Jean Carvalho Ortiz

SEM TITULO
AINDA

Campo Grande, MS

21 de novembro de 2018

Jean Carvalho Ortiz

SEM TITULO
AINDA

Trabalho de Conclusão do Curso de Ciência da Computação da Faculdade de Computação na Universidade Federal de Mato Grosso do Sul, na área de Segurança em Rede.

Universidade Federal de Mato Grosso do Sul - UFMS

Faculdade de Computação - FACOM

Ciência da Computação

Orientador: Carlos Alberto da Silva

Campo Grande, MS

21 de novembro de 2018

Jean Carvalho Ortiz
SEM TITULO
AINDA/ Jean Carvalho Ortiz. – Campo Grande, MS, 21 de novembro de 2018-
51 p. : il. ; 30 cm.

Orientador: Carlos Alberto da Silva

Conclusão de Curso – Universidade Federal de Mato Grosso do Sul - UFMS
Faculdade de Computação - FACOM
Ciência da Computação, 21 de novembro de 2018.

1. Nessus. 2. Ethical Hacking. 2. Network Security. I. Carlos Alberto da Silva. II. Universidade Federal de Mato Grosso do Sul. III. Faculdade de Computação. IV. SEM TITULO AINDA

Jean Carvalho Ortiz

SEM TITULO
AINDA

Trabalho de Conclusão do Curso de Ciência da Computação da Faculdade de Computação na Universidade Federal de Mato Grosso do Sul, na área de Segurança em Rede.

Trabalho aprovado. Campo Grande, MS, 24 de novembro de 2012:

Carlos Alberto da Silva
Orientador

Professor
Convidado 1

Professor
Convidado 2

Campo Grande, MS
21 de novembro de 2018

Que a Força esteja com você.

Agradecimentos

TODO

Resumo

TODO

Palavras-chave: nessus. segurança em rede. hacking ético.

Abstract

TODO

Keywords: nessus. network security. ethical hacking.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

SO	Sistema Operacional
Kali	Kali Linux
IP	*Internet Protocol*

Sumário

Introdução

Este trabalho tem como objetivo a análise de possíveis falhas de segurança em *websites*, utilizando a ferramenta **Nessus**.
Após verificação das falhas de segurança, serão apresentadas possíveis soluções para o problema em questão, assim como possíveis modos para explorar essas falhas. Elas serão classificadas conforme o dano que pode ser causado ao sistema.

Parte I

Preparação da pesquisa

1 Kali Linux

1.1 Escolha do Sistema Operacional

Para o desenvolvimento desse estudo foi escolhido o Kali Linux como sistema operacional, pois esse SO é enriquecido com várias ferramentas para realização de *Pentests*, entre outras atividades de *hacking*.
O Kali Linux é uma distribuição GNU/Linux baseada no Debian e é um sistema *Open-Source* distribuído sob a licença **GNU GPL**. Ele é desenvolvido e mantido pela Offensive Security Ltd.

2 Nessus

2.1 Sobre o Nessus

A ferramenta utilizada nesse estudo é a Nessus Home, que é uma versão para uso pessoal e estudos, as diferenças entre a versão *Professional* é que há uma limitação de 16 endereços de IP por escaneamento, não há acesso ao suporte da ferramenta e não é possível realizar verificações de conformidade e auditoria de conteúdo.
Nessus é desenvolvido e distribuido pela Tenable Network Security, Inc e distribuído sob os termos da Licença Pública Geral GNU. Ele é composto por um cliente e um servidor, sendo o *scan* feito pelo servidor.
O *nessusd* (servidor Nessus) realiza um escaneamento e portas ao alvo e após encontrar uma porta aberta, é executado diversos scripts escritos em NASL (Nessus Attack Scripting Language) que verificam as vulnerabilidade.

2.2 Instalação

Primeiramente para realizar a instalação do Nessus Home é necessário adquirir uma licença pelo URL http://www.nessus.org/products/nessus/nessus-plugins/obtain-an-activation-code. A licença de ativação será enviada para o e-mail registrado. Após realizar o registro, é necessário fazer o *download* do pacote de instalação através da URL http://www.tenable.com/products/nessus/select-your-operating-system, selecionando o seu SO.
Na distribuição Kali, a instalação pode ser feita através do terminal, navegando até a pasta onde foi feito o *download* e executar o comando: **sudo dpkg -i Nessus-*.deb**.
Após a instalação ser concluída, o terminal irá mostrar o endereço de acesso ao Nessus, por exemplo http://kali:8834/.
Para iniciar o serviço do Nessus, basta executar no terminal o comando: **service nessusd start**, acessar o endereço que foi dado anteriormente e entrar com o código de ativação. Será executado a compilação de todos os *plugins* utilizados pela ferramenta.

