Universidade Tecnológica Federal do Paraná – Câmpus Pato Branco
DAINF – Departamento Acadêmico de Informática

Análise de Segurança de Conversores Serial-Ethernet e Microcontroladores Tibbo

Willian Americano Lopes
walopes23@gmail.com

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Análise de Segurança de Conversores Serial-Ethernet e Microcontroladores Tibbo

Ildomar Gomes de Carvalho Junior
Rafael R. Obelheiro

SISTEMA DE CONTROLE INDUSTRIAL

- Automatizar processos industriais
- Constante monitoramento de dados

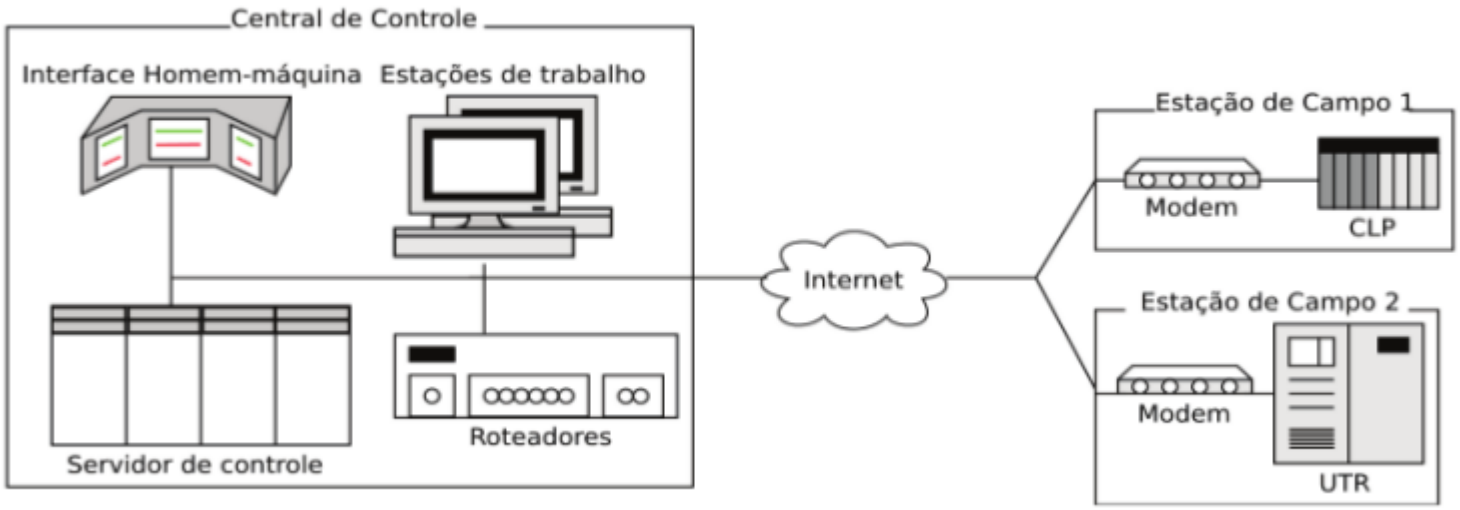


Fig. 1: Exemplo de SCI

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

TIBBO EM1206

- ASIC T1000 88 MHz
- 512K ou 1024K de Flash
- 2KB EEPROM
- Baud rate máximo de 921.600

Key Features

- 10/100 Base-T Ethernet port
- High-performance CPU (T1000)
- Mates with the RJ203 jack/magnetics front end
- 4 UARTs on 8 I/O lines, flexible mapping options
- Optional Wi-Fi connectivity (with the GA1000 add-on)
- 3.3V power

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

OBJETIVO

- Buscar vulnerabilidades que violem as propriedades de segurança (integridade, confidencialidade e disponibilidade) [ISO/IEC 2008]

- Injeção de ataques

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

INJEÇÃO DE FALTAS

- Técnica experimental
- Avaliar as propriedades de confiança no funcionamento (*dependability*)
- Segurança: Injeção de ataques

Vantagens:

