INSTITUTO FEDERAL DO PARANÁ

MARIA GABRIELE DE FREITAS XAVIER SOBRAL
RAINNY SANTOS DA CRUZ

ANÁLISE DE VULNERABILIDADE DE REDES LOCAIS, UM ESTUDO DE CASO: IFPR - CAMPUS PARANAGUÁ

V.3

PARANAGUÁ

2018

MARIA GABRIELE DE FREITAS XAVIER SOBRAL
RAINNY SANTOS DA CRUZ

ANÁLISE DE VULNERABILIDADE DE REDES LOCAIS, UM ESTUDO DE CASO: IFPR - CAMPUS PARANAGUÁ

V.3

Trabalho de Conclusão de Curso apresentado ao Curso Técnico em Informática do Instituto Federal do Paraná, como requisito parcial de avaliação.

Orientador: Diego Jonathan Hoss

PARANAGUÁ

2018

FOLHA DE APROVAÇÃO

MARIA GABRIELE DE FREITAS XAVIER SOBRAL
RAINNY SANTOS DA CRUZ

ANÁLISE DE VULNERABILIDADE DE REDES LOCAIS, UM ESTUDO DE CASO: IFPR - CAMPUS PARANAGUÁ

V.3

Trabalho de Conclusão de Curso aprovado como requisito parcial para a obtenção do título de Técnico, no Curso de Informática, Eixo de Informação e Comunicação, do Instituto Federal do Paraná, Câmpus Paranaguá, banca examinadora composta pelos seguintes integrantes:

Orientador: _____

Prof. Mestre Diego Jonathan Hoss

Eixo de Informação e Comunicação, IFPR

Avaliador: _____

Rodrigo Alves Zucarelli

Setor de Tecnologia da Informação, IFPR

Avaliador: _____

Antônio Carlos Vissotto Júnior

Setor de Tecnologia da Informação, IFPR

Paranaguá, 6 de novembro de 2018

AGRADECIMENTOS

Gostaríamos de agradecer o apoio das nossas famílias, amigos e professores que estiveram conosco durante esta longa caminhada e acreditaram no nosso potencial para podermos concluir o curso de Técnico em Informática, incluindo o Trabalho de Conclusão de Curso do mesmo. Nosso muito obrigada a todos que de alguma forma contribuíram para a entrega deste trabalho, e também durante estes quatro anos em que estivemos dentro da Instituição.

Em especial, agradecemos ao nosso orientador, orientador do eixo, professor e amigo, Diego Jonathan Hoss, que nos auxiliou e apoiou durante toda esta caminhada do nosso TCC, e também contribuiu para os nossos conhecimentos. E aos nossos melhores amigos Sabrina Rosa e Luiz Felipe Viana que estiveram conosco em todos os momentos, incluindo os encontros semanais, mas que deram todo o apoio para que este trabalho fosse concluído.

E por fim, agradecemos a Instituição, pela oportunidade de podermos fazer parte de algo tão rico em conhecimentos, que nos proporcionou ensino de qualidade, amizades e muita responsabilidade durante estes quatro anos.

Obrigada, IFPR.

“A amizade desenvolve a felicidade e reduz o sofrimento, duplicando a nossa alegria e dividindo a nossa dor”

Joseph Addison

RESUMO

As redes de computadores permitem a interligação entre dispositivos computacionais para que haja a troca de informações entre eles. Estes dispositivos podem estar conectados entre si por meio de redes locais ou através da Internet. Em ambos os casos, as informações trocadas na comunicação podem ser consideradas sensíveis e sigilosas. Neste sentido, se faz necessário a utilização de técnicas e mecanismos de segurança para garantir a integridade, confidencialidade e autenticidade das informações. A aplicação de técnicas e mecanismos de segurança no entanto, é uma tarefa complexa.

Neste sentido, este trabalho apresenta uma Análise de Vulnerabilidade de Redes Locais aplicada à rede do IFPR-Campus Paranaguá. O trabalho tem como objetivo identificar e avaliar os problemas de segurança bem como propor soluções para os problemas identificados.

As principais etapas do desenvolvimento deste trabalho são: analisar e relatar as falhas de segurança na rede, identificar tráfego malicioso, serviços de rede vulneráveis; encontrar aplicações com falhas de segurança.

Em seguida, é esperado a confecção de um relatório contendo as indicações sobre as vulnerabilidades da rede local bem como sugestões para a correção das mesmas. Auxiliando desta forma, os profissionais da Tecnologia de Informação que trabalham no campus, os quais não possuem recursos humanos suficientes para poder controlar estas falhas e, portando, resolvê-las.

Para a execução do trabalho é utilizando um conjunto de ferramentas de rede disponíveis no sistema operacional Kali Linux. Este sistema foi projetado para ser uma hospedeiro de ferramentas utilizadas em trabalhos vinculados à segurança da informação.

Palavras-chave: Redes de Computadores. Segurança da Informação. Ferramentas de Rede.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS

Abr. - Abril
Add. - Adicionar
Ago. - Agosto
Art. - Artigo
Dez. - Dezembro
Fev. - Fevereiro
Jul. - Julho
Jun. - Junho
Mai. - Maio
Mar. - Março
Nov. - Novembro
OE. - Objetivo Específico
Out. - Outubro
Set. - Setembro

LISTA DE SIGLAS

ARPANET - Advanced Research Projects Agency Network
BOOTP - BootStrap Protocol
CD - Compact Disc
CIFS - Sistema de Arquivos da Internet Comum
CPU - Central Processing Unit
DHCP - Protocolo de configuração dinâmica do Host
DNS - Domain Name System
EPMAP - End Point Mapper
HTTP - Protocolo de Transferência de Hipertexto
IEC - International Electrotechnical Commission
IFPR - Instituto Federal do Paraná
IP - Internet Protocol
ISO - International Organization for Standardization
MSRPC - Microsoft Distributed Computing Environment/Remote Procedure Call
NAS - Network Attached Storage
NAT - Network Address Translation
NBR - Associação Brasileira de Normas Técnicas
NDP - Network Data Management Protocol
NETBIOS - Network Basic Input/Output System
NTI - Núcleo de Tecnologia da Informação
NTP - Network Time Protocol
PIN - Personal Identification Number
SEMEPI - Semana de Ensino, Extensão, Pesquisa e Inovação do Litoral do Paraná
SMB - Server Message Block / Bloco de Mensagem de Servidor
SNMP - Protocolo Simples de gerenciamento de redes
SSH - Secure Shell
SSL - Secure Sockets Layer
T.I. - Tecnologia da Informação
TCC - Trabalho de Conclusão de Curso
TCP - Transmission Control Protocol
UDP - User Datagram Protocol

SUMÁRIO

1. INTRODUÇÃO

1.1. Justificativa

Após levantamento junto ao setor de T.I do Campus Paranaguá, foi constatado que o mesmo não possui nenhum tipo de ferramenta que forneça informações a respeito das vulnerabilidades de segurança dos dados. Assim, foi proposto este trabalho para identificar riscos que possam existir na rede em relação à segurança lógica e, sugerir soluções que consigam ser implementadas futuramente pelos técnicos da instituição.

1.2. Objetivos

Analisar e identificar as vulnerabilidades da rede local do Campus Paranaguá e auxiliar os profissionais de T.I. a resolver os problemas de segurança das redes de dados.

1.3. Estrutura do Trabalho

O trabalho inicialmente apresenta na seção 3.1.2 uma fundamentação teórica sobre o que é a segurança na área de redes, tanto a física quanto a lógica. Na área de segurança lógica apresenta os conceitos sobre as falhas em sistemas, serviços e dispositivos. Além disso, analisa sobre como usuários acabam tendo as suas contas invadidas, ou aqueles que costumam praticar esses ataques que foram descritos na seção 3.3.5. Posteriormente, o projeto visa mostrar as ferramentas de auditoria, varredura e scan, que podem investigar possíveis vulnerabilidades nas redes que é descrito na seção 3.1.6. As redes analisadas são as do Instituto Federal do Paraná e o intuito deste trabalho é mostrar as falhas se existirem, nestes ambientes apresentados na seção 3.3. O próximo passo é realizar pesquisas de ferramentas que podem auxiliar na resolução dos problemas de segurança como ocorre na seção 3.1.7. Por fim, a seção 3.4 apresenta a validação, que trata-se de retestar as falhas da rede e dos servidores para saber se as soluções que foram sugeridas obtiveram sucesso.

2. VISÃO DO PROJETO

2.1. Ambiente do Usuário

A infraestrutura de redes não possui recursos e ferramentas para identificar e solucionar problemas de segurança. Desta forma, os profissionais de T.I não podem garantir um bom desempenho para os usuários da rede.

2.2. Declaração do Problema

O problema de	falhas de segurança na rede
afeta	os profissionais na área de T.I
o impacto do qual é	a falta de controle de dados trafegados na rede
uma solução bem-sucedida deveria	utilizar ferramentas para monitorar e controlar o tráfego de dados na rede. Para que os profissionais de T.I possam solucionar os problemas.

QUADRO 01 – Declaração do Problema

2.3. Cronogramas

2.3.1. Objetivos Específicos:

OE1: Estudar sobre os conceitos de segurança de redes.

OE2: Estudar sobre ferramentas relacionadas a segurança de redes.

OE3: Analisar a infraestrutura de rede e serviços que compõem o cenário atual do Campus.

OE4: Realizar experimentos com ferramentas e técnicas para identificar falhas de segurança.

OE5: Implementar técnicas e ferramentas para solucionar as falhas de segurança.

OE6: Validar a eficácia das soluções aplicadas.

Fases do Projeto	FEV	MAR	ABR	MAI	JUN	JUL	AGO	SET	OUT	NOV	DEZ
Elaboração do Pré Projeto	x	x									
OE1		x	x								
OE2		x	x	x	x						
OE3	x	x	x								
OE4			x	x	x	x					
Pré-Banca					x						
Artigo do SEMEPI				x	x	x					
OE5						x	x	x	x		
OE6								x	x	x	
Entrega do TCC										x	x

QUADRO 02 - Cronograma

2.4. Necessidades Iniciais de Recursos

Livros, computadores com sistemas operacionais Linux para testar as ferramentas (Kali Linux).

2.5. Recursos do Projeto

Os membros da equipe deverão ter conhecimento do uso das ferramentas do Kali Linux antes de começar o desenvolver o projeto. Logo após a finalização das pesquisas de uso, será iniciado o desenvolvimento do trabalho com a utilização das ferramentas.

2.6. Orçamento

Existe um recurso, porém é a instituição que fornece os computadores usados durante o trabalho, e também a internet.

3. DESENVOLVIMENTO

3.1. Revisão de Literatura

3.1.1. Redes de Dados

Antigamente, os computadores eram máquinas grandes e complexas, muitas ocupavam uma sala por completo e não havia comunicação entre elas. O primeiro registro de transmissão de informações em longas distâncias através de computadores foi nos Estados Unidos. Eram quatro pontos, cada um em uma universidade, assim nasce a ARPANET, que mais tarde se tornaria a Internet. Nesta época, a preocupação era essencialmente em garantir a comunicação. Aspectos relacionados à segurança dos dados ainda não eram tão evidentes. Este cenário no entanto, mudou significativamente nos últimos anos. (KUROSE, 2006) (ALMEIDA, 2005) (ROSS, 2008).

