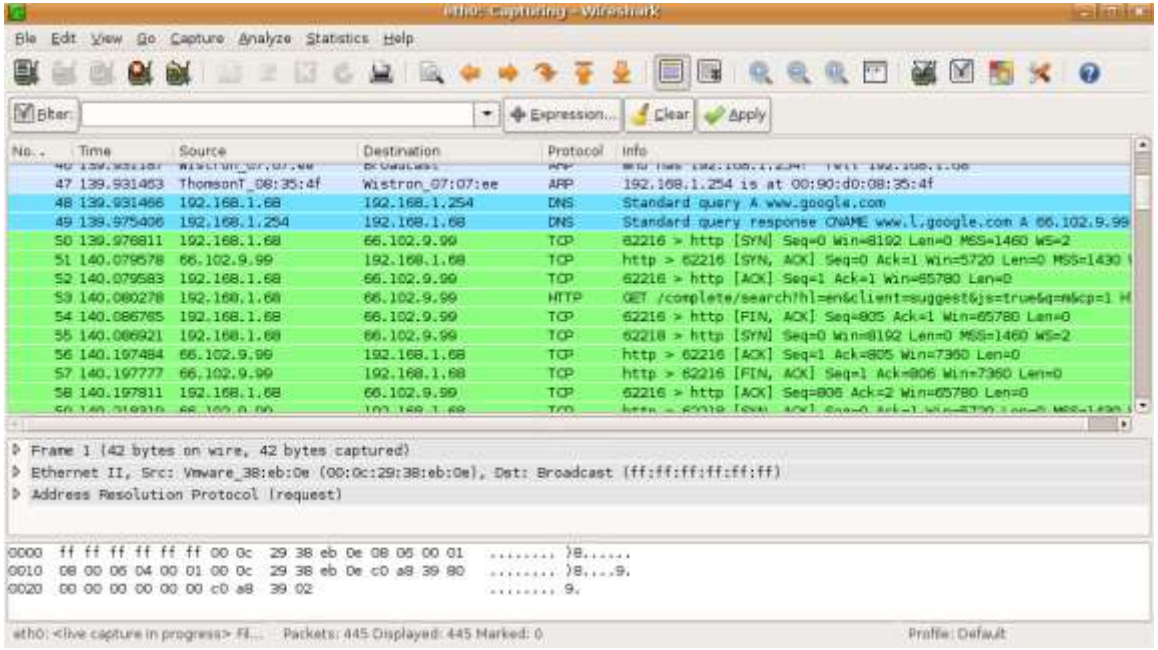
Disciplina: Segurança e Auditoria
Aula 11: Ferramentas

Professor: Rodrigo Rocha

WIRESHARK

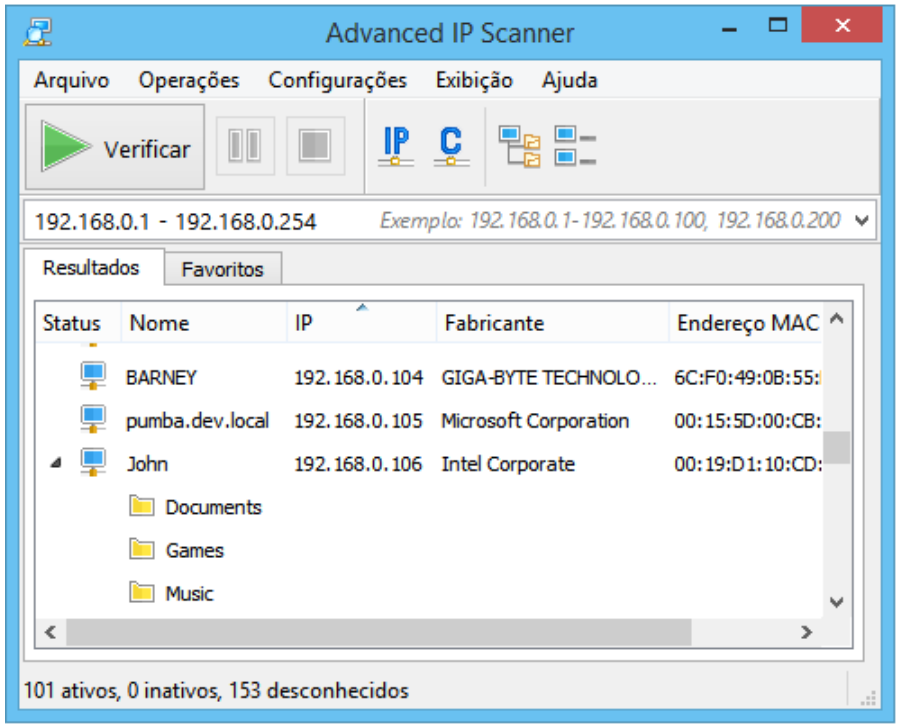


- Analisador de protocolo de Rede
- Permite analisar dados de rede em tempo real
- Suporte a diversos protocos de rede
- Exibe detalhes do fluxo das transmissões de dados capturadas
- Exibe informações da transmissão rede em detalhe das camadas do modelo TCP