- Deficiências
- Comportamento

INJEÇÃO DE FALTAS

- Avaliar a robustez da pilha TCP/IP
- Tráfego malicioso via rede
- Erros na codificação da pilha TCP/IP
- *Fuzzing*

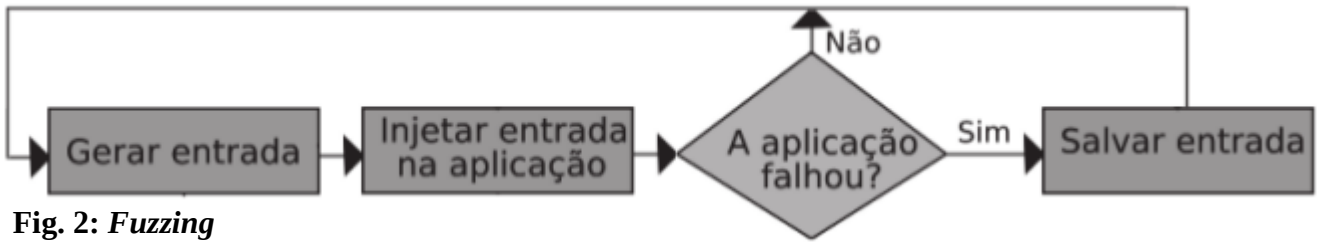


Fig. 2: *Fuzzing*

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

MÉTODO

Metodologia proposta por Pothamsetty e Balinsky (2003), analistas da Cisco.

