



ספר קורס



ניווט ופקודות בלינוקס

עמוד 1 -

כל הזכויות שמורות © סייבר סקול בע"מ, אילנות 7, ברמיאל | 077-7781383

מידע על ספר לימוד זה

ספר לימוד זה נועד לסייע לתלמידים ללמוד ולסקור את החומר המכוסה במהלך הקורס מבוא לאבטחת סייבר. הוא מכיל מידע, הרלוונטי לשיעורים הנלמדים בכיתה, וכן הפניות לפעילויות מעבדה שבדאי לתרגל כדי להגביר את רמת הידע שלכם. ספר לימוד זה כולל חומר על יסודות אבטחת הסייבר, תוך התמקדות בשיטות וטכנולוגיות.

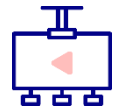
מקרא

קטעי טקסט צבעוניים עשויים להופיע לאורך ספר הלימוד כדי להפנות את הקוראים למקור ספציפי או להעשיר אותם במידע נוסף.

קטעי הטקסט כוללים:

משימת מעבדה

זהו זמן טוב לבחון את קבצי המעבדה הרלוונטיים (על פי קוד המעבדה) ולתרגל את מה שנלמד עד כה.



טוב לדעת

זהו מידע נוסף או תובנה לגבי נושא. נועד לצורכי העשרה בלבד ואינו חלק מחומרי הבחינה.



טיפ

כולל מידע שימושי שיכול לעזור ללמוד את החומר או לעבוד עם כלים ספציפיים.



מידע נוסף

כולל קישורים או הפניות לחומרים חיצוניים שבהם ניתן להשתמש כדי להרחיב את הידע בנושא.



ניווט ומניפולציית תוכן

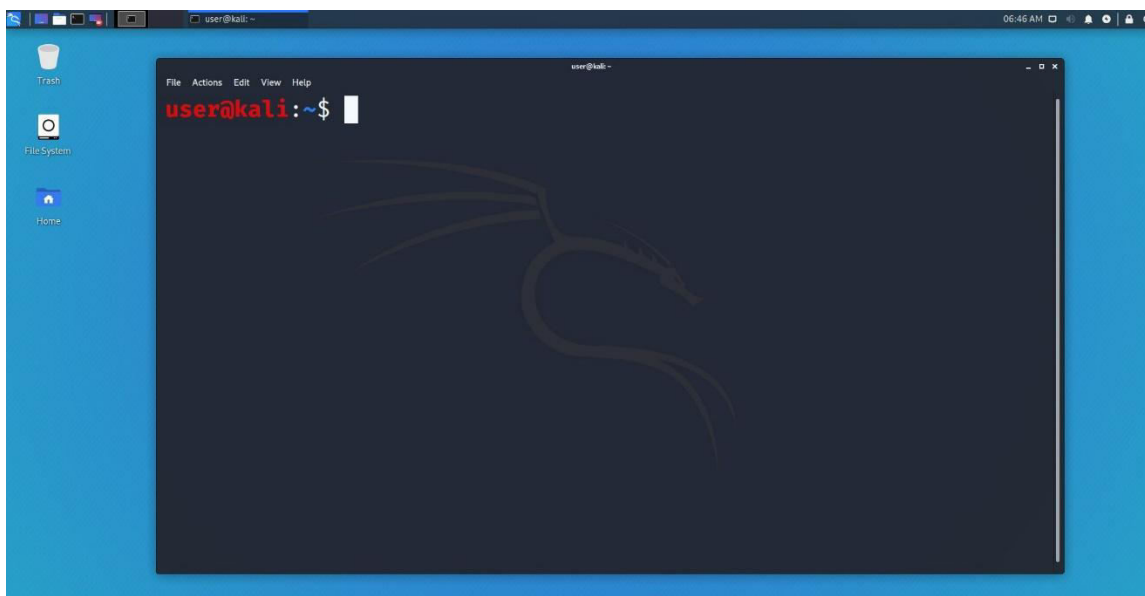
הכישורים הבסיסיים ביותר לשליטה במערכת ההפעלה Linux כוללים ניווט במערכת הקבצים והיכרות עם סביבת Linux. בעת כניסה לשרת, משתמשים נתקלים בתחילה בספריית הבית שלהם, המיועדת לאחסן קבצים וליצור ספריות עבור כל משתמש.

