דו"ח מעבדה- תרחיש מס' 1

# פרטים:

מגיש: מירב בוים 206489155

תאריך: 12.4.2018

שם התרחיש:

# תהליך ההתקפה:

סריקת פורטים לApache1 ו Apache3 , ניחוש סיסמאות ל Apache1 והתחברות.

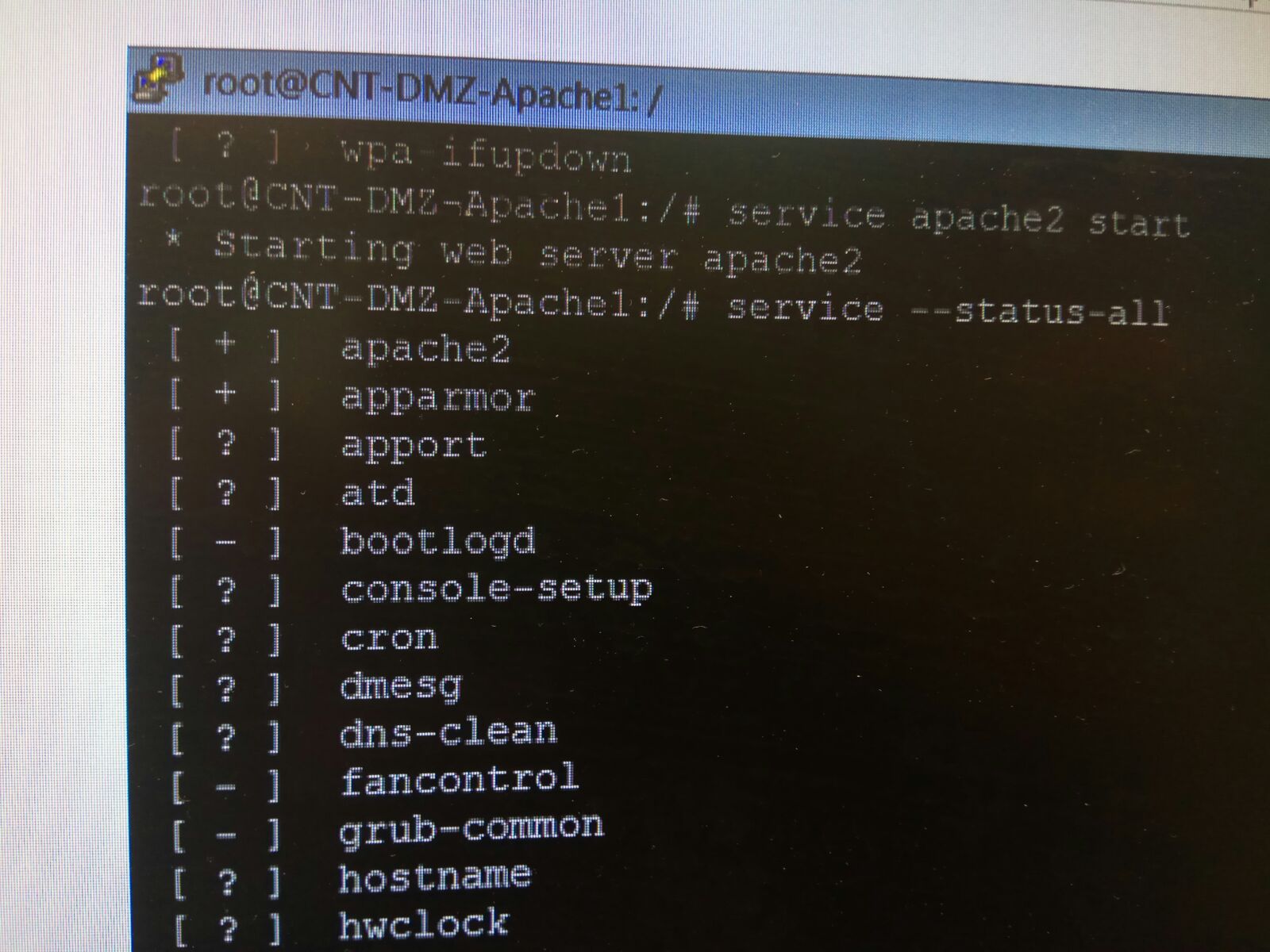
הפעלת תהליך שמריץ כל דקה תוכנית שמפילה את הסרוויס Apache2

