Hardening for Blue Teams

Edição 01 - Abril/2022

Security by Design

Secure File Transfer Protocol (SFTP)

Criado por: Felipe Silvany

SUMÁRIO

CONFIDENCIALIDADE

Este documento contém informações confidenciais ou privilegiadas, sendo seu sigilo protegido por lei, não sendo autorizado o uso, cópia ou divulgação das informações ou tomar qualquer ação baseada nessas informações.

Desta forma, os destinatários destes documentos comprometem-se em:

1. Não utilizar as informações confidenciais a que tiver acesso, para gerar benefício próprio exclusivo e/ou unilateral, presente ou futuro, ou para o uso de terceiros.

2. Não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso.

3. Não apropriar-se de material confidencial e/ou sigiloso da tecnologia que venha a ser disponível.

4. Não repassar o conhecimento das informações confidenciais, responsabilizando-se por todas as pessoas que vierem a ter acesso às informações, por seu intermédio, e obrigando-se, assim, a ressarcir a ocorrência de qualquer dano e/ou prejuízo oriundo de uma eventual quebra de sigilo das informações fornecidas.

SOBRE O AUTOR

Coordenador de Cybersecurity, com 20 anos de experiência na área de tecnologia, com sólidos conhecimentos em resposta à incidentes de segurança, SOC, hardering, análise de vulnerabilidades, pentest e grandes projetos de cybersecurity em ambientes onpremises, Cloud e mobile (AppSec).

Sólida experiência na implementação de soluções técnicas e estruturação de equipes de segurança de alta performance.

Responsável pela implementação de serviços, ferramentas e processos como: SOC/CSIRT 24x7, playbooks, Plano de Resposta à Incidentes de Segurança (RI), SIEM com base no MITRE ATT&CK, hardenização e baselines de segurança, exercícios de RedTeam como Pentest, análise de vulnerabilidades DAST e SAST na infraestrutura onpremises/cloud (OpSec), mobiles Android e IOS (AppSec) e definição de arquitetura segura com conceitos de Zero Trust. Implementação de ferramentas de BlueTeam como: NGAv/EDR, NGFw, MTLS, NAC, DLP, IDS, IPS, WAF, AppControl, Anti-DDoS e outras.

Graduado em "Sistema de Informação", Pós Graduado em "Projetos e Gerência de Redes" e com MBA em "Gestão Empresarial Estratégica". Membro da ISO/ABNT/CE-021 000.027 (Comissão Especial de Estudo de Segurança da Informação, Segurança Cibernética e Proteção da Privacidade de dados), membro da ANPPD (Associação Nacional dos Profissionais de Privacidade de Dados) e certificado nos mais conceituados frameworks internacionais, como: ISO27001, ISO20000, ITIL, COBIT, Scrum, Kanban e outros. Classificado entre os TOP 5 Ethical Hackers na maior plataforma de BugBounty do Brasil e primeiro colocado em diversos programas privados.

SOBRE ESTE DOCUMENTO

Este não é um e-book comum.

Você está prestes a obter um conhecimento privilegiado em segurança da informação e hardening.

Esta obra utiliza uma metodologia focada em *Security by Design* e implementação de boas práticas de segurança desde a concepção de projetos corporativos até sua passagem para produção.

A segurança deve ser sempre preventiva e pró ativa, nunca reativa.

Nesta primeira edição veremos boas práticas na estruturação de um servidor SFTP para troca de arquivos.

Edição 01 – Criação do Documento
Abril/2022 – Felipe Silvany

AGRADECIMENTOS

Ao meu filho, Thor, que me dá toda força para enfrentar todas as dificuldades e tribulações da vida com força e ânimo. À minha esposa, Fabiana, por sempre me apoiar em todos os desafios profissionais e perder várias noites de sono comigo. À minha mãe e meu pai, Maria Aparecida e Adilton, por terem me dado a maior herança que um homem por ter, o estudo. À Deus, que por intermédio do meu Senhor Jesus Cristo conduz a minha vida, me guia e me guarda.

