Reconnaissance Phase Report

Übersicht der erkannten Systeme

IP-Adresse	Hostname	Dienste (Ports)	Anmerkungen
192.168.20.10	kingslanding.sevenkingdoms.local (KINGSLANDING)	DNS (53), HTTP (80), Kerberos (88), RPC (135), NetBIOS (139), LDAP (389, 636, 3268, 3269), SMB (445), RDP (3389)	Active Directory Domänencontroller der Domäne `sevenkingdoms.local`. Microsoft-IIS, TLS für LDAP/RDP.
192.168.20.11	winterfell.north.sevenkingdoms.local (WINTERFELL)	DNS (53), Kerberos (88), RPC (135), NetBIOS (139), LDAP (389, 636, 3268, 3269), SMB (445), RDP (3389)	Zweiter Domänencontroller für Subdomäne `north.sevenkingdoms.local`.
192.168.20.12	meereen.essos.local (MEEREEN)	DNS (53), Kerberos (88), RPC (135), NetBIOS (139), LDAP (389, 636, 3268, 3269), SMB (445), RDP (3389)	Domänencontroller `essos.local`. SMB-Nachrichten-signierung erforderlich.
192.168.20.13	–	keine offenen Ports	möglicherweise Offline oder Filter

IP-Adresse	Hostname	Dienste (Ports)	Anmerkungen
192.168.20.14–21	–	alle gefiltert	keine Rückmeldung
192.168.20.22	castelblack.north.sevenkingdoms.local	HTTP (80), RPC (135), NetBIOS (139), SMB (445), SQL Server (1433), RDP (3389)	SQL Server 2019, Self-Signed TLS, SMB-Signierung nicht erforderlich.
192.168.20.23	braavos.essos.local (BRAAVOS)	HTTP (80), RPC (135), NetBIOS (139), SMB (445), SQL Server (1433), RDP (3389)	SQL Server 2019, Self-Signed TLS, SMB-Signierung deaktiviert (unsicher).

Erkenntnisse

- **Active Directory Infrastruktur**: Drei Domänencontroller in separaten Domains/Subdomains (`sevenkingdoms.local`, `north.sevenkingdoms.local`, `essos.local`) mit LDAP- und Kerberos-Diensten auf Standardports.
- **Webserver**: Microsoft IIS auf Port 80 mit TRACE-Methode aktiv, potentiell risikoreich.
- **Datenbanken**: Zwei Instanzen von Microsoft SQL Server 2019 (1433) mit selbst-signierten Zertifikaten.
- **SMB-Signierung**: Variiert zwischen Hosts:
  - Erforderlich und aktiviert auf MEEREEN.
  - Nicht erforderlich oder deaktiviert auf CASTLEBLACK und BRAAVOS.
- **Filter und Firewall**: Mehrere IPs zeigen vollständig gefilterte Ports (192.168.20.14–21), was auf Netzwerksegmentierung oder Firewalls hindeutet.

Vorschläge für weitere Schritte

1. **LDAP-Enumeration**
   - Anonymous Bind testen, um Benutzer- und Gruppeninformationen abzurufen.
   - LDAP-Suchanfragen automatisieren (z.B. mit `ldapsearch` oder `rpcclient`).
2. **Kerberos-Angriffe**
   - Pass-the-Ticket und Kerberoasting gegen Service-Konten prüfen.
   - Zeitabweichungen ausgleichen (-skew), um Ticket-Wiederverwendung zu ermöglichen.

3. **SMB-Schwachstellen**
    - Hosts mit deaktivierter oder nicht erforderlicher Signierung (CASTLEBLACK, BRAAVOS) auf SMB-Schwachstellen prüfen (z.B. SMBv1, EternalBlue).
    - Versuchen, gültige SMB-Sessions aufzubauen und Freigaben zu enumerieren.
4. **Webserver-Analyse**
    - HTTP TRACE deaktivieren.
    - Directory Enumeration („common.txt“, „robots.txt“).
    - Prüfen auf bekannte IIS-Schwachstellen (CVE-2020-0688 etc.).
5. **SQL Server Untersuchung**
    - Standard-Konten (sa) prüfen.
    - SQL-Injection Tests auf jeder Web-Applikation vor Ort.
6. **Firewall- und Segment-Analyse**
    - Network Mapping hinter den gefilterten Hosts (Traceroute, interne Scans).
    - Prüfen, ob VPNs oder ACLs Netzsegmente schützen.

Erstellt am 22.08.2025