heimdall

security research

A DIVISION OF ISH

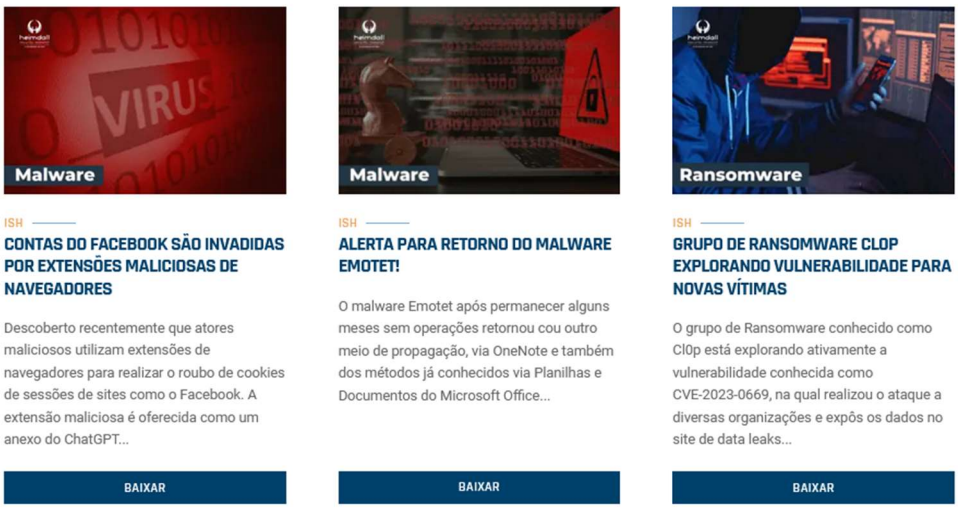
Riscos e recomendações para portas abertas em *firewall*

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



Sumário

1 INTRODUÇÃO

A segurança de redes desempenha um papel fundamental na proteção de sistemas contra ameaças cibernéticas. Um componente crucial na defesa de uma rede é o *firewall*, que atua como uma barreira entre a rede interna e a internet, controlando o tráfego de entrada e saída.

Uma porta aberta em um *firewall* pode representar um risco significativo para a segurança da rede. Cada porta aberta é uma brecha em potencial pela qual um atacante pode tentar acessar e explorar os sistemas. As portas abertas representam serviços e protocolos disponíveis para comunicação com a internet e, se não forem adequadamente protegidas, podem levar a consequências indesejadas, como:

- **Acesso não autorizado**: uma porta aberta pode permitir que um invasor tente se conectar a um sistema ou serviço sem a devida autorização. Isso pode levar ao roubo de informações confidenciais, modificação de dados ou comprometimento de recursos.
- **Exploração de vulnerabilidades**: as portas abertas podem ser alvos de ataques direcionados a serviços específicos que estão escutando nessas portas. Se houver vulnerabilidades conhecidas nesses serviços, os atacantes podem explorá-las para ganhar acesso não autorizado ou executar códigos maliciosos nos sistemas comprometidos.
- **Propagação de *malware***: alguns *malwares* e *worms* são projetados para se espalharem pela rede, explorando portas abertas e vulnerabilidades em sistemas remotos. Uma porta com um serviço vulnerável aberta pode permitir que um *malware* se espalhe rapidamente pela rede, afetando múltiplos sistemas.
- **Ataques de negação de serviço** (**DoS**): nos quais um atacante envia uma grande quantidade de tráfego malicioso para sobrecarregar os recursos do sistema ou serviço. Isso pode resultar em uma interrupção de serviço, tornando os recursos inacessíveis para usuários legítimos.

2 RISCOS DE SEGURANÇA DAS PORTAS TCP 135, 139 E 445 ABERTAS NO *FIREWALL*

As portas TCP **135**, **139** e **445** estão associadas a protocolos e serviços específicos do Windows. Seguem abaixo os riscos de segurança para cada uma dessas portas:

Porta TCP 135 (**RPC - *Remote Procedure Call***):

Riscos: a porta TCP 135 é usada pelo RPC, um mecanismo que permite a comunicação entre processos em sistemas Windows. Abrir essa porta pode expor seu sistema a ataques de negação de serviço (DoS) e exploração de vulnerabilidades conhecidas no RPC.

Exemplos de vulnerabilidades:

CVE-2021-1678: uma vulnerabilidade de execução remota de código (**RCE**) que afeta o componente RPC do Windows. Um invasor poderia explorar essa falha enviando solicitações especialmente criadas para um serviço RPC vulnerável e executar código arbitrário no sistema afetado.

CVE-2020-0796: também conhecida como "**SMBGhost**" ou "**CoronaBlue**", essa CVE afeta o protocolo SMBv3, que usa **RPC** para comunicação. Essa vulnerabilidade permite a execução remota de código em sistemas Windows 10 e Windows Server 2019. A exploração dessa falha pode resultar no comprometimento completo do sistema.

CVE-2017-0146: essa CVE é uma vulnerabilidade de estouro de *buffer* no serviço de transporte RPC (RpcXceoq). Um invasor remoto pode enviar um pacote especialmente criado para explorar essa falha e executar código arbitrário no sistema vulnerável.

CVE-2015-6128: vulnerabilidade de execução remota de código no serviço de chamada de procedimento remoto (RPCSS). Um invasor pode explorar essa falha enviando uma solicitação especialmente criada para o serviço RPCSS e executar código arbitrário no sistema afetado.