1 - RESUMO

O *Secure File Transfer Protocol* ou SFTP é um protocolo de transferência de arquivos e de manipulação funcional. É tipicamente utilizado com o protocolo de segurança SSH-2.

Seu propósito é semelhante ao do FTP convencional, porém em função do uso de criptografia nas conexões (através do estabelecimento de um túnel SSH) o tráfego de informações possui um incremento de segurança efetivo.

UNRESTRICTED FILE UPLOAD

Arquivos carregados representam um risco significativo para o servidor. O primeiro passo em muitos ataques é obter algum código do sistema para ser atacado. Então o atacante só precisa encontrar uma maneira de executar o código. O uso do upload de arquivo ajuda o invasor a realizar o primeiro passo.

As consequências do upload irrestrito de arquivos podem variar, incluindo a aquisição completa do sistema, um sistema de arquivos ou banco de dados sobrecarregados, encaminhamento de ataques para sistemas back-end, ataques do lado do cliente ou simples desfiguração. Depende do que o aplicativo faz com o arquivo carregado e especialmente onde ele foi armazenado.

Há duas classes de problemas aqui. O primeiro é com os metadados do arquivo, com o caminho e o nome do arquivo. Estes são geralmente fornecidos pelo transporte, como codificação de várias partes HTTP. Esses dados podem enganar o aplicativo para substituir um arquivo crítico ou armazenar o arquivo em um local inapropriado. Você deve validar os metadados com muito cuidado antes de executá-lo.

A outra classe de problemas é com o tamanho do arquivo ou conteúdo. A gama de problemas aqui depende inteiramente para que o arquivo é usado. Para se proteger contra esse tipo de ataque, você deve analisar tudo o que seu aplicativo faz com os arquivos e pensar cuidadosamente sobre quais processamentos estão envolvidos.

ZERO TRUST

O principal conceito trazido pelo Zero Trust é "*nunca confie, sempre verifique*", ou para autores mais conservadores "*confiar, mas sempre verificar*", o que significa que dispositivos e serviços não devem ser confiáveis (confiados) por padrão. Redes, como WAN, LAN corporativa, VPNs são hostis e inseguras por padrão, mesmo que estejam dentro do perímetro de segurança, por isso, todo acesso deve ser validado, mesmo que já tenha sido verificado anteriormente. O Zero Trust aborda princípios chaves como: Autenticação mútua (MFA, 2FA), autenticação de máquina, autenticação de usuário, monitoramento contínuo, registro de todos os logs de acessos, entre outros.

PRINCÍPIO DO MENOR PRIVILÉGIO

O princípio do menor privilégio é aquele que preza por delegar somente os privilégios necessários para que um determinado elemento (sistema ou pessoa) possa realizar sua função.

2 – CONCEITOS BÁSICOS

DESATIVE O FTP PADRÃO

Se o FTP padrão estiver sendo executado no servidor, você deve desabilitá-lo. FTP tem mais de 30 anos e não está preparado para suportar as ameaças modernas de segurança que enfrentamos hoje. O FTP carece de privacidade, integridade e torna bastante fácil para um hacker obter acesso, capturar ou modificar seus dados enquanto eles estão em trânsito. Sugerimos que você mude para uma alternativa mais segura como FTPS, SFTP ou ambos.

COLOQUE O SFTP ATRÁS DE UM GATEWAY OU PROXY

A DMZ é um segmento comum da rede para as organizações armazenarem seus servidores SFTP. O problema com a DMZ é que ela enfrenta a internet pública, tornando-a o segmento mais vulnerável a ataques. Se o servidor SFTP estiver na DMZ, os arquivos de dados e as credenciais do usuário geralmente também são armazenados lá, o que é um grande risco mesmo se os arquivos estiverem criptografados.