Diversas instituições necessitam do uso de redes de computadores para que haja comunicação entre os setores. Estas informações em muitos casos são consideradas sensíveis e carecem de proteção. Neste sentido tornam-se necessários técnicas e mecanismos de proteção e segurança para a informação que são apresentados na próxima seção.

3.1.2. Segurança

As redes de dados possibilitam que ocorram tráfegos de informações entre diversas máquinas e, em muitos casos, as redes estão suscetíveis a ataques, sejam eles para sequestro de informações, comprometer a rede, entre outras possibilidades. (BERTOLÍN, 2008).

Os problemas de segurança podem ocorrer em várias esferas da comunicação em rede, inclusive na internet. Sendo que esta pode ser utilizada como porta de entrada para a exploração de falhar em redes internas. (SOUSA, 2009).

Há três conceitos que são essenciais quando se fala em segurança de rede. Eles são listados nos tópicos a seguir (BARBOSA, 2006/2007).

- **Confidencialidade:** é a certeza de que a informação que está sendo transmitida será acessada somente por pessoas com a determinada autorização.
- **Integridade:** é a garantia de que a informação está segura com todos os dados completos.
- **Disponibilidade:** trata-se da confiança na obtenção da informação desejada quando o usuário tiver a autorização necessária.

Além disso, outros termos são empregados a esse tema, como a autenticidade que comprova a identidade do indivíduo via login, PIN ou uma característica própria. Tem-se também a legalidade, não repúdio e auditoria que registra os dados. Estes quatro aspectos relacionam-se entre si visando identificar, rastrear e certificar que tal dado foi gerado pelo determinado usuário (DO ESPÍRITO SANTO,2010).

Outro fator determinante vinculado a segurança da informação é a questão humana. Ela é considerada de suma importância e é o ponto mais fraco entre todos os fatores analisados, embora os objetos possuam menor privilégio (JUNIOR, 2009).

3.1.3. Proteção dos Dados

Existem algumas formas de proteger dados sensíveis. Essencialmente a proteção pode ocorrer em duas camadas. Estas camadas são identificadas como segurança física e segurança lógica.Elas são apresentadas em detalhes a seguir. (DOS SANTOS, 2017).

3.1.4. Segurança Física

A segurança física abrange toda a parte que o usuário possa ter contato fisicamente, até a estrutura onde a rede se instala, o edifício, portas, fechaduras, salas, e as máquinas. A conduta NBR ISO/IEC 17799:2001 fez subdivisões na segurança física e elas são apresentadas a seguir.

A segurança externa e de entrada, previne a admissão de pessoas não autorizadas através de travas, alarmes, grades, monitoramento de câmeras, vigias e alarmes. Contudo desastres naturais fazem com que as salas se localizem nos

andares mais altos, que sejam salas de cantos, com para-raios, ar-condicionado controlando a temperatura todo o momento, sem material inflamável ou líquido, além de que os cabos não estejam de fácil acesso.

A segurança da sala de equipamentos envolve em manter a integridade dos servidores em um lugar que possa haver um controle, seja contra qualquer circunstância do exterior que possa acontecer. A segurança dos equipamentos, consiste em proteger qualquer dispositivo de saída e entrada do servidor, travando pen-drives, disquetes e CD's caso tentem se conectar ao sistema. A redundância pode ser usada para suportar as falhas ocorridas devido ao *hardware*, podendo ser eles interfaces de rede, discos, servidores, CPU's e até energia elétrica.

A segurança no fornecimento de energia resume-se em estabilizar a voltagem, e fazer com que haja abastecimento elétrico constantemente, caso aconteça uma queda de energia, o prédio tem que estar preparado com um gerador a disposição. O Salvaguarda ou também conhecido e popularmente chamado de *backup*, é uma forma de armazenar a informação, para caso ocorra a perda do dado na origem, assim a informação necessária estará segura.

Quando certa informação é privada o seu descarte deve ser bem feito para que os dados não sejam recuperados de nenhuma forma, utilizando fragmentadoras quando for papel, excluindo qualquer cópia digital, e destruindo todos os materiais físicos.

3.1.5. Segurança Lógica

A parte da segurança que está ligada a *softwares* é chamada de segurança lógica, vários termos como senhas, firewalls, IDS, Redes privadas, criptografia, logins, entre outros se encaixam neste papel (MARCIANO, 2006). A seguir alguns conceitos serão descritos.

Firewall: O *Firewall* controla a entrada na rede, para isso, examina se cada protocolo passa pela porta correta. Assim apenas usuários autorizados podem ter livre acesso, evitando que pessoas indesejadas possam descobrir as suas falhas internas. Este processo é feito por meio de filtro de pacotes que analisam cada pacote individualmente, proxies que controlam a comunicação das máquinas internas e externas, redirecionamento de portas e NAT (FONTES, 2008).

Os *Firewalls* podem ser aplicações gratuitas, também conhecidas como *open source*. Alguns exemplos são: PfSense, Endian Firewall e OPNSense. Existem também algumas soluções pagas, tais como: Sonicwall, Cisco ASA e Juniper.

IDS: Além dos Firewalls, existem também os IDS (Intrusion Detection System), em português, Sistemas de Detecção de Intrusão. Os IDS buscam identificar algo de estranho na rede, são baseados no sistema imunológico do corpo humano, mediante do reconhecimento por assinatura ou comportamento.

Redes Privadas: As redes virtuais privadas (VPN, Virtual Private Network) utilizam a internet como intermédio e criptografia segura, se dividindo em dois tipos, entre redes e discada. (PEIXINHO, 2013).

A segurança, de um modo geral, é avaliada por meio de técnicas (análise de vulnerabilidades) e ferramentas. Algumas destas técnicas e ferramentas são descritas a seguir.

3.1.6. Análise de Vulnerabilidades

A obtenção de informações relacionada às vulnerabilidades que uma rede possui pode ser nomeada como Pentest, esta técnica vem acompanhada de outros termos, além de seguir uma ordem de passos. As etapas do pentest são a coleta de informações, enumeração, análises de vulnerabilidades, pentest e por fim,o relatório. A importância desse estudo se dá pelo fato de conhecer os riscos que a rede se expõe antes que essas informações sejam usadas com um propósito duvidoso. (MORIMOTO, 2011).

3.1.7. Ferramentas

A análise das vulnerabilidades é realizada, na maioria das vezes, utilizando uma ou mais ferramentas que permitem identificar e explorar falhas na redes de dados e sistemas. Algumas destas ferramentas são apresentadas a seguir:

3.1.7.1. Nmap

Trata-se de um dos principais sistemas *free open source* que é muito utilizado por profissionais de segurança na detecção de redes, análises e auditorias de segurança. Esta ferramenta é considerada essencial para gerar detalhes de

informações específicas em qualquer máquina que esteja ativa (NMAP, 2018).

3.1.7.2. Zenmap

É uma interface gráfica para a ferramenta Nmap.(ZENMAP, 2018).

3.1.7.3. Arping

Refere-se a uma ferramenta que está ativa em uma rede local e protegida por um firewall/gateway, o que acaba sendo uma informação útil para invasores (ARPING, 2018).

3.1.7.4. NetDiscover

É relativo a uma ferramenta de varredura de rede que permite relacionar todos os hosts que estão ativos. (NETDISCOVER, 2018).

3.1.7.5. Wireshark

É referente a uma ferramenta onde é permitido ver o que está acontecendo dentro da rede em um nível microscópico. Isto é, é possível inspecionar o conteúdo dos pacotes. (WIRESHARK, 2018).

3.1.7.6. Miranda

Diz respeito a uma ferramenta projetada para descobrir, consultar e interagir particularmente os dispositivos gateway da internet, que também são conhecidos como roteadores. (MIRANDA, 2018).

3.1.7.7. Hping

Trata-se de uma ferramenta utilizada para ataque de negação de serviço, para isso é preciso ter conhecimento sobre a relação cliente/servidor. É importante saber que as mensagens servidor/cliente são trocadas em três vias. (HPING, 2018).

3.1.7.8. NetStat

É alusivo a uma ferramenta que permite conhecer as conexões TCP ativas na rede e assim listar o conjunto das portas abertas. (NETSTAT, 2018).

3.1.7.9. NetCat

É respeitante a uma ferramenta que permite a conexão de um host com uma linha de comando. Ele é utilizado para ler e escrever através dessas conexões, utilizando protocolos TCP e UDP. (NETCAT, 2018).

3.1.8. Metasploit Framework

O *Metasploit framework* trata-se de um agrupamento das melhores plataformas de aprendizagem e investigação para o profissional de segurança ou do hacker ético. Dentro dele é possível encontrar centenas de *exploits, payloads* e ferramentas ainda mais avançadas que permite testar vulnerabilidades em diversas plataformas, sistemas operacionais, e servidores. Este *framework* deve ser utilizado com cuidado e somente para fins éticos. (VIEIRA, 2009).

3.1.9. Protocolos e Portas

Os protocolos servem para identificar qual tipo de informação é trafegado pela rede, para que assim haja uma padronização entre os dados transmitidos. (GALLO, 2003). Alguns dos protocolos utilizados nas redes são:

TCP: Este protocolo é utilizado para o envio de pacotes na internet, além de garantir de que eles foram entregues ao destino correto. O protocolo UDP é muito parecido com o TCP, porém não se certifica que o pacote foi recebido, deixando o processo mais rápido.(FOROUZAN, 2009) (COMER, 2015).

SMB: Trata-se de um protocolo de compartilhamento de arquivos em rede, o qual permite que os aplicativos de um computador façam leitura e gravação em arquivos e que possam solicitar serviços de programas do servidor dentro de uma rede de computadores. (BARREIROS).

As portas estão vinculadas aos protocolos, desse modo o as portas são o caminho em que cada protocolo passa para a que seja entregue cada tipo de informação.

3.2. Materiais e Métodos

O Kali Linux é a principal ferramenta utilizada no projeto. Ela trata-se de um sistema operacional Linux, baseado no Debian, que foi desenvolvido pela equipe da Offensive Security. No Kali é possível encontrar mais de 300 ferramentas de testes de invasão, penetração, força bruta, forense entre outras.

Ele costuma ser muito utilizada por hackers, pentesters, analistas e auditores de segurança da informação. Uma curiosidade deste sistema, é que ele não é nada mais que uma substituição ou evolução do BackTrack, que tratava-se de um sistema operacional baseado no Ubuntu, e tinha o mesmo objetivo de construção.

É interessante ressaltar que, o Kali Linux é um sistema gratuito, fácil de manusear, e é extremamente confiável. Além disso, ele possui, entre outras, todas as ferramentas já citadas e que são utilizadas neste trabalho. (BROAD, 2017).

3.3. Etapas Desenvolvidas

O desenvolvimento deste trabalho baseia-se na execução das cinco fases do Pentest. Isto é, inicialmente deve-se realizar a busca de informações. Em seguida é feito a enumeração dos serviços. A próxima etapa busca identificar as vulnerabilidades para que na fase seguinte elas possam ser validadas. Por fim, é proposto um relatório com as informações obtidas.

Neste sentido, as seções 3.3.1, 3.3.2 e 3.3.3 descrevem a primeira fase do pentest: o levantamento de informações. Para isto, foram utilizadas as ferramentas descritas na seção 3.1.7.