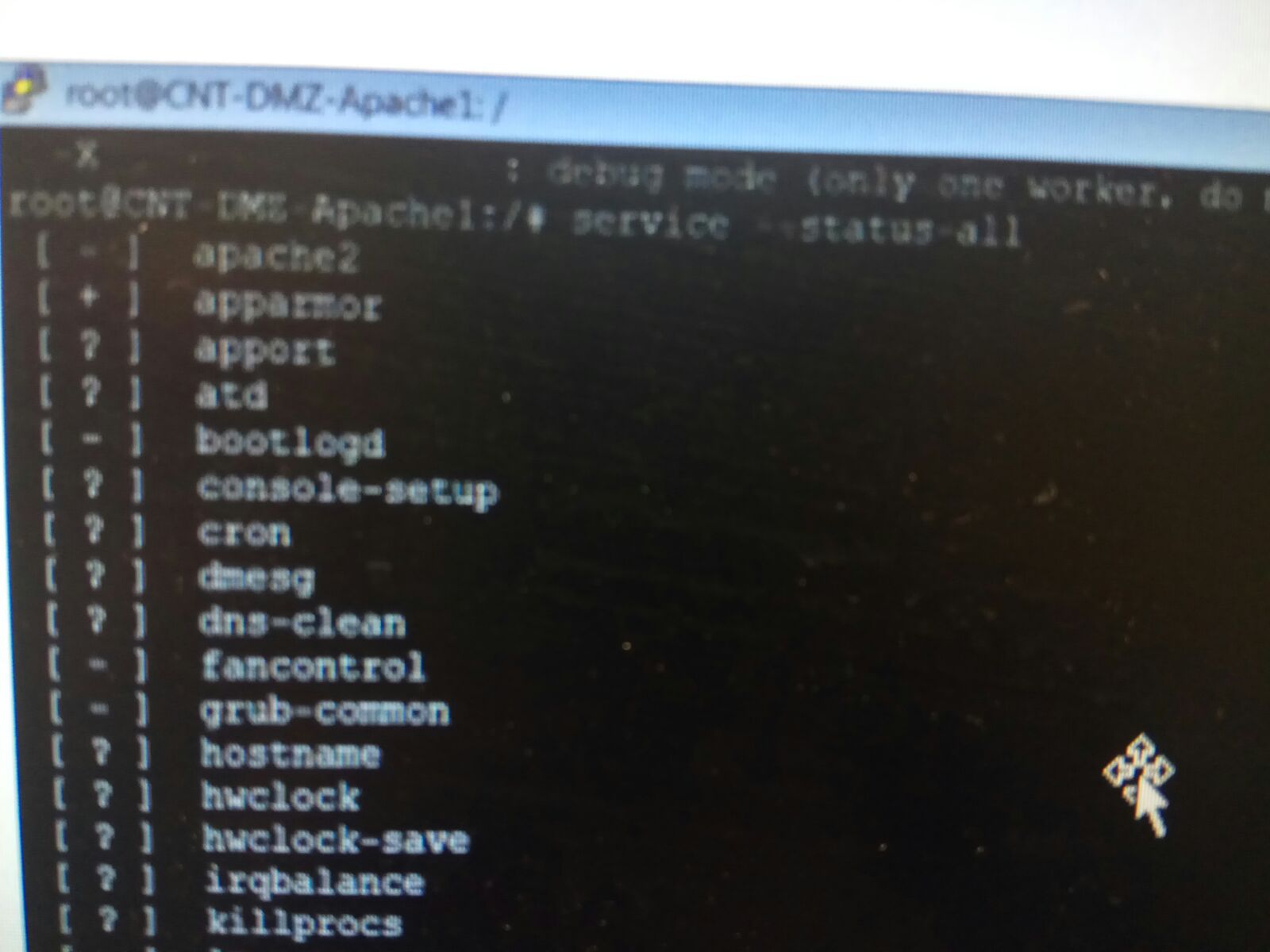
ושולח לעצמו את הקבציםpasswd ,shadow .

