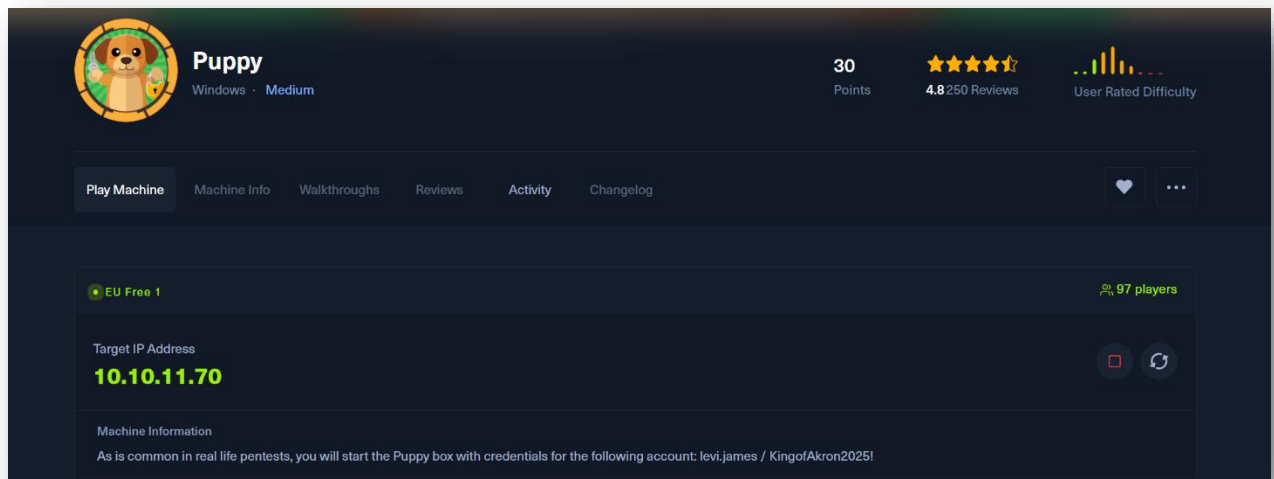


Enumerácia

HackTheBox - Windows + Linux

Prostredie: WINDOWS MACHINE (Stredne ťažký):



Cieľ → 10.10.11.70

Overenie, či je cieľ aktívny:

Príkaz:

ping -c 4 10.10.11.70

```
File Actions Edit View Help View Help
(root@kali)-[~]
# ping -c 4 10.10.11.70
PING 10.10.11.70 (10.10.11.70) 56(84) bytes of data.
64 bytes from 10.10.11.70: icmp_seq=1 ttl=127 time=113 ms
64 bytes from 10.10.11.70: icmp_seq=2 ttl=127 time=37.0 ms
64 bytes from 10.10.11.70: icmp_seq=3 ttl=127 time=151 ms
64 bytes from 10.10.11.70: icmp_seq=4 ttl=127 time=72.1 ms

— 10.10.11.70 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 36.992/93.270/150.816/42.787 ms
```

Výsledok vrátil, že služba beží, čiže má zmysel zahájiť útok

Scanning (Port-Scanning):

Príkaz:

nmap -sS -Pn -T4 -p- 10.10.11.70

```
(root@kali)-[~]
# nmap -sS -Pn -p- -T4 10.10.11.70
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 19:33 EDT
Nmap scan report for 10.10.11.70
Host is up (0.030s latency).
Not shown: 65512 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain
88/tcp    open  kerberos-sec
111/tcp   open  rpcbind
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
2049/tcp   open  nfs
3260/tcp   open  iscsi
3268/tcp   open  globalcatLDAP
3269/tcp   open  globalcatLDAPssl
5985/tcp   open  wsman
9389/tcp   open  adws
49664/tcp  open  unknown
49667/tcp  open  unknown
49669/tcp  open  unknown
49670/tcp  open  unknown
49690/tcp  open  unknown
53773/tcp  open  unknown
53804/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 97.50 seconds
```

Výsledok: Nmap zistil všetky dostupné porty cieľa, a na akých službách bežia, čo je veľmi dôležité pre enumeráciu, pretože tak vieme určiť, aký typ enumerácie máme použiť na konkrétny port

Nmap Enumerácia (Prechod z Scanning → Enumerácia):

Príkaz:

nmap -sS -sC -sV -p 53,88,111,.....,53804 10.10.11.70

-sS: SYN scan (port scanning)

-sC: default NSE skripty (napr. zisťovanie SSH kľúčov, HTTP hlavičiek) → enumerácia

-sV: zistí verzie služieb

```
(root@kali)-[~]
# nmap -sS -sC -sV -p 53,88,111,135,139,389,445,464,593,636,2049,3260,3268,3269,5985,9389,49664,49667,49669,49670,49690,53773,53804 10.10.11.70
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 19:42 EDT
Nmap scan report for 10.10.11.70
Host is up (0.25s latency).

Bug in iscsi-info: no string output.
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         Simple DNS Plus
88/tcp    open  kerberos-sec   Microsoft Windows Kerberos (server time: 2025-06-03 06:43:05Z)
111/tcp   open  rpcbind        2-4 (RPC #100000)
|_ rpcinfo:
|_  program version  port/proto  service
|_  100000  2,3,4          111/tcp     rpcbind
|_  100000  2,3,4          111/tcp6    rpcbind
|_  100000  2,3,4          111/udp     rpcbind
|_  100000  2,3,4          111/udp6    rpcbind
|_  100003  2,3            2049/udp    nfs
|_  100003  2,3            2049/udp6   nfs
|_  100005  1,2,3          2049/udp    mountd
|_  100005  1,2,3          2049/udp6   mountd
|_  100021  1,2,3,4        2049/tcp    nlockmgr
|_  100021  1,2,3,4        2049/tcp6   nlockmgr
|_  100021  1,2,3,4        2049/udp    nlockmgr
|_  100021  1,2,3,4        2049/udp6   nlockmgr
|_  100024  1              2049/tcp    status
|_  100024  1              2049/tcp6   status
|_  100024  1              2049/udp    status
|_  100024  1              2049/udp6   status
135/tcp   open  msrcpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
389/tcp   open  ldap           Microsoft Windows Active Directory LDAP (Domain: PUPPY.HTB0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
2049/tcp  open  nlockmgr       1-4 (RPC #100021)
3260/tcp  open  iscsi?
3268/tcp  open  ldap           Microsoft Windows Active Directory LDAP (Domain: PUPPY.HTB0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-server-header: Microsoft-HTTPAPI/2.0
|_ http-title: Not Found
9389/tcp  open  mc-nmf         .NET Message Framing
49664/tcp open  msrcpc         Microsoft Windows RPC
49667/tcp open  msrcpc         Microsoft Windows RPC
49669/tcp open  msrcpc         Microsoft Windows RPC
49670/tcp open  ncacn_http     Microsoft Windows RPC over HTTP 1.0
49690/tcp open  msrcpc         Microsoft Windows RPC
53773/tcp open  msrcpc         Microsoft Windows RPC
53804/tcp open  msrcpc         Microsoft Windows RPC
Service Info: Host: DC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: 7h00m00s
|_ smb2-security-mode:
|_   3:1:1:
|_     Message signing enabled and required
|_ smb2-time:
|_   date: 2025-06-03T06:44:59
|_   start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 218.04 seconds
```

Výsledok ukázal tieto informácie:

1. IP adresa cieľa je: 10.10.11.70
2. Host je živý: Host is up (0.25s latency)
3. OS: Windows DC (Domain Controller)
4. Doména cieľa je: DC.PUPPY.HTB (port 389, 3268)
5. SMBv2: Message Enabled and required (mierne zabezpečená)

Zhrnutie Nmap enumerácie:

- Odhalenie infraštruktúry Windows AD domény
- Odhalenie bežiacich služieb a ich verzie na konkrétnych portoch
- Cieľ beží na OS Windows
- Poskytol základný pivoting pre ďalšie nástroje ako ldapsearch, rpcclient, enum4linux-ng a pod.