Reconhecimento

- Identificar remotamente o SO e descobrir serviços de redes ativos

Análise por camadas

- Injeção dos pacotes e pesquisa de vulnerabilidades

Nmap

- Varredura de portas e do SO

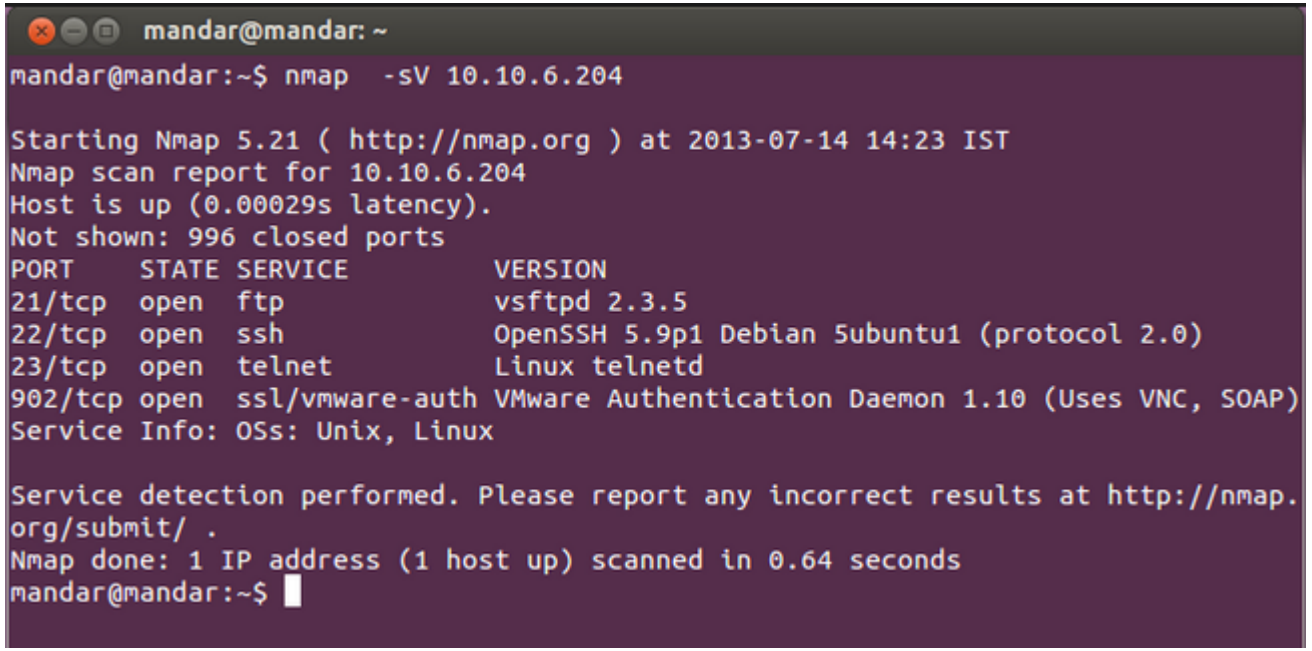


Fig. 3: NMap

Nessus

- Scanner de vulnerabilidade

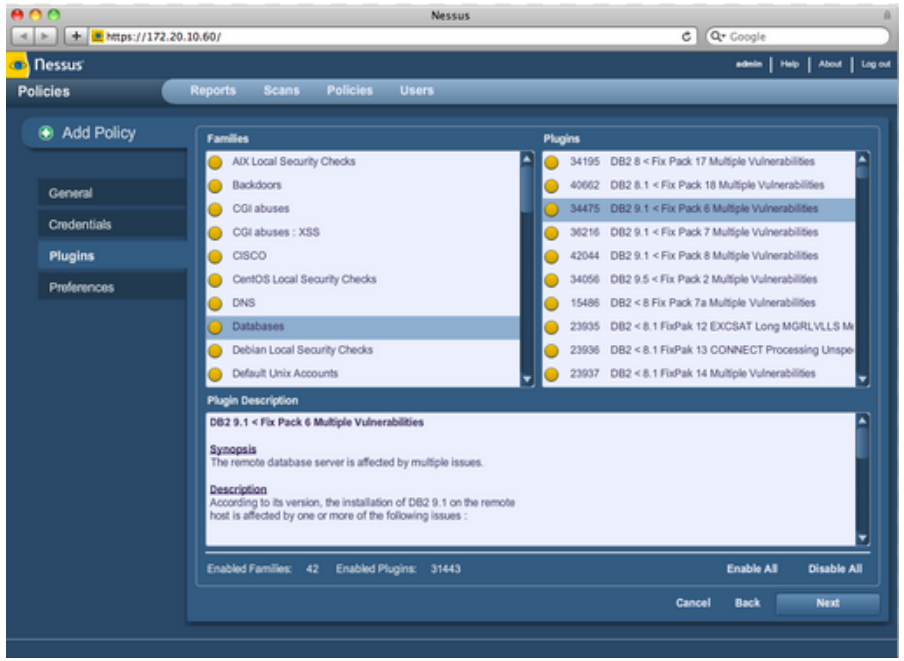


Fig. 4: Teanable Nesuss

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

FERRAMENTAS

IP Stack Integrity Checker

- Conjunto de ferramentas para executar o *fuzzing* na pilha TCP/IP
- Gera pacotes pseudo-aleatórios

- ESIC: gera *frames Ethernet*
- ISIC: gera pacotes UDP
- UDPSIC: gera datagramas UDP
- TCPSIC: gera pacotes TCP

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

FERRAMENTAS

Bruteforce Exploit Detector (BED)