Algumas organizações movem seus arquivos e credenciais de usuários para a rede privada, o que é mais seguro. O problema com este método, porém, é que isso exige que você abra portas na rede privada, o que cria um caminho para um ataque e pode não atender aos requisitos de conformidade.

Uma abordagem segura é usar um *DMZ Secure Gateway*, ou um Proxy Reverso aprimorado. O Gateway é um software que você instala em um servidor na DMZ.

Seus parceiros de negócio se conectam ao Gateway (*front-end*), e o Gateway enviará a sessão sobre o canal de controle para o servidor SFTP na rede privada (*back-end*). Arquivos e credenciais do usuário permanecem na rede privada, e não são necessárias portas de entrada.

USE CRIPTOGRAFIA FORTE E HASHING

As cifras de criptografia são usadas nos protocolos SFTP e FTPS para proteger os dados na transmissão. A cifra é um algoritmo complexo que pega os dados originais e, juntamente com a chave, produz os dados criptografados para transmitir. A primeira coisa que você deve fazer é desativar quaisquer cifras antigas e ultrapassadas como *Blowfish, 3DES, DES, RC2, WCQ, MD4, MD5, SHA1*, e use apenas cifras mais fortes como AES ou TDES. Criptografe dados em trânsito e em repouso.

Recomenda-se os seguintes algoritmos:

- Algoritmos de confidencialidade: AES-GCM-256 ou ChaCha20-Poly1305
- Algoritmos de integridade: SHA-256, SHA-384, SHA-512, Blake2, a família SHA-3
- Algoritmos de assinatura digital: RSA (3072 bits e superior), ECDSA com NIST P-384
- Principais algoritmos de estabelecimento: RSA (3072 bits e superior), DH (3072 bits ou superior), ECDH com NIST P-384

IMPLEMENTE UMA BLACKLIST OU WHITELIST DE IPS

Uma *blacklist* nega uma série de endereços IP de acessar o sistema, temporariamente ou permanentemente. Por exemplo, você pode bloquear o acesso de certos países ou determinados IPs/origens.
Outro método é listar apenas endereços IP autorizados para acessar o sistema, como seus parceiros comerciais.

IMPLEMENTE UMA BLACKLIST OU WHITELIST DE ARQUIVOS

Se você espera apenas que certos tipos de arquivos sejam carregados em seu servidor, você pode criar uma *Whitelist* para banir todos os outros tipos. Isso impedirá que você encontre problemas como:

- infecções por malware
- uploads desnecessários que só consomem espaço em disco
- questões legais causadas pelo upload de mídia pirata

NÃO UTILIZE SSL OU TLS 1.0/1.1

O TLS 1.0 é uma criptografia publicamente declarada como fraca e "quebrável" desde 2018 .
Os serviços que usam TLS 1.0 são considerados não compatíveis pelo PCI desde 30 de junho de 2018. Em Outubro de 2018 a Apple, Google, Microsoft e Mozilla anunciaram em conjunto que suspenderiam o uso do TLS 1.0 e 1.1 a partir de Março 2020.
Serviços que utilizam TLS 1.0 ou 1.1 estão diretamente expostos à ataques do tipo Man-in-the-midle e PoODLE.

Recomenda-se a utilização de TLS 1.2 ou 1.3.

DETECTE E RESPONDA À ATAQUES DE FORÇA BRUTA

Embora essas configurações de conformidade possam impedir que um ataque de força bruta seja bem-sucedido, isso não impedirá aos hackers de iniciar tal ataque. Assim, enquanto o ataque eventualmente falhar, ele ainda inundará seus registros com toneladas de entradas de tentativa de login fracassadas, o que geralmente causa ansiedade indevida aos seus administradores e impacta negativamente o desempenho do seu servidor.
Para impedir um ataque de força bruta, defina suas configurações de conexões para que uma conta de usuário seja automaticamente desativada ou um endereço IP seja automaticamente bloqueado (ou sinalizado) depois que um certo número de tentativas de login fracassadas for alcançado.

