Análise de vulnerabilidade em ambiente de servidor corporativo

Gabriela Melo do Vale[1], Luciana Pennafort Silva[2], Thiago Coqueiro[3].

Curso de Pós-Graduação em Segurança Computacional – Estácio de Belém IESAM – Campus de Belém
66055-260 – Belém – PA– Brasil

gabbimv@gmail.com[1], luciana.pennaforts@gmail.com[2], thiago.coqueiro@estacio.br[3]

Abstract. *This article describes the analysis and study of possible vulnerabilities in servers of a corporate network. Pointing out proposals and solutions for the computational security of analyzed servers, in order to improve the performance of the services offered by these applications within the corporate structure studied.*

Resumo. *Este artigo retrata a análise e estudo de possíveis vulnerabilidades em servidores de uma rede corporativa. Apontando propostas e soluções para a segurança computacional dos servidores analisados, para que ocorra a melhora no desempenho dos serviços oferecidos por essas aplicações dentro da estrutura corporativa estudada.*

1. Introdução

Segundo Coelho, Flavia E.S, et al. (Gestão da Segurança da Informação NBR 27001 e NBR 27002, 2014) a segurança da informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros e manipulação não autorizada. Objetivando a redução da probabilidade e do impacto de incidentes de segurança. Medidas de controles devem ser implantadas, monitoradas, analisadas minuciosamente, criticamente e em cima de relatórios apresentados por profissionais especialistas em segurança. Todas essas medidas realizadas para a melhoria da segurança no ambiente digital e tecnológico da organização.

Existem vários tipos de ameaças no mundo cibernético, porém as seguranças computacionais e da informação apresentam soluções para a prevenção, análise e correção de falhas na segurança de redes e servidores. Possibilitando a continuidade do negócio e maximizando o retorno sobre as oportunidades e investimentos do mesmo. Através da utilização de ferramentas adequadas, podemos minimizar os riscos no ambiente digital e aumentar a segurança das informações da empresa contidas no servidor. A segurança é obtida através de resultados da implementação de uma série de conjuntos para controlar, compreender políticas de segurança, processos, procedimentos e estruturas organizacionais. Em particular, os controles necessitam ser estabelecidos, implementados, monitorados e através de uma análise técnica, deverão ser propostas as melhores soluções de segurança, que atendam a estrutura da organização.

A vulnerabilidade é uma fragilidade que, ao ser estudada, pode comprometer a segurança de informações da organização. Falhas como configurações incorretas, sistemas não atualizados, entre outros fatores, resultam no ataque por parte de hackers e crackers. Comprometendo informações de suma importância para a organização. Há ferramentas que conseguem detectar vulnerabilidades através de uma análise da estrutura de configuração do servidor, retornando resultados e propondo, inclusive, possíveis soluções e relatórios.

O software Nessus, proporcionou uma análise mais acentuada em relação ao ambiente utilizado, retornando resultados sobre qual a porcentagem de segurança, apresentando os riscos à organização através de relatórios e indicando a solução mais adequada para a falha detectada, a fim de melhorar o ambiente da organização.

Este trabalho tem como objetivo, realizar análise de vulnerabilidade em ambiente corporativo de uma rede corporativa, utilizando um software específico em servidores *Linux* e *Windows*. Apresentando o grau de falhas na segurança das informações, como: crítico (*critical*), alto (*high*), médio (*médium*), baixo (*low*) ou info (*info*); os riscos que apresenta ao ambiente em questão, e quais as possíveis medidas que poderão ser aplicadas para fortalecer e proteger a segurança das informações dentro desse ambiente corporativo.

Como objetivos específicos, foi proposto analisar falhas na segurança das informações contidas no servidor, utilizando o *software Nessus;* apresentando relatórios gerados através dos resultados obtidos com a análise, e possíveis medidas de correção para as falhas encontradas.

