



ספר קורס



מתקפות תשתיות

עמוד 1 -

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

מידע על ספר לימוד זה

מסמך זה הוא ספר לימוד עבור הקורס המלא של האקינג אתי. הוא מכיל את כל המידע שהמנחה יציג בביתה.

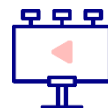
ספר הלימוד מלווה את הקורס כולו, לפי סדר כרונולוגי, משלב ההתחלה ועד לחומר המתקדם של הקורס.

מקרא

קטעי טקסט צבעוניים מופיעים לאורך מסמך זה כדי להפנות את הקורא למקור ספציפי, או להעשיר אותו במידע נוסף.

קטעי הטקסט הצבעוניים כוללים את הנושאים הבאים:

משימת מעבדה



יש לעיין בקבצי המעבדה התואמים כדי לתרגל את מה שנלמד עד כה. תיבת טקסט זו כוללת גם שאלות ספציפיות לתרגול.

טוב לדעת



מידע נוסף או תובנות לגבי הנושא. מידע זה נועד לצורך העשרה בלבד ואינו חלק מהחומרים עליהם תיבחנו.

טיפ



מידע שימושי שיש בו כדי לסייע לתלמידים ללמוד את החומר או לעבוד עם כלים מסוימים.

מידע נוסף



קישורים או הפניות לחומר חיצוני שניתן להשתמש בהם כדי להרחיב את הידיעות שלכם לגבי הנושא.

התקפות תשתית

Metasploit

סקירה של Metasploit

המינוחים הבאים מתייחסים להתקפות רשת:

נקודת תורפה: נקודת תורפה היא חולשה ספציפית במערכת, בחומרה או בתוכנה שתוקף יכול לנצל לביצוע פעולות לא מורשות.

ניצולים: ניצול מתרחש כאשר מתבצעת התקפה המבוססת על נקודת תורפה נתונה. ניצולים תמיד מכוונים לנקודות תורפה ספציפיות.

מטען מיועד: המטען המיועד הוא קטע הקוד הפועל על מערכת פגיעה לאחר ניצול. הקוד יכול גם להיות סוג של תוכנה זדונית המסוגלת לבצע פעולות לא מורשות שונות.

Local & Privilege Escalation Exploits						
This exploit category includes local exploits or privilege escalation exploits.						
Date Added	D	A	V	Title	Platform	Author
2018-06-15	🚩	-	🔒	Somnath IM Desktop.app 0.15 - Authentication Bypass	Windows	VortexNeo054
2018-06-13	🚩	-	🔒	R5i Inx Classic and FactoryTalk i Inx Gateway - Privilege Escalation	Windows	LiquidWorm
2018-06-13	🚩	-	🔒	glibc - 'roapath()' Privilege Escalation (Metasploit)	Linux	Metasploit
2018-06-13	🚩	-	🔒	Microsoft Windows 10 - Child Process Restriction Mitigation Bypass	Windows	Google...
2018-06-08	🚩	-	🔒	TrendMicro OfficeScan XG 11.0 - Change Prevention Bypass	Windows	hyprlinx
2018-06-07	🚩	-	🔒	Ftp Server 1.32 - Credential Disclosure	Android	ManhNho
2018-06-05	🚩	-	🔒	WebKitGTK+ < 2.21.3 - Crash (PoC)	Linux	Dhiraj Mishra
Denial of Service & Proof of Concept Exploits						
This exploit category includes proof of concept code or code that results in a denial of service or application crash.						
Date Added	D	A	V	Title	Platform	Author
2018-06-14	🚩	-	🔒	rtorrent 0.9.6 - Denial of Service	Linux	eco86
2018-06-11	🚩	-	🔒	WebKitGTK+ < 2.21.3 - 'WebKitFaviconDatabase' Denial of Service (Metasploit)	Linux	Dhiraj Mishra
2018-06-08	🚩	-	🔒	WebRTC - VP9 Missing Frame Processing Out-of-Bounds Memory Access	Multiple	Google...
2018-06-08	🚩	-	🔒	WebRTC - VP9 Frame Processing Out-of-Bounds Memory Access	Multiple	Google...
2018-06-08	🚩	-	🔒	WebKit - Use-After-Free when Resumming Generator	Multiple	Google...
2018-06-08	🚩	-	🔒	Google Chrome - Integer Overflow when Processing WebAssembly Locals	Multiple	Google...
2018-06-08	🚩	-	🔒	WebKit - WebAssembly Compilation Info Leak	Multiple	Google...

