Análise Técnica de Tráfego Modbus TCP
Detecção de Scripts Maliciosos em Redes Industriais (ICS/OT)

Este documento técnico descreve um procedimento prático e defensivo para análise de tráfego Modbus TCP em redes industriais, com foco na identificação de scripts maliciosos, escritas indevidas e comportamentos anômalos. São abordadas as ferramentas Wireshark e tcpdump, amplamente utilizadas em ambientes OT por permitirem análise passiva e segura.

1. Contexto de Segurança em Modbus TCP

O protocolo Modbus TCP não possui mecanismos nativos de autenticação, criptografia ou controle de acesso. Qualquer dispositivo com acesso à rede pode ler ou escrever registradores em um CLP. Por esse motivo, scripts simples escritos em Python, C ou JavaScript são frequentemente usados como vetores de ataque ou sabotagem.

2. Objetivo da Análise

- Identificar IPs não autorizados comunicando-se via Modbus TCP
- Detectar comandos de escrita (funções críticas)
- Reconhecer padrões típicos de automação maliciosa (intervalos perfeitos, repetição)
- Coletar evidências para resposta a incidentes OT

3. Análise com Wireshark

O Wireshark permite inspeção detalhada de pacotes Modbus TCP. Os filtros abaixo devem ser aplicados no campo de Display Filter.

Mostrar apenas tráfego Modbus

```
modbus
```

Mostrar apenas funções de escrita (alto risco)

```
modbus.func_code == 5 || modbus.func_code == 6 || modbus.func_code == 15 || modbus.func_code == 16 || modbus.func_code == 22
```

Escritas fora do IP do SCADA autorizado

```
modbus && !(ip.src == 192.168.1.10)
```

Escritas com intervalo muito curto (script)

```
modbus && frame.time_delta < 1
```

Encerramento frequente de conexão

```
modbus && tcp.flags.fin == 1
```

Pacotes de mesmo tamanho (possível replay)

```
modbus && frame.len == 66
```

4. Interpretação no Wireshark

Durante a análise, deve-se observar especialmente os campos: Transaction ID (sequencial perfeito indica script), Source IP, Source Port variável, função Modbus utilizada e registradores acessados. Escritas fora do horário operacional ou sem ordem do operador são indicadores fortes de atividade maliciosa.

5. Análise com tcpdump (Linha de Comando)

O tcpdump é ideal para ambientes Linux embarcados, firewalls industriais e gateways OT. Os comandos abaixo são usados para captura rápida e segura.

Capturar todo tráfego Modbus TCP

```
tcpdump -i eth0 port 502
```

Salvar captura para análise posterior

```
tcpdump -i eth0 port 502 -w modbus.pcap
```

Exibir IPs e portas sem resolução DNS

```
tcpdump -nn -i eth0 port 502
```

Visualizar payload ASCII

```
tcpdump -i eth0 port 502 -A
```

Ver timestamps para identificar intervalos perfeitos

```
tcpdump -tt -i eth0 port 502
```

Capturar apenas um host suspeito

```
tcpdump -i eth0 host 192.168.1.99 and port 502
```

Limitar quantidade de pacotes

```
tcpdump -i eth0 port 502 -c 200
```

Rotação automática de arquivos

```
tcpdump -i eth0 port 502 -G 300 -W 10 -w modbus_%H%M.pcap
```

6. Procedimento Recomendado em Caso de Detecção

- Não interromper o CLP imediatamente
- Bloquear o IP suspeito no firewall industrial
- Salvar capturas como evidência
- Identificar fisicamente o equipamento de origem
- Auditar estações de engenharia e acessos remotos

7. Conclusão

A análise de tráfego Modbus TCP é uma das formas mais eficazes de detectar scripts maliciosos em redes industriais. Combinando Wireshark e tcpdump, é possível identificar rapidamente atividades não autorizadas sem interferir no processo produtivo.