1. Introdução; 2. Fundamentação teórica; 3. Metodologia e resultados esperados;

4. Estudo de Caso; 5. Conclusão.

2. Fundamentação Teórica

Segundo Melo, Sandro (Exploração de Vulnerabilidades em Redes TCP/IP, 2107) *Análise de Vulnerabilidade* trata do processo de identificação de falhas e vulnerabilidades conhecidas presentes no ambiente e que o expõem a ameaças. Essas falhas podem ser ocasionadas por erros de programação, configuração incorreta, falta de atualização do sistema e aplicativos ou simplesmente falha humana. Ao utilizarmos um aplicativo que faça a análise, o mesmo irá mapear os programas e serviços que possam conter falhas e vulnerabilidades, reportando esses resultados através de relatórios. Desse modo poderemos tratar e mitigar as falhas encontradas, garantindo maior segurança ao ambiente e estabelecendo uma nova linha de base para futuras análises.

Dentre as diversas ferramentas existentes, o *Port Scanner, Protocolo Analyzer, Honeypots/Honey/nets*, *Vunerability Scanners* serão usados como referência nos processos de análise. Abaixo, nos itens de 2.1 a 2.5, a descrição de cada uma delas.

2.1 *Port Scanner*

Trata-se de uma ferramenta utilizada para fazer a varredura das portas do protocolo TCP/IP de cada host analisado na rede, identificando quais destas portas estão abertas ou expostas. Este resultado ajuda a identificar quais serviços estão rodando em um determinado host, quais estão devidamente filtrados, e se há exposição desnecessária de serviços.

2.2 *Protocol Analyzer*

São definidos como analisadores de protocolos ou *Sniffers*, ferramentas capazes de visualizar o tráfego de rede, capturando pacotes trafegados e permitindo a análise de seu conteúdo, ajuda a identificar o comportamento "padrão" de sua rede na hora de estabelecer uma "linha de base", também é possível monitorar a comunicação de seus dispositivos e aplicações, observando o que está sendo trafegado, identificando erros, e verificando que tipo de informação é transmitida.

2.3 *Honeypots/Honeynets*

Frequentemente utilizados para atrair ameaças que normalmente seriam direcionadas a seu ambiente de produção. Analisam ataques, estudando a forma como ocorreu, o que pôde ser danificado ou comprometido, quais vulnerabilidades foram exploradas e quais serviços afetados.

Essas informações permitem que você tome conhecimento desses métodos e possa aprender a se prevenir contra eles no futuro.

2.4 *Vulnerability Scanners*

São ferramentas inteligentes capazes de *scanear* uma aplicação, analisando serviços, versões de software, sistemas operacionais, bancos de dados e outros elementos em seu ambiente, identificando versões desatualizadas, patches de correção não aplicados, má configuração e outros detalhes que possam expô-lo a ameaças.

Essas ferramentas "aprendem", sendo constantemente alimentadas com informações de novos *patches* de correção e atualizações de sistema dos fornecedores, garantindo que seu ambiente seja checado contra as mais novas descobertas de vulnerabilidades.

2.5 O *Software Tenable Nessus Vulnerability Scanner*

É uma solução de avaliação de vulnerabilidades muito conhecida devido a sua excelência e tecnologia avançada. Identifica as vulnerabilidades e problemas de configuração que hackers usam para penetrar a rede. O *Nessus* suporta uma grande gama de dispositivos de rede, sistemas operacionais, bancos de dados, aplicações em infraestruturas físicas, virtuais e na nuvem, o qual faz varreduras para vírus, *malwares*, *backdoors*, *hosts* de comunicação com os sistemas infectados por *botnets*, processos conhecido-desconhecidos, bem como serviços da web com *links* para conteúdos maliciosos.

Seu relatório é de fácil compreensão, com possibilidade de exploração, modificação de gravidade, agendamento de verificação e entrega de relatórios de correção por e-mail.

3. Metodologia e resultados esperados

Durante o processo de análise de vulnerabilidade nos servidores de uma rede corporativa, foi definida a ferramenta a ser utilizada para fazer a captura dos dados necessários, de modo que, resultados apresentados classificam-se em: crítico, alto, médio, baixo e info (informação). A ênfase foi dada aos resultados de vulnerabilidades críticas e altas de servidores. Onde serão apresentadas possíveis soluções para a melhoria da segurança, protegendo informações importantes da empresa.