רשימת פונקציות ניצול שתוקף יכול להריץ

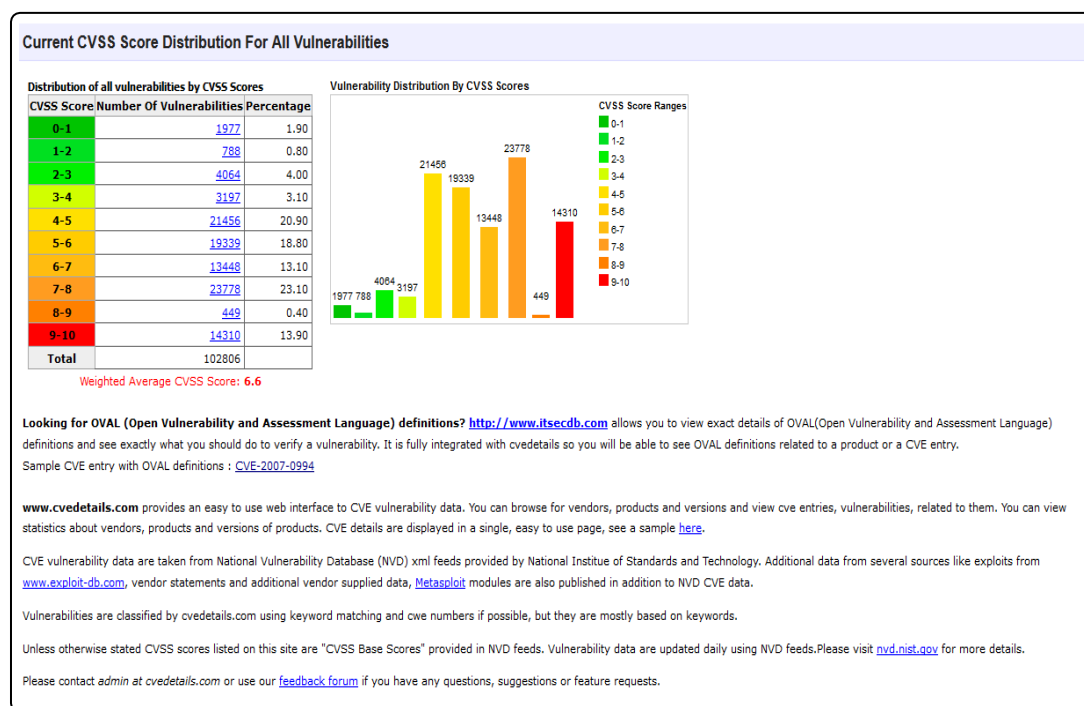
מנועי חיפוש

לנקודות תורפה יש לעתים פונקציית ניצול שבאמצעותה התוקף יכול להשיג יתרון. ניצולים אלה עשויים להעניק לתוקף יכולת להוציא לפועל קוד מרחוק במחשב מרוחק ועשויים להעניק לו גישה להרשאות גבוהות יותר או לפגוע במטרה מספיק כדי ליצור מניעת שירות. ניתן למצוא את רוב ניצולי האינטרנט באינטרנט באתרים הבאים:

פרטי CVE: אתר אינטרנט המספק תיעוד של נקודות תורפה וחשיפות נפוצות שונות, כולל חומרתן (לפי דירוג מנהל האתר), הפרקטיות שלהן וסקירה רחבה של המוצרים והמערכות המושפעות.

מסד נתונים מנצל: ארכיון עצום המאסף ניצולים, קוד ומידע אחר הקשור לאבטחה, כולל מסד הנתונים של Google Hacking (GHDB), מאגר מידע של שאילתות חיפוש. ל- Exploit Database יש כלי חיפוש לא מקוון בשם SearchSploit (המתואר בסעיף הבא) המותקן מראש במערכת ההפעלה Kali Linux.

Cve.mitre.org: אתר שמקטלג ומסכם מספר רב של CVEs. חלק מהתיאורים כוללים הפניות לנתונים טכניים.



אתר פרטי CVE (cvedetails.com)

SearchSploit

ל-Database Exploit יש כלי חיפוש לא מקוון המובנה במערכת ההפעלה Kali Linux. **SearchSploit** הוא כלי שעובד עם Exploit Database, אך לא עם מסד הנתונים של Google Hacking. ניתן גם להוריד אותו באינטרנט למערכות Mac ו-Windows.