3.3.1. Análise do NTI

A primeira coleta foi realizada no NTI, que teve obrigatoriamente a instalação do Kali Linux e do auxílio de ferramentas como o ZenMap e o NetDiscover. A execução desta fase é descrita em etapas denominadas "Passos". Esta abordagem

foi utilizando a fim de que todo o trabalho possa ser reproduzido pelos profissionais de TI do Campus Paranaguá. Os passos são descritos a seguir.

1º PASSO: Utilizando uma máquina localizada no NTI com o Kali Linux instalado, foi possível obter o IP do gateway.

```
root@kali-nti:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.20.4.135  netmask 255.255.255.0  broadcast
10.20.4.255
        inet6 fe80::dad3:85ff:fe6d:264  prefixlen 64  scopeid
0x20<link>
        ether d8:d3:85:6d:02:64  txqueuelen 1000  (Ethernet)
        RX packets 5144  bytes 513087 (501.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77  bytes 10121 (9.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0
collisions 0
        device interrupt 18

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Loopback Local)
        RX packets 4  bytes 156 (156.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 156 (156.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0
collisions 0

root@kali-nti:~# route -n
Tabela de Roteamento IP do Kernel
Destino         Roteador        MÃ¡scaraGen.    OpÃ§Ãµes
MÃ©trica Ref    Uso Iface
0.0.0.0         10.20.4.1       0.0.0.0         UG    100    0
0 eth0
10.20.4.0       0.0.0.0         255.255.255.0   U     100    0
0 eth0
```

Figura 1 - IP Gateway

Como pode ser visto em destaque na Figura 1, utilizando inicialmente o comando “ifconfig” foi obtido informações sobre as configurações de rede da máquina, em seguida foi utilizado o comando "route -n". Este comando retornou informações sobre o endereço IP do gateway da rede, identificado como 10.20.4.1.

2º PASSO: A ferramenta Zenmap foi usada para fazer varreduras no IP 10.20.4.1, obtido no passo 1. A partir disso, é possível encontrar portas abertas no gateway da rede, são elas:

- **Porta 22/TCP**

- Padrão: SSH - Usada para logins seguros, transferência de arquivos e redirecionamento de porta.
- Serviço: ssh
- Versão: OpenSSH 7.2 (protocol 2.0)

- **Porta 53/TCP**

- Padrão: DNS
- Serviço: Domain
- Versão: (generic dns response: NOTIMP)

- **Porta 10000/TCP**

- Padrão: NDP, é um protocolo destinado a transportar dados entre dispositivos NAS e dispositivos de backup. Porém, neste caso estava sendo utilizado por uma aplicação web.
- Serviço: ssl/http nginx e snet-sensor-mgmt

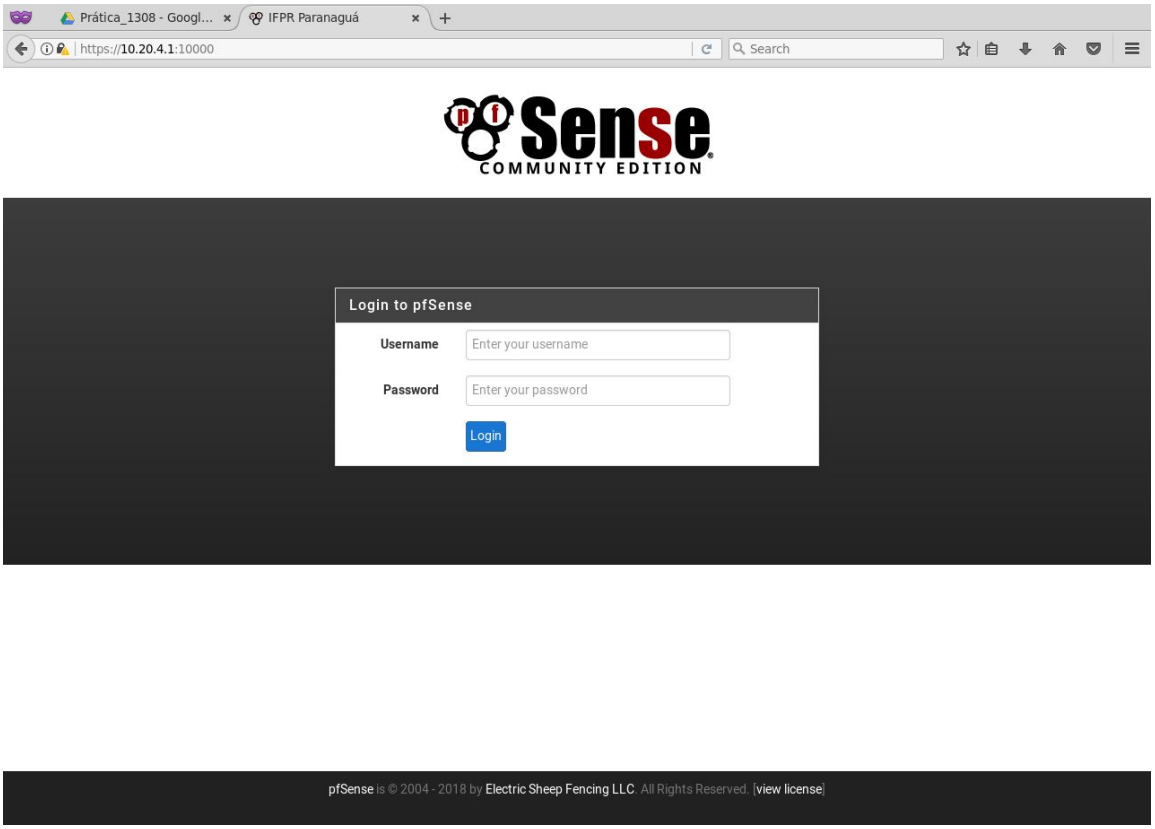


FIGURA 2 - Interface do PfSense

Na Figura 2, a porta 10000 está aberta com a página direcionada para um login de uma aplicação web. Trata-se de um *Firewall open source* chamado PfSense Community Edition. Pode-se, portanto, deduzir que a porta não está sendo utilizada da forma padrão propositalmente.

- **Porta 53/UDP**

- Padrão: DNS
- Serviço: Domain
- Versão: (generic dns response: NOTIMP)

- **Porta 123/UDP**

- Padrão: NTP
- Serviço: NTP
- Versão: NTP v4.2.8p8@1.3265-o (secondary server)

- **Porta 67/UDP**
- Padrão: BOOTP server; também utilizada por DHCP
- Serviço: dhcps?
- Versão: ?

Após efetuar a varredura no gateway pode-se encontrar os serviços que atendem nas portas aberta. Isto não representa, necessariamente, um risco. Contudo, são a partir destas informações que um usuário mal intencionado pode iniciar a exploração de vulnerabilidades da rede.

Em seguida, foi continuada a busca por informações sobre a rede, descrita no passo 3.

3º PASSO: Utilizando a ferramenta NetDiscover no NTI, foi realizada a varredura da rede local e dois IPs ganharam destaque (vide Figura 3):

```
| Currently scanning: Finished!   |   Screen View: Unique Hosts

 575 Captured ARP Req/Rep packets, from 8 hosts.   Total size:
34500

_____________________________________________________________________
_____________
   IP            At MAC Address     Count     Len  MAC Vendor /
Hostname
 -----------------------------------------------------------------
-------------
 10.20.2.254     00:1f:45:b2:dd:df    535   32100  Enterasys
 10.20.2.1       2c:76:8a:bb:e6:3b      5     300  Hewlett
Packard
 10.20.2.4       78:2b:cb:6e:3d:79      1      60  Dell Inc.
 10.20.2.15      d8:d3:85:6d:02:b0      1      60  Hewlett
Packard
 10.20.2.16      a4:5d:36:2a:9e:98      1      60  Hewlett
Packard
 10.20.2.17      64:1c:67:7a:94:f6      1      60  DIGIBRAS
INDUSTRIA DO BRASIL
 10.20.2.50      2c:76:8a:bb:e9:99      1      60  Hewlett
Packard
 192.168.0.120   78:2b:cb:6e:3d:7b     30    1800  Dell Inc.
```

FIGURA 3 - Resultado da execução do NetDiscover no NTI.

A partir dos resultados obtidos pelo NetDiscover, foi possível explorar informações sobre os dois dispositivos cujos endereços IP são destacados na Figura 3. Eles são descritos a seguir.

10.20.2.254: Este IP se destaca por possuir mais acessos em comparação aos outros. A partir do endereço MAC[1] é possível identificar o fabricante do dispositivo (Enterasys). A marca Enterasys trata-se de uma companhia que oferece serviços e produtos na área de rede, tais como switchs e roteadores. (ENTERASYS, 2018).

A existência desse IP na varredura pode ser considerado preocupante. Isto é, a quantidade de tráfego direcionada ao equipamento sinaliza que ele é um concentrador de rede. Logo, se algum indivíduo mal intencionado com conhecimentos em informática descobrí-lo, poderá conseguir fazer ataques direcionados a ele. Para confirmar esse tráfego e obter mais informações sobre o equipamento, foi realizada outra varredura utilizando a ferramenta Zenmap, descritos no passo 4.

4º PASSO: Após realizar a varredura com o Zenmap no IP 10.20.4.254, foi obtido o resultado sobre portas abertas:

- **Porta 23/TCP**
- Padrão: Telnet
- Serviço: telnet
- Versão: Enterasys C2H124-48 switch telnetd

- **Porta 80/TCP**
- Padrão: World Wide Web HTTP
- Serviço: http
- Versão: Embedded HTTP Server (Enterasys C5124 switch http config)

- **Porta 161/UDP**
- Padrão: SNMP
- Serviço: snmp

- Versão: SNMPv1 server (public)

Os resultados indicam que além de receber muito tráfego, o dispositivo possui uma interface web que pode ser acessada na porta 80. A Figura 4 mostra a página web sendo acessada.

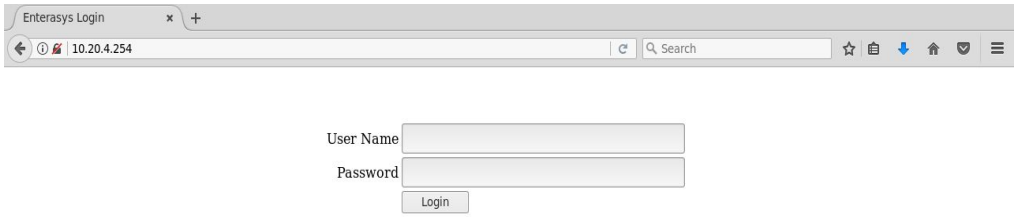


FIGURA 4 - Acesso a página web disponível no IP 10.20.4.254

Como foi visto na Figura 4, é possível ter acesso a uma página web que está em aberto, rodando no endereço IP 10.20.4.254.

192.168.0.120: Este IP não deveria aparecer na varredura da rede, visto que seu endereço foge ao escopo dos demais.

- 192.168.0.1

| Interface: eth0
| Version: 2
| Group: 224.0.0.2
| Description: All Routers on this Subnet

-

5º PASSO: Foi feita outra varredura no IP 192.168.0.120:

| 192.168.0.1
| Interface: eth0
| Version: 2

| Group: 224.0.0.2
| Description: All Routers on this Subnet

| 192.168.0.1
| Interface: eth0
| Version: 2
| Group: 239.255.255.250
| Description: Organization-Local Scope (rfc2365)

O resultado da varredura sobre o IP 192.168.0.120 não retornou informações úteis. Assim, ele foi descartado nas análises seguintes.