Foram utilizados como forma de conhecimento, livros, artigos científicos, tutoriais e softwares de análise como o *Nessus*, que irá apontar riscos e falhas de segurança nos servidores Linux e Windows para o desenvolvimento do estudo de caso.

O estudo de caso foi realizado com um notebook *Dell System Vostro 3450* com sistema *Windows 7 Professional SP1 64-bit*, *Navegador Firefox Quantum 57.03 64-bit*, Instalação do *Tenable Nessus Vulnerability Scanner (https://localhost:8834/#/scans/folders/my-scans)*, onde, através do escaneamento da rede corporativa composta por 100 equipamentos incluindo *hosts* (servidores *Windows* e *Linux*), roteadores *Cisco*, *Switch* gerenciável, *Proxy/Firewall*, concentradores, foi dado ênfase à duas aplicações, sendo uma *Linux* e outra *Windows*. Nos resultados fora apresentada a quantidade de vulnerabilidades encontradas em relação aos dois servidores. Onde quatro falhas identificadas foram escolhidas, sendo, duas de grau crítico e duas em nível alto. Apresentou-se uma solução que deverá ser aplicada para prevenir ou reparar a cada uma dessas vulnerabilidades.

Figura 1. Interface Software Nessus.

Os resultados obtidos pela análise de vulnerabilidade retornaram informações suficientes sobre o estado de exposição a ameaças. Apontando o que pode ocorrer, com que frequência e o grau vulnerável (se crítico, alto, médio, baixo ou informação) que a aplicação apresenta. Descrito através de relatórios técnicos, aponta quais serviços e sistemas estão sujeitos e a quais tipos de ameaças.

4. Estudo de Caso

4.1 Análise de vulnerabilidade em ambiente de servidor corporativo

4.1.1 Análise de vulnerabilidade com uso da Ferramenta Nessus.

A análise foi realizada na rede de um grupo corporativo composto em média por cem equipamentos conectados em rede, incluindo servidores *Linux* e *Windows*, homologação e de produção, *switch* gerenciável, roteadores e concentradores. Foram encontradas vulnerabilidades de classificação crítica, alta, média, baixa e info (informação), como aponta a tabela de resultados e o gráfico abaixo:

Tabela 1. Relatório de resultados da análise de vulnerabilidade.

VULNERABILIDADE	QUANTIDADE	PERCENTUAL
Crítico/ *CRITICAL*	39,00	8,00%
Alto/ *HIGH*	56,00	11,47%
Médio/ *MEDIUM*	113,00	23,15%
Baixo/ *LOW*	23,00	4,72%
Informação/ *INFO*	257,00	52,66%
TOTAL	488,00	100,00%

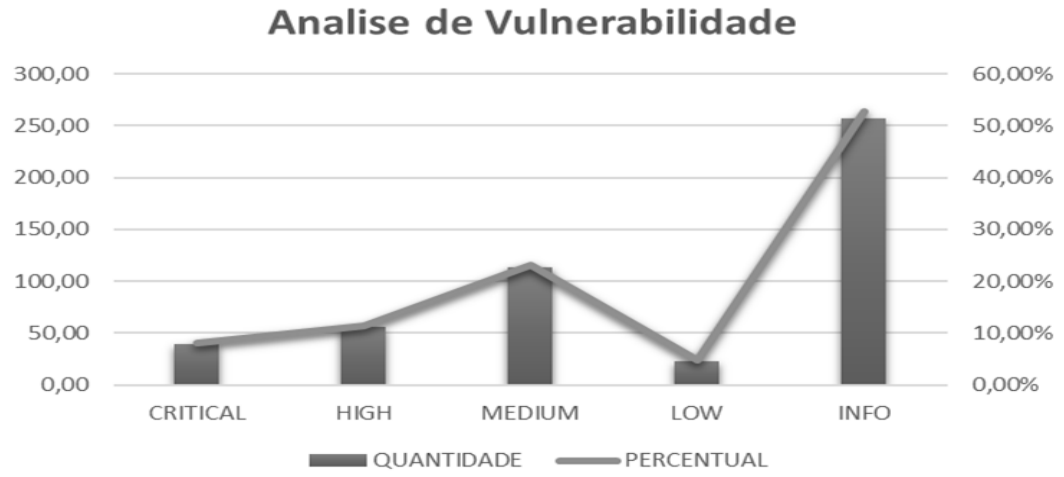

Figura 2. Gráfico de análise de vulnerabilidade.

