VULNERABILIDADE EM SERVIDORES

Isabel Cabral Freire da Silva [1]
Anderson santos da silva [2]
Querte Teresinha Conzi Mehlecke [3]

RESUMO

A maioria das redes com presença na web irão expor algum servidor da web e de e-mail. Esses servidores possuem falhas de segurança que em sua maioria provêm de tecnologias PHP e ASP.NET que são tecnologias complexas, mas ainda assim com chances de grandes vulnerabilidades. Um tipo comum de falha é chamada SQL Injection, que consiste no invasor acrescentar códigos SQL num formulário, para obter acesso a informações ocultas do usuário final. Além disso existe a adulteração de parâmetros, um tipo de ataque básico, em que pode ser alterados informações de cookies e campos de formulários. Outra forma de modificar esses dados é com uso de softwares que interceptam tráfego numa rede. Em tempos recentes criaram-se ainda ataques que atingem as comunicações externas do servidor e estas já estão sendo utilizadas por cibercriminosos e empresas de Bug Hunting. Embora os servidores de e-mail não tenham tantas vulnerabilidades, eles lidam com o trafego de e-mail com anexos maliciosos que são a forma mais simples de se burlar um firewall.

Palavras-chave: cibercriminosos, vulnerabilidade em servidores, trafego, Bug, Hunting.

[1]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. isabelfreireh3013@gmail.com

[2]Professor do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. Anderson_silva@alcidesmaya.edu.br

[3]Professora do Curso Superior em Tecnologia em Redes de Computadores – Faculdade Alcides Maya. querte_mehleck@alcidesmaya.edu.br

ABSTRACT

Most networks with a web presence will expose some web and email server. These servers have security flaws that mostly come from PHP and ASP.NET technologies, which are complex technologies, but still with great vulnerabilities. A common type of flaw is called SQL Injection, which does not contain attackers adding SQL codes to a form, to gain access to hidden information from the end user. In addition, there is parameter tampering, a type of basic attack, in which information on cookies and form fields can be changed. Another way to modify this data is with the use of software that intercepts traffic on a network. In recent times they have even been created that reach the external communications of the server and these are already being used by cybercriminals and Bug Hunting companies. Although e-mail servers do not have so many vulnerabilities, they deal with e-mail traffic with malicious attachments that are the simplest way to bypass a firewall.

Keywords: cybercriminals, VULNERABILITY IN SERVERS, traffic, Bug, Hunting.

Explicação da vulnerabilidade

O que é? Onde ocorre? Quais características ela apresenta?

Em segurança de computadores, uma **vulnerabilidade** é uma fraqueza que permite que um atacante reduza a garantia da informação de um sistema. **Vulnerabilidade** é a interseção de três elementos: uma suscetibilidade ou falha do sistema, acesso do atacante à falha e a capacidade do atacante de explorar a falha.

neglicenciam a atualização de servidores Linux, bem como aplicações que rodam nestes servidores.

Pode-se destacar, alguns dos motivos da falta de atualização de servidores Linux:

• falta de mão de obra especializada;

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396 - Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

• maior dificuldade em atualizar um parque grande de servidores;
• falsa afirmação de que o sistema operacional Linux é mais seguro.

- **Nível de ameaça**

Exemplo de uma vulnerabilidade grave em sistemas Linux é a vulnerabilidade CVE-2017-7494, que afeta o serviço de compartilhamento de arquivos Samba. Essa vulnerabilidade recebeu a pontuação CVSS nível 10 (CVSS – índice que mede a gravidade de uma vulnerabilidade). Isso porque, ela pode ser facilmente explorada remotamente de modo não autenticado, fornecendo ao atacante acesso ao shell do sistema operacional e causando impacto muito parecido ao da vulnerabilidade MS17-010 de Windows. (grande problema para manter a segurança está no baixo investimento da grande maioria das empresas nessa área, fazendo uso de equipamentos e sistemas defasados e desatualizados.)

- **Estratégias de como detectar ela**

  - **Quais estratégias mínimas preciso usar para me defender?**

O ataque de brute force ou força bruta é uma técnica que consiste em tentativas de descoberta de senhas/logins através de processos ou programa. Como é inviável que esse tipo de ataque seja feito manualmente, existem diversos programas específicos para essa técnica. Basicamente o programa le um arquivo e realiza o ataque ao servidor. No conteúdo do arquivo utilizado, são configurados letras e números em diversas línguas. Existem também algumas bases de usuário/senha que estão disponíveis em sítios na Internet e vários atacantes estão montando suas próprias listas e ferramentas para utilizar esse ataque. Essa atividade maliciosa é uma estratégia de invasão ao seu servidor com o intuído recuperar informações confidenciais ou utilizá-lo para realizar outros ataques. Existem maneiras de se defender desse tipo de ataque, que vão desde uma simples troca de porta do serviço até configurações de novos serviços e regras em firewall. Outros métodos de segurança são chaves ssh, um firewall, VPNs e redes privadas; também infraestrutura de chave pública e criptografia SSL/TLS e ambientes de execução isolada.

Possibilidade de uso futuro

Como isso pode evoluir?

Pode serem mais aplicadas as soluções em Cloud com serviços de migração, **servidores**, e-mails, arquivos, etc.

Será que pode ser feita em outros sistemas?

soluções em Cloud com serviços de migração, **servidores**, e-mails, arquivos, etc.

Existe alguma variação simples que pode transformar ela em uma nova vulnerabilidade?

As técnicas de Hardening são elaboradas e tratadas para que se obtenha um aumento significativo na segurança dos servidores. Isto permite alcançar níveis de segurança mais altos, com um desempenho constante do ponto de vista da confiabilidade dos sistemas. Este trabalho teve como objetivo: revisar as principais técnicas de *Hardening* aplicadas a servidores que utilizam sistemas operacionais *Windows* e *Linux*, bem como analisá-las e documentá-las em forma de manual de boas práticas para aqueles que carecem de segurança aplicada a servidores no dia-a-dia de sua organização. Demonstrando as percepções necessárias para determinar quais as etapas e caminhos que devem ser seguidos perante os problemas exibidos nos servidores. Procurando ressaltar a importância da equipe de segurança da informação a qual é responsável por desenvolver, estudar e implementar técnicas, garantindo a integridade, confiabilidade e disponibilidade dos dados.

4º Seminário de Tecnologia Gestão e Educação – ISSN 2675-1623 - Faculdade e Escola Técnica Alcides Maya – Rua Dr. Flores, 396 - Centro Histórico de Porto Alegre – Rio Grande do Sul – outubro – 2020.

REFERÊNCIAS

Locaweb. **O que está procurando?** 2020. disponível em: < https://ajuda.locaweb.com.br/>. acessado em 20/11/2020.

Ocean Digital. **Welcome to the developer cloud**. 2020. disponível em: < https://www.digitalocean.com/>. acessado em 20/11/2020.

Repositório Digital. **Direito fundamental à privacidade: desdobramentos possíveis até o direito à extimidade**. 2020. disponível em:<https://paimon.cpd.ufsm.br/>. acessado em 20/11/2020.