Automatizovaná Enumerácia (SMB + RPC + LDAP):

Príkaz:

enum4linux-ng 10.10.11.70

Enum4linux automaticky spustí viaceré overené techniky na získanie informácií zo **SMB**, **RPC** a **LDAP**

```
(root@kali)~# enum4linux-ng 10.10.11.70
ENUM4LINUX - next generation (v1.3.4)

=====
| Target Information |
=====
[*] Target ..... 10.10.11.70
[*] Username ..... ''
[*] Random Username .. 'ujdibhuo'
[*] Password ..... ''
[*] Timeout ..... 5 second(s)

=====
| Listener Scan on 10.10.11.70 |
=====
[*] Checking LDAP
[+] LDAP is accessible on 389/tcp
[*] Checking LDAPS
[+] LDAPS is accessible on 636/tcp
[*] Checking SMB
[+] SMB is accessible on 445/tcp
[*] Checking SMB over NetBIOS
[+] SMB over NetBIOS is accessible on 139/tcp

=====
| Domain Information via LDAP for 10.10.11.70 |
=====
[*] Trying LDAP
[+] Appears to be root/parent DC
[+] Long domain name is: PUPPY.HTB

=====
| NetBIOS Names and Workgroup/Domain for 10.10.11.70 |
=====
[-] Could not get NetBIOS names information via 'nmblookup': timed out

=====
| SMB Dialect Check on 10.10.11.70 |
=====
[*] Trying on 445/tcp
[+] Supported dialects and settings:
Supported dialects:
SMB 1.0: false
SMB 2.02: true
SMB 2.1: true
SMB 3.0: true
SMB 3.1.1: true
Preferred dialect: SMB 3.0
SMB1 only: false
SMB signing required: true

=====
| Domain Information via SMB session for 10.10.11.70 |
=====
[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found domain information via SMB
NetBIOS computer name: DC
NetBIOS domain name: PUPPY
DNS domain: PUPPY.HTB
FQDN: DC.PUPPY.HTB
Derived membership: domain member
Derived domain: PUPPY

=====
| RPC Session Check on 10.10.11.70 |
=====
[*] Check for null session
[+] Server allows session using username '', password ''
[*] Check for random user
[-] Could not establish random user session: STATUS_LOGON_FAILURE
```

| Domain Information via RPC for 10.10.11.70 |

[+] Domain: PUPPY
[+] Domain SID: S-1-5-21-1487982659-1829050783-2281216199
[+] Membership: domain member

File Sys

| OS Information via RPC for 10.10.11.70 |

[*] Enumerating via unauthenticated SMB session on 445/tcp
[+] Found OS information via SMB
[*] Enumerating via 'srvinfo'
[-] Could not get OS info via 'srvinfo': STATUS_ACCESS_DENIED
[+] After merging OS information we have the following result:
OS: Windows 10, Windows Server 2019, Windows Server 2016
OS version: '10.0'
OS release: ''
OS build: '20348'
Native OS: not supported
Native LAN manager: not supported
Platform id: null
Server type: null
Server type string: null

| Users via RPC on 10.10.11.70 |

[*] Enumerating users via 'querydispinfo'
[-] Could not find users via 'querydispinfo': STATUS_ACCESS_DENIED
[*] Enumerating users via 'enumdomusers'
[-] Could not find users via 'enumdomusers': STATUS_ACCESS_DENIED

| Groups via RPC on 10.10.11.70 |

[*] Enumerating local groups
[-] Could not get groups via 'enumalsgroups domain': STATUS_ACCESS_DENIED
[*] Enumerating builtin groups
[-] Could not get groups via 'enumalsgroups builtin': STATUS_ACCESS_DENIED
[*] Enumerating domain groups
[-] Could not get groups via 'enumdomgroups': STATUS_ACCESS_DENIED

| Shares via RPC on 10.10.11.70 |

[*] Enumerating shares
[+] Found 0 share(s) for user '' with password '', try a different user

| Policies via RPC for 10.10.11.70 |

[*] Trying port 445/tcp
[-] SMB connection error on port 445/tcp: STATUS_ACCESS_DENIED
[*] Trying port 139/tcp
[-] SMB connection error on port 139/tcp: session failed

| Printers via RPC for 10.10.11.70 |

[-] Could not get printer info via 'enumprinters': STATUS_ACCESS_DENIED

Completed after 19.75 seconds

Výsledky z automatizovanej enumerácie pomocou nástroja

Enum4linux:

1. LDAP (389/TCP) & LDAPS (636/TCP) **sú dostupné (otvorené)**
2. SMB pripojenie cez port 445/TCP **je funkčné**
3. SMB cez NetBIOS pomocou 139/TCP portu **je tiež dostupné**
4. DNS Doména: **PUPPY.HTB**
5. Podporované verzie SMB:
 - a. **SMB 1.0 → zablokovaná (bežná ochrana)**
 - b. **SMB 2.0/2.1/3.0/3.1.1 → podporované**
6. SMB signing = **enabled and required**
7. OS cez RPC: **Windows 10, Windows Server 2016 & 19**
8. SID (Unikátny identifikátor domény): **S-1-5-21**
9. Používateľské/Session/Group enumerácie: **Zlyhali kvôli neprístupnosti resp. absencii loginu (Anonymous Session nemá oprávnenie)**

Pokus o anonymný prístup & SMB enumerácia cez NSE skripty:

Príkaz:

smbclient -L //10.10.11.70/ -N

nmap --script=smb-enum* 10.10.11.70

```
(root@kali)-[~]
# smbclient -L //10.10.11.70/ -N
Anonymous login successful
Host:
  Sharename      Type            Comment
  ----
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.70 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(root@kali)-[~]
# nmap -p 139,445 --script=smb-enum* 10.10.11.70
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 19:53 EDT
Nmap scan report for 10.10.11.70
Host is up (0.31s latency).

PORT      STATE SERVICE
139/tcp   open  netbios-ssn
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)
445/tcp   open  microsoft-ds
|_smb-enum-services: ERROR: Script execution failed (use -d to debug)

Nmap done: 1 IP address (1 host up) scanned in 15.49 seconds
```

Výsledky týchto 2 príkazov:

NSE SMB skripty sa pokúsili získať informácie o službách a zdieľaniach cez SMB, ale nepodarilo sa pripojiť → **ERROR: Script execution failed**.

To znamená, že pravdepodobne server odmieta anonymný prístup, alebo cez SMB signing blokuje skriptové útoky bez overenia.

Pokus o anonymný prístup k zdieľaným priečinkom pomocou **smbclient** bol úspešný: **Anonymous login successful**, ale nedokázal sa napojiť na SMB1 (**Unable to connect with SMB1 → no workgroup available**).

To znamená, že SMBv1 je zakázaný, čo je bežná ochrana, a taktiež pravdepodobne neexistuje žiadna voľne dostupná zdieľaná zložka

Alternatíva ku SMB enumerácii:

CrackMapExec (CME):

→ Spustí SMB enumeráciu na cieľovej IP adrese

Príkaz:

crackmapexec smb 10.10.11.70

```
(root@kali)~# crackmapexec smb 10.10.11.70
[*] First time use detected
[*] Creating home directory structure
[*] Creating default workspace
[*] Initializing SMB protocol database
[*] Initializing FTP protocol database
[*] Initializing RDP protocol database
[*] Initializing SSH protocol database
[*] Initializing WINRM protocol database
[*] Initializing MSSQL protocol database
[*] Initializing LDAP protocol database
[*] Copying default configuration file
[*] Generating SSL certificate
SMB      10.10.11.70    445    DC      [*] Windows Server 2022 Build 20348 x64 (name:DC) (domain:PUPPY.HTB) (signing:True) (SMBv1:False)
```

Výsledky príkazu:

→ IP adresa cieľa: 10.10.11.70

→ Port: 445 (typický pre SMB)

→ Doména: PUPPY.HTB

→ OS: Windows Server 2022 Build 20348 x64

→ SMBv1: False → zakázaný (bežná ochrana)

→ Signing: True → podpisy SMB relácii musia byť skontrolované, čo môže blokať niektoré útoky

RPC Enumerácia:

Pokus o pripojenie k RPC cez SMB pomocou anonymného používateľa:

Príkaz:

rpcclient -U "" 10.10.11.70

```
(root@kali)-[~]  
# rpcclient -U "" 10.10.11.70  
Password for [WORKGROUP\]:  
Cannot connect to server.  Error was NT_STATUS_LOGON_FAILURE
```

Výsledok pokusu hovorí, že:

→ Server **odmietol anonymné pripojenie**

→ Neposkytol ani možnosť „null session“, teda pripojenie bez mena a heslá, čo znamená, že **nie je možné enumerovať používateľov, skupiny, zdieľané priečinky bez platných prihlasovacích údajov cez RPC**

Nmap skript na enumeráciu MSRPC (Microsoft Remote Procedure Call) na známych portoch:

Príkaz:

nmap -p 111, 135, 593 --script=msrpc-enum 10.10.11.70

```
(root@kali)-[~]  
# nmap -p 111,135,593 --script=msrpc-enum 10.10.11.70  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 19:58 EDT  
Nmap scan report for 10.10.11.70  
Host is up (0.12s latency).  
  
PORT      STATE SERVICE  
111/tcp   open  rpcbind  
135/tcp   open  msrpc  
593/tcp   open  http-rpc-epmap  
  
Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

Výsledok tohto príkazu vrátil porty, ktoré sú otvorené, čiže **služby bežia**. Avšak nevrátil žiadne iné informácie, pretože **anonymný prístup nie je povolený**, alebo **žiadne RPC endpointy nie sú verejne prístupné**.

Záver RPC enumerácie:

- Anonymný prístup je zablokovaný, čo bolo potvrdené rpcclientom, a NSE skriptom
- RPC Služby sú aktívne na portoch 111, 135 a 593, ktoré boli potvrdené nmap-om

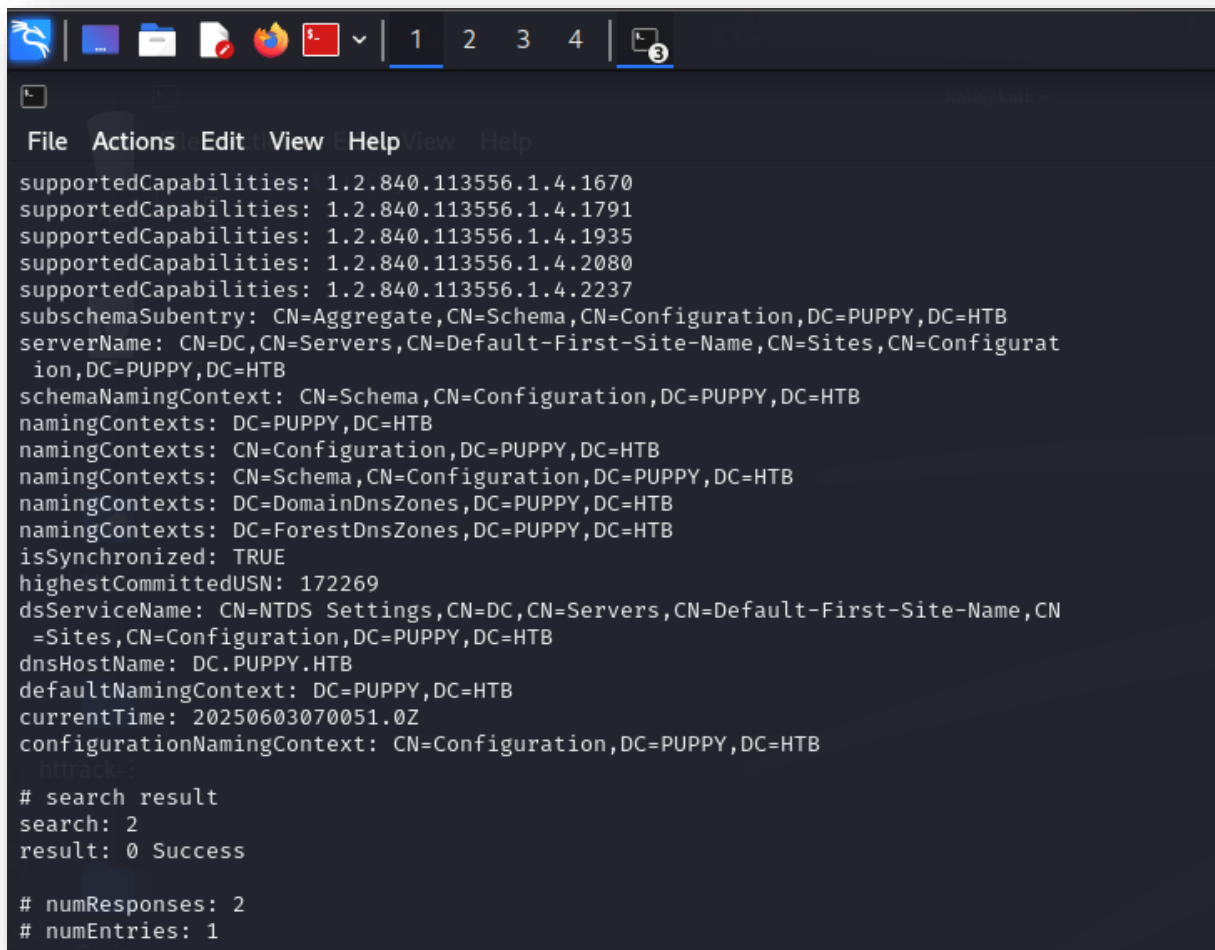
LDAP Enumerácia:

Základný anonymný LDAP dopyt, ktorý načíta základné info o doméne zo základného objektu (base):

Príkaz:

ldapsearch -x -H ldap://10.10.11.70 -s base

```
(root@kali)-[~]
# ldapsearch -x -H ldap://10.10.11.70 -s base
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: ALL
#
#
dn:
domainFunctionality: 7
forestFunctionality: 7
domainControllerFunctionality: 7
rootDomainNamingContext: DC=PUPPY,DC=HTB
ldapServiceName: PUPPY.HTB:dc$@PUPPY.HTB
isGlobalCatalogReady: TRUE
supportedSASLMechanisms: GSSAPI
supportedSASLMechanisms: GSS-SPNEGO
supportedSASLMechanisms: EXTERNAL
supportedSASLMechanisms: DIGEST-MD5
supportedLDAPVersion: 3
supportedLDAPVersion: 2
supportedLDAPPolicies: MaxPoolThreads
supportedLDAPPolicies: MaxPercentDirSyncRequests
supportedLDAPPolicies: MaxDatagramRecv
supportedLDAPPolicies: MaxReceiveBuffer
supportedLDAPPolicies: MaxPreAuthReceiveBuffer
supportedLDAPPolicies: InitRecvTimeout
supportedLDAPPolicies: MaxConnections
supportedLDAPPolicies: MaxConnIdleTime
supportedLDAPPolicies: MaxPageSize
supportedLDAPPolicies: MaxBatchReturnMessages
supportedLDAPPolicies: MaxQueryDuration
supportedLDAPPolicies: MaxDirSyncDuration
supportedLDAPPolicies: MaxTempTableSize
supportedLDAPPolicies: MaxResultSetSize
supportedLDAPPolicies: MinResultSets
supportedLDAPPolicies: MaxResultSetsPerConn
supportedLDAPPolicies: MaxNotificationPerConn
supportedLDAPPolicies: MaxValRange
supportedLDAPPolicies: MaxValRangeTransitive
supportedLDAPPolicies: ThreadMemoryLimit
supportedLDAPPolicies: SystemMemoryLimitPercent
supportedControl: 1.2.840.113556.1.4.319
supportedControl: 1.2.840.113556.1.4.801
supportedControl: 1.2.840.113556.1.4.473
supportedControl: 1.2.840.113556.1.4.528
supportedControl: 1.2.840.113556.1.4.417
supportedControl: 1.2.840.113556.1.4.619
supportedControl: 1.2.840.113556.1.4.841
supportedControl: 1.2.840.113556.1.4.529
supportedControl: 1.2.840.113556.1.4.805
supportedControl: 1.2.840.113556.1.4.521
supportedControl: 1.2.840.113556.1.4.970
supportedControl: 1.2.840.113556.1.4.1338
supportedControl: 1.2.840.113556.1.4.474
supportedControl: 1.2.840.113556.1.4.1339
supportedControl: 1.2.840.113556.1.4.1340
supportedControl: 1.2.840.113556.1.4.1413
supportedControl: 2.16.840.1.113730.3.4.9
supportedControl: 2.16.840.1.113730.3.4.10
supportedControl: 1.2.840.113556.1.4.1504
supportedControl: 1.2.840.113556.1.4.1852
supportedControl: 1.2.840.113556.1.4.802
supportedControl: 1.2.840.113556.1.4.1907
supportedControl: 1.2.840.113556.1.4.1948
supportedControl: 1.2.840.113556.1.4.1974
supportedControl: 1.2.840.113556.1.4.1341
supportedControl: 1.2.840.113556.1.4.2026
supportedControl: 1.2.840.113556.1.4.2064
```



```
File Actions Edit View Help View Help
supportedCapabilities: 1.2.840.113556.1.4.1670
supportedCapabilities: 1.2.840.113556.1.4.1791
supportedCapabilities: 1.2.840.113556.1.4.1935
supportedCapabilities: 1.2.840.113556.1.4.2080
supportedCapabilities: 1.2.840.113556.1.4.2237
subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=PUPPY,DC=HTB
serverName: CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configurat
ion,DC=PUPPY,DC=HTB
schemaNamingContext: CN=Schema,CN=Configuration,DC=PUPPY,DC=HTB
namingContexts: DC=PUPPY,DC=HTB
namingContexts: CN=Configuration,DC=PUPPY,DC=HTB
namingContexts: CN=Schema,CN=Configuration,DC=PUPPY,DC=HTB
namingContexts: DC=DomainDnsZones,DC=PUPPY,DC=HTB
namingContexts: DC=ForestDnsZones,DC=PUPPY,DC=HTB
isSynchronized: TRUE
highestCommittedUSN: 172269
dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-Site-Name,CN
= Sites,CN=Configuration,DC=PUPPY,DC=HTB
dnsHostName: DC.PUPPY.HTB
defaultNamingContext: DC=PUPPY,DC=HTB
currentTime: 20250603070051.0Z
configurationNamingContext: CN=Configuration,DC=PUPPY,DC=HTB
# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Výsledky tohto základného anonymného LDAP dopytu zistili, že:

→ Host je: **DC.PUPPY.HTB**

→ LDAP verzia: **2 & 3 je podporovaná**

→ rootDomainNamingContext: **DC = PUPPY, DC = HTB**

→ teda doména je: **PUPPY.HTB**

→ namingContexts (názvy kontextov): **DNS zóny, rôzne DC konfigurácie, schémy**

→ Podporované SASL mechanizmy (supportedSASLmechanisms): **EXTERNAL, GSSAPI, DIGEST-MD5**

→ Funkčnosť DC (Domain Controller): **7**

→ čo zodpovedá **Windows Serveru 2016 & 19**

LDAP NSE skripty:

→ Použitie všetkých LDAP skriptov na portoch 389 a 636

nmap -p 389, 636 --script=ldap* 10.10.11.70

--script=ldap* : spustí všetky skripty, ktoré začínajú na „ldap“

```
File Actions Edit View Help View Help
(root@kali)~# nmap -p 389,636 --script=ldap* 10.10.11.70
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-02 20:01 EDT
NSE: [ldap-brute] passwords: Time limit 10m00s exceeded.
NSE: [ldap-brute] passwords: Time limit 10m00s exceeded.
NSE: [ldap-brute] usernames: Time limit 10m00s exceeded.
Nmap scan report for 10.10.11.70
Host is up (0.67s latency).

Bug in ldap-brute: no string output.
PORT      STATE SERVICE
389/tcp   open  ldap
| ldap-rootdse:
| LDAP Results
| <ROOT>
|   domainFunctionality: 7
|   forestFunctionality: 7
|   domainControllerFunctionality: 7
|   rootDomainNamingContext: DC=PUPPY,DC=HTB
|   ldapServiceName: PUPPY.HTB:dc=$@PUPPY.HTB
|   isGlobalCatalogReady: TRUE
|   supportedSASLMechanisms: GSSAPI
|   supportedSASLMechanisms: GSS-SPNEGO
|   supportedSASLMechanisms: EXTERNAL
|   supportedSASLMechanisms: DIGEST-MD5
|   supportedLDAPVersion: 3
|   supportedLDAPVersion: 2
|   supportedLDAPPolicies: MaxPoolThreads
|   supportedLDAPPolicies: MaxPercentDirSyncRequests
|   supportedLDAPPolicies: MaxDatagramRecv
|   supportedLDAPPolicies: MaxReceiveBuffer
|   supportedLDAPPolicies: MaxPreAuthReceiveBuffer
|   supportedLDAPPolicies: InitRecvTimeout
|   supportedLDAPPolicies: MaxConnections
|   supportedLDAPPolicies: MaxConnIdleTime
|   supportedLDAPPolicies: MaxPageSize
|   supportedLDAPPolicies: MaxBatchReturnMessages
|   supportedLDAPPolicies: MaxQueryDuration
|   supportedLDAPPolicies: MaxDirSyncDuration
|   supportedLDAPPolicies: MaxTempTableSize
|   supportedLDAPPolicies: MaxResultSetSize
|   supportedLDAPPolicies: MinResultSets
|   supportedLDAPPolicies: MaxResultSetsPerConn
|   supportedLDAPPolicies: MaxNotificationPerConn
|   supportedLDAPPolicies: MaxValRange
|   supportedLDAPPolicies: MaxValRangeTransitive
|   supportedLDAPPolicies: ThreadMemoryLimit
|   supportedLDAPPolicies: SystemMemoryLimitPercent
|   supportedControl: 1.2.840.113556.1.4.319
|   supportedControl: 1.2.840.113556.1.4.801
|   supportedControl: 1.2.840.113556.1.4.473
|   supportedControl: 1.2.840.113556.1.4.528
|   supportedControl: 1.2.840.113556.1.4.417
|   supportedControl: 1.2.840.113556.1.4.619
|   supportedControl: 1.2.840.113556.1.4.841
|   supportedControl: 1.2.840.113556.1.4.529
|   supportedControl: 1.2.840.113556.1.4.805
|   supportedControl: 1.2.840.113556.1.4.521
|   supportedControl: 1.2.840.113556.1.4.970
|   supportedControl: 1.2.840.113556.1.4.1338
|   supportedControl: 1.2.840.113556.1.4.474
|   supportedControl: 1.2.840.113556.1.4.1339
|   supportedControl: 1.2.840.113556.1.4.1340
|   supportedControl: 1.2.840.113556.1.4.1413
|   supportedControl: 2.16.840.1.113730.3.4.9
|   supportedControl: 2.16.840.1.113730.3.4.10
|   supportedControl: 1.2.840.113556.1.4.1504
|   supportedControl: 1.2.840.113556.1.4.1852
|   supportedControl: 1.2.840.113556.1.4.802
|   supportedControl: 1.2.840.113556.1.4.1907
|   supportedControl: 1.2.840.113556.1.4.1948
|   supportedControl: 1.2.840.113556.1.4.1974
|   supportedControl: 1.2.840.113556.1.4.1341
```

```

| supportedControl: 1.2.840.113556.1.4.841
| supportedControl: 1.2.840.113556.1.4.529
| supportedControl: 1.2.840.113556.1.4.805
| supportedControl: 1.2.840.113556.1.4.521
| supportedControl: 1.2.840.113556.1.4.970
| supportedControl: 1.2.840.113556.1.4.1338
| supportedControl: 1.2.840.113556.1.4.474
| supportedControl: 1.2.840.113556.1.4.1339
| supportedControl: 1.2.840.113556.1.4.1340
| supportedControl: 1.2.840.113556.1.4.1413
| supportedControl: 2.16.840.1.113730.3.4.9
| supportedControl: 2.16.840.1.113730.3.4.10
| supportedControl: 1.2.840.113556.1.4.1504
| supportedControl: 1.2.840.113556.1.4.1852
| supportedControl: 1.2.840.113556.1.4.802
| supportedControl: 1.2.840.113556.1.4.1907
| supportedControl: 1.2.840.113556.1.4.1948
| supportedControl: 1.2.840.113556.1.4.1974
| supportedControl: 1.2.840.113556.1.4.1341
| supportedControl: 1.2.840.113556.1.4.2026
| supportedControl: 1.2.840.113556.1.4.2064
| supportedControl: 1.2.840.113556.1.4.2065
| supportedControl: 1.2.840.113556.1.4.2066
| supportedControl: 1.2.840.113556.1.4.2090
| supportedControl: 1.2.840.113556.1.4.2205
| supportedControl: 1.2.840.113556.1.4.2204
| supportedControl: 1.2.840.113556.1.4.2206
| supportedControl: 1.2.840.113556.1.4.2211
| supportedControl: 1.2.840.113556.1.4.2239
| supportedControl: 1.2.840.113556.1.4.2255
| supportedControl: 1.2.840.113556.1.4.2256
| supportedControl: 1.2.840.113556.1.4.2309
| supportedControl: 1.2.840.113556.1.4.2330
| supportedControl: 1.2.840.113556.1.4.2354
| supportedCapabilities: 1.2.840.113556.1.4.800
| supportedCapabilities: 1.2.840.113556.1.4.1670
| supportedCapabilities: 1.2.840.113556.1.4.1791
| supportedCapabilities: 1.2.840.113556.1.4.1935
| supportedCapabilities: 1.2.840.113556.1.4.2080
| supportedCapabilities: 1.2.840.113556.1.4.2237
| subschemaSubentry: CN=Aggregate,CN=Schema,CN=Configuration,DC=PUPPY,DC=HTB
| serverName: CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=PUPPY,DC=HTB
| schemaNamingContext: CN=Schema,CN=Configuration,DC=PUPPY,DC=HTB
| namingContexts: DC=PUPPY,DC=HTB
| namingContexts: CN=Configuration,DC=PUPPY,DC=HTB
| namingContexts: CN=Schema,CN=Configuration,DC=PUPPY,DC=HTB
| namingContexts: DC=DomainDnsZones,DC=PUPPY,DC=HTB
| namingContexts: DC=ForestDnsZones,DC=PUPPY,DC=HTB
| isSynchronized: TRUE
| highestCommittedUSN: 172273
| dsServiceName: CN=NTDS Settings,CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=PUPPY,DC=HTB
| dnsHostName: DC.PUPPY.HTB
| defaultNamingContext: DC=PUPPY,DC=HTB
| currentTime: 20250603071124.0Z
| configurationNamingContext: CN=Configuration,DC=PUPPY,DC=HTB
_
636/tcp open  ldapssl
Service Info: Host: DC; OS: Windows

Nmap done: 1 IP address (1 host up) scanned in 601.74 seconds

```

```

root@kali:~#

```

Výsledky NSE skriptov LDAP enumerácie opisujú:

→ Opäť potvrdili, že doménou cieľa je **PUPPY.HTB**

→ Server je **LDAP DC (Domain Controller)**

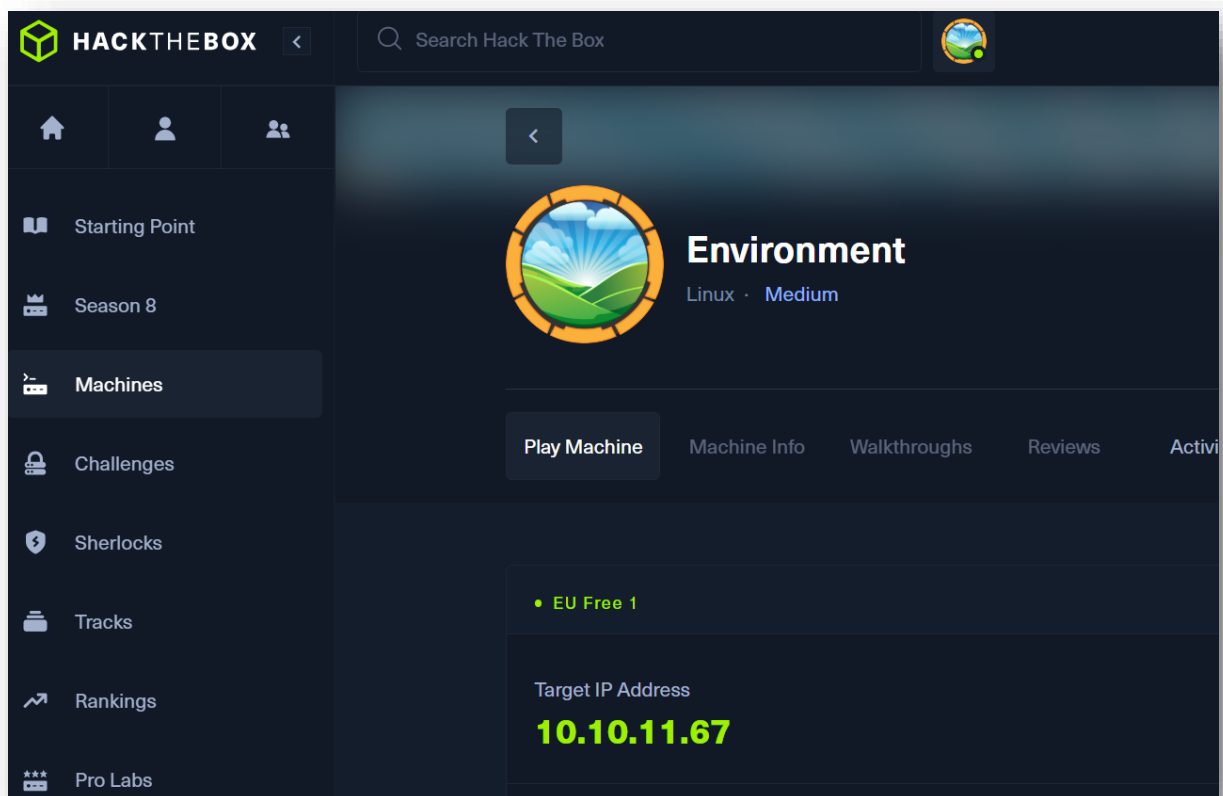
→ isGlobalCatalogReady: **TRUE**

→ Server je pripravený ako globálny katalóg

→ DNS Host Name: **DC.PUPPY.HTB**

→ OS: **Windows**

Prostredie: LINUX MACHINE (Stredne ťažký):



Cieľ → 10.10.11.67

Overenie, či je cieľ aktívny:

Príkaz:

ping -c 4 10.10.11.67

```
File Actions Edit View Help

(root@kali)-[~]
# ping -c 4 10.10.11.67
PING 10.10.11.67 (10.10.11.67) 56(84) bytes of data:
64 bytes from 10.10.11.67: icmp_seq=1 ttl=63 time=107 ms
64 bytes from 10.10.11.67: icmp_seq=2 ttl=63 time=105 ms
64 bytes from 10.10.11.67: icmp_seq=3 ttl=63 time=108 ms
64 bytes from 10.10.11.67: icmp_seq=4 ttl=63 time=100 ms
--- 10.10.11.67 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 100.406/105.264/108.091/3.025 ms
```

Výsledok vrátil, že služba beží, čiže môžeme prejsť na Linux enumerácie

Nmap Enumerácia + Port-Scanning

V tejto fáze zistíme, ktoré porty sú otvorené, aké služby na nich bežia, spustí preddefinované NSE skripty na zistenie SSH kľúčov a pod.

Príkaz:

nmap -sS -sV -T4 -p- 10.10.11.67

nmap -sC -sV -T4 -p 22, 80 10.10.11.67

```
(root@kali)-[~]
# nmap -sS -sV -Pn -T4 -p- 10.10.11.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-05 13:24 EDT
Warning: 10.10.11.67 giving up on port because retransmission cap hit (6).
Nmap scan report for environment.htb (10.10.11.67)
Host is up (0.030s latency).
Not shown: 65497 closed tcp ports (reset), 36 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
80/tcp    open  http     nginx 1.22.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 362.03 seconds

(root@kali)-[~]
# nmap -sC -sV -T4 -p 22,80 10.10.11.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-05 13:32 EDT
Nmap scan report for environment.htb (10.10.11.67)
Host is up (0.052s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u5 (protocol 2.0)
| ssh-hostkey:
|_  256 5c:02:33:95:ef:44:e2:80:cd:3a:96:02:23:f1:92:64 (ECDSA)
|_  256 1f:3d:c2:19:55:28:a1:77:59:51:48:10:c4:4b:74:ab (ED25519)
80/tcp    open  http     nginx 1.22.1
|_ http-title: Save the Environment | environment.htb
|_ http-server-header: nginx/1.22.1
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.63 seconds
```

Dostali sme **výsledky**, že:

→ **Port 22/TCP je otvorený (SSH):**

→ ktorý beží na OpenSSH 9.2p1

→ na systéme Debian s patchom 2+deb12u5

→ silný indikátor, že je to Debian 12

→ **Detaily o hostiteľských SSH kľúčov:**

→ ECDSA: 256 bit → 5c:02:.....:64

→ ED25519: 256 bit → 1f:3d:.....:ab

→ **Port 80/TCP je otvorený (HTTP):**

→ beží na Nginx 1.22.1 (Web Server)

→ Hlavička: Server: nginx/1.22.1

→ HTTP titulok stránky: Save the Environment

→ OS: **Windows**

→ Zvyšné porty sú buď **zatvorené** alebo **filtrované**

SSH Enumerácia (port 22):

Príkaz:

nmap -p22 --script=ssh2-enum-algos 10.10.11.67

→ Jedná sa o NSE skript pre enumeráciu kryptografických algoritmov, ktorý daný SSH server podporuje

→ Tento skript som použil na zistenie, ktoré šifrovacie algoritmy sú povolené na SSH serveri.