2.3 Configuração

Para a realização dos testes foi realizado a criação de uma politica de *plugins*, na qual são definidos quais as vulnerabilidades que serão buscadas durante o *scan*.
Para esse estudo foi utilizado um *scan* completo do *website* utilizando todos os *plugins*

disponíveis, na qual retornam várias informações sobre a página, além de suas vulnerabilidades.

Parte II

Testes

3 Plugins

3.1 Plugins Utilizados

Os *plugins* utilizados nesse estudo e os seus respectivos *IDs* no Nessus são os seguintes:

10815 Web Server Generic XSS

11229 Web Server info.php / phpinfo.php Detection

15855 POP3 Cleartext Logins Permitted

26194 Web Server Transmits Cleartext Credentials

31705 SSL Anonymous Cipher Suites Supported

33850 Unix Operating System Unsupported Version Detection

40984 Browsable Web Directories

42873 SSL Medium Strength Cipher Suites Supported

44135 Web Server Generic Cookie Injection

45411 SSL Certificate with Wrong Hostname

46803 PHP expose_php Information Disclosure

51192 SSL Certificate Cannot Be Trusted

54582 SMTP Service Cleartext Login Permitted

58987 PHP Unsupported Version Detection

62565 Transport Layer Security (TLS) Protocol CRIME Vulnerability

65702 Git Repository Served by Web Server

65821 SSL RC4 Cipher Suites Supported (Bar Mitzvah)

70658 SSH Server CBC Mode Ciphers Enabled

71049 SSH Weak MAC Algorithms Enabled

85582 Web Application Potentially Vulnerable to Clickjacking

90067 WordPress User Enumeration

90317 SSH Weak Algorithms Supported

3.2 Descrição dos Plugins

3.2.1 Web Server Generic XSS

O host remoto está executando um servidor Web que não consegue desinfectar adequadamente solicitações de JavaScript malicioso. Um invasor remoto pode explorar esse problema, por meio de um pedido especialmente criado, para executar arbitrariamente HTML e código de script no navegador de um usuário dentro do contexto de segurança do site afetado.

3.2.2 Web Server info.php / phpinfo.php Detection

Muitos tutoriais de instalação do PHP instruem o usuário a criar um arquivo PHP que chama a função PHP ' phpinfo () ' para fins de depuração. Vários aplicativos PHP também podem incluir esse arquivo. Ao acessar esse arquivo, um invasor remoto pode descobrir uma grande quantidade de informações sobre o servidor Web remoto, incluindo:

- O nome do usuário que instalou o PHP e se eles são um usuário SUDO.
- O endereço IP do host.
- A versão do sistema operativo.
- A versão do servidor Web.
- O diretório raiz do servidor Web.
- Informações de configuração sobre a instalação remota do PHP.

3.2.3 POP3 Cleartext Logins Permitted

O host remoto está executando um *DAEMON* POP3 que permite logons de texto sem criptografia em conexões não criptografadas. Um invasor pode descobrir nomes de usuário e senhas farejando o tráfego para o *DAEMON* POP3 se um mecanismo de autenticação menos seguro (por exemplo, comando USER, AUTH PLAIN, AUTH LOGIN) é usado.

3.2.4 Web Server Transmits Cleartext Credentials

O servidor Web remoto contém vários campos de formulário HTML contendo uma entrada do tipo '*password*' que transmitem suas informações para um servidor Web remoto em texto não criptografado.
Um invasor que está escutando o tráfego entre o navegador da Web e o servidor pode obter logins e senhas de usuários válidos.

3.2.5 SSL Anonymous Cipher Suites Supported

O host remoto suporta o uso de codificadores SSL anônimos. Embora isso permita que o administrador configure um serviço que criptografa o tráfego sem ter que gerar e configurar certificados SSL, ele não oferece nenhuma maneira de verificar a identidade do host remoto e torna o serviço vulnerável a um ataque *man-in-the-middle*.
Observação: Isso é consideravelmente mais fácil de explorar se o invasor estiver na mesma rede física.

3.2.6 Unix Operating System Unsupported Version Detection

De acordo com seu número de versão autorrelatada, o sistema operacional UNIX em execução no host remoto não é mais suportado.
A falta de suporte implica que nenhum novo *patch* de segurança para o produto será liberado pelo fornecedor. Como resultado, é provável que contenha vulnerabilidades de segurança.