Pode-se observar na tabela 1, que foram identificadas quatrocentas e oitenta e oito vulnerabilidades no ambiente corporativo, sendo a porcentagem de 8,00% (trinta e nove máquinas) de falhas em grau crítico e 11,47% (cinquenta e seis máquinas) de vulnerabilidade em nível alto.

Quatro servidores foram escolhidos de acordo com a relevância das falhas apresentadas, dois utilizando sistema operacional *Windows Server* e outros dois rodando *Linux Debian*.

4.2 Análises em Servidores *Windows Server*.

4.2.1 Máquina *SIG6_POS_SERVER – IP 10.0.0.123*

O Servidor com sistema operacional *Microsoft Windows 2000 Server Service Pack 4* obteve análise com duração de trinta e oito minutos, onde está instalada a aplicação do SIG6. Como resultado de sua análise, o mesmo apresentou cento e treze vulnerabilidades, sendo dezessete em nível crítico, três em grau alto, oito baixos e oitenta e quatro de *info*.

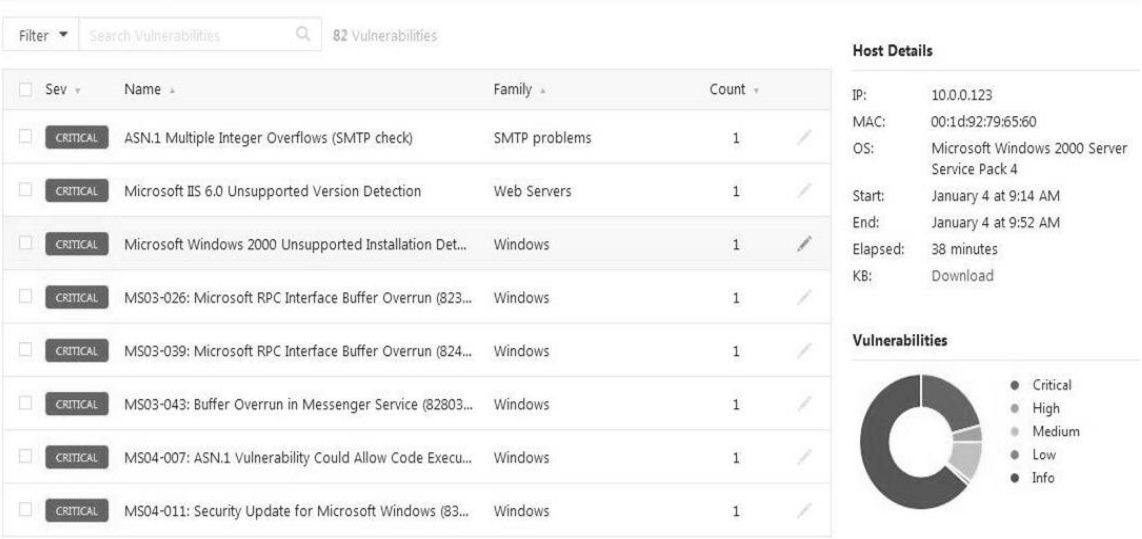

Figura 3. Análise do servidor SIG6, vulnerabilidades encontradas.

4.2.1.1 Descrição da Vulnerabilidade *ASN.1 Multiple Integer Overflows (SMTP check).*

É uma vulnerabilidade crítica, a qual informa que o *host* remoto do *Windows* possui uma biblioteca *ANS.1*. Esse problema pode levar ao limite suportado pelo buffer baseado na pilha, um invasor poderá explorar essa vulnerabilidade, importando um script com código arbitrário onde poderá executa-lo posteriormente.

Em particular, quando enviado um pacote malformado de autorização *SMTP*, esse *check* vai determinar que o host remoto não foi corrigido, dando possibilidades de intrusão.