→ Overil som si, že server podporuje silné algoritmy ako curve25519 a chacha20, čo je z bezpečnostného pohľadu dobré.

```
(root@kali)-[~]
# nmap -p22 --script=ssh2-enum-algos 10.10.11.67
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-05 13:39 EDT
Nmap scan report for environment.htb (10.10.11.67)
Host is up (0.11s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
| ssh2-enum-algos:
|   kex_algorithms: (12)
|   | sntrup761x25519-sha512
|   | sntrup761x25519-sha512@openssh.com
|   | curve25519-sha256
|   | | curve25519-sha256@libssh.org
|   | ecdh-sha2-nistp256
|   | ecdh-sha2-nistp384
|   | ecdh-sha2-nistp521
|   | diffie-hellman-group-exchange-sha256
|   | diffie-hellman-group16-sha512
|   | diffie-hellman-group18-sha512
|   | | htrtrack diffie-hellman-group14-sha256
|   | kex-strict-s-v00@openssh.com
|   server_host_key_algorithms: (4)
|   | rsa-sha2-512
|   | | rsa-sha2-256
|   | ecdsa-sha2-nistp256
|   | ssh-ed25519
|   encryption_algorithms: (6)
|   | chacha20-poly1305@openssh.com
|   | aes128-ctr
|   | aes192-ctr
|   | aes256-ctr
|   | aes128-gcm@openssh.com
|   | aes256-gcm@openssh.com
|   mac_algorithms: (10)
|   | umac-64-etm@openssh.com
|   | umac-128-etm@openssh.com
|   | hmac-sha2-256-etm@openssh.com
|   | hmac-sha2-512-etm@openssh.com
|   | hmac-sha1-etm@openssh.com
|   | umac-64@openssh.com
|   | umac-128@openssh.com
|   | hmac-sha2-256
|   | hmac-sha2-512
|   | hmac-sha1
|   compression_algorithms: (2)
|   | none
|   | zlib@openssh.com
|_

Nmap done: 1 IP address (1 host up) scanned in 0.58 seconds
```

Výsledky:

Kryptografické algoritmy, ktoré sú serverom podporované:

1. `kex_algorithms` (výmenné algoritmy):

→ Používajú sa na bezpečnú dohodu kľúčov medzi klientom a serverom

→ napr. `curve25519-sha256`; `diffie-hellman-group14-sha256`

2. `server_host_key_algorithm` (kľúče servera):

→ Sú to algoritmy, ktorými sa server autentifikuje klientovi

→ napr. `rsa-sha2-512`, `ssh-ed25519`

3. `encryption_algorithms` (symetrické šifry):

→ Používajú sa na zašifrovanie dát

→ typický `AES` je bežný a rýchly

→ napr. `chacha20`, `aes256-ctr`

4. `mac_algorithms` (Message Authentication Code (MAC)):

→ Používajú sa na integritu (napr. že správa nebola zmenená):

→ `etm` = `Encrypt-Then-Mac`, bezpečnejšia než `MAC-Then-Crypt`

→ napr. `hmac-sha2-512-etm@openssh.com`, `umac-128-etm@openssh.com`

5. `compression_algorithms` (kompresia dát):

→ `none`: bez kompresie

→ napr. `zlib@openssh.com`

Tento skript som použil na zistenie, ktoré šifrovacie algoritmy sú povolené na SSH serveri.

Overil som si, že server podporuje silné algoritmy ako curve25519 a chacha20, čo je z bezpečnostného pohľadu dobré.

Zneužitie týchto algoritmov:

Ak by sa vo výsledkoch nachádzal nejaký zastaralý kľúč, ako napr. **rsa-sha1**, útočník by mohol použiť **tzv. kolízny útok**, teda kópiu správy s legitímnym podpisom

Web Server Enumerácia:

V tejto fáze som použil 3 nástroje, curl, nikto & whatweb, na detekciu konfigurácie, funkcionality a potenciálnych zraniteľností webového servera.

Príkaz:

curl -I 10.10.11.67

→ získa iba HTTP hlavičky odpovede pomocou -I:

```
(root@kali)~[~]
# curl -I 10.10.11.67
HTTP/1.1 301 Moved Permanently
Server: nginx/1.22.1
Date: Thu, 05 Jun 2025 17:48:45 GMT
Content-Type: text/html
Content-Length: 169
Connection: keep-alive
Location: http://environment.htb

(root@kali)~[~]
# echo "10.10.11.67 environment.htb" >> /etc/hosts
```

Výsledok príkazu:

→ Server odpovedá presmerovaním (301) na doménu <http://environment.htb>

Následne som túto doménu zapísal do systému, aby som si zľahčil a mohol ju používať ako URL namiesto IP adresy pomocou príkazu echo:

echo "10.10.11.67 environment.htb" >> /etc/hosts

WHATWEB → Zistíme, aké technológie bežia na stránke:

Príkaz:

whatweb <http://environment.htb>

```
(root@kali)~[~]
$ whatweb http://environment.htb
http://environment.htb [200 OK] Cookies[XSRF-TOKEN,laravel_session], Country[RESERVED][ZZ], HTML5, HTTPServer[nginx/1.22.1], HttpOnly[laravel_session], IP[10.10.11.67],
Laravel, Script, Title[Save the Environment | environment.htb], UncommonHeaders[x-content-type-options], X-Frame-Options[SAMEORIGIN], nginx[1.22.1]
```

Výsledok WHATWEB:

- Cookies: **XSRF-TOKEN, laravel_session**
- HTTPServer: **nginx 1.22.1**
- Laravel
- HTML5
- IP: **10.10.11.67**
- Title: **Save the Environment**
- Základné bezpeč.hlavičky: **X-Frame-Options, X-Content-Type-Options**

Význam výsledku:

- **Laravel využívanie:** PHP framework, ktorý býva často zraniteľný v .env súboroch, alebo v nesprávnych súborových oprávneniach
- **Obsahuje cookies:** laravel_session, XSRF-TOKEN, čo potvrdilo **LARAVEL BACKEND**
- Server je **nginx 1.22.1**

```
(root@kali)-[~]
```


Výsledky detailnej analýzy whatwebu:

- Status: **200 OK** (server odpovedal úspešne)
- IP adresa cieľa: **10.10.11.67**
- Web Server: **Nginx 1.22.1**
- Framework: **Laravel (PHP framework)**
- Cookies: **laravel_session, XSRF_TOKEN** (štandardné Laravel cookies)
- HttpOnly: **Áno** → cookies sa nedá čítať cez JS
- X-Frame-Options: **SAMEORIGIN** → ochrana proti clickjacking útokom
- X-Content-Type-Options: **nosniff** → zabraňuje sniffing útokom
- HTML5, Script: **stránka používa HTML5 a JavaScript**

Zneužiteľnosť z pozície útočníka:

1. **Laravel:** Je známy tým, že obsahuje širokú škálu zraniteľností, ktoré sú kritické, najmä ak sú v debug móde. Hacker tak môže hľadať .env súbor, ktorý často obsahuje kritické dáta
2. **Cookies:** laravel_session & XSRF-TOKEN naznačujú, že sa používa CSRF ochrana, ale útočník stále môže testovať, či je zle implementovaná
3. **Nginx 1.22.1:** veľmi ľahko sa dá overiť, či existujú zraniteľnosti na túto verziu web.servera (cez CVE databázu)
4. **HTTP hlavičky:** Sú pomerne **dobré nastavené**, ktoré chránia proti **clickjacking** či **sniffing útokom**, ale nie sú totálnou ochranou, ak útočník ich obíde skrze vykreslenia obsahu v inej doméne pomocou **PROXY**

NIKTO → Scanner známych web.zraniteľností:

Príkaz:

nikto -h http://environment.htb

```
(root@kali)-[~]
└─$ nikto -h http://environment.htb
- Nikto v2.5.0

+ Target IP: 10.10.11.67
+ Target Hostname: environment.htb
+ Target Port: 80
+ Start Time: 2025-06-05 13:50:02 (GMT-4)

+ Server: nginx/1.22.1
+ /: Cookie XSRF-TOKEN created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /5jYrpeNE.svc: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /login/: This might be interesting.
+ /api/soap/?wsdl=1: Retrieved access-control-allow-origin header: *.
+ 7962 requests: 0 error(s) and 4 item(s) reported on remote host
+ End Time: 2025-06-05 13:56:07 (GMT-4) (365 seconds)

+ 1 host(s) tested
```

Výsledky:

1. **Cookies: XSRF-TOKEN vytvorený bez HttpOnly** → možný **JavaScript injection**
2. **X-Content-Type-Options header chýba** → môže viesť k **sniffing útoku**, kedy prehliadač **interpretuje obsah nesprávne** (napr. JS ako HTML5)
3. **Zaujímavé zistenia:**

/login → login formulár, ktorý je dôležitý pre Brute-Force útok (napr. získavanie hesiel)

/api/soap/?wsdl=1 → **SOAP endpoint** (Web Server Definition Language)

→ tento endpoint môže byť **zraniteľný** skrze **RCE (Remote Code Execution)** alebo **autentifikačný bypass**

Gobuster (Brute-Force) → Vyhľadávanie skrytých a nezabezpečených častiach web.infraštruktúry:

Príkaz:

```
gobuster dir -u http://environment.htb -w /usr/share/wordlists/dirb/common.txt
```

→ **dir** : Disturbing režim (enumeruje adresáre a súbory)

→ **-u** : URL cieľa

→ **-w** : wordlist, ktorý sa použil (v tomto prípade common.txt)

```
(root@kali)~# gobuster dir -u http://environment.htb -w /usr/share/wordlists/dirb/common.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://environment.htb
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

./bash_history (Status: 403) [Size: 153]
./cvsignore (Status: 403) [Size: 153]
./history (Status: 403) [Size: 153]
./hta (Status: 403) [Size: 153]
./htaccess (Status: 403) [Size: 153]
./forward (Status: 403) [Size: 153]
./config (Status: 403) [Size: 153]
./git/HEAD (Status: 403) [Size: 153]
./bashrc (Status: 403) [Size: 153]
./cache (Status: 403) [Size: 153]
./cvs (Status: 403) [Size: 153]
./htpasswd (Status: 403) [Size: 153]
./listing (Status: 403) [Size: 153]
./sh_history (Status: 403) [Size: 153]
./rhosts (Status: 403) [Size: 153]
./ssh (Status: 403) [Size: 153]
./profile (Status: 403) [Size: 153]
./passwd (Status: 403) [Size: 153]
./perf (Status: 403) [Size: 153]
./mysql_history (Status: 403) [Size: 153]
./listings (Status: 403) [Size: 153]
./subversion (Status: 403) [Size: 153]
./swf (Status: 403) [Size: 153]
./web (Status: 403) [Size: 153]
./svn/entries (Status: 403) [Size: 153]
./svn (Status: 403) [Size: 153]
/build (Status: 301) [Size: 169] [→ http://environment.htb/build/]
/favicon.ico (Status: 200) [Size: 0]
/index.php (Status: 200) [Size: 4602]
/login (Status: 200) [Size: 2391]
/logout (Status: 302) [Size: 358] [→ http://environment.htb/login]
/mailling (Status: 405) [Size: 244854]
/robots.txt (Status: 200) [Size: 24]
/storage (Status: 301) [Size: 169] [→ http://environment.htb/storage/]
/up (Status: 200) [Size: 2126]
/upload (Status: 405) [Size: 244852]
/vendor (Status: 301) [Size: 169] [→ http://environment.htb/vendor/]
Progress: 4614 / 4615 (99.98%)

Finished
```

Výsledky rozdelené podľa HTTP status kódu:

403 Forbidden (väčšina výsledkov):

→ Znamená, že súbory a adresáre existujú, ale moja požiadavka nemá povolenie ho zobrazit'

Napr.

`.bash_history`

`.git/HEAD`

`.htaccess`

`.htpasswd`

`.mysql_history`

301 Moved Permanently:

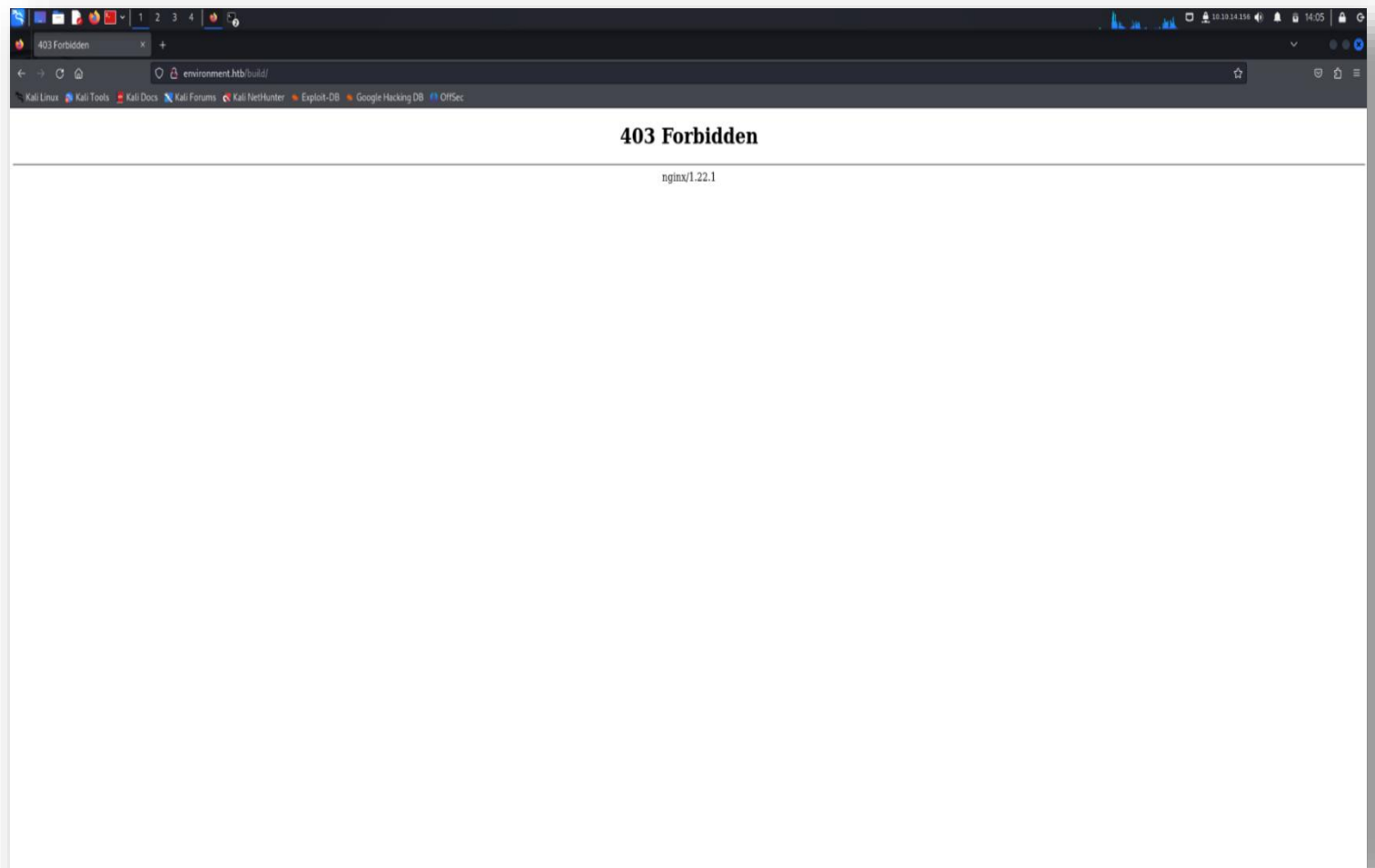
→ Znamená, že existuje funkčný adresár, ktorý presmerováva

Napr.

