# NTLM-Relaying:

## Ein einfacher Weg Netzwerke zu kompromittieren

8COM
CYBER SECURITY

1 Grundlagen

2 Typische Szenarien

3 Demo

4 Maßnahmen

8COM CYBER SECURITY

Fighting Cybercrime

NTLM-Relaying: Ein einfacher Weg Netzwerke zu kompromittieren

8COM CYBER SECURITY

# 1 Grundlagen

Fighting Cybercrime

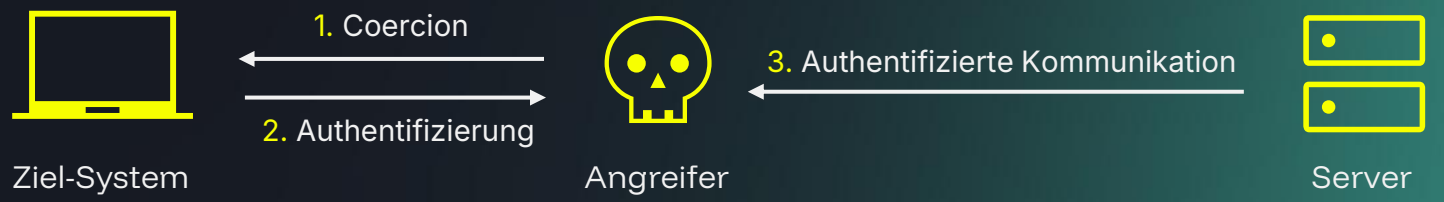
# Grundlagen

## NTLM

- Veraltetes Authentifizierungsprotokoll
- Seit 2000 durch Kerberos abgelöst
- Anfällig für Relaying-Angriffe

## Coercion

- Erzwingung einer Authentifizierung zu einem beliebigen Ziel
- Gezielt für Computeraccounts: PetitPotam, PrinterBug
- Opportunistisch für Benutzeraccounts: .lnk, .ms-library
- Opportunistisch für Benutzeraccounts: LLMNR, mDNS, NetBIOS Poisoning
- Protokolle: SMB, HTTP



NTLM-Relaying: Ein einfacher Weg Netzwerke zu kompromittieren

8COM CYBER SECURITY

# 2 Typische Szenarien

Fighting Cybercrime

# Typische Szenarien

| Client-/Server-Kompromittierung | ADCS: ESC8 | Exchange/SCCM/MECM Server | Benutzer-Kompromittierung |
|---|---|---|---|
| Ausgangsprotokoll: HTTP | Ausgangsprotokoll: SMB, HTTP | Ausgangsprotokoll: SMB | Ausgangsprotokoll: SMB, HTTP |
| Zielprotokoll: LDAP, LDAPS | Zielprotokoll: HTTP, HTTPS | Zielprotokoll: SMB | Zielprotokoll: SMB |
| Aktion: Shadow Credentials, RBCD | Aktion: Zertifikatsanfrage | Aktion: SAM/LSA auslesen | Aktion: SAM/LSA auslesen, Dateizugriff |
| Lokale Privilegienerweiterung, Kompromittierung von kritischen Systemen | Kompromittierung von kritischen Systemen z.T. Domänencontroller | Kompromittierung kritischer Systeme | Kompromittierung kritischer Benutzer |

NTLM-Relaying: Ein einfacher Weg Netzwerke zu kompromittieren

8COM CYBER SECURITY

# 3 Demo

Fighting Cybercrime

NTLM-Relaying: Ein einfacher Weg Netzwerke zu kompromittieren

8COM CYBER SECURITY

# 4 Maßnahmen

Fighting Cybercrime

# Maßnahmen

- SMB-Signing erzwingen
- LDAP-Signing erzwingen
- Channel Binding erzwingen (Extended Protection for Authentication)
- NTLMv1 deaktivieren und idealerweise NTLM komplett deaktivieren (schwer umsetzbar)
- Veraltete Protokolle deaktivieren (LLMNR, NetBIOS, mDNS)
- Anzeigen von Miniaturansichten abschalten

# Sie haben noch Fragen?

## Sprechen Sie mich gerne an!

8COM
CYBER SECURITY


**Robin Meier**
Penetration Tester

robin.meier@8com.de
www.8com.de


8com.de/newsletter