Solução

Como o Sistema operacional é *Windows 2000*, pode-se migrar o sistema para o *Windows 2003* e depois para o *Windows 2008*, posteriormente para o *Windows 2012* e realizar as atualizações necessárias. Outra solução será a atualização do sistema com o conjunto de *patch do Windows* para o NT, 2000, XP e 2003.
Porta atacada: 25/ tcp/ smtp.

4.2.2 Máquina vermelha IP 10.49.10.43.

Servidor virtual de produção com sistema operacional *Microsoft Windows Server 2008 R2 Standard*, a análise durou cerca de três minutos, está instalada a aplicação do *FORPONTO* e *FORPONTO WEB*. Em sua análise de vulnerabilidade o mesmo apresentou quarenta falhas de segurança, sendo uma crítica (critical), uma alta *(high)*, cinco médias *(médium),* uma baixa *(low)* e trinta e duas informações *(info)*.

A vulnerabilidade em questão enquadra-se em nível alto. Trata-se da facilidade de acesso remoto MS12-020, que será descrita abaixo.

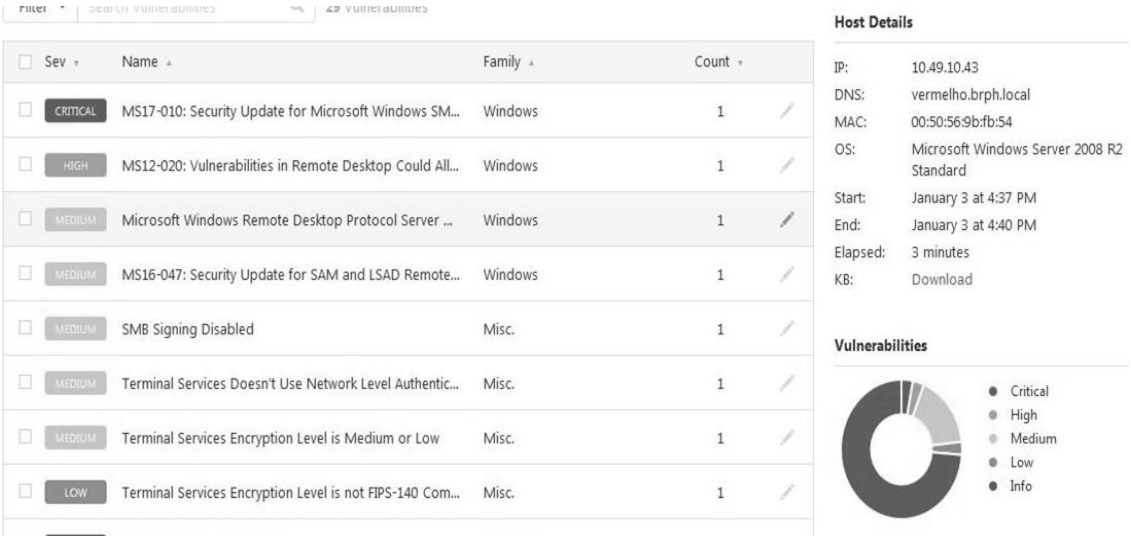

Figura 4. Análise de vulnerabilidade do servidor vermelho 10.49.10.43.

4.2.2.1 Descrição da Vulnerabilidade MS12-020 na Área de Trabalho Remota que pode permitir a execução de código remoto (2671387).

O protocolo RDP (*Remote Desktop Protocol*), apresenta uma vulnerabilidade de grau alto (*high*). Quando não realizada a atualização, essa vulnerabilidade de código remoto arbitrária na implementação do *RDP* no *host* remoto do Windows, ocorre devido a como o RDP acessa um objeto na memória que foi inicializado ou que foi excluído.

Se o RDP for ativado no sistema afetado, um invasor remoto não autenticado poderia utilizar essa falha para fazer com que o sistema execute o código arbitrário enviando uma sequência de pacotes RDP especialmente criados para ele. Esse plugin também verifica uma vulnerabilidade de negação de serviço (DDoS) no Terminal *Server* (TS).

O script não irá detectar a vulnerabilidade se a configuração permitir conexões somente de computadores que executam a Área de Trabalho Remota com Autenticação de Nível de Rede esteja habilitada ou a camada de segurança estiver definida como 'SSL (TLS 1.0)' no host remoto. A porta atacada em questão é a 3389.