3.2.7 Browsable Web Directories

Vários plugins Nessus identificaram diretórios no servidor Web que são navegáveis.

3.2.8 SSL Medium Strength Cipher Suites Supported

O host remoto suporta o uso de codificadores SSL que oferecem criptografia de força média. Nessus considera a força média como qualquer criptografia que usa comprimentos de chave pelo menos 64 bits e menos de 112 bits, ou então que usa o conjunto de criptografia 3DES.
Observe que é consideravelmente mais fácil burlar a criptografia de força média se o invasor estiver na mesma rede física.

3.2.9 Web Server Generic Cookie Injection

O host remoto está executando um servidor Web que não consegue adequadamente desinfectar seqüências de solicitações de JavaScript maliciosos. Aproveitando esse problema, um invasor pode ser capaz de injetar *Cookies* arbitrários. Dependendo da estrutura do aplicativo Web, pode ser possível lançar um ataque de "fixação de sessão"usando esse mecanismo. O Nessus não verificou se o ataque de fixação da sessão é viável e este não é o único vetor de fixação de sessão.

3.2.10 SSL Certificate with Wrong Hostname

O atributo 'commonName' (CN) do certificado SSL apresentado para este serviço é para uma máquina diferente.

3.2.11 PHP expose_php Information Disclosure

A instalação do PHP no servidor remoto é configurada de forma a permitir a divulgação de informações potencialmente sensíveis a um invasor por meio de uma URL especial. Tal URL dispara um *"Easter Egg* embutido no próprio PHP.

Outros *"Easter Eggs* provavelmente existem, mas Nessus não verificou eles.

3.2.12 SSL Certificate Cannot Be Trusted

O certificado X.509 do servidor não é confiável. Esta situação pode ocorrer de três maneiras diferentes, em que a cadeia de confiança pode ser quebrada, como indicado abaixo:

- Primeiro, a parte superior da cadeia de certificados enviada pelo servidor pode não ser descendente de uma autoridade de certificação pública conhecida. Isso pode ocorrer quando a parte superior da cadeia é um certificado não reconhecido, auto-assinado ou quando certificados intermediários que conectariam a parte superior da cadeia de certificado a uma autoridade de certificação pública conhecida estão ausentes.

- Em segundo lugar, a cadeia de certificados pode conter um certificado que não é válido no momento da verificação. Isso pode ocorrer quando a verificação ocorre antes de uma das datas *notBefore* do certificado, ou após uma das datas *notAfter* do certificado.

- Em terceiro lugar, a cadeia de certificados pode conter uma assinatura que não correspondeu às informações do certificado ou não pôde ser verificada. Assinaturas ruins podem ser corrigidas obtendo o certificado com a assinatura incorreta para ser re-assinado pelo seu emissor. As assinaturas que não puderam ser verificadas são o resultado do emissor do certificado usando um algoritmo de assinatura que o Nessus não suporta ou não reconhece.

Se o host remoto for um host público em produção, qualquer quebra na cadeia torna mais difícil para os usuários verificarem a autenticidade e a identidade do servidor Web. Isso pode facilitar a realização de ataques *man-in-the-middle* contra o host remoto. "

3.2.13 SMTP Service Cleartext Login Permitted

O host remoto está executando um servidor SMTP que anuncia que ele permite logons de texto não criptografado em conexões não criptografadas. Um invasor pode ser capaz de descobrir nomes de usuário e senhas farejando tráfego para o servidor se um mecanismo de autenticação menos seguro (ou seja, LOGIN ou PLAIN) é usado.

3.2.14 PHP Unsupported Version Detection

De acordo com sua versão, a instalação do PHP no host remoto não é mais suportada.

A falta de suporte implica que nenhum novo *patch* de segurança para o produto será liberado pelo fornecedor. Como resultado, é provável que contenha vulnerabilidades de segurança.

3.2.15 Transport Layer Security (TLS) Protocol CRIME Vulnerability

O serviço remoto tem uma das duas configurações que são conhecidas por serem necessárias para o ataque de CRIME:

- A compactação SSL/TLS está habilitada.
- TLS anuncia o protocolo SPDY anteriores à versão 4.

O Nessus não tentou lançar o ataque CRIME contra o serviço remoto, apenas verificou que é possivel realizar o ataque.

3.2.16 Git Repository Served by Web Server

O servidor Web no host remoto permite o acesso de leitura a um repositório git. Essa falha potencial pode ser usada para baixar o conteúdo do servidor Web que, de outra forma, pode ser privado.

