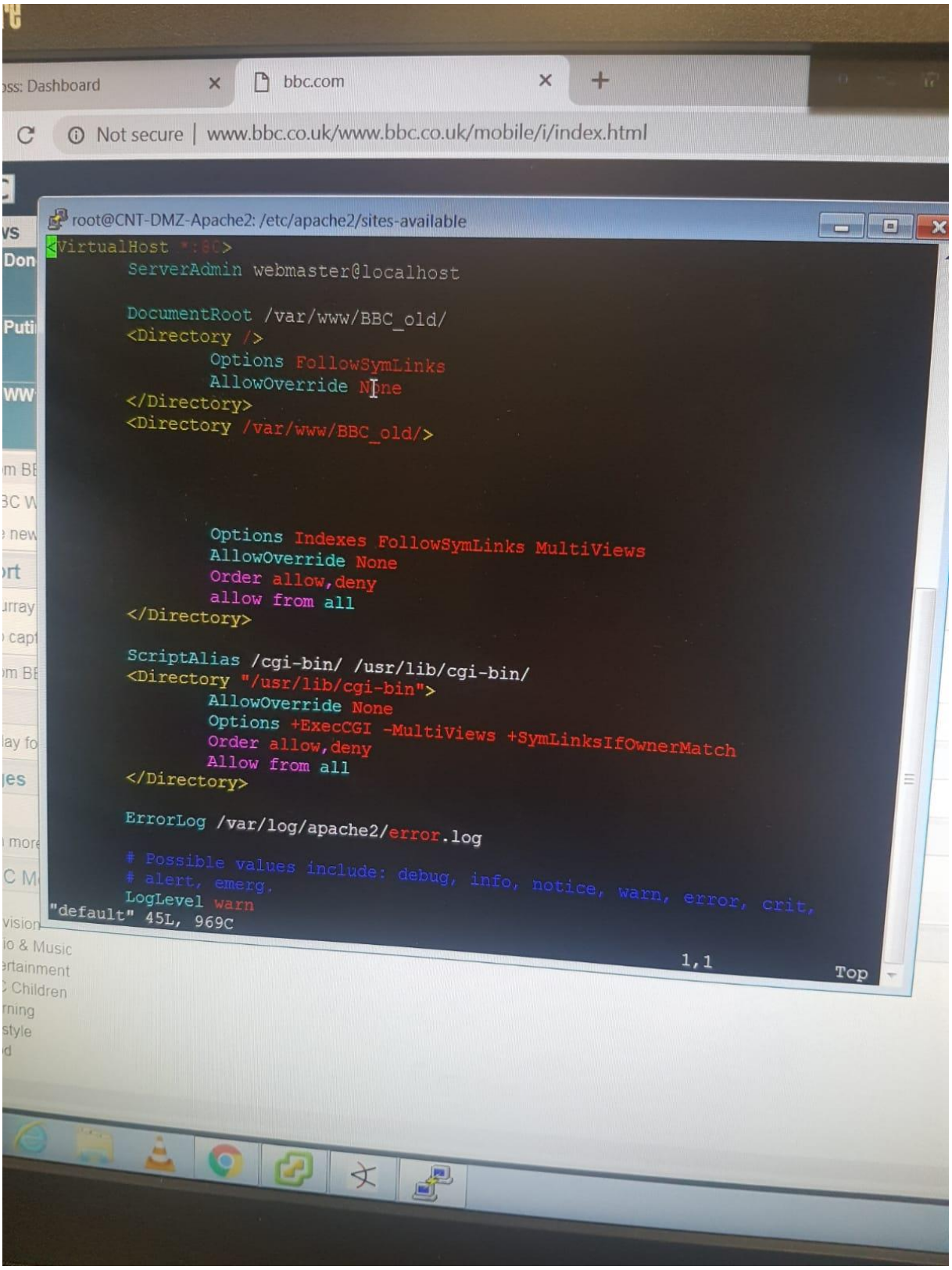
הצוות התחלק לראש צוות(רועי סעדון), שהעביר את המידע ושיתף את הארגון, אחראי על ה firewall (אוראל מרדכי) וביצוע חסימת דרכי היציאה והכניסה של התוקף דרך ה - FRIEWALL, וכל השאר התעסקו בבדיקה של האתרים ובחיפוש בתוך התיקיות של השרת.

חוסרים/קשיים

קצת חוסר סנכרון של ראש הצוות בין אנשי הצוות ,אבל חוץ מזה לא נתקלנו בבעיות.

תמונות נוספות מהתרחיש :

כאן התחברנו דרך הputty בשרת וחיפשנו את התיקייה עם הקבצים ששונו :



כאן מצאנו את הקובץ index ששונה: