

Windows Insecurity Penetrated v0.11 – Outline

1 Introduction

2 Enumerating the Target

- 2.1 Ping Scans (Ping Sweeps)
- 2.2 TCP Ping Scans (TCP Ping Sweeps)
- 2.3 List Scans
- 2.4 Port Scanning
 - 2.4.1 TCP Connect Port Scan
 - 2.4.2 SYN Stealth Port Scan (Half Open Scan)
 - 2.4.3 UDP Port Scan
 - 2.4.4 Decoy Port Scan
 - 2.4.5 Version Port Scan
- 2.5 Banner Grabbing
- 2.6 OS Fingerprinting
 - 2.6.1 Active OS Fingerprinting
 - 2.6.2 Passive OS Fingerprinting
- 2.7 Vulnerability Scanning
 - 2.7.1 Manual Vulnerability Scanning
 - 2.7.2 Automatic Vulnerability Scanning

3 Exploiting Services

- 3.1 SMB/Netbios
 - 3.1.1 Description of Service
 - 3.1.2 Vulnerability Information
 - 3.1.3 Description of the Vulnerability
 - 3.1.4 Exploit Demonstration
 - 3.1.5 How to Close the Hole
- 3.2 SNMP
 - 3.2.1 Description of Service
 - 3.2.2 Vulnerability Information
 - 3.2.3 Description of the Vulnerability
 - 3.2.4 Exploit Demonstration
 - 3.2.5 How to Close the Hole
- 3.3 MSRPC
 - 3.3.1 Description of Service
 - 3.3.2 Vulnerability Information
 - 3.3.3 Description of the Vulnerability
 - 3.3.4 Exploit Demonstration
 - 3.3.5 How to Close the Hole
- 3.4 IIS Webserver
 - 3.4.1 Description of Service
 - 3.4.2 Vulnerability Information
 - 3.4.3 Description of the Vulnerability
 - 3.4.4 Exploit Demonstration
 - 3.4.5 How to Close the Hole

4 Password Cracking

- 4.1 Grabbing Password Hashes from SAM
 - 4.1.1 Obtaining Local Administrative Privileges from Local Host's SAM file
 - 4.1.2 Obtaining Network Administrative Privileges from the Domain Controller's SAM file
 - 4.1.3 How it is done
- 4.2 Sniffing Passwords
- 4.3 Keylogging Passwords
 - 4.3.1 Software Keyloggers
 - 4.3.2 Hardware Keyloggers

5 Covering Tracks

- 5.1 Clearing Logs
- 5.2 Hiding Files

6 Keeping Covert Access: Backdoors

- 6.1 Listening backdoors
- 6.2 Shoveling backdoors (reverse backdoors)

7 Conclusion

8. Credits

9. GNU Free Documentation License

10.References

Appendix A: Vulnerability Databases

Appendix B: Common Ports Used by Windows

Appendix C: Tools Used and Mentioned in this Project