- Testes *fuzzing* na aplicação WEB

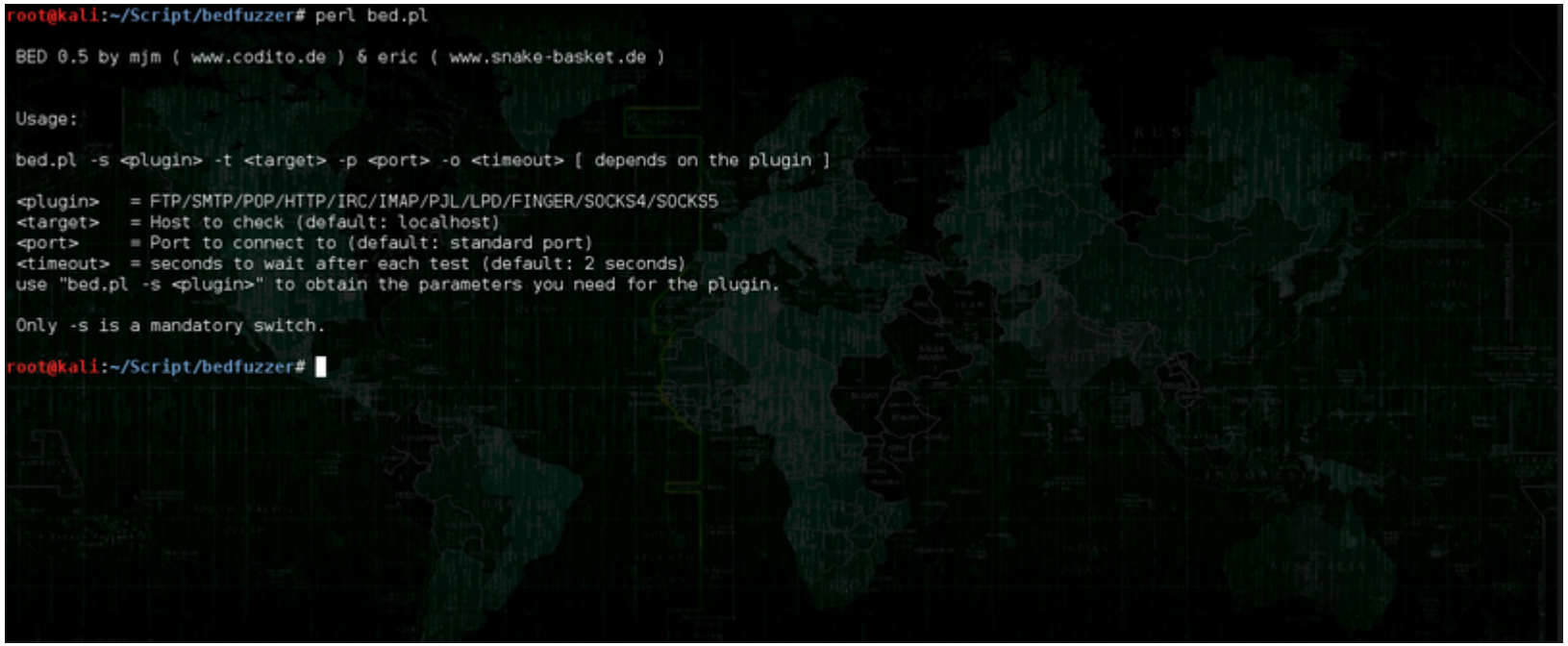


Fig. 5: BED

Scapy

- *Scripts* para reproduzir as vulnerabilidades encontradas

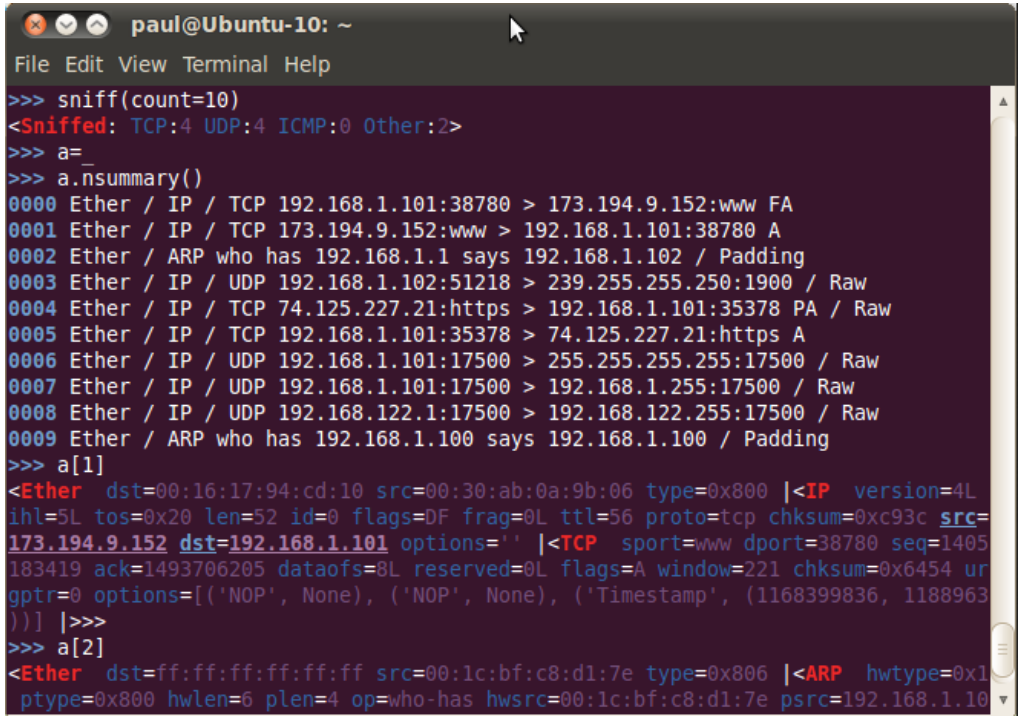


Fig. 6: Scapy

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

FERRAMENTAS

Wireshark

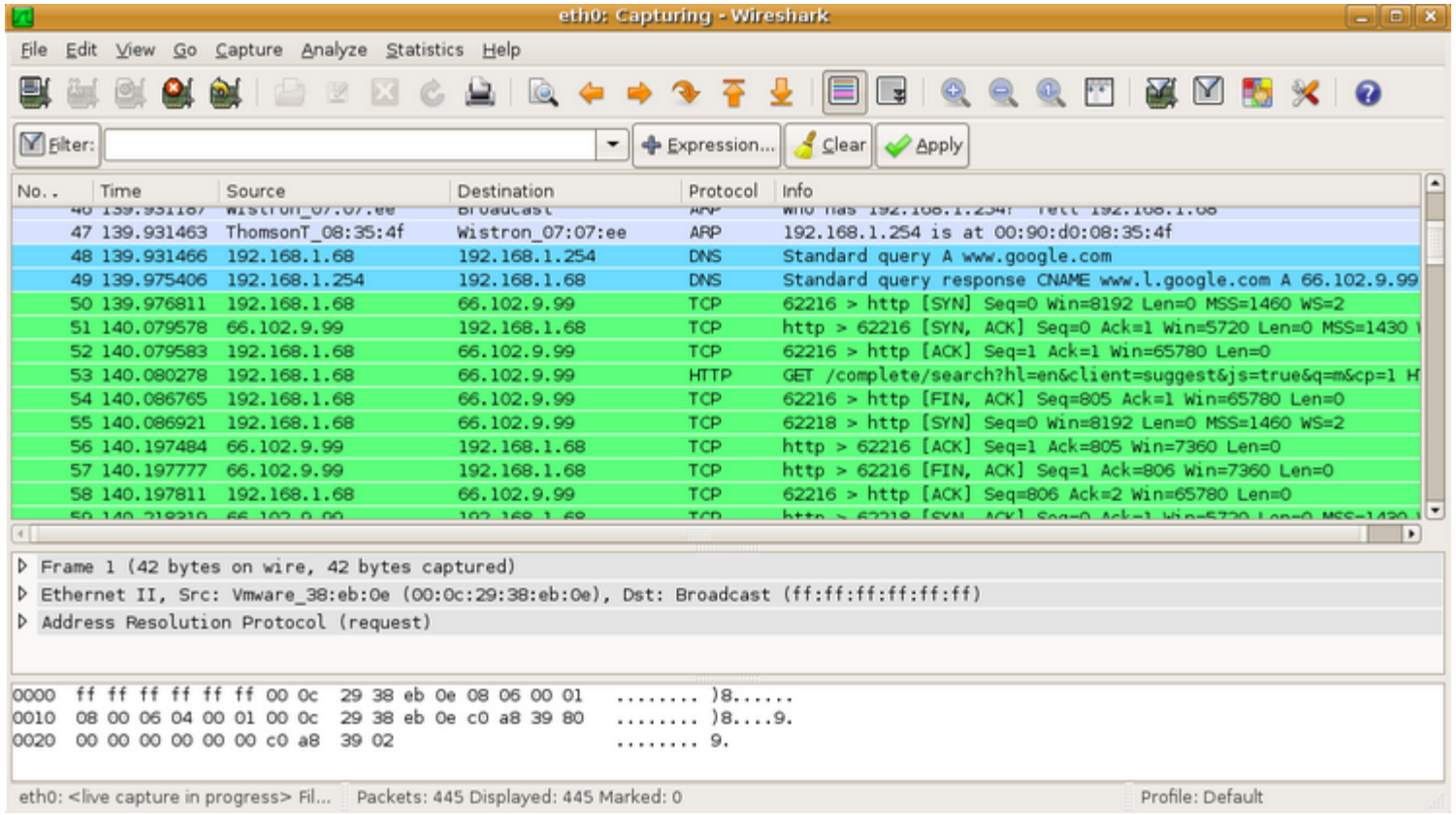


Fig. 7: Wireshark

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

RESULTADOS

Reconhecimento

Análise por camadas

- Ethernet
- IP/UDP
- TCP
- Aplicação

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

RECONHECIMENTO