SearchSploit מעדכנת את רשימת הניצולים שלה בעזרת Exploit Database, ואוספת את המידע העדכני ביותר על ניצולים ונקודות תורפה, הכתובות במגוון שפות תכנות.

ניתן לחפש ניצול במסוף Linux באופן הבא:

searchsploit -u -מעדכן את מסד הנתונים של הכלי.

searchsploit [term] - מוצא את כל הניצולים התואמים את מונח החיפוש.

searchsploit -nmap [file] - מספק בדיקה צולבת אוטומטית עם שירותים שנמצאו על ידי כלי הסריקה של Nmap.

פקודות ה-SearchSploit שהוזכרו למעלה מפרטות את כל הניצולים הקשורים למונח שצוין על ידי המשתמש ואת הנתוב שאליו יועברו.

שימוש ב-SearchSploit

כדי להשתמש בניצולים הכלולים בכלי, התוקפים חייבים להעביר תחילה את הניצולים ממאגר הנתונים של הכלי אל המחשב שלהם. ניתן לעשות זאת באמצעות הפקודה הבאה:

searchsploit -m [full path of the exploit]


לאחר מכן, יש לשנות את הרשאות הסקריפט באמצעות הפקודה **chmod**, והניצול יופעל.

```

root@kali:~# searchsploit OpenSSH
-----
Exploit Title | Path
              | (/usr/share/exploitdb/)
-----
Debian OpenSSH - (Authenticated) Remot | exploits/linux/remote/6094.txt
Dropbear / OpenSSH Server - 'MAX_UNAUT | exploits/multiple/dos/1572.pl
FreeBSD OpenSSH 3.5p1 - Remote Command | exploits/freebsd/remote/17462.txt
Novell Netware 6.5 - OpenSSH Remote St | exploits/novell/dos/14866.txt
OpenSSH 1.2 - '.scp' File Create/Overw | exploits/linux/remote/20253.sh
OpenSSH 2.3 < 7.7 - Username Enumerati | exploits/linux/remote/45210.py
OpenSSH 2.3 < 7.7 - Username Enumerati | exploits/linux/remote/45233.py
OpenSSH 2.x/3.0.1/3.0.2 - Channel Code | exploits/unix/remote/21314.txt
OpenSSH 2.x/3.x - Kerberos 4 TGT/AFS T | exploits/linux/remote/21402.txt
OpenSSH 3.x - Challenge-Response Buffe | exploits/unix/remote/21578.txt
OpenSSH 3.x - Challenge-Response Buffe | exploits/unix/remote/21579.txt
OpenSSH 4.3 p1 - Duplicated Block Remo | exploits/multiple/dos/2444.sh
OpenSSH 6.8 < 6.9 - 'PTY' Local Privil | exploits/linux/local/41173.c
OpenSSH 7.2 - Denial of Service | exploits/linux/dos/40888.py
OpenSSH 7.2p1 - (Authenticated) xauth | exploits/multiple/remote/39569.py
OpenSSH 7.2p2 - Username Enumeration | exploits/linux/remote/40136.py
OpenSSH < 6.6 SFTP (x64) - Command Exe | exploits/linux_x86-64/remote/45000.c
OpenSSH < 6.6 SFTP - Command Execution | exploits/linux/remote/45001.py
OpenSSH < 7.4 - 'UsePrivilegeSeparatio | exploits/linux/local/40962.txt
OpenSSH < 7.4 - agent Protocol Arbitra | exploits/linux/remote/40963.txt
OpenSSH < 7.7 - User Enumeration (2) | exploits/linux/remote/45939.py
OpenSSH SCP Client - Write Arbitrary F | exploits/multiple/remote/46516.py
OpenSSH/PAM 3.6.1p1 - 'gossh.sh' Remot | exploits/linux/remote/26.sh
OpenSSH/PAM 3.6.1p1 - Remote Users Dis | exploits/linux/remote/25.c
OpenSSHd 7.2p2 - Username Enumeration | exploits/linux/remote/40113.txt

```

שימוש ב-SearchSploit



משימת מעבדה: SearchSploit
יש לתרגל עבודה עם SearchSploit והורדת סקריפט.