3.2.17 SSL RC4 Cipher Suites Supported (Bar Mitzvah)

O host remoto suporta o uso de RC4 em um ou mais conjuntos de codificação. A cifra RC4 é falho em sua geração de um fluxo pseudo-aleatório de bytes para que uma grande variedade de pequenas distorções são introduzidos no fluxo, diminuindo sua aleatoriedade. Se o texto sem formatação for criptografado repetidamente (por exemplo, *Cookies* HTTP) e um invasor conseguir obter muitos (ou seja, dezenas de milhões) de textos cifrados, o invasor poderá derivar o texto sem formatação.

3.2.18 SSH Server CBC Mode Ciphers Enabled

O servidor SSH está configurado para suportar criptografia de encadeamento de bloco de codificação (CBC). Isso pode permitir que um invasor recupere a mensagem de texto sem formatação do texto cifrado.
Este plugin só verifica as opções do servidor SSH e não verifica se há versões de software vulneráveis.

3.2.19 SSH Weak MAC Algorithms Enabled

O servidor SSH remoto está configurado para permitir algoritmos de MD5 ou MAC 96 bits, ambos considerados fracos.
Este plugin só verifica as opções do servidor SSH e não verifica se há versões de software vulneráveis.

3.2.20 Web Application Potentially Vulnerable to Clickjacking

O servidor web remoto não define um cabeçalho de resposta X-Frame-Options ou um cabeçalho de resposta Content-Security-Policy 'frame-ancestors' em todas as respostas de conteúdo. Isto poderia potencialmente expor o site para um *clickjacking* ou ataque de reparação de interface do usuário, no qual um invasor pode enganar um usuário para clicar em uma área da página vulnerável que é diferente do que o usuário percebe. Isso pode resultar em transações fraudulentas ou maliciosas.

X-Frame-Options foi proposto pela Microsoft como uma maneira de atenuar os ataques de *clickjacking* e atualmente é suportado por todos os fornecedores dos principais navegadores de Internet.

Content-Security-Policy (CSP) foi proposto pela W3C Web Application Security Working Group, com crescente apoio entre todos os fornecedores dos principais navegadores, como uma forma de atenuar o *clickjacking* e outros ataques. A Directiva de política 'frame-ancestors' restringe quais fontes podem incorporar o recurso protegido.

Observe que enquanto o X-Frame-Options e cabeçalhos de resposta Content-Security-Policy não são as únicas mitigações para *clickjacking*, eles são atualmente os métodos mais confiáveis que podem ser detectados através da automação. Portanto, este plugin pode produzir resultados falsos positivos se forem implantadas outras estratégias de mitigação (por exemplo, frame-busting JavaScript) ou se a página não executa quaisquer transações confidenciais.

3.2.21 WordPress User Enumeration

A versão do WordPress hospedado no servidor web remoto é afetada pela enumeração de vulnerabilidade de usuário. Um invasor remoto não autenticado, pode explorar isto para aprender os nomes de usuários válidos do WordPress.
Esta informação pode ser usada para montar mais ataques.

3.2.22 SSH Weak Algorithms Supported

Nessus detecta que o servidor SSH remoto está configurado para usar a codificação de fluxo Arcfour ou nenhuma cifra. RFC 4253 desaconselha usar o Arcfour devido a um problema com chaves fracas.

3.3 Hosts Testados

Para realizar a escolha dos *hosts* não houve um critério especifico, foram pegos sites na qual frequentei recentemente. Os alvos desse estudo são os seguintes:

- alexanderfleming.com.br
- alphamu.com.br
- boticario.com.br
- cantinaromana.com.br
- digix.com.br
- jera.com.br
- locaweb.com.br
- megapowerms.com.br
- paradanerd.com.br
- terra.com.br

Os testes foram iniciados no dia 25 de setembro de 2018 às 19:30 (UTC -4) e foram concluídos no dia 26 de setembro de 2018 às 12:15 (UTC -4), sendo gerado o relatório pelo **Nessus** às 12:19 do mesmo dia.