Filtros aplicados no Wireshark

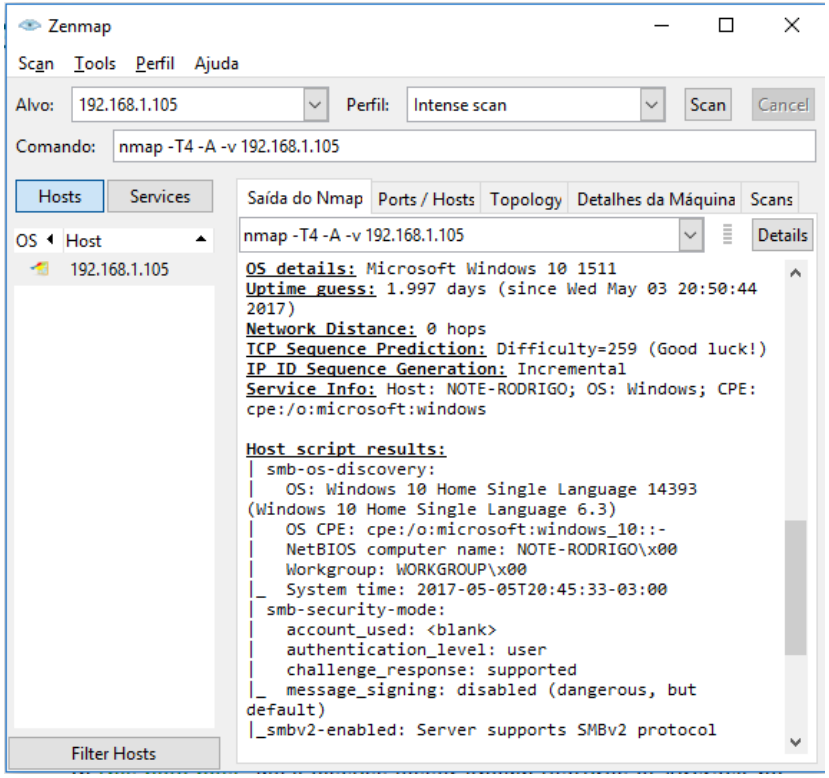
FILTRO	EXPLICAÇÃO	EXEMPLO
ip.addr	endereço IPv4 de destinou ou origem	ip.addr == 10.10.10.10
ip.dst	endereço de destino IPv4	ip.addr == 10.10.10.10
ip.src	endereço de origem IPv4	ip.src == 10.10.10.10
ip.proto	Protocolo IP (decimal)	ip.proto == 1
ipv6.addr	endereço IPv6 de origem ou destino	ipv6.addr == 2001 :: 5
ipv6.src	endereço IPv6 de origem	ipv6.addr == 2001 :: 5
ipv6.dst	endereço de destino IPv6	ipv6.dst == 2001 :: 5
tcp.port	porta TCP de destino ou origem	tcp.port == 20
tcp.dstport	porta TCP de destino	tcp.dstport == 80
tcp.srcport	porta TCP de origem	tcp.srcport == 60234
udp.port	porta UDP de destino ou origem	udp.port == 513
udp.dstport	porta UDP de destino	udp.dstport == 513
udp.srcport	porta UDP de origem	udp.srcport == 40000
icmp.type	Código do tipo ICMP (decimal)	icmp.type == 8

Advanced IP Scanner



- Escaneia todos os dispositivos de rede
- Acesso a pastas compartilhadas e servidores FTP
- Fornece controle remoto dos computadores (via RDP e Radmin)
- Descoberta de endereços em MAC
- Ligar/desligar computadores em rede remotamente
- Executado como uma edição portátil
- Exportar para CSV

NMAP



- Exploração de rede e auditoria de segurança
- Inventário de rede
- Gerenciamento de agendamentos de atualização de serviços
- Monitoramento do tempo de atividade do host ou do serviço
- Projetado para escanear rapidamente grandes redes, mas funciona bem contra hosts únicos
- Identifica quais serviços os hosts estão oferecendo e que sistemas operacionais, que tipo de filtros de pacotes / firewalls Estão em uso, e dezenas de outras características

Dúvidas... Sugestões...

Dúvidas?

Sugestões?