ESCANEIE PREVIAMENTE ARQUIVOS RECEBIDOS

Todos os arquivos recebidos pelo servidor devem ser previamente escaneados por um EDR, antivírus ou outro endpoint de segurança. Devido ao grande volume de arquivos que são carregados para servidores de transferência de arquivos, há sempre uma boa chance de alguns desses arquivos estarem infectados com malware. Agora, todos sabemos o quão disruptivo e

destrutivo alguns desses malwares podem ser. Alguns tipos de malware, como ransomware, podem danificar redes inteiras ou, no caso do WannaCry, várias redes.
Por isso, é importante empregar soluções que detectem e eliminem essas ameaças à medida que entram no seu servidor.

INSPECIONE O CONTEÚDO DE SAÍDA USANDO DLP
Algumas violações de dados acontecem como resultado de um ataque cibernético deliberado. Outros acontecem simplesmente por causa de um ato não intencional, como um usuário acidentalmente carregando uma planilha contendo dados altamente confidenciais para uma pasta compartilhada.

Para evitar vazamentos acidentais de dados no SFTP, implemente um recurso DLP (prevenção de perda de dados). As regras incorporadas de DLP podem detectar o vazamento de vários tipos de dados confidenciais

2 – HARDENING

Garanta que as contramedidas abaixo estejam implementadas em seu servidor SFTP. Responda "*sim*" caso as contramedidas de segurança estejam implementadas e forneça maiores detalhes técnicos junto à resposta. Responda "*não*" caso as contramedidas de segurança não estejam implementadas no ambiente e considere como um gap de segurança.

1. Renomeie a conta administrativa default da solução (administrator, administrador, root ou outras).
2. Desative o serviço de ftp padrão.
3. Aplique os patches de segurança mais recentes do Sistema Operacional.
4. Garanta que o software do servidor SFTP esteja atualizado com as últimas versões estáveis do fabricante.
5. Garanta que o servidor possui um Endpoint de segurança instalado, EDR, Antivírus ou outros. Especifique no caso de outros.
6. Desative o NetBIOS14 sobre TCP/IP
7. Garanta que o servidor foi submetido à testes de segurança, invasão (Pentest) ou vulnerabilidade. Exemplifique especificando datas.
8. Garanta que o servidor não esteja posicionado em uma DMZ. Envie uma ilustração da arquitetura mostrando o posicionamento do servidor SFTP na rede.
9. Os dados devem ser imediatamente removidos do servidor SFTP após o download pelo destinatário. Quanto mais tempo mantemos o dado disponível no servidor, maior é a exposição das informações.
10. Garanta que a credencial de acesso ao SFTP não possua permissão à nível do Sistema Operacional ou administrativa.
11. Implemente uma White List de IPs que são autorizados a acessar o servidor, ou não sendo possível, implemente uma black list de IPs não autorizados.