4 Resultados

4.1 Contagem de Riscos

4.1.1 Total de riscos encontrados

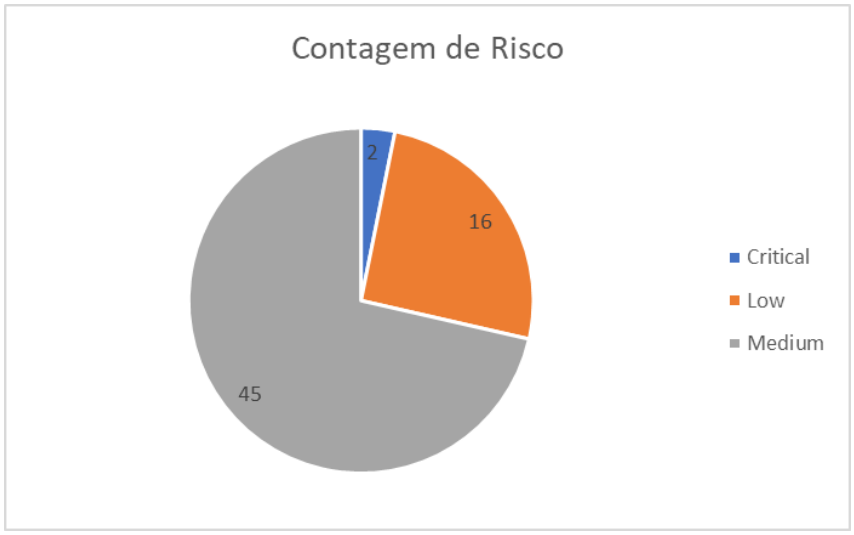

Figura 1 – Contagem de risco dos hosts testados

4.1.2 Alexander Fleming

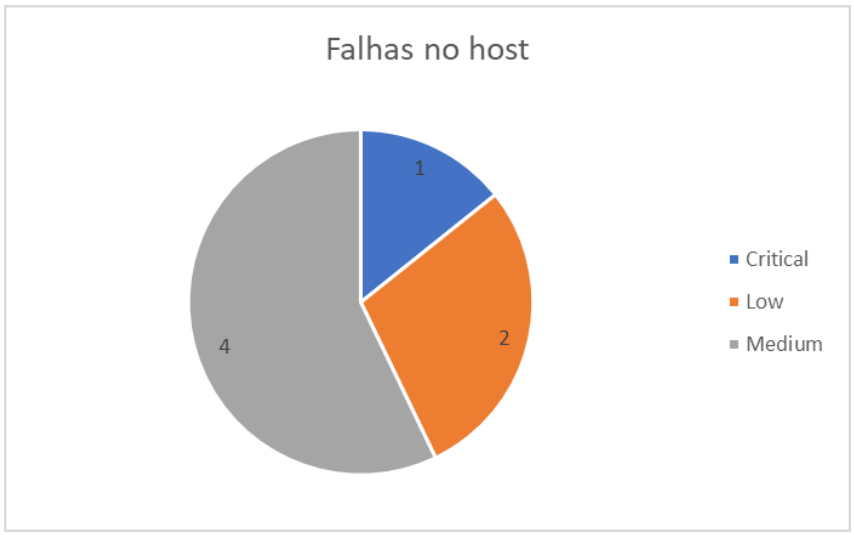

Figura 2 – Contagem de risco do host alexanderfleming.com.br

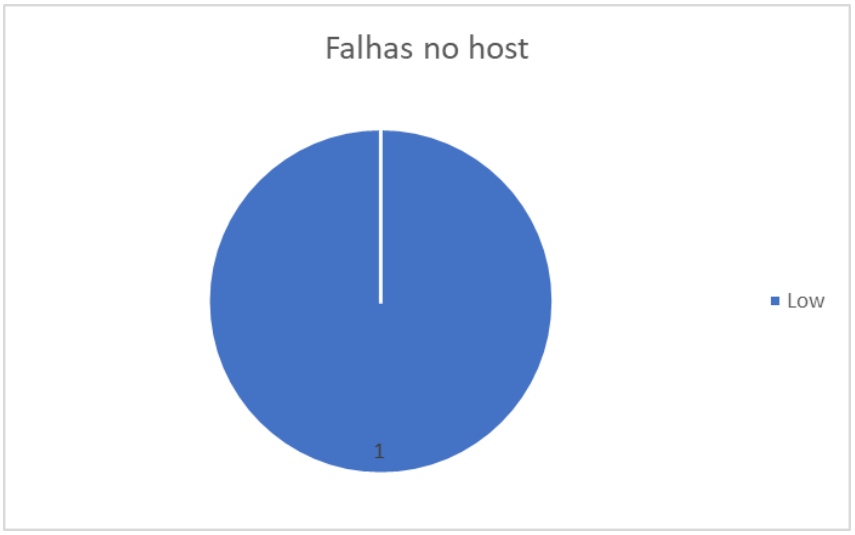

Figura 3 – Contagem de risco do host alphamu.com.br

4.1.3 AlphaMU

4.1.4 Boticario

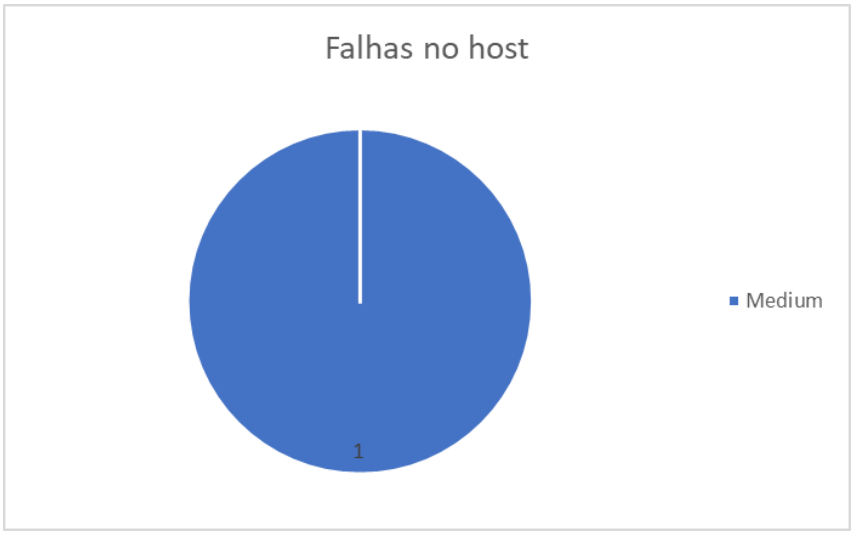

Figura 4 – Contagem de risco do host boticario.com.br

4.1.5 Cantina Romana

4.1.6 Digix

4.1.7 FACOM, Google e Registro.br

Não foi encontrada nenhuma falha nos hosts facom.ufms.br, google.com.br e registro.br