Solução

A Microsoft lançou um conjunto de *patches* para Windows XP, 2003, Vista, 2008, 7, and 2008 R2, ou *Fixit*, que não substitui as atualizações de segurança, o recomendável para combater essa vulnerabilidade, para isso, é fazer as atualizações sempre que estiverem disponíveis e deixar o sistema sempre atualizado.

4.3 Análise de vulnerabilidade em Servidor Linux Sig_linux1 IP 10.0.0.2.

Falha de segurança em nível crítico, detecção da Versão do PHP e Apache não suportada. Neste servidor de produção, com aplicação *Linux* onde rodam os serviços de *Proxy/firewall*, a versão do sistema *Linux* instalada é o *Debian Jessie* 8.0, *kernel* 3.16, em sua análise de vulnerabilidade que durou cerca de onze minutos, apresentou cento e oito vulnerabilidades como resultado, distribuídas da seguinte forma: uma vulnerabilidade crítica (*critical*), quatorze em nível alto *(high)*, vinte e duas em grau médio *(médium)*, seis vulnerabilidades do tipo baixo (*low)* e sessenta e cinco informação *(info).*

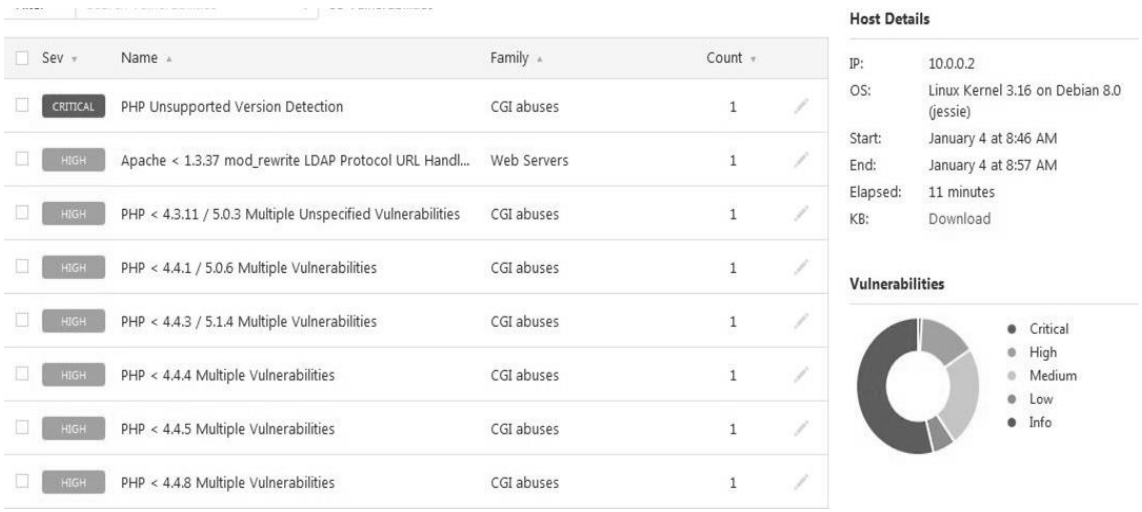

Figura 5. Análise de Vulnerabilidade servidor Linux Debian 10.0.0.2.

4.3.1 Descrição da vulnerabilidade serviços como *PHP* e *Apache* com problemas de atualização.

A versão da aplicação PHP e Apache é muito antiga e não mais suportada, isto é, não possui suporte para recursos atuais, o que ocasiona vulnerabilidade no sistema. A ausência deste suporte, implica que nenhum novo suporte de segurança para o produto será lançado ao fornecedor, ocasionando aberturas para ataques.

Solução

É necessário realizar a atualização da versão do PHP encontrada 4.3.10-15 para a versão mais atual 7.2.x. Atualizar o Apache da versão obsoleta 1.3.33 para a versão 2.5. Manter o Linux atualizado sempre, realizando o *upgrade* e *update* do sistema. A porta atacada em questão é a 80, protocolo *TCP*.