# תהליך הזיהוי:

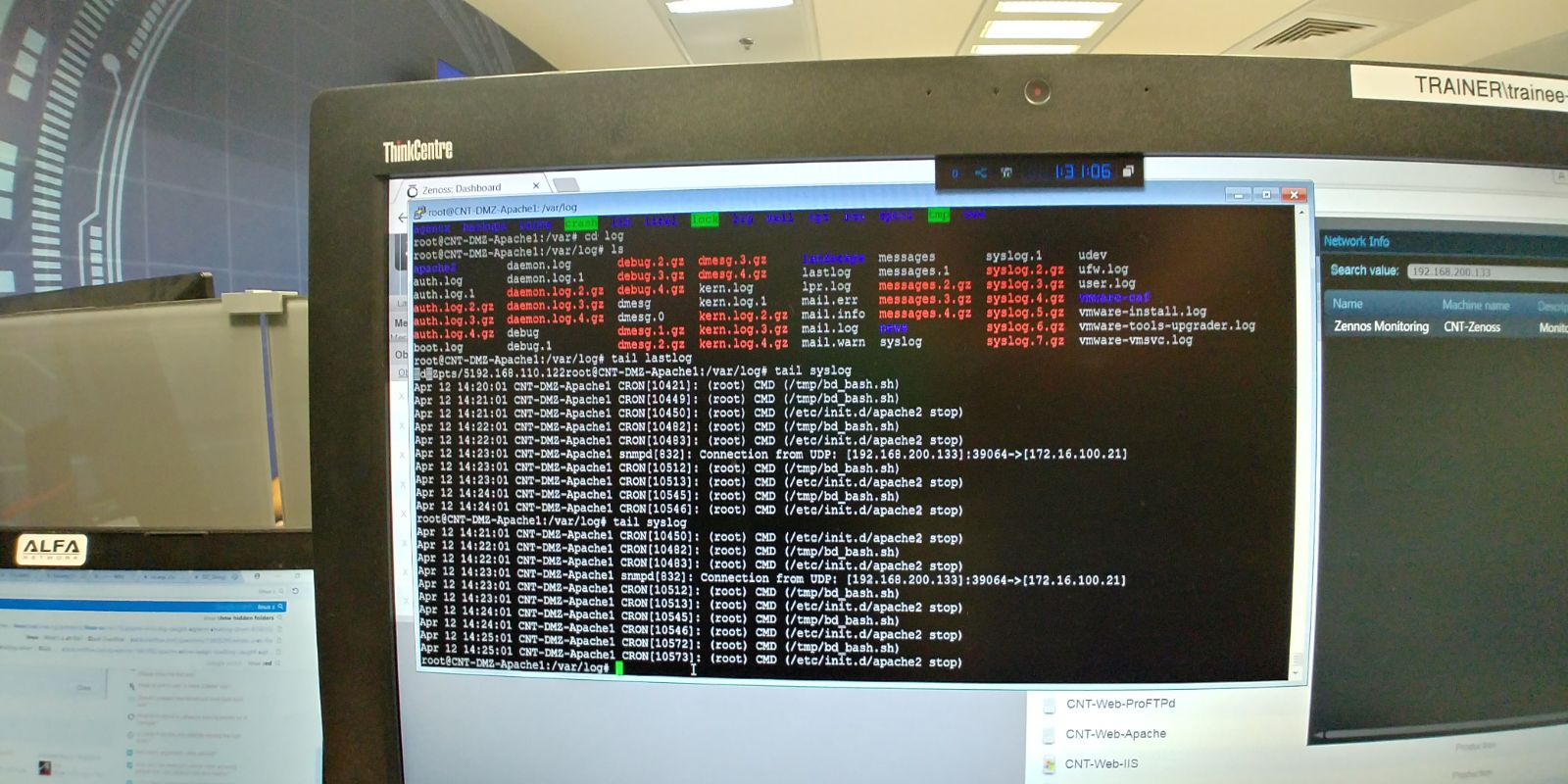
זיהינו ב ArcSight שכתובת חיצונית 199.203.100.30 מבצעת סריקת פורטים על Apache3, וכתובת חיצונית 199.203.100.178 מבצעת סריקת פורטים וניחוש סיסמאות על Apache2.

ראינו ב Zenoss שהסרוויס Apache2 נפל. נכנסנו ל Apache1 עם putty והעלנו את הסרוויס (ע"י הפקודה service Apache2 start ) וגילינו שהוא שוב נפל (ע"י הפקודה service –status-all ).