- Identificação do SO e da pilha TCP/IP
- SO: ?
  SW: NMap
- 3 portas abertas:

  Porta 23: Não roda o TELNET → aplicação de gerenciamento do módulo
  Porta 80: HTTP e gerenciamento
  Porta 1001: conversão serial-*Ethernet*

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

ETHERNET

Testes:

1. Aplicação do *fuzzing* nos campos do cabeçalho *Ethernet*
   SW: ESIC
   Não demonstrou vulnerabilidade ao *fuzzing*

2. SW: Nessus
   Vulnerabilidade: Etherleak
   RFC 1042: tamanho mínimo para os quadros *Ethernet*
   Dados vem de *buffers*

ETHERNET

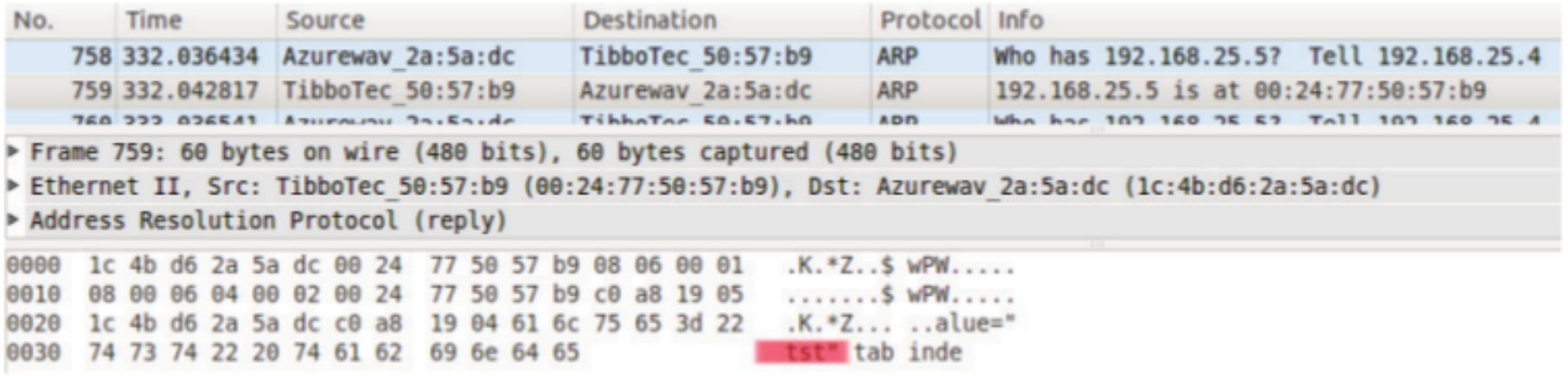


Fig. 8: Requisição ARP

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

IP E UDP

- Utilizados ISIC e UDPSIC, separadamente
- Não foi vulnerável ao *fuzzing*
- Fluxo de dados causou *flooding*

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

TCP

Três testes realizados

1. Utilizando o SW TCPSIC
   Vulnerável ao *flooding* mas não ao *fuzzing*

2. Eficiência do gerador de números iniciais de sequência
   Aleatoriedade
   Nmap: Aleatoriedade fraca
   Nessus: Aleatoriedade forte
   Análise manual utilizando *script* no Scapy