3.3.2. Análise do Laboratório 4

A fim de validar as informações obtidas na análise do NTI (seção 3.3.1), foi realizada a coleta de informações a partir do laboratório 4. Nesta etapa, foram realizados os mesmos passos que no NTI. Isto foi necessário para que pudessem ser realizadas as comparações das informações adquiridas de ambas as redes analisadas.

1° PASSO: Utilizando uma máquina do laboratório de informática com o Kali Linux instalado, foi possível obter o IP e o gateway:

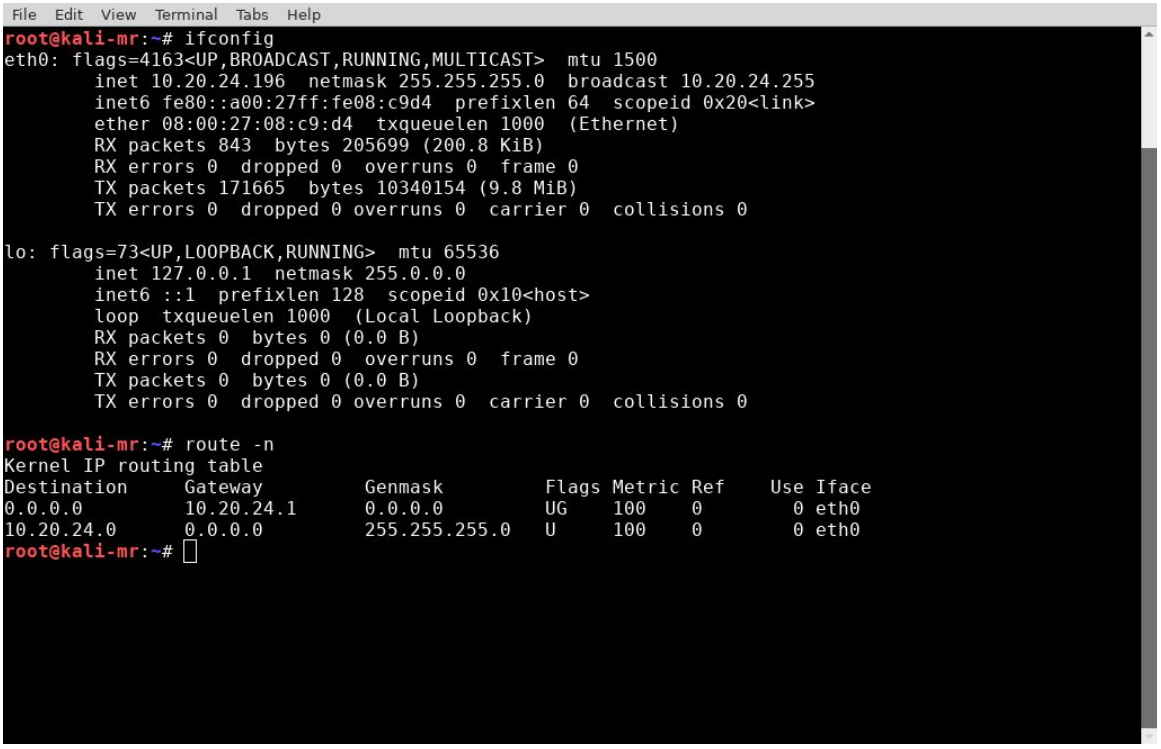


FIGURA 5 - Terminal

Como foi visto em uma das figuras anteriormente, a utilização do comando "route -n" novamente retornou informações sobre o endereço IP como mostra na Figura 5, identificado como 10.20.24.1. É importante salientar que a máscara de rede (255.255.255.0) indica que o IP 10.20.24.1 pertence a uma rede diferente da encontrada no NTI (10.20.4.0/24).

2º PASSO: A ferramenta Zenmap foi usada para fazer varreduras no IP 10.20.24.1, gateway da rede. A partir disso, chegamos ao resultado sobre portas abertas:

- **Porta 22/TCP**

- Padrão: SSH
- Serviço: ssh
- Versão: OpenSSH 7.2 (protocol 2.0)

- **Porta 53/TCP**

- Padrão: DNS
- Serviço: Domain

- Versão:

- **Porta 10000/TCP**
- Padrão: NDP
- Serviço: ssl/http nginx e snet-sensor-mgmt

- **Porta 53/UDP**
- Padrão: DNS
- Serviço: Domain
- Versão: ZyXEL P-660HW-D1 wireless ADSL router dnsd

- **Porta 123/UDP**
- Padrão: NTP
- Serviço: NTP
- Versão: NTP v4.2.8p8@1.3265-o (unsynchronized)

- **Porta 67/UDP**
- Padrão: BOOTP server, também utilizada por DHCP
- Serviço: dhcps?
- Versão: ?

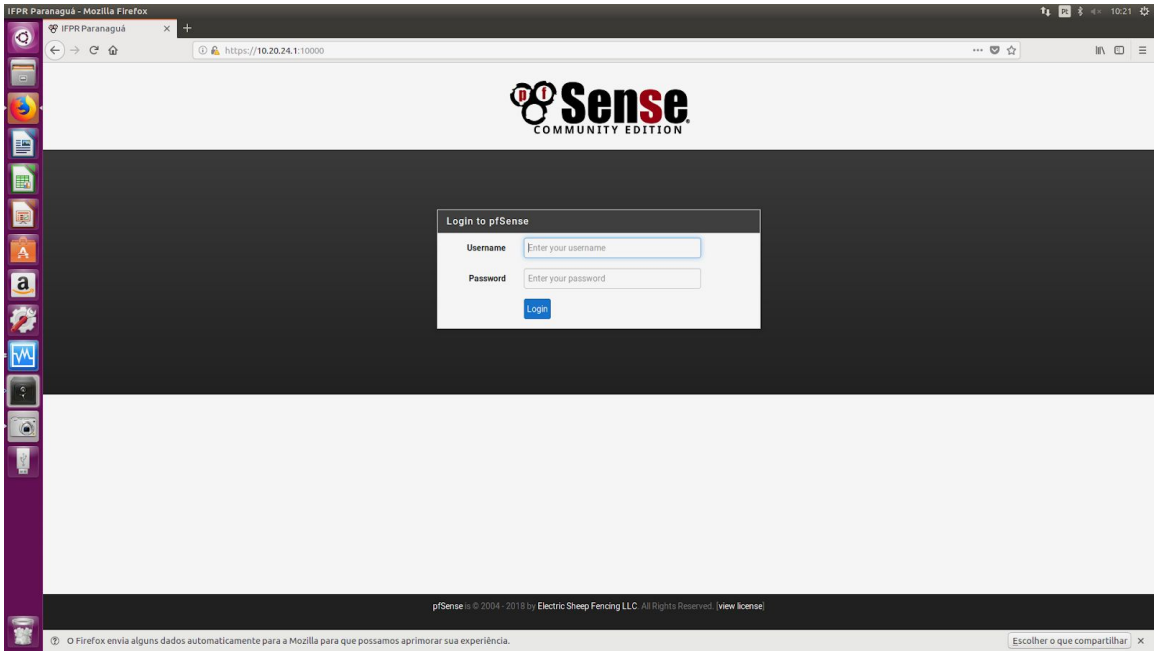


FIGURA 6 - Interface do PfSense

É possível notar que os resultados obtidos na execução do Zenmap a partir do Laboratório 4 retornam as mesmas informações obtidas no NTI. Assim, pode-se afirmar que trata-se do mesmo equipamento que atua como gateway. A Figura 6 mostra a mesma interface web disponível no Laboratório 4 e no NTI.

3º PASSO: Utilizando a ferramenta NetDiscover no Laboratório 4, foi descoberto o IP:

```
_____________________________________________________________________
_____________
   IP            At MAC Addr^Cs     Count     Len  MAC Vendor /
Hostname
root@kali-mr:
~# ---------------------------------------------------------------
-
 10.20.24.1      2c:76:8a:bb:e6:3b  36219 2173140  Hewlett
Packard
 10.20.24.112    28:f1:0e:fc:ca:53     11     660  Dell Inc.
 10.20.24.101    28:f1:0e:fc:c8:e9      2     120  Dell Inc.
 10.20.24.111    28:f1:0e:fc:c8:d4      1      60  Dell Inc.
 10.20.24.120    28:f1:0e:fc:c8:e2      5     300  Dell Inc.
 10.20.24.183    28:f1:0e:fc:c7:9f      5     300  Dell Inc.
 10.20.24.254    00:1f:45:b2:dd:df      4     240  Enterasys
 10.20.24.103    28:f1:0e:fc:c9:fd      4     240  Dell Inc.
 10.20.24.119    28:f1:0e:fc:c0:8f      5     300  Dell Inc.
 10.20.24.104    28:f1:0e:fc:c4:98      4     240  Dell Inc.
 10.20.24.106    28:f1:0e:fc:c8:74      4     240  Dell Inc.
 10.20.24.105    28:f1:0e:fc:c8:c5     10     600  Dell Inc.
 10.20.24.113    28:f1:0e:fc:c0:b3      4     240  Dell Inc.
 10.20.24.114    28:f1:0e:fc:c8:f2      7     420  Dell Inc.
 10.20.24.115    28:f1:0e:fc:c8:f0      6     360  Dell Inc.
 10.20.24.118    28:f1:0e:fc:c4:6a      2     120  Dell Inc.
 10.20.24.107    28:f1:0e:fc:c7:cc      4     240  Dell Inc.
```

FIGURA 7 - Interface NetDiscover

É possível visualizar na Figura 7 a varredura realizada na rede através do uso da ferramenta NetDiscover, localizada em uma das máquinas do Laboratório 4. Na figura pode-se confirmar o endereço 10.20.24.1 como concentrador de rede devido ao grande número de pacotes destinados a ele.

Além do IP do gateway, pode-se notar a existência do IP 10.20.24.254, apontado pelo NetDiscover como da marca Enterasys. Isto significa que trata-se do mesmo equipamento encontrado a partir das varreduras feitas no NTI. Para confirmar esta hipótese, foi executado o passo 4, descrito a seguir.