מסוף

אחת הדרכים העיקריות שבהן משתמש יכול להתממשק עם מערכת ההפעלה Linux היא באמצעות המסוף שלה. בדומה לשורת הפקודה במכונות מערכת ההפעלה Windows, היא מקבלת פקודות המבצעות פעולות של מערכת ההפעלה, כגון יצירת קבצים וספריות, הפעלה ועצירה של שירותים, יצירת משימות מתוזמנות ועוד.

המסוף מאפשר למשתמשים לתקשר ישירות עם המערכת. הוא מריץ מעטפת המספקת את היכולת להתממשק עם שירותי מערכת ההפעלה. יישומי Shell כוללים את Bash עבור Linux, שאף היא שפת פקודה שניתן להשתמש בה לתכנות.

הערה: לעתים קרובות משתמשים במונח קונסולה כדי לתאר מכשיר שיכול לקבל קלט משתמש ולהשתמש בתוכנת מסוף.



ניווט ופקודות תוכן

הפקודה שמציגה את הספרייה הנוכחית בהפעלת מסוף היא **pwd**.

```
root@kali:/usr/local/man
```

```
usr/local/man/
```

הפקודה שבה משתמשים כדי להחליף ספרייה בהפעלת המסוף הנוכחית היא **cd**.

```
root@kali:~# cd /usr
root@kali:/usr# cd local
root@kali:/usr/local# cd man
root@kali:/usr/local/man#
```

הדוגמאות הבאות מראות איך להזין את הנתבי המלא של יעד. אם הפקודה מתחילה בקו נטוי (/), היא תחפש את התחלתה של מערכת הקבצים - ספריית השורש.

```
root@kali:~# cd /usr/local/man
root@kali:/usr/local/man#
```

הפקודה **ls**, ללא דגלים נוספים, מפרטת קבצים וספריות בפורמט בסיסי, כלומר ללא פרטים כגון סוג קובץ, גודל, תאריך ושעה ששוננו, הרשאות, קישורים וכו'.

```
root@kali:~# ls
root@kali:~/Desktop# ls
bigtable.csv  mess  torshammer
```

כדי להציג רשימה של כל הקבצים, כולל קבצים וספריות מוסתרים, יש להשתמש בדגל

-a

```
root@kali:~/Desktop# ls -a
111.  ..  .html  bigtable.csv  mess  torshammer
```

הדגל **/-** מצביע על גודל הפריט, תאריך ושעה ששונה, שם הקובץ או התיקיה, הבעלים של הקובץ וההרשאות שלו. התכונות הנוספות **root root-l -rw-r--r--** מייצגות את ההרשאות והבעלות על הקבצים ויוסברו בהמשך.

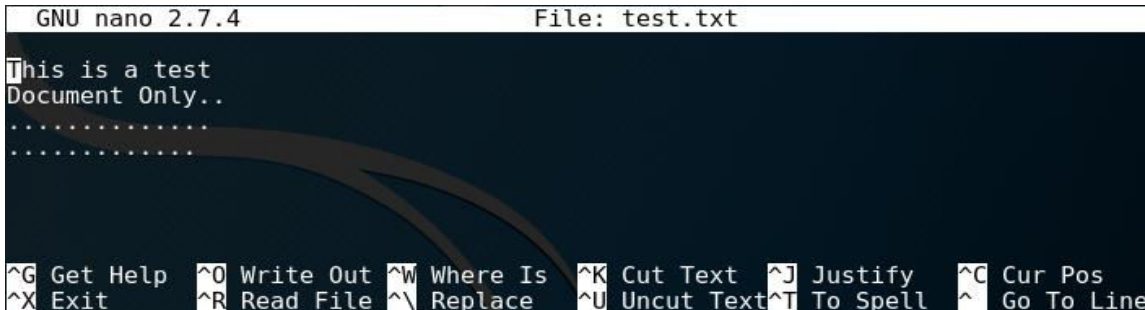
```
root@kali:~/Desktop# ls -l
total 70220
-rw-r--r-- 1 root root 71884714 Sep  3 05:48 bigtable.csv
drwxr-xr-x 13 root root  4096 Oct 28 04:09 mess
drwxr-xr-x  2 root root  4096 Oct 28 04:10 torshammer
```