3 PORTA TCP 139 (NETBIOS *SESSION SERVICE*)

Riscos: a porta TCP 139 é usada pelo serviço de sessão NetBIOS, que permite que dispositivos Windows compartilhem recursos em rede, como arquivos e impressoras. Abrir essa porta pode permitir ataques de enumeração de informações, captura de senhas, acesso não autorizado a recursos compartilhados e propagação de *malware* através de *worms,* como o conhecido "**WannaCry**".

Exemplos de vulnerabilidades:

CVE-2020-16897: vulnerabilidade de divulgação de informações quando extensões NetBIOS sobre TCP (NBT) (NetBT) manipulam objetos na memória de maneira inadequada, também conhecida como 'Vulnerabilidade de divulgação de informações NetBT'.

CVE-2017-0174: o Windows NetBIOS no Windows Server 2008 SP2 e R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold e R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703 e Windows Server 2016 permitem uma vulnerabilidade de negação de serviço quando lidam incorretamente com pacotes NetBIOS, também conhecidos como "vulnerabilidade de negação de serviço do Windows NetBIOS".

CVE-2023-0854: estouro de *buffer* no registro NetBIOS QNAME e no processo de comunicação de impressoras multifuncionais e impressoras a *laser* para escritórios/pequenos escritórios, o que pode permitir que um invasor no segmento de rede acione a falta de resposta do produto afetado ou execute um código arbitrário.

4 PORTA TCP 445 (SMB - *SERVER MESSAGE BLOCK*)

Riscos: a porta TCP 445 é usada pelo SMB, um protocolo para compartilhamento de arquivos, impressoras e outros recursos em redes Windows. Abrir essa porta pode expor sistemas a ataques de exploração de vulnerabilidades conhecidas no SMB. Isso pode levar à execução remota de código, acesso não autorizado a arquivos e propagação de *malware*.

Exemplos de vulnerabilidades:

CVE-2020-0796 (**SMBGhost**): essa CVE foi descoberta em 2020 e é uma vulnerabilidade crítica que afeta o SMBv3. Permite a execução remota de código em sistemas Windows 10 e Windows Server 2019. A exploração dessa vulnerabilidade pode permitir que um invasor assuma o controle completo do sistema.

CVE-2017-0143 (**EternalBlue**): essa CVE ganhou notoriedade em 2017 quando foi usada no ataque global do *ransomware* WannaCry. É uma vulnerabilidade de estouro de *buffer* no SMBv1 que permite a execução remota de código em sistemas afetados. Essa falha pode permitir a propagação de *malware* por meio da rede.

CVE-2017-0144 (**EternalRomance**): essa CVE também foi utilizada no ataque do *ransomware* WannaCry. É uma vulnerabilidade no SMBv1 que permite a execução remota de código. Os invasores podem explorar essa falha para controlar sistemas vulneráveis.

CVE-2018-1140: vulnerabilidade de execução remota de código no componente SMBv3.1.1 do Windows. A exploração dessa falha permite que um invasor execute código arbitrário em um sistema comprometido.

Obs. Lembre-se de que essas são apenas algumas das CVEs conhecidas nestas portas e serviços. É importante manter os sistemas atualizados com as correções e atualizações de segurança mais recentes fornecidas pelos fabricantes de *software*, para mitigar riscos associados a essas vulnerabilidades. Além disso, é essencial implementar boas práticas de segurança, como a filtragem adequada de portas e a adoção de políticas de segurança robustas.

5 RECOMENDAÇÕES

Porta TCP 135 (RPC - *Remote Procedure Call*):

- Implemente regras de *firewall* que permitam o tráfego da porta TCP 135 apenas a partir de fontes confiáveis e restrinjam o acesso externo não autorizado.
- Mantenha os sistemas operacionais e aplicativos atualizados com os *patches* de segurança mais recentes para mitigar possíveis vulnerabilidades conhecidas.
- Considere utilizar autenticação forte e criptografia para proteger as comunicações RPC.

Porta TCP 139 (NetBIOS *Session Service*):

- Avalie a necessidade de manter a porta TCP 139 aberta e considere alternativas mais seguras, como o uso do SMB versão 2 ou superior, que utiliza a porta TCP 445.
- Caso seja necessário manter a porta TCP 139 aberta, restrinja o acesso a ela por meio de regras de *firewall* que permitam apenas tráfego de fontes confiáveis.
- Desative o uso do NetBIOS onde não é estritamente necessário, uma vez que o protocolo é legado e apresenta riscos de segurança.

Porta TCP 445 (SMB - *Server Message Block*):

- Implemente regras de *firewall* que permitam o tráfego da porta TCP 445 apenas a partir de fontes confiáveis e restrinjam o acesso externo não autorizado.
- Mantenha os sistemas operacionais e aplicativos atualizados com os *patches* de segurança mais recentes para mitigar possíveis vulnerabilidades conhecidas no SMB.
- Considere utilizar autenticação forte, criptografia e políticas de segurança adequadas para proteger os recursos compartilhados pelo SMB.

Além dessas recomendações específicas para cada porta, é importante seguir as práticas recomendadas de segurança em geral, como implementar uma política de segurança em várias camadas, utilizar *firewalls* de borda, monitorar ativamente atividades suspeitas na rede e manter-se atualizado com as últimas ameaças e soluções de segurança.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**

heimdall
security research

A DIVISION OF ISH