4º PASSO: A ferramenta Zenmap foi usada para fazer varreduras desta vez no IP 10.20.24.254. A partir disso, chegamos ao resultado de que algumas portas estão abertas:

- **Porta 23/TCP**
- Padrão: Telnet
- Serviço: telnet
- Versão: Enterasys C2H124-48 switch telnetd

- **Porta 80/TCP**
- Padrão: World Wide Web HTTP
- Serviço: http
- Versão: Embedded HTTP Server (Enterasys C5124 switch http config)

- **Porta 161/UDP**
- Padrão: SNMP
- Serviço: snmp
- Versão: SNMPv1 server; Enterasys Networks SNMPv3 server (public)

broadcast-igmp-discovery:
| 10.20.24.254
| Interface: eth0

| Version: 2
| Group: 224.0.0.1
| Description: All Systems on this Subnet (rfc1112)

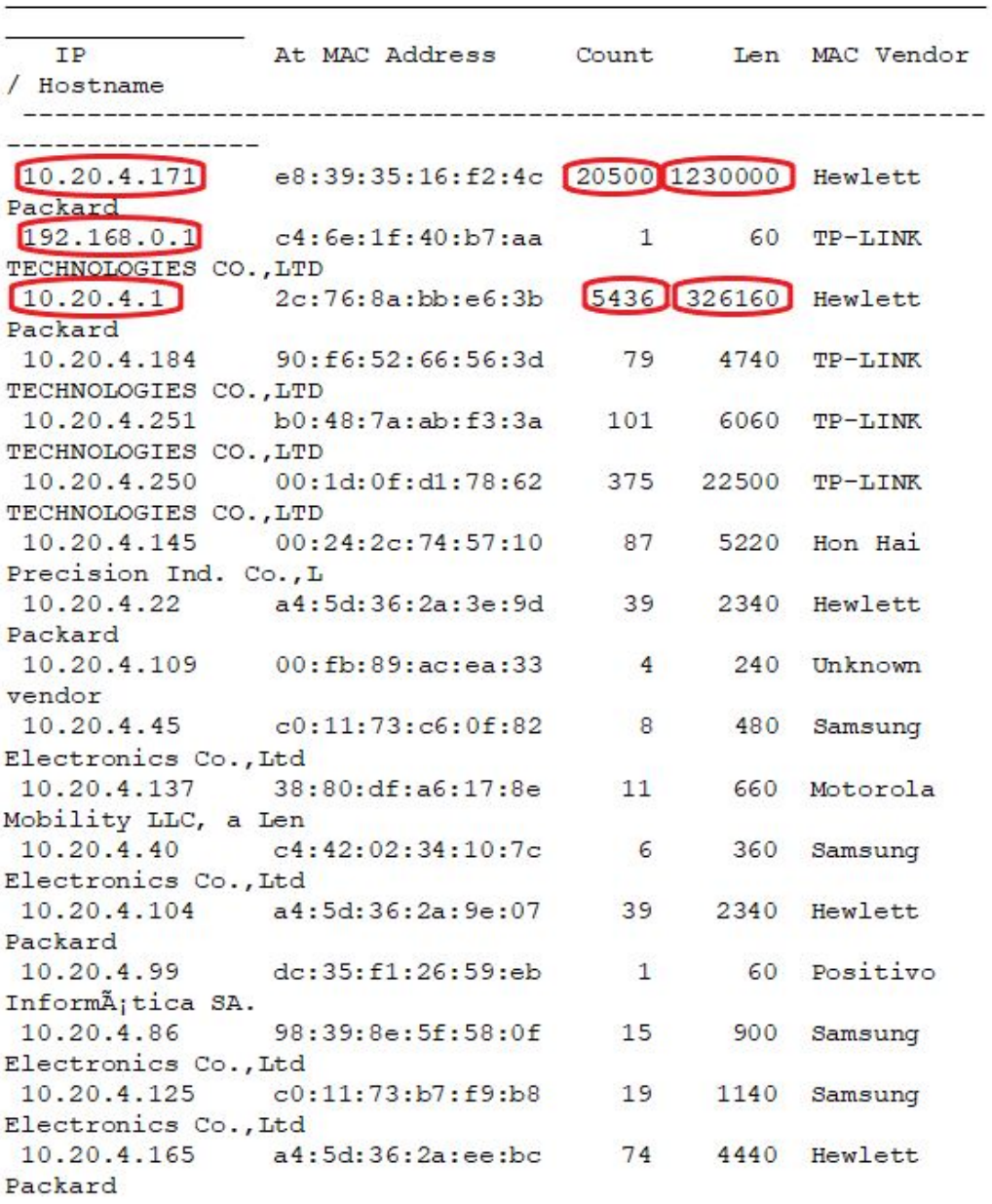
broadcast-ping:

| IP: 10.20.24.254 MAC: 00:1f:45:b2:dd:df

3.3.3. Confirmação das Informações do NTI

Os passos realizados no tópico 3.3.1 para a prática da análise do NTI foram refeitos, para haver a confirmação dos dados obtidos. Nesta etapa, porém, um endereço apareceu e se destacou em meio aos outros no momento da execução dos testes.

1º PASSO: Uma nova varredura foi feita no NTI para confirmar as informações:



IP	At MAC Address	Count	Len	MAC Vendor / Hostname
10.20.4.171	e8:39:35:16:f2:4c	20500	1230000	Hewlett Packard
192.168.0.1	c4:6e:1f:40:b7:aa	1	60	TP-LINK TECHNOLOGIES CO.,LTD
10.20.4.1	2c:76:8a:bb:e6:3b	5436	326160	Hewlett Packard
10.20.4.184	90:f6:52:66:56:3d	79	4740	TP-LINK TECHNOLOGIES CO.,LTD
10.20.4.251	b0:48:7a:ab:f3:3a	101	6060	TP-LINK TECHNOLOGIES CO.,LTD
10.20.4.250	00:1d:0f:d1:78:62	375	22500	TP-LINK TECHNOLOGIES CO.,LTD
10.20.4.145	00:24:2c:74:57:10	87	5220	Hon Hai Precision Ind. Co.,L
10.20.4.22	a4:5d:36:2a:3e:9d	39	2340	Hewlett Packard
10.20.4.109	00:fb:89:ac:ea:33	4	240	Unknown vendor
10.20.4.45	c0:11:73:c6:0f:82	8	480	Samsung Electronics Co.,Ltd
10.20.4.137	38:80:df:a6:17:8e	11	660	Motorola Mobility LLC, a Len
10.20.4.40	c4:42:02:34:10:7c	6	360	Samsung Electronics Co.,Ltd
10.20.4.104	a4:5d:36:2a:9e:07	39	2340	Hewlett Packard
10.20.4.99	dc:35:f1:26:59:eb	1	60	Positivo InformÃ¡tica SA.
10.20.4.86	98:39:8e:5f:58:0f	15	900	Samsung Electronics Co.,Ltd
10.20.4.125	c0:11:73:b7:f9:b8	19	1140	Samsung Electronics Co.,Ltd
10.20.4.165	a4:5d:36:2a:ee:bc	74	4440	Hewlett Packard

FIGURA 8 - Resultado da execução da ferramenta NetDiscover no Laboratório 4.

Na Figura 8 é possível visualizar uma varredura realizada para a confirmação das informações no NTI em decorrência dos passos realizados anteriormente, através do uso da ferramenta NetDiscover. Existe, no entanto, um IP (10.20.4.171) que possuía muitos acessos. Para ele, foi realizado também algumas varreduras em busca de informações.

2º PASSO: Durante a varredura do IP 10.20.4.171 foram encontrados muitos acessos, o que pode ser considerado momentâneo. A ferramenta Zenmap encontrou algumas portas abertas neste IP.

- **Porta 139/TCP:**

- Padrão: NetBios
- Serviço: NETBIOS-SSN
- Versão: Microsoft Windows netbios-ssn

- **Porta 445/TCP:**

- Padrão: CIFS
- Serviço: MICROSOFT-DS
- Versão:Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: ADM.PGUA)

- **Porta 135/TCP:**

- Padrão: EPMAP
- Serviço: MSRPC
- Versão: Microsoft Windows RPC

- **Porta 49158/TCP:**

- Padrão: ?
- Serviço: MSRPC
- Versão: Microsoft Windows RPC

- **Porta 137/UDP:**

- Padrão: NetBios
- Serviço: NETBIOS-SSN
- Versão: Samba nmbd netbios-ns (workgroup: ADM)

- **Porta 42966/TCP:**

  - Padrão: ?

- Serviço: SSL/UNKNOWN
- Versão: ?

Os resultados da varredura mostraram um conjunto de portas abertas não vistas nos demais dispositivos analisados. Uma destas portas é a 445. Por padrão, o serviço que roda nesta porta é o SAMBA que implementa o protocolo SMB. Um serviço responsável pelo compartilhamento de arquivos em redes locais. Por conta desta característica, este serviço foi escolhido para ser estudado com mais detalhes.

3.3.4. Enumeração: Varredura do Protocolo SMB

Após finalizar a etapa de coleta de informações, foi iniciada a busca de vulnerabilidades (enumeração) seguida da etapa de validação. Como descrito, o serviço Samba, que implementa o protocolo SMB, pode ser encontrado especificamente em redes locais. Assim, os esforços foram direcionados para o serviço Samba e o protocolo SMB.

A literatura traz uma vulnerabilidade específica em relação ao protocolo SMB. Esta vulnerabilidade pode ser explorada por um ransomware, conhecido como Wannacry (TECHNET, 2018). O Wannacry trata-se de um ransomware que é definido como “sequestrador” de arquivos de máquinas assim que os criptografam, e em seguida pedem dinheiro para devolver os arquivos junto de toda a extensão. No ano de 2017, o Wannacry derrubou mais de 200 mil máquinas. (TECHTUDO, 2017).

Partindo desta premissa, foram elaborados um conjunto de passos em busca da vulnerabilidade no protocolo SMB na rede local e que pode ser explorada pelo wannacry. O objetivo desta etapa é enumerar a vulnerabilidade e testá-la.

Para a realização dos testes, inicialmente é proposto a validação da vulnerabilidade via Zenmap, descrita nos passos a seguir.

1° PASSO: Copiar o código que se encontra na página do Git Hub (https://github.com/cldrn/nmap-nse-scripts/blob/master/scripts/smb-vuln-ms17-010.nse) e salvar com o nome (smb-vuln-ms17-010)) em um bloco de notas na área de trabalho. Altere a sua extensão de txt para nse.

2º PASSO: Com o Zenmap já aberto, aperte em Perfil localizado na parte superior lado esquerdo e selecione a opção New Profile or Command.

3° PASSO: Em Nome do perfil, escreva **wannacry vscan windows**. Na aba em cima aperte em Scripting, depois em Add.

4º PASSO: Selecione o arquivo que foi salvo na área de trabalho e aperte em Abrir. É muito importante conferir se a extensão está mesmo como nse, aperte em Save Changes. Agora pode utilizá-lo quando for escolher o perfil no Zenmap.

3.3.5. Validação: Varredura da rede com o Wannacry VSCAN Windows

Para a obtenção das vulnerabilidades localizadas no serviço do Samba (protocolo SMB), foi utilizada a sequência de passos anteriores no tópico 3.3.4, em conjunto com a ferramenta Zenmap.

1° PASSO: Foi feita uma varredura na Super Rede para ter uma visão macro da rede local. Assim é buscado saber quais são as sub-redes que se encontram em 20.20.0.0/16 e se algum dispositivo nesta rede possui o serviço Samba rodando. Após a execução da varredura, identificou-se alguns dispositivos na sub-rede 10.20.2.0/24 que possuíam a porta 445 aberta (porta do SMB).

2º PASSO: A sub-rede escolhida foi a 10.20.2.0/24, na mesma, todos os hosts foram verificados pela varredura na busca de quais são as portas abertas e de qual o IP específico está relacionado. Ao final, foi obtida a informação de que a vulnerabilidade ms17-010 foi identificada. O resultado é mostrado na Figura 9.

Host script results:
| smb-vuln-ms17-010):
| VULNERABLE:
| Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
| State: VULNERABLE

```
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_
```

Figura 9. Resultado da varredura Wannacry VSCAN Windows.

3º PASSO: A partir dessa etapa, foi escolhido um host (não divulgado por questões de segurança) em específico para validar a vulnerabilidade. Para isso, estudos foram realizados sobre ferramentas de exploração da vulnerabilidade ms17-010, que existe apenas para o sistema operacional Windows.

4º PASSO: Após a escolha do host e o estudo das ferramentas, foi identificado a possibilidade de exploração a partir da ferramenta metasploit framework. A sequência de comandos utilizados para explorar a vulnerabilidade não é descrito aqui por questões de segurança e sigilo. Contudo, toda a execução bem como os comandos executados foram relatados para os profissionais da área de T.I do Campus.