4.4 Servidor de produção virtual IP 10.49.10.14.

Servidor de produção virtual onde está instalada a aplicação de orçamento da empresa, utilizando o *Glassfish Server* 3.1.2.2, a análise durou em torno de três minutos, foram encontradas cinquenta e duas vulnerabilidades no servidor com sistema operacional *Linux Debian* 7.0, *kernel* 3.2, devido a não atualização do sistema operacional e da aplicação *Oracle Glassfish server*, o mesmo apresentou uma vulnerabilidade de grau crítico (*critical*), sete em nível alto (*high*), cinco em nível médio (*médium*), três vulnerabilidades baixas (*low*) e trinta e seis de informação (*info*).

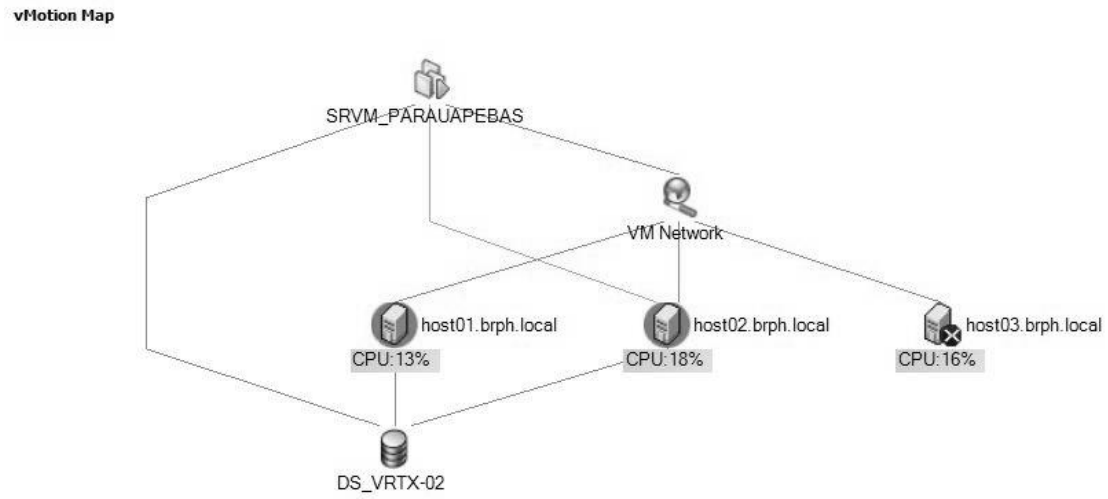

Figura 6. Topologia da Rede

4.4.1 Descrição da vulnerabilidade detecção de versão *Oracle Glassfish Server* 3.1.2.x inferior à mais atual 3.1.2.15.

De acordo com o analisado, a versão do *Oracle Glassfish Server* executado no host remoto é desatualizada, portanto, há vulnerabilidades criticas como: vulnerabilidade de divulgação de informação na versão agrupada da biblioteca *libcurl* na função *smb_request_state()*, devido ao uso de valores válidos sem a verificação dos limites, um invasor remoto não autenticado pode explorar isso, através de um servidor *SMB (Server Message Block)* malicioso para divulgar conteúdos de memória arbitrários (CVE-2015-3237). Outra falha não especificada é no subcomponente *Web Container,* o qual permite que um invasor remoto não autenticado execute o código arbitrário (CVE-2016-3607). A porta em risco é a 9080.

Solução

Atualizar a versão do sistema e da aplicação *Oracle Glassfish Server* 3.1.2.2 para *Oracle Glassfish Server* versão 3.1.2.15 ou posterior como referenciado no aviso de Atualização de *Patch Oracle Critical* de julho de 2016.

5 Conclusão

Quando solicitada a implantação de um servidor, sendo ele *Linux* ou *Windows*, é importante que sejam realizadas atualizações sempre que lançadas pelo fornecedor. A fim de corrigir possíveis brechas que a versão anterior possuía e mitigar riscos de ataque. Promovendo assim, uma maior segurança das informações e processos da empresa a nível computacional.

