Erfolg/DOKU Aufklärung mit Legion

> **Ziel-VM:** `10.0.0.2` | **Scanner Tool:** Legion (Nmap/Nikto Frontend) | **Artefakt:** `findings.json`

1. Zielsetzung

Bevor irgendein Exploit ausprobiert wurde, sollte eine vollständige Aufklärung der Ziel-VM (`10.0.0.2`) durchgeführt werden. Ziel war es festzustellen, welche Ports offen sind, welche Dienste dahinterstecken, welches Betriebssystem eingesetzt wird und ob bekannte Schwachstellen vorliegen.

Eine vollständige Übersicht über die Angriffsfläche dient als Entscheidungsgrundlage, um festzulegen, welche Angriffsvektoren sinnvoll sind und welche verworfen werden können.

Erfolgskriterien

- [x] Alle offenen Ports und aktiven Dienste identifizieren
- [x] Betriebssystem und genaue Versionen bestimmen
- [x] Verdächtige Versionsstände identifizieren, die auf bekannte CVEs hindeuten
- [x] Testergebnisse exportieren (`findings.json`) und als Dokumentationsnachweis sichern

2. Vorgehen

Schritt 1: Legion starten

Legion ist ein grafisches Werkzeug auf Kali Linux, welches im Hintergrund automatisierte Scans über Werkzeuge wie Nmap oder Nikto ausführt. Nach Eingabe der Ziel-IP liefert das Tool eine strukturierte Übersicht der identifizierten Ports, Dienste und potenziellen Findings.

- **Startpfad:** `Kali-Menü` ? `01 - Information Gathering` ? `Legion`

Konfiguration:

- **Target:** `10.0.0.2`
- **Scan-Modus:** Standard (Quick Scan mit Service Detection)

- **Aktion:** Auswahl bestätigen („Submit“)

Schritt 2: Scan-Ablauf

Legion hat im Hintergrund automatisch folgende Analysephasen durchlaufen:

1. **Host Discovery:** Prüfung der Erreichbarkeit der Ziel-IP
2. **Port-Scan:** TCP-Portscan zur Feststellung offener Ports
3. **Service Detection:** Identifikation der Dienste und Versionsbestimmung pro Port
4. **OS-Fingerprinting:** Analyse der TCP/IP-Stack-Eigenschaften zur Betriebssystembestimmung
5. **Vulners-Plugin:** Automatischer Abgleich der erkannten Versionsstände mit bekannten CVE-Datenbanken

Schritt 3: Analyse der Ports & Dienste

Für die Zieladresse `10.0.0.2` wurden insgesamt **20 offene Ports** identifiziert:

Port	Dienst	Produkt / Version
21	ftp	Microsoft ftpd
22	ssh	OpenSSH 7.1
80	http	Microsoft IIS httpd 7.5
135	msrpc	Microsoft Windows RPC
139	netbios-ssn	Microsoft Windows netbios-ssn
445	microsoft-ds	Windows Server 2008 R2
3306	mysql	MySQL 5.5.20-log
3389	ms-wbt-server	RDP
4848	http	Oracle GlassFish Application Server
5985	http	Microsoft HTTPAPI httpd 2.0
7676	java-message-service	Java Message Service 301
8009	ajp13	Apache Jserv Protocol v1.3
8080	http	Oracle GlassFish (Servlet 3.1)
8181	intermapper	–
8383	http	Apache httpd
9200	http	Elasticsearch REST API 1.1.1
49152–49155	msrpc	Microsoft Windows RPC

Schritt 4: OS-Fingerprinting

Die automatisierte Systemerkennung von Legion lieferte folgendes Ergebnis:

Plaintext

```
OS Match: Microsoft Windows Vista SP2 / Windows 7 / Windows Server 2008 R2 / Windows 8.1
OS Accuracy: 100
```

> [!NOTE]
> **Betriebssystem-Bestätigung:**
> Die Einschätzung deckt sich mit dem Zielsystem: Es handelt sich um einen **Windows Server 2008 R2**.

Schritt 5: Identifikation verdächtiger Findings

Bei der Durchsicht der Treffer fielen mehrere veraltete Versionsstände und potenzielle Schwachstellen auf:

- **Port 445 (SMB):** Windows Server 2008 R2 ohne aktuellen Patchstand ist ein primärer Kandidat für MS17-010 (EternalBlue).
- **Port 9200 (Elasticsearch 1.1.1):** Veraltete Version, anfällig für RCE ohne Authentifizierung (CVE-2014-3120).
- **Port 3306 (MySQL 5.5.20):** Häufige Schwachstelle durch unzureichend gesicherte oder leere Standard-Passwörter.
- **Port 4848 / 8080 (GlassFish):** Mögliche Angriffsfläche über Standard-Administrator-Zugangsdaten.
- **Port 21 (FTP):** Microsoft ftpd; zu prüfen auf zugelassenen anonymen Zugriff (Anonymous Login).

Schritt 6: Datenexport (`findings.json`)

Die von Legion generierte Exportdatei `findings.json` wurde gesichert und in die Systemdokumentation übernommen, um die Rohdaten des Scans als Nachweis bereitzuhalten.

3. Zusammenfassung der Ergebnisse

Kategorie	Befund
Offene Ports	20 Ports identifiziert
Betriebssystem	Windows Server 2008 R2
Kritische Dienste	SMB (445), Elasticsearch (9200), MySQL (3306), GlassFish (4848/8080)
Vermutete Schwachstellen	EternalBlue (MS17-010), Elasticsearch RCE (CVE-2014-3120), Schwache DB-Logins
Datenbasis	Exportiert in `findings.json`

Auf Basis dieser Ergebnisse wurden die nachfolgenden Schritte geplant. Aufgrund des alten Windows-Builds auf Port 445 war **EternalBlue** der primäre Zielvektor. **Elasticsearch** (Port 9200) stellte aufgrund des veralteten Softwarestandes den sekundären Testvektor dar.

4. Fazit & Learnings

> [!TIP]
> **Key Takeaway:**
> Aufklärung bildet die notwendige Grundlage für jede weitere Analyse. Ohne eine strukturierte Erfassung der Port- und Dienstlandschaft bleiben wesentliche Angriffsflächen unentdeckt.

- **Nutzen von Automatisierung:** Legion fasst Standard-Werkzeuge zusammen und liefert schnell eine übersichtliche Grafikauswertung, ohne dass jeder Scan-Befehl manuell eingegeben werden muss.
- **Bedeutung von Versionsständen:** Veraltete Versionen (z. B. Elasticsearch 1.1.1, MySQL 5.5.20, IIS 7.5) weisen verlässlich auf das Vorhandensein bekannter CVEs hin.
- **Dokumentation:** Die Nutzung struktureller Exporte wie `findings.json` ermöglicht eine lückenlose Nachvollziehbarkeit der gesammelten Rohdaten.

Revision #1
Created 29 September 2026 08:21:16 by Admin
Updated 29 September 2026 08:25:05 by Admin