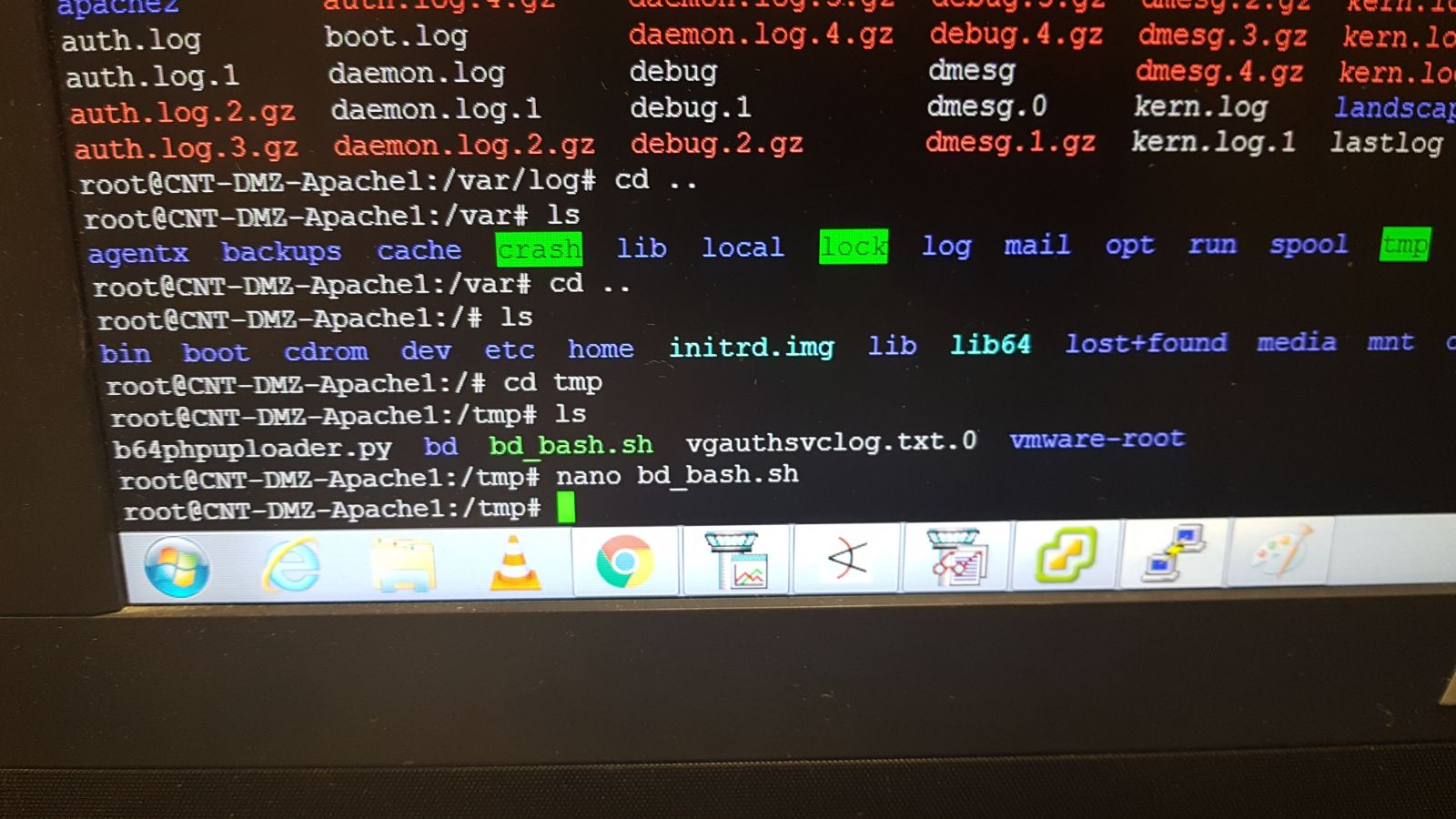




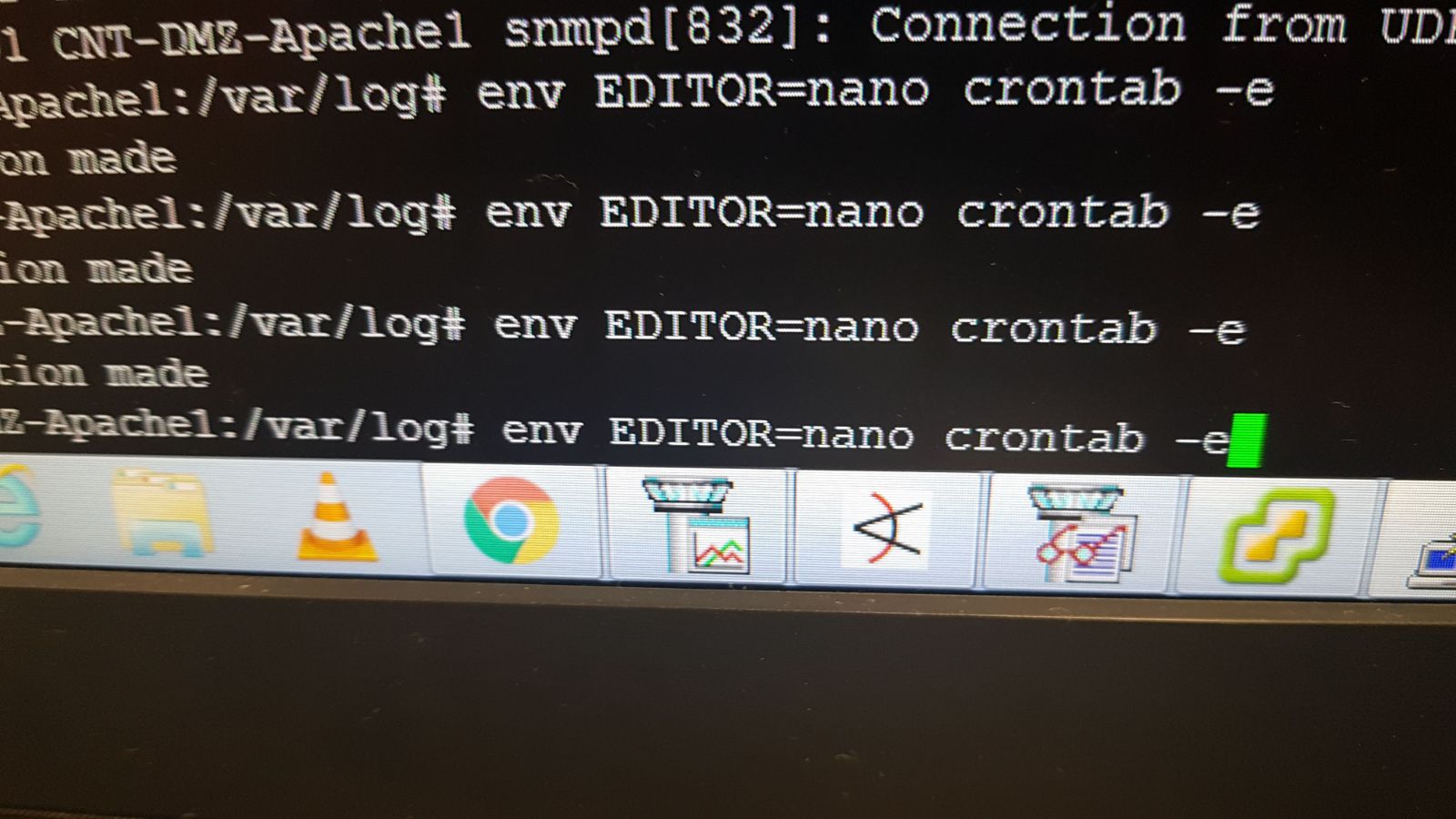
בדקנו בlog וגילינו שכל דקה רצה פקודה להפלת Apache2 והפעלת הbash .