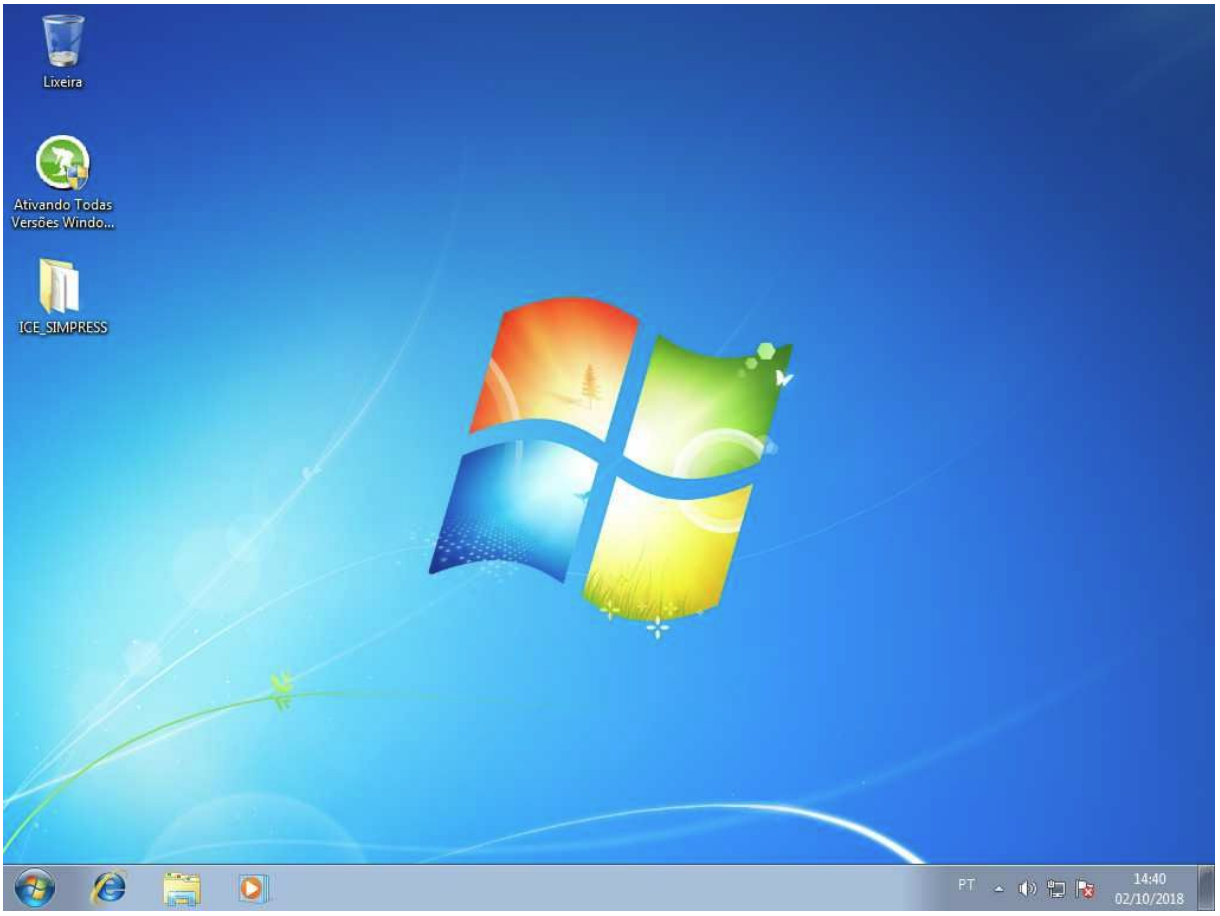


FIGURA 9 - Host Acessado

A Figura 10 mostra um print retirado de uma máquina em que se teve acesso remotamente, porém nenhum dado foi interceptado ou alterado neste trabalho, e qualquer tipo de atividade neste sentido é crime segundo o Art. 154A do Código Penal - Decreto Lei 2848/40

3.4. Relatório: Propostas de Correção

Uma das sugestões mais simples que é possível dar ao usuário é que seja realizada a atualização do Windows, principalmente se esta se referindo ao Windows XP ou Windows 7, pois são versões já ultrapassadas com vulnerabilidades conhecidas. Além disso, outras forma de proteção podem ser feitas por meio de softwares específicos para tal função.

A Microsoft propõe como solução alternativa para essa vulnerabilidade, desabilitar o SMBv1, seguindo os seguintes passos (que são encontrados no site da própria Microsoft) (MS17-010, 2018):

- **Para os sistemas operacionais de uso cliente:**

1. De início abra o Painel de Controle, depois clique em Programas e em seguida Ativar ou desativar recursos do Windows.
2. Abra a janela de Recursos de Windows e desmarque a caixa de seleção Suporte a Compartilhamento de Arquivos SMB1.0/CIFS e em seguida clique em OK para fechar a janela.
3. Por fim, reinicie o sistema.

- **Para os sistemas operacionais de uso servidor:**

1. De início abra o Gerenciador de Servidor, depois clique no menu Gerenciar e em seguida selecione Remover Funções e Recursos.
2. Abra a Janela de Recursos e depois desmarque a caixa de seleção Suporte a Compartilhamento de Arquivos SMB1.0/CIFS e em seguida clique em OK para fechar a janela.
3. Por fim, reinicie o sistema.

- **Impacto que o sistema sofrerá com a solução alternativa:** O protocolo SMBv1 será desabilitado.

- **Como desfazer esta solução alternativa:** Refaça todos os passos da solução alternativa, ao invés de restaurar o recurso de Suporte a Compartilhamento de Arquivos SMB1.0/CIFS para torná-lo ativo. (MS17-010, 2018**)**

3.5. Comparativos Gerais dos Resultados Obtidos

Os passos realizados no NTI e no laboratório 4 foram iguais, para que fosse possível observar e fazer comparações entre as duas redes. Um ponto a ser ressaltado foi que todas as portas abertas se mostraram as mesmas, contudo encontram-se em diferentes redes. Assim, pode-se concluir que esses IPs são destinados para o dispositivo de rede. O laboratório 4 está a disposição dos alunos, então se alguém com más intenções quiser tentar comprometer a rede, terá acesso

às informações necessárias para tal, como no NTI. Isso ficou evidente ao obter acesso em um dispositivo a partir do NTI, conforme relatado na seção 3.3.5.

3.6. Comparativo entre Previsto e Realizado

O escopo deste trabalho é analisar falhas de segurança existentes na rede do campus e propor soluções, então isso foi cumprido, pois uma falha foi identificada em meio de diversas varreduras realizadas e foram propostas soluções para solucioná-la.

3.7. Lições Aprendidas

Todos esses anos na instituição nos tornaram pessoas mais responsáveis e com a realização deste trabalho estudos sobre conceitos e ferramentas foram necessários. Mesmo tenhamos decidido não seguir na área, esse conhecimento obtido relacionado a informática em geral e mais especialmente em redes que é o foco do nosso TCC, não será desperdiçado, pois lembraremos disso por muito tempo já que a nossa realidade nos faz utilizar destas informações diariamente.

3.8. Trabalhos Futuros

As sugestões que forem sugeridas podem ser implementadas futuramente pelos técnicos do campus dentro da rede, ou pode ser o tema de algum outro Trabalho de Conclusão de Curso.

4. CONSIDERAÇÕES FINAIS

A escolha de desenvolver um trabalho voltado para a área de segurança desde o início foi em prol da melhoria da rede de uma instituição renomada como o IFPR Campus Paranaguá. Concordamos desde o princípio que queríamos defender algo que fosse reutilizado, portanto, nós temos muito a agradecer aos técnicos do Campus, Rodrigo e Antônio pela oportunidade que nos proporcionou.

Desenvolver um trabalho como o de conclusão de curso não é nenhum pouco simples, o caminho é árduo. Foram horas de pesquisas, estresse e até um pouco de desespero. Mas tudo se encaminha bem quando têm-se um bom orientador e uma ótima dupla ao lado. O nosso trabalho tem grande importância não só no campus, como nas nossas vidas. Crescemos e lidamos com a responsabilidade de correr atrás e até brigar quando necessário.

A boa relação que mantemos desde o início do projeto foi o essencial para que no fim desse certo. Iniciar varreduras e encontrar as vulnerabilidades, lidar com a frustração dos resultados negativos e vibrar com cada um dos positivos, testar uma nova ferramenta, aprender a mexer e conhecer um pouco mais sobre o novo. Adquirir experiência.

Com todo o nosso coração, concluímos que o Instituto nos fez pessoas melhores, nos preparou para enfrentar a vida e todos os demônios que ela nos apresenta. O nosso TCC tem uma grande parcela de culpa nisso, o desenvolvimento desse trabalho nos trouxe grandes aprendizados em todos os sentidos possíveis. Hoje, ficamos felizes em colaborar para que os técnicos tenham acesso às falhas de segurança dentro da rede e de ter tido força para conseguirmos enfrentar cada obstáculo que a vida colocou em nosso caminho.

A vitória é nossa.

REFERÊNCIAS

ALMEIDA, José Maria Fernandes de. **Breve história da Internet**. 2005.

ARPING. <https://github.com/ThomasHabets/arping>, Acesso em: 01 ago. 2018.

BARBOSA, M. B.. **Segurança da Informação**. Departamento de Informática Universidade do Minho, 2006/2007.

BARREIROS, Caio Carone. **Redes de Computadores I: Samba**. UFRJ <https://www.gta.ufrj.br/grad/01_2/samba/samba.htm>, Acesso em: 01 out. 2018.

BERTOLÍN, Javier Areitio et al. **Seguridad de la información. Redes, informática y sistemas de información**. Editorial Paraninfo, 2008.

MS17-010 - Boletim de Segurança da Microsoft – Crítico: <https://docs.microsoft.com/pt-br/security-updates/securitybulletins/2017/ms17-010> Acesso em: 23 out. 2018

BROAD, James; BINDNER, Andrew. **Hacking com Kali Linux: Técnicas práticas para testes de invasão**. Novatec Editora, 2017.

COMER, Douglas. **Interligação de Redes com TCP/IP–: Princípios, Protocolos e Arquitetura**. Elsevier Brasil, 2015.

DELFINO, Pedro. **27 ferramentas para hackers que podem ser usadas no Kali Linux (PARTE 1)**: <http://e-tinet.com/linux/27-ferramentas-hackers-kali-linux-parte-1/>, Acesso em: 25 fev. 2018

DELFINO, Pedro. **30 ferramentas para hackers que podem ser usadas no Kali Linux (PARTE 2)**: <http://e-tinet.com/linux/30-ferramentas-para-hackers-kali-linux/>, Acesso em: 25 fev. 2018

DO ESPÍRITO SANTO, Adrielle Fernanda Silva. **Segurança da Informação**. 2010

DOS SANTOS, Ivanilton Quinto; GULO, Carlos ASJ. **Segurança da Informação**. 2017.

ENTERASYS.<https://br.extremenetworks.com/produtos/>, Acesso em: 13 ago. 2018.

FONTES, Edison. **Praticando a segurança da informação**. Brasport, 2008.

FOROUZAN, Behrouz A.; FEGAN, Sophia Chung. **Protocolo TCP/IP-3**. AMGH Editora, 2009.