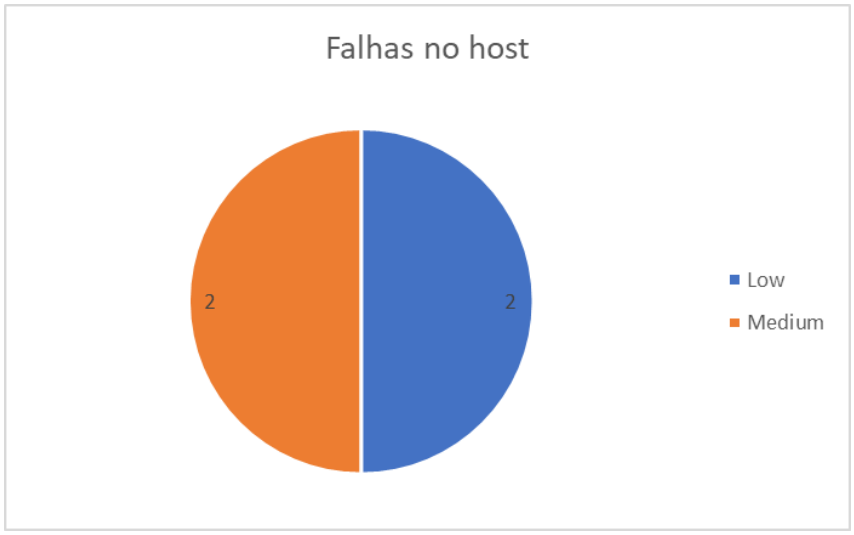

Figura 5 – Contagem de risco do host cantinaromana.com.br

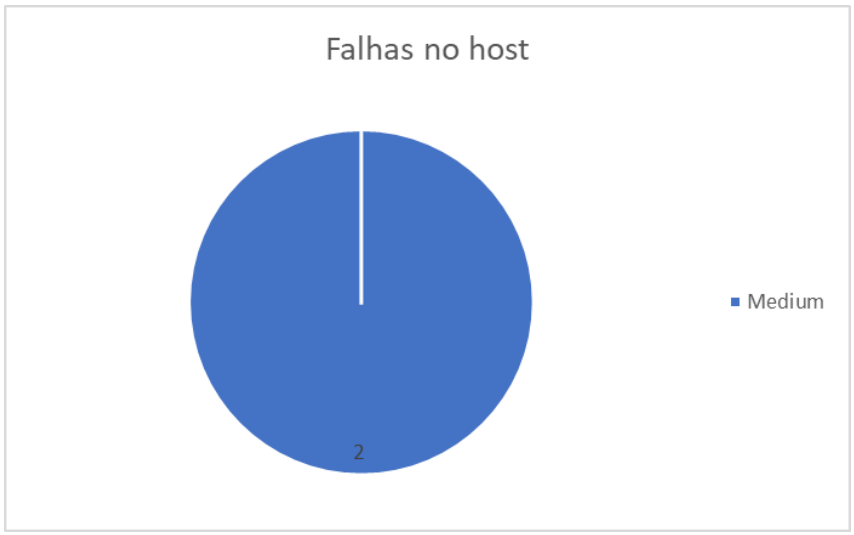

Figura 6 – Contagem de risco do host digix.com.br

4.1.8 Jera

4.1.9 Locaweb

4.1.10 MegaPowerMS

4.1.11 Parada Nerd

4.1.12 Terra