Metasploit

Metasploit היא מסגרת שפותחה לבודקי חדירות לאיתור ולניצול של נקודות תורפה. זהו הממשק המשולב למסגרת Metasploit שמגיעה עם Kali Linux.
Metasploit כולל מודולים נפרדים המאפשרים הרחבה ודינמיות.

```
root@kali:~# msfconsole
# cowsay++
< metasploit >
-----
      \      (oo)
       \      ( )
        \      )\
         ||--|| *

      =[ metasploit v5.0.60-dev ]
+ -- --=[ 1947 exploits - 1089 auxiliary - 333 post ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

msf5 > 
```

ממשק Msfconsole

סריקת Metasploit

אפשר להריץ סריקות Nmap באמצעות המסגרת של Metasploit. הסריקה כוללת הרצת Nmap מה-Msfconsole באמצעות הפקודה **db_nmap**, או באמצעות Nmap עם הדגל **-oX** עבור פלט של קובץ XML. לאחר מכן, יש להשתמש בפקודה **db_import** כדי לייבא את תוצאות הסריקה אל מסד הנתונים של Metasploit.

ל-Msfconsole יש גם מגוון גדול של סורקים שניתן לצפות בהם על ידי הרצת **search** ל-**portscan**. כל הסריקות נשמרות במסד הנתונים. כדי לראות תוצאות מסוננות של סריקה, יש להריץ את הפקודה **.services**.

```
.....CCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCC
.....
fffffffffffffffffffffffffff
fffffffff.....
fffffffffffffffffffffffffff
fffffffff.....
fffffffff.....
fffffffff.....
.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
In swapper task - not syncing

      =[ metasploit v5.0.60-dev                               ]
+ -- --=[ 1947 exploits - 1089 auxiliary - 333 post           ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops                ]
+ -- --=[ 7 evasion                                           ]

msf5 > db_nmap
[*] Usage: db_nmap [--save | [--help | -h]] [nmap options]
msf5 > db_nmap 10.21.0.0/24 -PN
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-25 04:38 EST
```

שימוש ב-db_nmap של Msfconsole

חיפוש Msfconsole

Msfconsole היא אחת מדרכי העבודה הנפוצות ביותר עם Metasploit.

הפקודות המשמשות ב-Msfconsole כוללות:

Search [term] - מחפש את כל המודולים המתאימים למונח החיפוש.

Use exploit/multi/handler - handler גנרי להרצת ניצולים ומטענים מיועדים במחשבי מטרה.

Use [name] – קובע באיזה מודול להשתמש.

הגדרת מודול

שיטה	הסבר
Use [name]	מגדירה את המודול שיש להשתמש בו
Set RPORT [IP]	מגדירה את כתובת ה-IP
Set RPORT [port]	מגדירה את המטרה בפורט המרוחק
Set LHOST [IP]	מגדירה את מארח ה-IP המקומי
Set LPORT [port]	מגדירה את מספר הפורט המקומי
Exploit or run	מריצה את הניצול

תיאורי מודול

Metasploit הוא כלי רב עוצמה התומך במגוון כלים המסייעים לתוקף לבצע תקיפה ברשת של הקורבן.

מודולי Metasploit כוללים את הדברים הבאים:

ניצולים: מודול הניצול מטפל בכל הפקודות הממוקדות בנקודת תורפה מסוימת הנמצאת במערכת או באפליקציה. הוא כולל הזרקת קוד, הצפת מנגנון זיכרון זמני וניצול של אפליקציות אינטרנט וניידים.

מטענים מיועדים: מטען מיועד הוא קוד מעטפת ספציפי שרץ על מחשב יעד לאחר שניצול מצליח לפגוע במערכת והתוקף משיג יכולת ביצוע. המטען הייעודי יכול להגדיר כיצד להתחבר לתוקף ואילו פקודות צריכות לפעול על מערכת היעד לאחר השגת שליטה עליה.

כלי עזר: מודולי עזר מבצעים פעולות שאינן קשורות לתהליכי ניצול. דוגמאות למודולי עזר כוללים סורקים המזהים נקודות תורפה של יעדים, כלי מניעת שירות וכלים נוספים המסייעים לתהליך הניצול, אך אינם מעורבים ישירות בהשגת גישה ליעד.

מקודדים: מקודדים מצפינים מטענים ייעודיים כדי להתחמק מזהוי על ידי אבטחת נקודת הקצה. מקודדים נפוצים כוללים את **Non-AlphaNumeric, Shikata Ga Nai** ואת **BloXor**. רוב המקודדים של Metasploit מיושנים ואינם יעילים עוד כנגד אמצעי אבטחה מוגדרים היטב של נקודות קצה.

NOPs: NOPs הם פיסות קוד קטנות המשמשות בעיקר עבור ריפוד ותזמון. הם לא מיועדים לשימוש עצמאי.

משימת מעבדה: Metasploit

יש לתרגל עבודה עם תכונות MetaSploit שונות.