GALLO, Michael A. et al. **Comunicação entre computadores e tecnologias de rede**. Pioneira Thomson Learning, 2003.

HPING. <http://www.hping.org/>, Acesso em: 01 ago. 2018.

JUNIOR, Helio Bertolini et al. **Segurança da Informação**. In: Anais do Congresso Nacional Universidade, EAD e Software Livre. 2009.

KUROSE, James F.; ROSS, Keith W. **Redes de Computadores e a Internet**. Uma nova, 2006.

MARCIANO, João Luiz Pereira; LIMA-MARQUES, Mamede. **O enfoque social da segurança da informação**. Ciência da Informação, v. 35, n. 3, 2006.

MIRANDA. <https://tools.kali.org/information-gathering/miranda>, Acesso em: 01 ago. 2018.

MORIMOTO, Carlos Eduardo. **Redes, Guia Prático: Ampliada e Atualizada**. Porto Alegre. Sul Editores. 2011.

MUNHOZ, Vinicius. **TECHTUDO: WannaCry, o ransomware que fez o mundo chorar na sexta-feira (12)**:

<https://www.tecmundo.com.br/virus/13275-ransomware-conheca-o-invasor-que-sequestra-o-computador.htm>, Acesso em: 15 out. 2018.

NETCAT. <http://netcat.sourceforge.net/>, Acesso em: 01 ago. 2018.

NETDISCOVER. <https://github.com/alexxy/netdiscover>, Acesso em: 01 ago. 2018.

NETSTAT. <https://github.com/ecki/net-tools/blob/master/netstat.c>, Acesso em: 01 ago. 2018.

NMAP. <https://nmap.org/>, Acesso em: 01 ago. 2018.

PEIXINHO, IVO DE CARVALHO. **Introdução à Segurança de Redes**. Rio de Janeiro: RNP/ESR, 2013.

ROSS, Julio. **Redes de computadores**. Julio Ross, 2008.

SILVA, Fabio. **PFSENSE, Firewall gratuito e poderoso**: <https://fabiosilva.com.br/2016/04/25/pfsense-firewall-gratuito-e-poderoso/>. Acesso em: 10 set. 2018.

SOUSA, Lindeberg Barros. **Redes de computadores**. Dados Voz e Imagem, 2009.

TECHNET, Wannacry attacks, 2018. <https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/> Acesso em: 15 out. 2018.

VIEIRA, Luiz. **Viva o Linux.** <https://www.vivaolinux.com.br/artigo/Metasploit-Framework> Acesso em: 02. dez. 2018.

WIRESHARK. <https://www.wireshark.org/>, Acesso em: 01 ago. 2018.

ZENMAP. <https://zmap.io/>, Acesso em: 01 ago. 2018.

APÊNDICE E/OU ANEXOS

wannacry vscan windows - Sub-Rede (10.20.2.1-254)

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-02 12:54 -03
NSE: Loaded 44 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 12:54
Completed NSE at 12:54, 0.00s elapsed
Initiating NSE at 12:54
Completed NSE at 12:54, 0.00s elapsed
Initiating Ping Scan at 12:54
Scanning 254 hosts [4 ports/host]
Completed Ping Scan at 12:54, 4.21s elapsed (254 total hosts)
Initiating Parallel DNS resolution of 254 hosts. at 12:54
Completed Parallel DNS resolution of 254 hosts. at 12:54, 0.00s elapsed
Nmap scan report for 10.20.2.2 [host down]
Todos os endereços se encontram na mesma situação [host down]...
Nmap scan report for 10.20.2.253 [host down]
Initiating SYN Stealth Scan at 12:54
Scanning 11 hosts [1000 ports/host]
Discovered open port 445/tcp on 10.20.2.5
Discovered open port 445/tcp on 10.20.2.12
Discovered open port 445/tcp on 10.20.2.15
Discovered open port 445/tcp on 10.20.2.7
Discovered open port 445/tcp on 10.20.2.6
Discovered open port 80/tcp on 10.20.2.12
Discovered open port 445/tcp on 10.20.2.4
Discovered open port 445/tcp on 10.20.2.16
Discovered open port 80/tcp on 10.20.2.17
Discovered open port 53/tcp on 10.20.2.1
Discovered open port 111/tcp on 10.20.2.4
Discovered open port 111/tcp on 10.20.2.50
Discovered open port 22/tcp on 10.20.2.1
Discovered open port 22/tcp on 10.20.2.16
Discovered open port 22/tcp on 10.20.2.4
Discovered open port 22/tcp on 10.20.2.50
Discovered open port 3389/tcp on 10.20.2.12
Discovered open port 3389/tcp on 10.20.2.5
Discovered open port 23/tcp on 10.20.2.254
Discovered open port 21/tcp on 10.20.2.16
Discovered open port 135/tcp on 10.20.2.12
Discovered open port 135/tcp on 10.20.2.15
Discovered open port 135/tcp on 10.20.2.5
Discovered open port 135/tcp on 10.20.2.7
```

Discovered open port 5900/tcp on 10.20.2.15
Discovered open port 135/tcp on 10.20.2.6
Discovered open port 139/tcp on 10.20.2.5
Discovered open port 139/tcp on 10.20.2.4
Discovered open port 139/tcp on 10.20.2.12
Discovered open port 5900/tcp on 10.20.2.16
Discovered open port 139/tcp on 10.20.2.7
Discovered open port 139/tcp on 10.20.2.15
Discovered open port 5900/tcp on 10.20.2.50
Discovered open port 443/tcp on 10.20.2.12
Discovered open port 139/tcp on 10.20.2.6
Discovered open port 139/tcp on 10.20.2.16
Discovered open port 80/tcp on 10.20.2.254
Discovered open port 10000/tcp on 10.20.2.16
Discovered open port 27000/tcp on 10.20.2.5
Discovered open port 27000/tcp on 10.20.2.7
Discovered open port 25735/tcp on 10.20.2.6
Discovered open port 2103/tcp on 10.20.2.12
Discovered open port 1801/tcp on 10.20.2.12
Discovered open port 49153/tcp on 10.20.2.12
Discovered open port 49153/tcp on 10.20.2.5
Discovered open port 49153/tcp on 10.20.2.7
Discovered open port 49153/tcp on 10.20.2.15
Discovered open port 2107/tcp on 10.20.2.12
Discovered open port 49153/tcp on 10.20.2.6
Discovered open port 25734/tcp on 10.20.2.6
Discovered open port 49167/tcp on 10.20.2.7
Discovered open port 49167/tcp on 10.20.2.5
Discovered open port 49158/tcp on 10.20.2.15
Discovered open port 49155/tcp on 10.20.2.7
Discovered open port 49155/tcp on 10.20.2.5
Discovered open port 49155/tcp on 10.20.2.15
Discovered open port 49155/tcp on 10.20.2.6
Discovered open port 5357/tcp on 10.20.2.7
Discovered open port 5357/tcp on 10.20.2.15
Discovered open port 5357/tcp on 10.20.2.5
Discovered open port 5357/tcp on 10.20.2.6
Discovered open port 902/tcp on 10.20.2.50
Discovered open port 901/tcp on 10.20.2.4
Discovered open port 49154/tcp on 10.20.2.12
Discovered open port 49154/tcp on 10.20.2.7
Discovered open port 7070/tcp on 10.20.2.12
Discovered open port 49152/tcp on 10.20.2.12
Discovered open port 49152/tcp on 10.20.2.7

Discovered open port 1947/tcp on 10.20.2.15
Discovered open port 49154/tcp on 10.20.2.5
Discovered open port 49154/tcp on 10.20.2.15
Discovered open port 49154/tcp on 10.20.2.6
Discovered open port 49152/tcp on 10.20.2.5
Discovered open port 49152/tcp on 10.20.2.15
Discovered open port 49152/tcp on 10.20.2.6
Discovered open port 49157/tcp on 10.20.2.15
Discovered open port 49157/tcp on 10.20.2.6
Discovered open port 49156/tcp on 10.20.2.12
Discovered open port 49156/tcp on 10.20.2.6
Discovered open port 6006/tcp on 10.20.2.12
Discovered open port 8081/tcp on 10.20.2.12
Discovered open port 49160/tcp on 10.20.2.12
Discovered open port 5800/tcp on 10.20.2.50
Discovered open port 2105/tcp on 10.20.2.12
Discovered open port 5800/tcp on 10.20.2.15
Discovered open port 5800/tcp on 10.20.2.16
Completed SYN Stealth Scan against 10.20.2.4 in 1.07s (10 hosts left)
Completed SYN Stealth Scan against 10.20.2.7 in 1.07s (9 hosts left)
Completed SYN Stealth Scan against 10.20.2.12 in 1.07s (8 hosts left)
Completed SYN Stealth Scan against 10.20.2.50 in 1.07s (7 hosts left)
Completed SYN Stealth Scan against 10.20.2.5 in 1.10s (6 hosts left)
Completed SYN Stealth Scan against 10.20.2.6 in 1.10s (5 hosts left)
Completed SYN Stealth Scan against 10.20.2.15 in 1.10s (4 hosts left)
Completed SYN Stealth Scan against 10.20.2.16 in 1.10s (3 hosts left)
Discovered open port 443/tcp on 10.20.2.17
Discovered open port 10000/tcp on 10.20.2.1
Discovered open port 902/tcp on 10.20.2.17
Discovered open port 427/tcp on 10.20.2.17
Discovered open port 8300/tcp on 10.20.2.17
Discovered open port 8000/tcp on 10.20.2.17
Completed SYN Stealth Scan against 10.20.2.1 in 20.24s (2 hosts left)
Discovered open port 9080/tcp on 10.20.2.17
Completed SYN Stealth Scan against 10.20.2.17 in 22.14s (1 host left)
Completed SYN Stealth Scan at 12:54, 24.49s elapsed (11000 total ports)
Initiating Service scan at 12:54
Scanning 93 services on 11 hosts
Service scan Timing: About 35.48% done; ETC: 12:56 (0:00:56 remaining)
Completed Service scan at 12:57, 169.26s elapsed (93 services on 11 hosts)
Initiating OS detection (try #1) against 11 hosts
Retrying OS detection (try #2) against 5 hosts
Retrying OS detection (try #3) against 3 hosts
Retrying OS detection (try #4) against 3 hosts

```
Retrying OS detection (try #5) against 3 hosts
Initiating Traceroute at 12:57
Completed Traceroute at 12:57, 0.03s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 12:57
Completed Parallel DNS resolution of 12 hosts. at 12:57, 0.00s elapsed
NSE: Script scanning 11 hosts.
Initiating NSE at 12:57
Completed NSE at 12:58, 31.61s elapsed
Initiating NSE at 12:58
Host is up (0.00039s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.5 (protocol 2.0)
53/tcp    open  domain   (generic dns response: NOTIMP)
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
10000/tcp open  ssl/http nginx
|_http-server-header: nginx
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.70%I=7%D=10/2%Time=5BB394D0%P=x86_64-pc-linux-gnu%r
(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x85\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03")%r(DNSStatusRequestTCP,E,"\0\x0c\0\0\x90\x04\0\0
SF:\0\0\0\0\0\0");
Warning: OSScan results may be unreliable because we could not find at least 1
open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Uptime guess: 0.002 days (since Tue Oct  2 12:55:52 2018)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros

TRACEROUTE (using port 53/tcp)
HOP RTT     ADDRESS
1   0.19 ms 10.20.2.1

Nmap scan report for 10.20.2.4
Host is up (0.00059s latency).
Not shown: 995 closed ports
```

```
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 5.5p1 Debian 6+squeeze3 (protocol 2.0)
111/tcp open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2           111/tcp  rpcbind
|   100000  2           111/udp  rpcbind
|   100024  1         38748/udp  status
|_  100024  1         52440/tcp  status
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: PGUA)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: PGUA)
901/tcp open  http        Samba SWAT administration server
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/2%OT=22%CT=1%CU=43025%PV=Y%DS=2%DC=
T%G=Y%TM=5BB395A
OS:1%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=105%TI=Z%II=I%TS=8
)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11N
W7%O5=M5B4ST11NW7%
OS:O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%
W6=16A0)ECN(R=Y%
OS:DF=Y%T=40%W=16D0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=4
0%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=
AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%
RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 101.974 days (since Fri Jun 22 13:35:41 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-ms17-010): This system is patched.