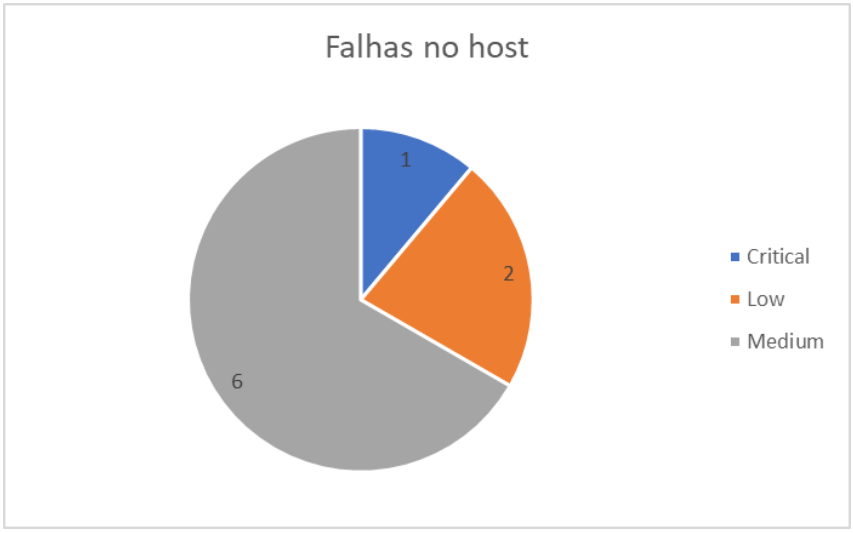

Figura 7 – Contagem de risco do host jera.com.br

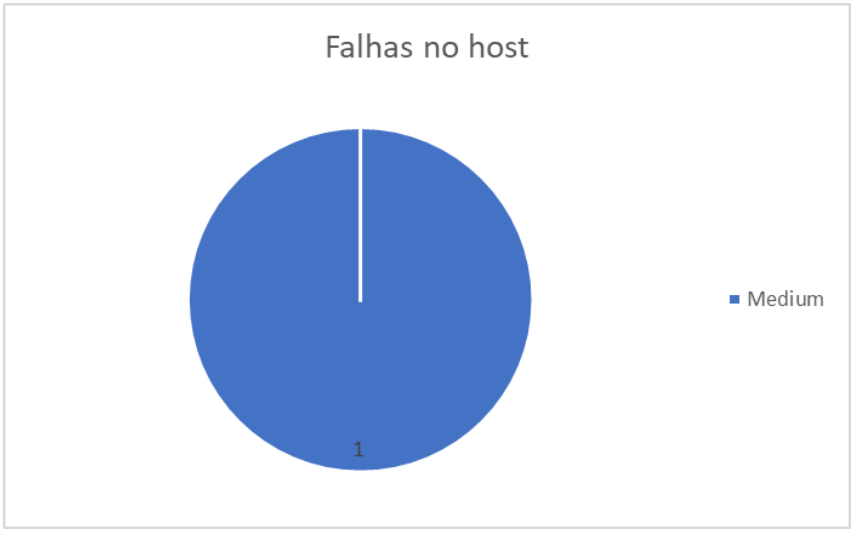

Figura 8 – Contagem de risco do host locaweb.com.br

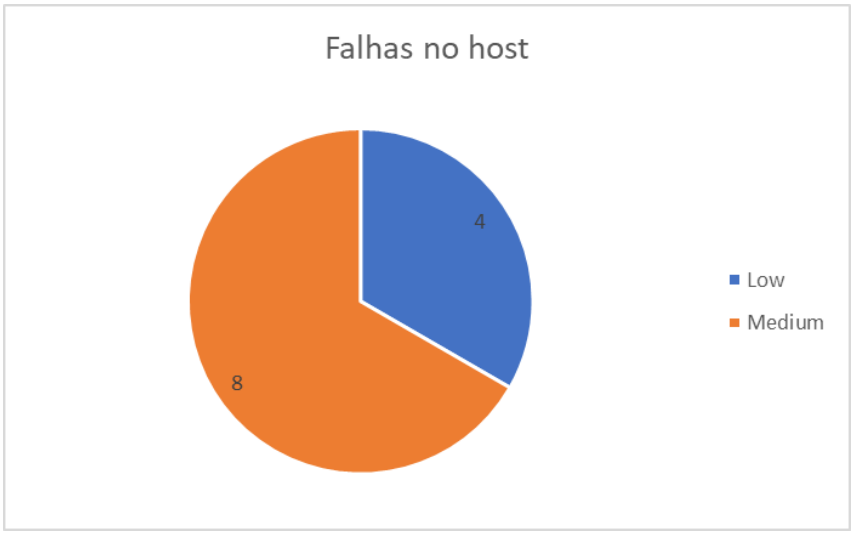

Figura 9 – Contagem de risco do host megapowerms.com.br