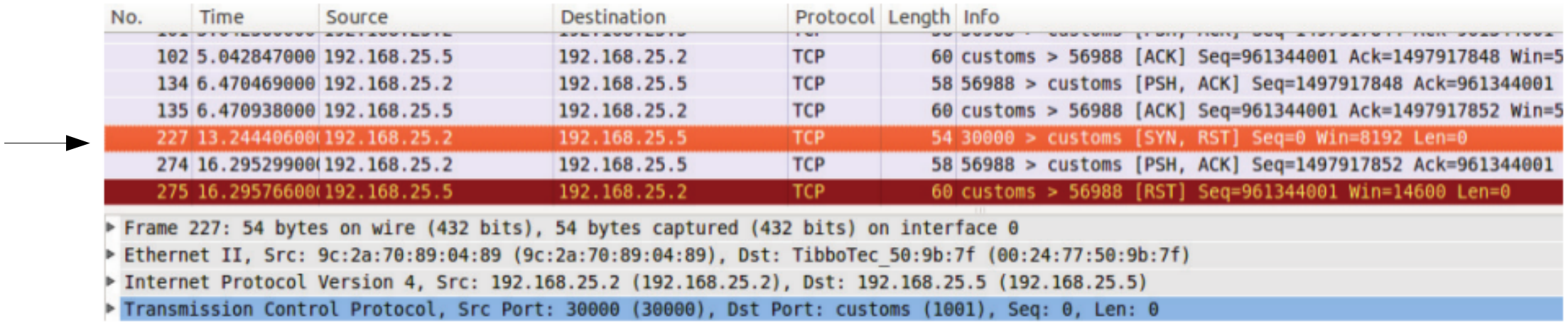
Envia segmentos SYN para o EM1206 e imprime os números de sequência usado na resposta SYN-ACK
Incrementa o valor em 64000 a cada 500ms
Viola a RFC 6528

3. Reset Spoofing

Possível encerrar conexão enviando pacotes RST ilegítimos
Script pelo Scapy
Enviou pacotes com as *flags* SYN e RST para uma conexão estabelecida, utilizando nª de sequência e ACK errados

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

TCP



No.	Time	Source	Destination	Protocol	Length	Info
102	5.042847000	192.168.25.5	192.168.25.2	TCP	60	customs > 56988 [ACK] Seq=961344001 Ack=1497917848 Win=5
134	6.470469000	192.168.25.2	192.168.25.5	TCP	58	56988 > customs [PSH, ACK] Seq=1497917848 Ack=961344001
135	6.470938000	192.168.25.5	192.168.25.2	TCP	60	customs > 56988 [ACK] Seq=961344001 Ack=1497917852 Win=5
227	13.24440600(	192.168.25.2	192.168.25.5	TCP	54	30000 > customs [SYN, RST] Seq=0 Win=8192 Len=0
274	16.29529900(	192.168.25.2	192.168.25.5	TCP	58	56988 > customs [PSH, ACK] Seq=1497917852 Ack=961344001
275	16.29576600(	192.168.25.5	192.168.25.2	TCP	60	customs > 56988 [RST] Seq=961344001 Win=14600 Len=0

▸ Frame 227: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▸ Ethernet II, Src: 9c:2a:70:89:04:89 (9c:2a:70:89:04:89), Dst: TibboTec_50:9b:7f (00:24:77:50:9b:7f)
▸ Internet Protocol Version 4, Src: 192.168.25.2 (192.168.25.2), Dst: 192.168.25.5 (192.168.25.5)
▸ Transmission Control Protocol, Src Port: 30000 (30000), Dst Port: customs (1001), Seq: 0, Len: 0

Fig. 9: Reset Spoofing

APLICAÇÃO

4 Vulnerabilidades

1. Autocomplementar campo senha

Não desabilitar o autocomplemento oferece um risco de perda de confidencialidade

2. Comportamento do servidor diante de ataques *fuzzing*

SW BED

flooding: GET e POST

3. Roubo de *cookies* de uma seção

Conversor dá um *cookie* para identificar que está autenticado

Script pelo Scapy

Enviou pacotes com as *flags* SYN e RST para uma conexão estabelecida, utilizando nª de sequência e ACK errados

