HomeLab Security Project

Offensive & Defensive Security mit BSI-Grundschutz-Mapping

André-Michele Joannou | michelejoannou.work | LinkedIn | michele.joannou@web.de

Projektziel

Eigenständiger Aufbau einer IT-Security-Laborumgebung mit Enterprise-Hardware. 8 Angriffstechniken durchgeführt (MITRE ATT&CK), mit Wazuh SIEM erkannt und jeweils einer konkreten BSI-Grundschutz-Maßnahme zugeordnet. Das Projekt demonstriert: **Offensive Security** (Angriffe verstehen), **Detection Engineering** (Angriffe erkennen) und die **Compliance-Brücke** (Schutzmaßnahmen ableiten).

Dokumentierte Angriffstechniken → BSI-Maßnahmen

Angriff	MITRE	BSI-Maßnahme	Schutzmaßnahme
Kerberoasting	T1558.003	ORP.4.A22	Passwortqualität Service Accounts
AS-REP Roasting	T1558.004	APP.2.2.A9	Schutz der Authentisierung im AD
LLMNR Poisoning	T1557.001	APP.2.2.A10	Sicherer DNS-Einsatz im AD
Scheduled Task	T1053.005	NET.1.1.A4	Netztrennung in Zonen
DCSync	T1003.006	ORP.4.A2	Einrichtung/Entzug von Berechtigungen
Golden Ticket	T1558.001	APP.2.2.A15	Trennung Admin-/Produktionsumgebung
WMI Execution	T1047	SYS.2.2.3.A18	Einschränkung Remoteunterstützung
Account Discovery	T1087	OPS.1.1.5.A3	Konfiguration der Protokollierung

Alle BSI-Referenzen verifiziert gegen BSI IT-Grundschutz Kompendium Edition 2023.

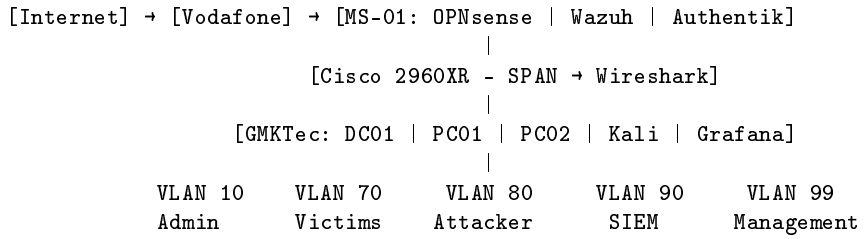
Infrastruktur

Hardware & Netzwerk:

- Proxmox HA-Cluster (2 Nodes + QDevice)
- OPNsense Firewall mit Suricata IDS
- Windows Active Directory (DC + 2 Clients)
- 10 VLANs auf Cisco Catalyst 2960XR
- SPAN/Port-Mirroring für Wireshark

Security Stack:

- Wazuh SIEM mit 5 Custom Detection Rules
- Wireshark (Traffic-Analyse via SPAN)
- Authentik SSO/IAM (OIDC, 2FA)
- Grafana + Prometheus Monitoring
- Cloudflare Tunnel + 2FA



Komplette Kill Chain (8 MITRE ATT&CK Techniken)

```
LLMNR Poisoning (T1557.001) → NTLMv2-Hash ohne User-Interaktion
        ↓
AS-REP Roasting (T1558.004) → tom.jones Credentials
        ↓
Kerberoasting (T1558.003) → svc_sql Service Account
        ↓
BloodHound (T1087) → Attack Path: GenericAll auf Domain Admin
        ↓
Targeted Kerberoasting → Domain Admin Credentials
        ↓
Lateral Movement / atexec (T1053.005) → SYSTEM auf PC01 + PC02
        ↓
DCSync (T1003.006) → Alle Domain-Hashes inkl. krbtgt
        ↓
Golden Ticket (T1558.001) → Persistenter Zugriff ohne Passwort
        ↓
WMI Shell (T1047) → Neuer Domain Admin (Detection umgangen → neue Rule)
```

Detection Engineering — 5 Custom Wazuh Rules

Rule	Level	Event ID	MITRE	Detection-Logik
100100	12	4769	T1558.003	RC4-Encryption bei TGS-Request
100101	10	4768	T1558.004	PreAuth-Type = 0
100102	12	4698	T1053.005	Remote Scheduled Task Creation
100103	14	4662	T1003.006	DS-Replication GUIDs
100104	12	4688	T1047	Parent Process = wmiprvse.exe

Jede Rule erkennt ein spezifisches Verhaltensmuster (IOC). Wechselt der Angreifer das Tool, wird eine neue Rule nötig — Detection ist iterativ.

Demonstrierte Kompetenzen

Red Team

- AD Pentesting
- Password Cracking
- Lateral Movement
- Network Attacks
- Domain Compromise

Blue Team

- SIEM (Wazuh)
- Detection Engineering
- Network Forensics
- Adaptive Defense
- Monitoring

Compliance-Brücke

- BSI Grundschutz
- MITRE ATT&CK
- Risikobewertung
- Maßnahmenableitung
- Dokumentation

Lessons Learned

- **Adaptive Defense:** *"Als ich von atexec auf wmiexec wechselte, war ich wieder unsichtbar. Eine Detection Rule reicht nie — Angreifer und Verteidiger spielen dasselbe Spiel."*
- **Detection Engineering:** *"Wazuh ist ein Framework, keine fertige Lösung. Custom Rules sind essentiell. Und selbst die müssen ständig erweitert werden — weil jedes Tool einen anderen Fingerprint hinterlässt."*
- **BSI als Brücke:** *"Jeder erfolgreiche Angriff macht eine fehlende Schutzmaßnahme sichtbar. BSI Grundschutz liefert die Sprache, um technische Schwachstellen in konkrete Maßnahmen zu übersetzen."*
- **Kill Chain:** *"Einzelne Schwachstellen sind allein nicht kritisch — aber in Kombination führen sie zum vollständigen Domain Compromise. Deshalb braucht Sicherheit Tiefe, nicht nur Einzelmaßnahmen."*

Projektverlauf

Phase	Zeitraum	Schwerpunkt
1–3	Dez 2025 – Jan 2026	Infrastruktur: Proxmox-Cluster, OPNsense, VLANs, Wazuh SIEM
4	Jan 2026	Kerberoasting, AS-REP Roasting, BloodHound, Domain Compromise
5	Jan/Feb 2026	LLMNR Poisoning, Lateral Movement (atexec), Wireshark SPAN
6	Feb 2026	DCSync, Golden Ticket, WMI, Detection Rules 100103–100104
7	Feb 2026	Dokumentation, Portfolio-Website, LinkedIn-Serie (9 Posts)

Ansatz: Jeder Angriff wird dokumentiert, erkannt und einer konkreten BSI-Grundschutz-Maßnahme zugeordnet. Angriffe verstehen ist das Werkzeug — Unternehmen systematisch schützen ist das Ziel.

Vollständige Dokumentation: michelejoannou.work