הפקודה **cat** מאפשרת צפייה בתוכן הקובץ ללא אפשרות לערוך אותו.

```
root@kali:~/Desktop# cat test.txt
זהו מסמך
בלבד בדיקה
.....
.....
```

הפקודה **nano** מאפשרת צפייה בתוכן הקובץ, עריכת קבצים, שינוי שם הקובץ ועוד. Nano הוא עורך טקסט שמופעל באמצעות הפקודה **nano**.

```
root@kali:~# nano test.txt
```



במערכות Linux, כמעט הכל הוא בפורמט של קובץ, ואם זה לא קובץ, אז זה תהליך. קובץ לא בהכרח כולל רק טקסט, תמונות ותוכניות מקומפלות, אלא יכול להכיל גם מחיצות, מנהלי התקני חומרה וספריות. קבצי Linux תמיד תלויי רישיות. שני קבצים יכולים לחלוק את אותו השם, אך שמותיהם יהיו בעלי אותיות רישיות שונות. לדוגמה, **File.txt** ו-**file.txt** הם שני קבצים שונים.

ישנם שלושה סוגי קבצים בסיסיים:

קבצים רגילים

אלה הם קבצים במערכת שמכילים נתונים, טקסט או הוראות תכנית. קבצי תצורה שייכים לסוג זה של קבצים. הם כוללים נתונים הניתנים לשינוי המשפיעים על פעולות ושירותים שונים במערכת. התצורה שלהם בדרך כלל מוגדרת בעת שימוש במערכות Linux.

קבצים מיוחדים

קובץ מיוחד משמש לייצוג הקלט/פלט של מכשיר פיזי כגון מדפסת. ישנם שני סוגים של קבצים מיוחדים.

➤ **קבצי Block** מתכתבים עם התקנים המבצעים I/O ביחידות נתוני בלוקים.

➤ **קבצי תווים מיוחדים** מתכתבים עם מכשירים המבצעים I/O תו אחד בכל פעם. זה אומר שהנתונים נכתבים שמונה סיביות בכל פעם.

ספריות

ספריות מאחסנות קבצים רגילים ומיוחדים כאחד. עבור משתמשים המכירים את מערכות ההפעלה Windows או Mac, ספריות UNIX דומות לתיקיות.

ב-Linux ניתן ליצור קבצים באמצעות פקודות שונות, כגון:

? **touch <filename>**

? **vi <filename>**

? **nano <filename>**

? **gedit <filename>**

Vi, Nano ו-Gedit הם עורכי טקסט. Gedit הוא עורך GUI, וכל היתר הם מבוססי-מסוף. ניתן להפנות כמעט כל פלט לקובץ באמצעות התחביר << בסוף הפקודה, שמוסיף את הערך לסוף הקובץ. ניתן להשתמש ב- < כדי לעקוף את תוכן הקובץ.

```
root@kali:~# echo "hello" > text.txt
root@kali:~# echo "hello" >> text.txt
```

```
root@kali:~
```

העתקה והעברה של קבצים ממיקום אחד לאחר

filename (שם הקובץ) ו-**destination** (יעד) יכולים להיות נתיבים מוחלטים או יחסיים. פרמטר ה-**destination** יכול לכלול שם קובץ ומאפשר למשתמש להגדיר שם קובץ חדש לקובץ שהועתק.

