

RELATÓRIO

Durante a varredura foram encontrados 21 hosts ativos na rede. De acordo com os hosts, identificamos também suas respectivas portas e serviços ativos.

PORTA	SERVIÇO
23	telnet

23/TELNET – É um serviço de terminal que permite que um usuário conecte-se a outra máquina, durante a conexão o usuário pode ter acesso a todos os recursos(ou pelo menos aqueles que sua senha permite), e como se ele estivesse trabalhando nesta máquina fisicamente.

O telnet é uma aplicação que utiliza o protocolo TCP para transportar os dados, pois ele necessita de certeza da entrega dos pacotes entre as máquinas conectadas.

PORTA	SERVIÇO
80	http

80/HTTP - Protocolo de transferência de Hipertexto (*Hypertext Transfer Protocol*). É um protocolo de comunicação(camada de aplicação do MODELO OSI).Ele é a base de comunicação de dados WWW(World Wide Web). Hipertexto é um texto estruturado que usa ligações lógicas(hiperlinks) entre nós contendo texto. O HTTP é um protocolo para a troca de hipertextos.

PORTA	SERVIÇO
135	msrpc

Quando um computador recebe uma conexão na porta 135, ele sabe como dirigir o tráfego para o "*Endpoint Mapper*" (EPMAP) de *Remote Procedure Call* (RPC). Existem muitas implementações de RPC, cada uma com diferentes portas atribuídas. Esta é a RPC original produzida pelo Grupo Aberto para seu Ambiente Distribuído *Computer* (DCE).

RPC está integrado em muitas aplicações, e por isso o protocolo padrão para direcionar o tráfego da porta precisa de uma outra camada para a porta 135. O *Endpoint Mapper* recebe conexões RPC e redireciona o tráfego para outros portos designados para as aplicações em que RPC está integrado. O problema é que a *Endpoint Mapper* é explorada por vírus. Repetidas ligações para a porta 135 podem fazer com que o serviço pare. Isso é chamado de ataque de negação de serviço.

PORTA	SERVIÇO
-------	---------

Ela possui uma função específica, ela é usada pra transferência de dados no serviço *NetBios*, ela faz parte de um conjunto de três portas que utilizam o serviço de compartilhamento de arquivo e impressora em redes *Microsoft*, cada porta tem sua especificação, a porta 137 UDP é usada para navegação, incluindo a visualização dos compartilhamentos disponíveis, a porta 138 UDP para resolução de nomes da rede.

PORTA	SERVIÇO
445	netbios-ssn

A porta TCP 445 é a porta equivalente ao serviço SMB(*Server Message Block*), usada para compartilhamento de arquivos numa rede. A partir do *Windows 2000*, a *Microsoft* trocou as portas TCP 139(*NetBios*) e 137-138, fazendo com o SMB trafegar acima do TCP/IP pela porta 445. Ou seja, na sua rede INTERNA, é um mal necessário

PORTA	SERVIÇO
9999	abyss

Porta para servidor web *Abyss* interface de gerenciamento web remoto.

PORTA	SERVIÇO
49155	TCP / UDP

Porta TCP **49155** usa o Protocolo de Controle de Transmissão. O TCP é um dos principais protocolos de redes TCP / IP. TCP é um protocolo orientado a conexão, requer handshaking para configurar as comunicações end-to-end. Somente quando uma conexão é configurada dados do usuário podem ser enviadas bi-direcional através da ligação.

Atenção! TCP garante a entrega de pacotes de dados na porta **49155** na mesma ordem em que foram enviados. Comunicação garantida através de TCP porta **49155** é a principal diferença entre TCP e UDP. Porta UDP **49155** não teria garantido a comunicação como TCP. UDP na porta **49155** fornece um serviço confiável e datagramas podem chegar duplicados, fora de ordem, ou em falta sem aviso prévio. UDP na porta **49155** pensa que a verificação e correção de erros não é necessário ou executados na aplicação, evitando a sobrecarga desse tratamento no nível de interface de rede. UDP (User Datagram Protocol) é um protocolo de camada de transporte mínima orientado a mensagem (protocolo é documentado . em IETF RFC 768) . Exemplos de aplicação que muitas vezes usam UDP: voz sobre IP (VoIP), a mídia e os jogos multiplayer em tempo real de fluxo contínuo. Muitas aplicações web usam UDP, por exemplo, o Sistema de Nome de Domínio (DNS), o Routing Information Protocol (RIP), o Dynamic Host Configuration Protocol (DHCP), o Simple Network Management Protocol (SNMP).