APLICAÇÃO

4. Envio não criptografado da senha do conversor

Três maneiras de acessar o EM1206:

- Página WEB embarcada
- DS Manager
- Aplicação que roda na porta 23

Enviam a senha de rede de forma aberta

DS MANAGER → envia a senha por *broadcast*

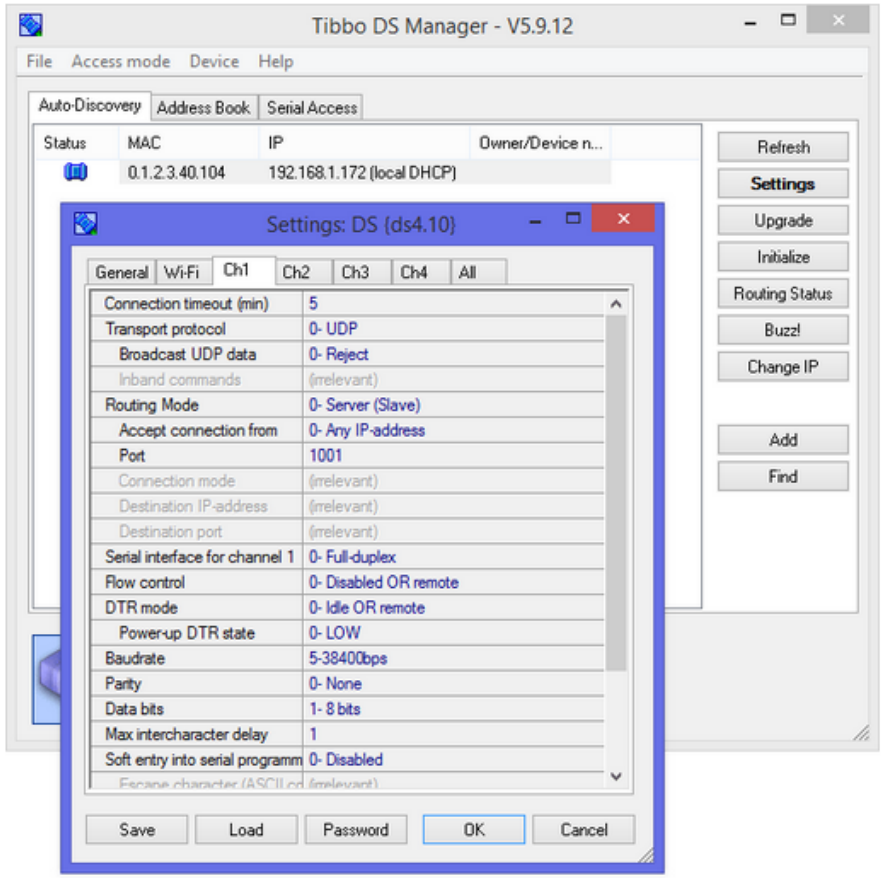


Fig. 10: DS Manager

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

RESULTADOS

Tabela 1. Vulnerabilidades encontradas no módulo EM1206 da Tibbo.

Camada	Problemas Encontrados
Ethernet	Etherleak
IP	*Flooding*
UDP	*Flooding*
TCP	*Flooding*, Aleatoriedade Fraca do Número Inicial de Sequência e *Reset Spoofing*
HTTP	Autocompletar Senha, *Flooding*, Roubo de *Cookie* e Transmissão de Senha Não Criptografada

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

CONCLUSÕES

- Nível de segurança do Tibbo EM1206 é baixo
- Sugere metodologias para ataques *fuzzing*
- Sugere comparação com outros dispositivos
- Sugere métricas para medir a robustez de um dispositivo embarcado diante *flooding*

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

REFERÊNCIAS

[1] http://tibbo.com/store/soi/em1206.html?page=products/modules/x20x/em1206

[2] Pothamsetty, V and Balinsky, A (2003). **A structured and practical methodology for security evaulation of a IP based stack** (version 0.2).

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Perguntas?

Sugestões?

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

Obrigado!