בפקודה **cp** משתמשים להעתקת קבצים וספריות.

```
root@kali:~# cp text.txt ../text.txt
```

בפקודה **mv** משתמשים כדי להזיז קבצים וספריות.

```
root@kali:~# mv text.txt ../text.txt
```

בפקודה **rm** משתמשים כדי למחוק קובץ קיים.

```
root@kali:~# rm text.txt
```

בפקודה **mkdir** משתמשים כדי ליצור ספרייה חדשה.

```
root@kali:~# mkdir newdir
```

בפקודה **rmdir** משתמשים כדי למחוק ספרייה קיימת.

```
root@kali:~# rmdir newdir
```

קבלת עזרה

ניתן להשתמש באפשרות העזרה עבור רוב הפקודות כדי להציג תוכן לגבי השימוש בהן. התוכן עשוי לכלול דוגמאות של התחביר ודגלים אפשריים. בנוסף, כאשר חלק מהפקודות מוזנות ללא אפשרויות, מוצגים השימוש והפורמט שלהן. בדגל **--help** (או **-h**) משתמשים כדי לקבל מידע על פקודה.

```
root@kali:~# ping -h
```

```
Usage: ping [-aAbBdDfhLnOqrRUvV64] [-c count] [-i interval] [-I interface[
-] m mark] [-M pmtudisc_option] [-l preload] [-p pattern] [-Q tos[
-] s packetsize] [-S sndbuf] [-t ttl] [-T timestamp_option[
-] w deadline] [-W timeout] [hop1 ...] destination
Usage: ping -6 [-aAbBdDfhLnOqrRUvV] [-c count] [-i interval] [-I interface[
-] l preload] [-m mark] [-M pmtudisc_option[
-] N nodeinfo_option] [-p pattern] [-Q tclass] [-s packetsize[
-] S sndbuf] [-t ttl] [-T timestamp_option] [-w deadline[
-] W timeout] destination
```

בנוסף, ניתן להשתמש בפקודה **man** כדי לפתוח מידע הקשור לבינארי. המדריך מכיל מידע שסופק על ידי מפתח הבינארי ולעיתים קל יותר לקריאה.

```
root@kali:~# man ping
```

```
PING(8)                                iputils                                PING(8)
NAME
    ping - send ICMP ECHO_REQUEST to network hosts

SYNOPSIS
    ping [-aAbBdDfhLnOqrRUvV46] [-c count] [-F flowlabel] [-i interval]
        [-I interface] [-l preload] [-m mark] [-M pmtudisc_option]
        [-N nodeinfo_option] [-w deadline] [-W timeout] [-p pattern]
        [-Q tos] [-s packetsize] [-S sndbuf] [-t ttl]
        [-T timestamp_option] [hop...] {destination}

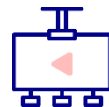
DESCRIPTION
    ping uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit
    an ICMP ECHO_RESPONSE from a host or gateway. ECHO_REQUEST datagrams
    ("pings") have an IP and ICMP header, followed by a struct timeval and
    then an arbitrary number of "pad" bytes used to fill out the packet.

    ping works with both IPv4 and IPv6. Using only one of them explicitly
    can be enforced by specifying -4 or -6.

    ping can also send IPv6 Node Information Queries (RFC4620).
    Intermediate hops may not be allowed, because IPv6 source routing was
    deprecated (RFC5095).

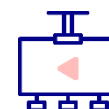
OPTIONS
    -4
Manual page ping(8) line 1 (press h for help or q to quit)
```

תרגול קצר: עזרה עם פקודות



- יש לקבל עזרה לפקודות ניווט ומניפולציות תוכן.
- יש להדפיס מידע עזרה על הפקודות שנלמדו בשיעור.
- יש לעיין בפלט כדי להבין איך משתמשים בפקודות.
- יש להוסיף דגלים לכמה פקודות.
- יש להריץ את הפקודות עם הדגלים שנבחרו.

משימת מעבדה: מסוף Linux



יש לתרגל פקודות מסוף Linux לניווט מערכת ולמניפולציה של קבצים.