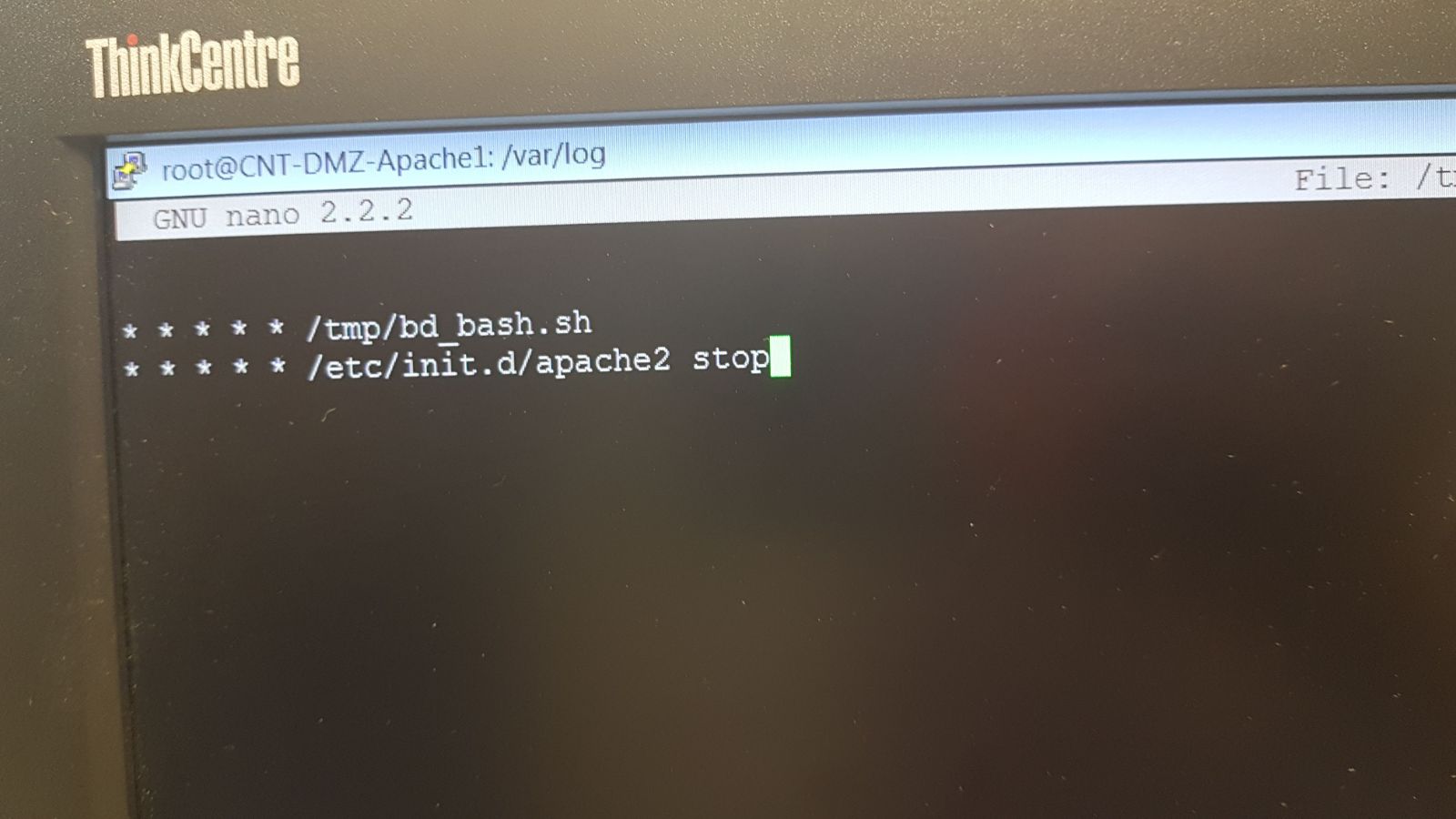


עשינו חיפוש ב Apache1 ומצאנו את הקובץ bs\_bash.sh וחקרנו אותו. ראינו שיש בו פקודות שמריצות קובץ python שמעתיק את הקבצים passwd ,shadow .



הגענו ל cron וגילינו שיש שתי פקודות שרצות כל דקה, פקודה שמפילה את הסרוויס Apache2 ופקודה שמריצה את bs\_bash.sh.





קראנו ובדקנו מה אלה הקבצים passwd ,shadow.

# תהליך הגנה:

חסמנו את התקשורת פנימה והחוצה עם 199.203.100.178 בfirewall



מחקנו את הקובץ bs\_bash.sh והשבתנו את המשימות ב cron.

הרמנו את הסרוויס Apache2.

שינינו סיסמא.

# תהליך הגנה מונעת:

סגירת פורט 20

ניהול הרשאות גישה לכתיבה וקריאה לתקיות וקבצים.

שינוי סיסמאות בארגון לסיסמאות חזקות יותר

# הפרצות באבטחת הארגון

ssh היה פתוח.

סיסמאות פשוטות וקלות לניחוש.

# כלים שפיתחנו

לא פיתחנו

# אופן עבודת הצוות

חלוקת העבודה בין כולם, כל אחד בדק מה שהיה יכול והיה צורך בכך.

כל אחד שקרא על דבר מסויים באינטרנט שיתף והסביר לשאר חברי הקבוצה.

# חוסרים/קשיים

קושי לזהות את מטרת התוקף.

קושי לעלות את השרת שנפל ולהבין מה גורם לנפילתו מחדש.