12. Implemente uma blacklist de extensões de arquivos não permitidas para upload ou uma Whitelist que permita somente as extensões necessárias para banir todo o resto.
13. Implemente bloqueio de requisições ao servidor com base em Geo-localização. (ex: liberar somente requisições do Brasil).
14. Não use nenhuma versão de SSL, TLS 1.0 ou TLS 1.1.
15. Utilize um modelo de autenticação Private Key RSA (SSH2-RSA 2048 por exemplo), garantindo que além da chave pública já existente também seja necessário a chave privada.
16. Garanta a utilização de criptografias e hashs fortes, para proteger a transmissão de dados.
17. Garanta que cifras mais antigas e desatualizadas, como Blowfish, 3DES, DES, RC2, WCQ, MD4, MD5, SHA1 e outras não sejam autorizadas. Utilize apenas cifras mais fortes, como AES, TDES ou outras.
18. Todas as transferências devem ser devidamente registradas para permitir a prova de entrega e verificar se os downloads são acessados apenas por partes autorizadas.
19. Solicite reautenticação de sessões inativas.
20. Garanta que sessões idle sejam desconectadas.
21. Garanta que uma única credencial não consiga se conectar a partir de duas ou mais origens ao mesmo tempo (Viagem Impossível).
22. Garanta que mensagens padrões do sistema ou mensagens de erro sejam suprimidas por páginas customizadas, garantindo que não seja feito o disclosure de informações que tragam versões do software que está sendo utilizado.
23. Garanta que exista um acordo sobre confidencialidade dos dados armazenados (NDA) e suas responsabilidades com o fornecedor, dado que temos terceiros com acesso ou manipulação de nossos dados. Para LGPD o processador e controlador dos dados são responsáveis e existem sanções/multas, que aumentam o risco ao tipo de exposição caso não exista o item formalizado.

3 – QUESTIONÁRIO TÉCNICO

Garanta que o Questionário Técnico abaixo seja preenchido de forma clara e com a maior riqueza de detalhes técnicos pelo fornecedor ou time técnico orgânico, junto com o item *"2 – Hardening"*.

1. O servidor SFTP é dedicado para a sua empresa ou compartilhado para outros clientes?
2. Existe controle através de logs sobre quem acessa aos dados em repouso? Explique.
3. Existe controle dos profissionais técnicos que acessam o servidor SFTP para atividades administrativas, como atualizações, backup e outros permitindo a identificações destes caso necessário? Explique.
4. Existe duplo fator de autenticação (2FA/MFA) para os profissionais que acessam o servidor à nível do sistema operacional?
5. Existe algum controle que garanta que todo arquivo enviado pelo cliente é recebido pelo servidor e não foi interceptado durante a transferência? Explique.
6. Por quantos tempo os dados em repouso são mantidos no servidor SFTP antes de serem expurgados?
7. Qual criptografia é usada para a transferência dos dados em trânsito?
8. Os dados em repouso são criptografados? Qual criptografia?
9. Qual a arquitetura da infraestrutura ou onde o servidor está posicionado na rede? Por favor envie um desenho ilustrando o servidor sftp na infraestrutura.
10. Existe um firewall, WAF ou outra proteção de perímetro antes do servidor SFTP? Explique.
11. Qual o endereço de acesso ao servidor sftp utilizado pela solução?

4 - CONCLUSÃO

O *SSH File Transfer Protocol (sFTP)* é um meio seguro de transmissão de arquivos, desde que implementado de forma correta. Atente-se não somente aos dados em trânsito, mas aos dados após serem armazenados no servidor (dados em repouso). Estes precisam também estar criptografados e excluídos imediatamente após serem consumidos.

O FTP tem mais de 30 anos e não está preparado para suportar as ameaças modernas de segurança que enfrentamos hoje. O FTP carece de privacidade e integridade e torna bastante fácil para um hacker obter acesso, capturar ou modificar seus dados enquanto eles estão em trânsito. Sugerimos que você mude para uma alternativa mais segura como FTPS, SFTP ou ambos.

5 – LEITURA ADICIONAL

- https://attack.mitre.org/techniques/T1071/002/
- https://cheatsheetseries.owasp.org/cheatsheets/Transport_Layer_Protection_Cheat_Sheet.html
- https://www.sans.org/white-papers/1462/
- https://csrc.nist.gov/glossary/term/least_privilege
- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://www.keylength.com/en/8/
- https://www.keylength.com/en/4/
- https://cryptome.org/2016/01/CNSA-Suite-and-Quantum-Computing-FAQ.pdf
- https://github.com/MobSF/owasp-mstg/blob/master/Document/0x04g-Testing-Cryptography.md#identifying-insecure-andor-deprecated-cryptographic-algorithms-mstg-crypto-4