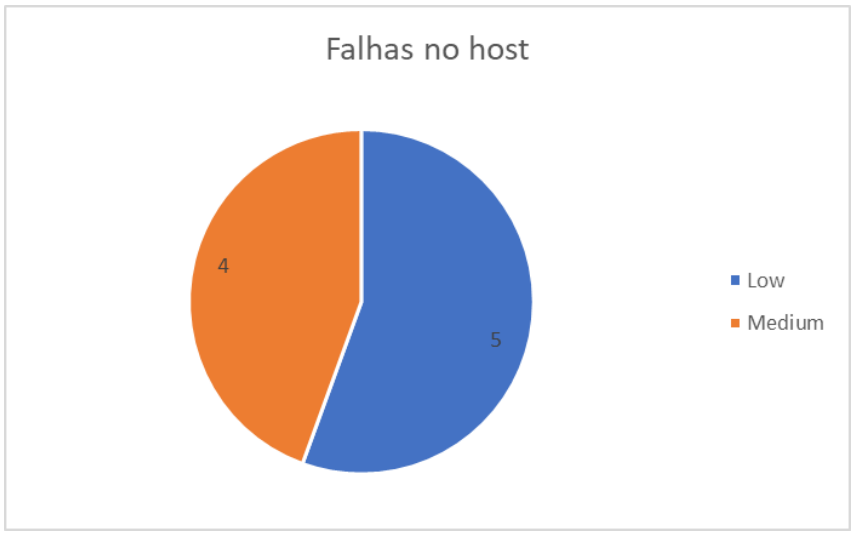

Figura 10 – Contagem de risco do host paradanerd.com.br

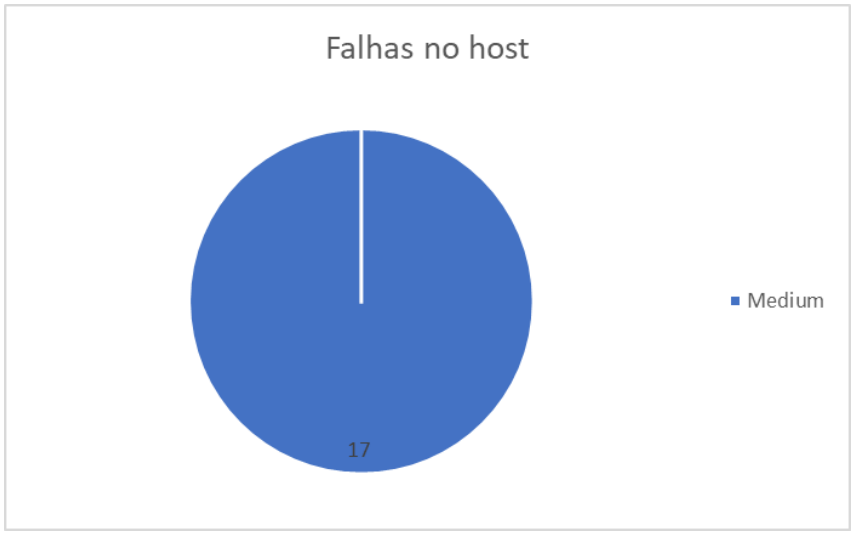

Figura 11 – Contagem de risco do host terra.com.br

5 Comparações

6 Possíveis soluções para os problemas

7 Explorando as falhas

8 Conclusão