A análise de vulnerabilidade trata do processo da identificação de falhas de segurança conhecidas e presentes no ambiente em questão e que expõem a empresa a ameaças. Os resultados obtidos através da análise realizada pelo *Nessus* alimentaram com informações suficientes, o atual nível de ameaças que os servidores estão expostos. Mostrou a relação do que pode vir a acontecer, até que ponto pode ser preocupante. Sendo gerado um relatório técnico detalhado dos serviços e sistemas que estão sujeitos, e a quais tipos de ameaças. Dessa forma, o analista de segurança terá de forma completa o conhecimento necessário para planejar adequadamente a correção dessas falhas de segurança. É comum que empresas utilizem versões desatualizadas e vulneráveis do Apache, PHP, *GlassFish* e etc. em seus servidores web, simplesmente por não manterem um processo de análise e monitoramento dessas ferramentas.

Mesmo que inúmeros patches de correção tenham sido lançados e anunciados pelos fornecedores corrigindo tais falhas. Quando não há um processo ou uma rotina de acompanhamento dessas mudanças de uma forma contínua, a tendência é que o ambiente pare ou deixe de funcionar com o tempo, no que diz respeito à segurança da informação. Essa falha é uma oportunidade para agentes maliciosos, que constantemente exploram vulnerabilidades não corrigidas em sistemas, protocolos e serviços.

A segurança da informação vem se destacando cada vez mais no meio corporativo, ocasionando um aumento no orçamento do setor de Tecnologia da Informação. Empresas investem em pessoal capacitado, programas de segurança, em software de análise de vulnerabilidade, em softwares que realizam análise do tráfego de rede. Buscando proteger seus dados, informações e negócios. Aumento justificável pela importância das informações trafegadas na rede de computadores e armazenadas em seus servidores.

Diante do analisado e estudado, concluiu-se que a maior parte de vulnerabilidades encontradas ocorreu devido à falta de atualização no sistema operacional dos servidores da rede corporativa e versão das aplicações neles contidas. Por outro lado, ocorrem falhas de segurança por configurações incorretas, portas de serviços abertas e expostas a ataques.

Segundo os autores Kurose e Ross, (Redes de Computadores- Uma abordagem top-down, 2014) “Ataque de vulnerabilidade envolve o envio de algumas mensagens bem elaboradas a uma aplicação vulnerável ou a um sistema operacional sendo executado em um hospedeiro direcionado. Se a sequência correta de pacotes é enviada a uma aplicação ou sistema operacional vulnerável, o serviço pode parar ou, pior, o hospedeiro pode pifar.”

Referências

Cert (Computer Emergency Response Team), disponível em https://www.cert.br/stats/incidentes/2016-jan-dec/top-asn.html. (2016)

Coelho, Flavia E.S; Araújo, Luiz G.S & Bezerra, Edson K. (2014) "Gestão da Segurança da Informação NBR 27001 e NBR 27002", editora: Rede Nacional de Ensino e Pesquisa RNP, páginas 91-92.

Melo, S. "Exploração de Vulnerabilidades em Redes TCP/IP" (2017), editora: Alta Books, 3ª edição, capitulo 11, páginas 267-292, Rio de Janeiro.

Security, Perallis. Disponível em http://www.perallis.com/solucoes/analise-de-vulnerabilidades?gclid=Cj0KCQiAvrfSBRC2ARIsAFumcm8eqC5ZblCYIBn_wsjO0p4crI3QxNUNj8_2FSlcpstOCQjzRz0JMEMaAq3gEALw_wcB
(Acesso em dezembro/2017).

PHP, disponível: http://php.net/manual/en/migration72.php. (Acesso em janeiro/2018).

Blog.infolink, disponível em http://blog.infolink.com.br/analise-de-vulnerabilidades-em-ti/, (Acesso em dezembro/2017).

Microsoft, disponível: https://support.microsoft.com/pt-br/help/2671387/ms12-020-vulnerabilities-in-remote-desktop-could-allow-remote-code-exe,
(Acesso em janeiro/2018).

Apache HTTP Server Project, disponível em https://httpd.apache.org/docs/trunk/pt-br/, (Acesso em janeiro/2018).

Oracle, disponível em http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html, (Acesso em janeiro/2018).

Jim F. Kurose e Keith W. Ross, "Redes de Computadores- Uma abordagem top-down" editora: Pearson, 6º edição, capítulo 1, página 42, (2014).