[/build/](#)

[/storage/](#)

[/vendor/](#)



→ Overuje sa ich často cez manuálne prehľadávanie

→ niekedy môžu obsahovať konfigurácie, logy, testovacie PHP súbory

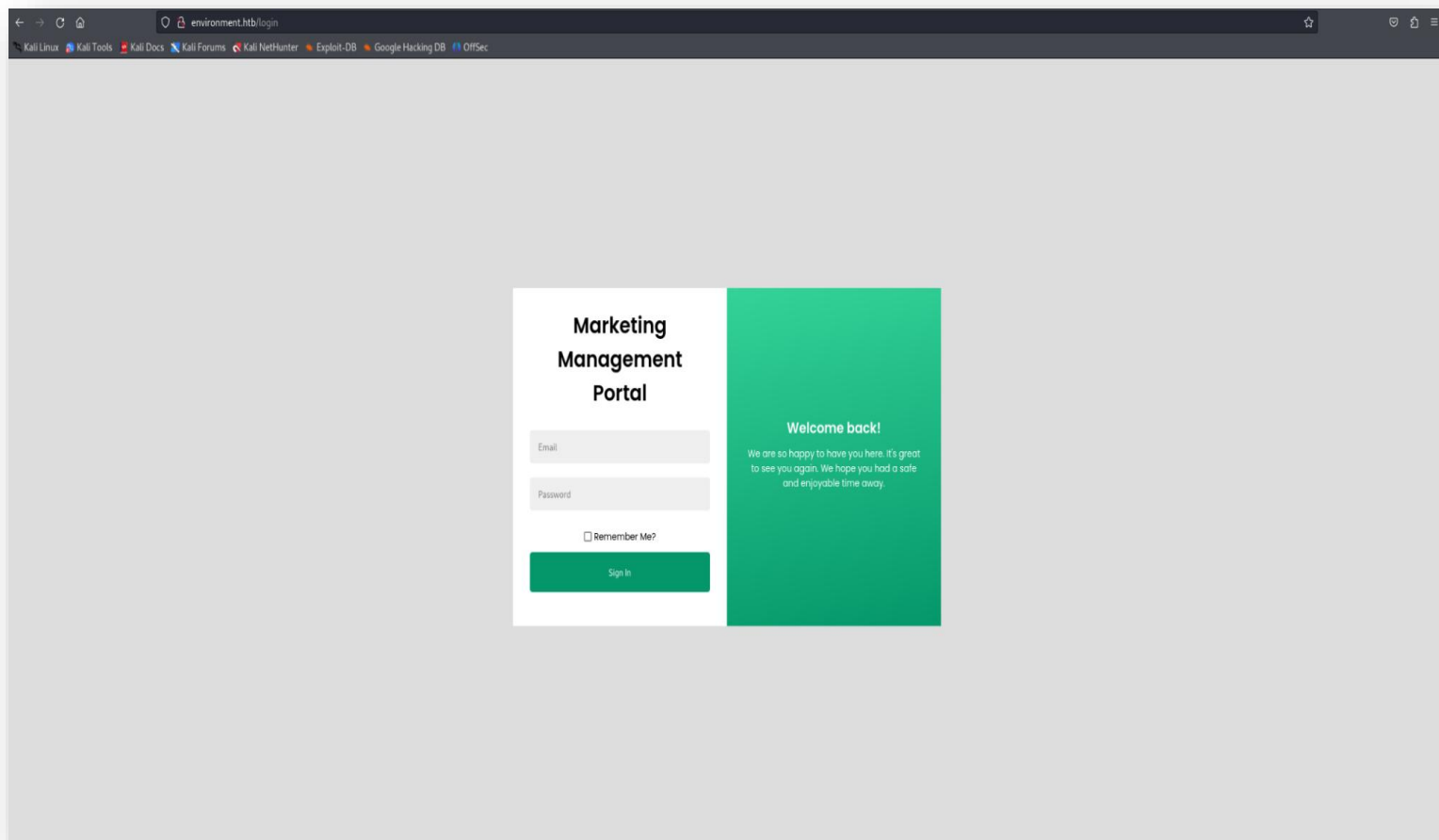
200 OK:

→ Znamená, že súbor alebo adresár je verejne dostupný a vrátil normálnu odpoveď

Napr.

[/index.php](#)

[/login](#)



[/login](#) → cieľ pre Brute-Force; autentifikačný bypass

[/index.php](#) → vstupný bod aplikácie, užitočný pre zistenie frameworkov

302 Found (presmerovanie):

Napr.

[/logout](#)

405 Method Not Allowed:

→ Existuje, ale nepodporuje metódu GET

Napr.

[/upload](#)

[/mailing](#)

HTTP metadáta (Web Server Enumerácia):

Príkaz:

```
nmap -p 80 --script=http-methods, http-headers, http-enum, http-title,  
http-server-header, http-php-version 10.10.11.67
```

→ Tento príkaz spustí NSE skriptovanie na HTTP port 80 cieľa 10.10.11.67, pričom skripty sa zamerajú na:

1. **http-methods** → zisťuje podporované HTTP metódy (napr. GET, POST, DELETE, PUT...)
2. **http-headers** → zobrazí HTTP hlavičky odpovede
3. **http-enum** → enumeruje známe URL cesty (napr. robots.txt, /admin, /login)
4. **http-title** → zisťuje titulok HTML stránky
5. **http-server-header** → extrahuje Server: hlavičku (napr. nginx/1.22.1)
6. **http-php-version** → Pokus o zistenie verzie PHP

Výsledky tohto **NSE skriptovania** na HTTP port 80:

1. Port 80/TCP (HTTP služba) je otvorený

- Podporované metódy: GET, HEAD
- Nezistil PUT alebo DELETE, čo by boli potenciálne zraniteľnostné metódy

2. HTTP hlavičky:

- Server: **nginx/1.22.1**: verzia web.servera
- Set-Cookie: **Laravel framework používa cookies ako:**
 - **XSRF-TOKEN**
 - **laravel_session**
- X-Frame-Options: **SAMEORIGIN**: **zabraňuje „clickjacking“**
útokom
- X-Content-Type-Options: **nosniff**: **znižuje riziko sniffing**
útokov
- Content-Encoding: **gzip** → **kompresia**

3. Enumerované cesty:

- **/login**: možnosť **Brute-Force**
- **/robots.txt**: môže **obsahovať cesty**, ktoré si **admin neželá, aby boli prehľadávané**

4. Titulok stránky: Save the Environment (pravdepodobne názov projektu)

Zneužitie týchto výsledkov z pozície útočníka:

1. **Nginx 1.22.1** → vyhľadávanie zraniteľností (CVE) na túto verziu servera
2. **Laravel Cookies** → Známe zraniteľností (napr. **RCE** pri nesprávnej konfigurácii .env súbora)
3. **/login** → Možnosť **Brute-Force** útoku pre získanie hesiel či SQL injection
4. **X-Frame-Options; X-Content-Type-Options** → Ak by boli povolené riskantné metódy ako **PUT & DELETE**, bolo by možné zmeniť obsah, vložiť shell atď.

Záver:

V tomto dokumente som zdokumentoval celý proces enumerácie cieľa z pohľadu útočníka, pričom som využil rôzne nástroje a techniky zamerané na Windows aj Linux systémy.

Postupoval som od sieťového skenovania cez Nmap, cez aktívnu enumeráciu protokolov ako SMB, RPC, LDAP či HTTP, až po využitie nástrojov ako enum4linux-ng, rpcclient, whatweb, gobuster a ffuf.

Každý výstup bol analyzovaný z hľadiska potenciálneho zneužitia, teda ako by daná informácia mohla pomôcť útočníkovi v ďalších fázach útoku, ako je privilege escalation, credential harvesting alebo priamy prienik do systému.

Dôležité poznatky z tejto fázy:

Aj „neškodné“ informácie ako verzia servera, session cookie alebo názov frameworku môžu byť kľúčom k zneužitiu zraniteľností.

Ak je služba správne zabezpečená (napr. SMB signing enabled), útočnické možnosti sa výrazne obmedzujú.

Neúspešné výstupy sú rovnako dôležité → signalizujú ochrany alebo uzavreté vektory, ktoré treba obísť inak.

Enumerácia nie je len fáza pred útokom pretože je to samotný základ, bez ktorého nie je možné vykonať cielený a efektívny exploit. Tento proces zároveň prehľbuje schopnosť myslieť ako útočník a rozpoznávať slabé miesta v infraštruktúre.