TRACEROUTE (using port 23/tcp)
HOP RTT     ADDRESS
1   0.25 ms 10.20.4.1
2   0.30 ms 10.20.2.4
```

```
Nmap scan report for 10.20.2.5
Host is up (0.00091s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
LABS)
3389/tcp  open  tcpwrapped
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
27000/tcp open  flexlm       FlexLM license manager
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49167/tcp open  msrpc        Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or
Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 102.871 days (since Thu Jun 21 16:04:27 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=265 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SERVERAUTOCAD; OS: Windows; CPE:
cpe:/o:microsoft:windows

Host script results:
| smb-vuln-ms17-010):
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

```
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

TRACEROUTE (using port 23/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 10.20.2.4
2   0.49 ms 10.20.2.5

Nmap scan report for 10.20.2.6
Host is up (0.0017s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
25734/tcp open  flexlm       FlexLM license manager
25735/tcp open  flexlm       FlexLM license manager
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or
Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 102.711 days (since Thu Jun 21 19:55:08 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: SOLIDWORKS; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-vuln-ms17-010):
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
```

```
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacr
ypt-attacks/

TRACEROUTE (using port 23/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 10.20.2.4
2   0.57 ms 10.20.2.6

Nmap scan report for 10.20.2.7
Host is up (0.0014s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
27000/tcp open  flexlm       FlexLM license manager
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49167/tcp open  msrpc        Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or
Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 102.768 days (since Thu Jun 21 18:32:07 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
```

```
IP ID Sequence Generation: Incremental
Service Info: Host: ARCGIS; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-vuln-ms17-010):
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacr
ypt-attacks/

TRACEROUTE (using port 23/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 10.20.2.4
2   0.47 ms 10.20.2.7

Nmap scan report for 10.20.2.12
Host is up (0.0013s latency).
Not shown: 982 closed ports
PORT      STATE SERVICE           VERSION
80/tcp    open  http              Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
135/tcp   open  msrpc             Microsoft Windows RPC
139/tcp   open  netbios-ssn       Microsoft Windows netbios-ssn
443/tcp   open  ssl/http          Microsoft IIS httpd 8.5
|_http-server-header: Microsoft-IIS/8.5
445/tcp   open  microsoft-ds      Microsoft Windows Server 2008 R2 - 2012
microsoft-ds
1801/tcp  open  msmq?
2103/tcp  open  msrpc             Microsoft Windows RPC
2105/tcp  open  msrpc             Microsoft Windows RPC
2107/tcp  open  msrpc             Microsoft Windows RPC
3389/tcp  open  ssl/ms-wbt-server?
6006/tcp  open  X11:6?
```

7070/tcp open ssl/realserver?
8081/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: new360.nddprint.com
49152/tcp open msrpc   Microsoft Windows RPC
49153/tcp open msrpc   Microsoft Windows RPC
49154/tcp open msrpc   Microsoft Windows RPC
49156/tcp open msrpc   Microsoft Windows RPC
49160/tcp open msrpc   Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows 2012
OS CPE: cpe:/o:microsoft:windows_server_2012:r2
OS details: Microsoft Windows Server 2012 or Windows Server 2012 R2
Uptime guess: 32.956 days (since Thu Aug 30 14:01:51 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE:
cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms17-010): Could not connect to 'IPC$'

TRACEROUTE (using port 23/tcp)
HOP RTT   ADDRESS
-   Hop 1 is the same as for 10.20.2.4
2   0.46 ms 10.20.2.12

Nmap scan report for 10.20.2.15
Host is up (0.0016s latency).
Not shown: 987 closed ports
PORT   STATE SERVICE   VERSION
135/tcp   open msrpc   Microsoft Windows RPC
139/tcp   open netbios-ssn Microsoft Windows netbios-ssn
445/tcp   open microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
1947/tcp open http   Aladdin/SafeNet HASP license manager 19.00
|_http-server-header: HASP LM/19.00
5357/tcp open http   Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
5800/tcp open vnc-http   RealVNC E4
|_http-server-header: RealVNC/E4
5900/tcp open vnc   RealVNC Enterprise (protocol 4.1)
49152/tcp open msrpc   Microsoft Windows RPC
49153/tcp open msrpc   Microsoft Windows RPC

```
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or
Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Uptime guess: 20.521 days (since Wed Sep 12 00:27:31 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: ROBOTICS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms17-010): This system is patched.

TRACEROUTE (using port 23/tcp)
HOP RTT     ADDRESS
-   Hop 1 is the same as for 10.20.2.4
2   0.44 ms 10.20.2.15

Nmap scan report for 10.20.2.16
Host is up (0.00060s latency).
Not shown: 993 closed ports
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.0.8 or later
22/tcp    open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol
2.0)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
5800/tcp  open  vnc-http    RealVNC E4
|_http-server-header: RealVNC/E4
5900/tcp  open  vnc         RealVNC Enterprise (protocol 4.1)
10000/tcp open  http        MiniServ 1.881 (Webmin httpd)
|_http-server-header: MiniServ/1.881
No exact OS matches for host (If you know what OS is running on it, see
https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/2%OT=21%CT=1%CU=30897%PV=Y%DS=2%DC=
T%G=Y%TM=5BB395A
```

OS:1%P=x86_64-pc-linux-gnu)SEQ(SP=108%GCD=1%ISR=107%TI=Z%II=I%TS=A
)OPS(O1=M
OS:5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11N
W7%O5=M5B4ST11NW7%
OS:O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%
W6=7120)ECN(R=Y%
OS:DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40
%S=O%A=S+%F=AS%RD=
OS:0%Q=)T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=
AR%O=%RD=0%Q=)
OS:T6(R=N)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%
RIPCK=G%RUCK=G%
OS:RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 26.140 days (since Thu Sep 6 09:37:03 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host: CFTV; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_smb-vuln-ms17-010): This system is patched.

TRACEROUTE (using port 23/tcp)
HOP RTT   ADDRESS
-   Hop 1 is the same as for 10.20.2.4
2   0.40 ms 10.20.2.16

Nmap scan report for 10.20.2.17
Host is up (0.00071s latency).
Not shown: 990 filtered ports
PORT   STATE SERVICE   VERSION
22/tcp   closed ssh
80/tcp   open   http   VMware ESXi Server httpd
427/tcp open   svrloc?
443/tcp open   ssl/http   VMware ESXi Web UI
| vmware-version:
| Server version: VMware ESXi 6.7.0
| Build: 8169922
| Locale version: INTL 000
| OS type: vmnix-x86
|_ Product Line ID: embeddedEsx
902/tcp open   ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC,
SOAP)

5988/tcp closed wbem-http
5989/tcp closed wbem-https
8000/tcp open http-alt?
8300/tcp open tmi?
9080/tcp open ssl/soap gSOAP 2.8
|_http-server-header: gSOAP/2.8
Aggressive OS guesses: VMware ESXi 4.1.0 (94%), VMware ESXi 5.1 (93%), m0nowall 1.3b16 firewall (FreeBSD 6.3-RELEASE) (92%), VMware ESXi 4.1 (92%), VMware ESXi 4.0 (91%), FreeBSD 5.5-RELEASE (90%), Isilon IQ 200 NAS device (90%), VMware ESXi 5.0 (89%), NAS4Free (FreeBSD 10.2-RELEASE) (89%), FreeBSD 6.2-RELEASE (88%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 102.803 days (since Thu Jun 21 17:42:46 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=165 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: ServidorESXi.pgua; CPE: cpe:/o:vmware:esxi, cpe:/o:vmware:ESXi:6.7.0

TRACEROUTE (using port 22/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 10.20.2.4
2 0.33 ms 10.20.2.17

Nmap scan report for 10.20.2.50
Host is up (0.0017s latency).
Not shown: 995 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
| program version port/proto service
| 100000 2 111/tcp rpcbind
| 100000 2 111/udp rpcbind
| 100024 1 38917/tcp status
|_ 100024 1 51284/udp status
902/tcp open ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
5800/tcp open vnc-http RealVNC E4
|_http-server-header: RealVNC/E4
5900/tcp open vnc RealVNC Enterprise (protocol 4.1)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32

OS details: Linux 2.6.32
Uptime guess: 103.209 days (since Thu Jun 21 07:57:44 2018)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 23/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 10.20.2.4
2 0.42 ms 10.20.2.50

Nmap scan report for 10.20.2.254
Host is up (0.0037s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
23/tcp open telnet Enterasys C2H124-48 switch telnetd
80/tcp open http Embedded HTTP Server (Enterasys C5124 switch http config)
|_http-server-header: Embedded Web Server
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.70%E=4%D=10/2%OT=23%CT=1%CU=32974%PV=Y%DS=2%DC=T%G=Y%TM=5BB395A
OS:1%P=x86_64-pc-linux-gnu)SEQ(SP=0%GCD=FA01%ISR=9A%TI=I%II=I%SS=S%TS=U)OPS
OS:(O1=NNM5B4SNW0%O2=NNM5B4SNW0%O3=M5B4NW0%O4=NNM5B4SNW0%O5=NNM5B4SNW0%O6=N
OS:NM5B4S)WIN(W1=1000%W2=1000%W3=1000%W4=1000%W5=1000%W6=1000)ECN(R=Y%DF=N%
OS:T=41%W=1000%O=NNM5B4SNW0%CC=N%Q=)T1(R=Y%DF=N%T=41%S=O%A=S+%F=AS%RD=0%Q=)
OS:T2(R=N)T3(R=N)T4(R=N)T5(R=Y%DF=N%T=100%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T5(R
OS:=N)T6(R=N)T7(R=N)U1(R=Y%DF=N%T=41%IPL=138%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK
OS:=G%RUD=G)IE(R=Y%DFI=S%T=41%CD=Z)

Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=0 (Trivial joke)
IP ID Sequence Generation: Incremental
Service Info: Device: switch; CPE: cpe:/h:enterasys:c2h124-48, cpe:/h:enterasys:c5124

TRACEROUTE (using port 587/tcp)
HOP RTT ADDRESS
- Hop 1 is the same as for 10.20.2.4
2 1.15 ms 10.20.2.254

NSE: Script Post-scanning.
Initiating NSE at 12:58
Completed NSE at 12:58, 0.00s elapsed
Initiating NSE at 12:58
Completed NSE at 12:58, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 254 IP addresses (11 hosts up) scanned in 250.31 seconds
Raw packets sent: 15948 (717.386KB) | Rcvd: 9364 (390.934KB)