Avaliação de requisitos de Disponibilidade e Desempenho por meio de testes de sobrecarga

Evaluation of Availability and Performance requirements through overload tests

Carlos A M S Teles [1], Raphael Carlos Santos Machado[1,2]

[1] PPCIC - CEFET/RJ; [2] PPGMQ - INMETRO

E-mail: carlos.teles@cefet-rj.br, rcmachado@inmetro.gov.br

Resumo: Progressivamente, a proteção de sistemas computacionais e segurança da informação tem sua relevância reconhecida. Observa-se maior foco nos requisitos de confidencialidade e integridade, no entanto há pouco avanço no estabelecimento de padrões de disponibilidade e desempenho. No presente trabalho, analisamos requisitos de segurança da informação em editais públicos brasileiros, demonstrando uma preocupação moderada em definir padrões rigorosos de disponibilidade e desempenho. Estabelecemos definições para tais requisitos, além de argumentarmos que estes podem ser rigorosamente validados mediante ensaios sistemáticos. Propomos um ambiente de testes que permite a realização de ensaios de disponibilidade e desempenho em cenários de sobrecarga.

Palavras-chave: disponibilidade, desempenho, segurança, integridade e sobrecarga.

Abstract: Progressively, the protection of computer systems and information security has its relevance recognized. There is a greater focus on confidentiality and integrity requirements, there is little advance in establishing availability and performance standards. In this paper, we analyze information security requirements in Brazilian public notices, showing a moderate concern to define strict standards of availability and performance. We have established definitions for such requirements, and we argue that we can validate through systematic assays. We propose a test environment that allows performing tests of availability and performance in scenarios of overload.

Keywords: availability, performance, security, integrity and overload.

1. INTRODUÇÃO

Somos cada vez mais dependentes das redes corporativas, internet e sistemas, ou seja, deste ambiente tecnológico. Este possui um conjunto de variáveis tecnológicas que podem impactar positiva ou negativamente as organizações [1].

A cada ano que passa, nosso tempo é consumido cada vez mais por novas tecnologias e devido ao aumento da velocidade de acesso à internet, que geram mudanças dia a dia, aumenta-se a quantidade de troca de informações, através de e-mails, mensagens através de aplicativos, compras, transações bancarias, conteúdos sob

demanda e diversos tipos de informação pessoal ou comercial são percorridos pela rede.

Entretanto, este ambiente tecnológico não é um local seguro, confiar-lhe tantas informações nos tornaram reféns e mostrou-se um local encantador para os hackers, com tanta informação pessoal e de empresas, circulando sem a devida segurança.

A Segurança da Informação é influenciada por três propriedades principais: Confidencialidade para limitar o acesso à informação somente a agentes autorizados; Integridade para preservar que as informações tenham suas características fiéis à sua origem e que qualquer alteração durante o processo tenha sido realizada com autorização e controle e; Disponibilidade que garanta que a informação esteja acessível aos autorizados a todo tempo que precise ser resgatada [2].

Ainda sobre a Disponibilidade é possível medi-la através do cálculo: percentual entre tempo funcional e tempo total de uso. É aplicada em acordos de níveis de serviços (*SLA – Service Level Agreement)* [3].

O Desempenho é responsável pela medição e disponibilização das informações sobre aspectos dos serviços e dispositivos de rede. Esses dados são usados para garantir que redes e sistemas operem em conformidade com a qualidade de serviço acordado com seus usuários [3].

Para garantir as três propriedades principais da Segurança da Informação utiliza-se algumas medidas de Disponibilidade e Desempenho para Sistemas e Redes de Informação.

Uma das técnicas para inutilizar estas propriedades são os Ataques. Nesta atividade, onde um atacante utiliza um computador ou vários, conectados à rede, para remover outro computador ou vários, de operação, ou serviços do mesmo ou fazer sua conexão a uma rede conectada à Internet ficar indisponível, é feita a tentativa de obtenção de dados e podem causar falhas relacionadas à segurança, disponibilidade, desempenho e até por fim indisponibilidade de redes e sistemas, podendo acarretar perdas importantes para a sociedade. Uma falha de desempenho em um sistema hospitalar, ocasionada em função de um programa malicioso que consome a CPU do sistema, pode causar a demora no atendimento das pessoas. Uma falha de disponibilidade em um sistema bancário, ocasionada em função de problema em banco de dados, pode gerar a perda financeira para várias pessoas. Entretanto, estes problemas podem ser difíceis de serem detectados.

Um tipo de ataque muito utilizado é o Ataque Distribuído de Negação de Serviço (*DDoS - Distributed Denial of Service*). Estes podem ser classificados: esgotamento de recursos e esgotamento de banda [4,5].

O protocolo BGP (*Border Gateway Protocol)* pode auxiliar na proteção de um ataque, através de configurações nos roteadores, como rotas específicas e outras configurações.

Além disso, um dos problemas identificados é que os atacantes modificam constantemente suas ferramentas para contornar os sistemas de segurança. E os pesquisadores modificam suas abordagens para detectar novos ataques [6].

2. REQUISITOS DE DISPONIBILIDADE E DESEMPENHO

Em nosso artigo analisaremos as informações de Governo das diversas esferas (Municipal Estadual e Federal). Assim, nossa base para extração de informações serão Licitações e documentos publicados pelos diversos órgãos.

2.1. Casos de Requisitos de Disponibilidade e Desempenho

Em nossa análise sobre os recursos através das Licitações, escolhemos aleatoriamente quatro editais disponíveis nos sites dos respectivos órgãos lançados entre 2015 e 2017. Abaixo teremos um pequeno resumo dos mesmos.

Prefeitura de Monte Carmelo [7], foi solicitada a Disponibilidade de 99,5% por mês. Não solicitou medidas de Desempenho. Segurança solicitou uma proteção de rede com características de NGFW (*Next Generation Firewall*) para segurança de informação perimetral.

Senado Federal [8], foi solicitada a Disponibilidade de 99,8% por mês. Não solicitou medidas de Desempenho. Para Segurança, foi solicitado um Serviço de Proteção Proativo Anti-*DDoS*, com capacidade para identificar, comunicar e mitigar quaisquer tipos de ataques que utilizem indevidamente os recursos de rede em IPV4 ou IPV6.

Câmara dos Deputados [9], foi solicitada a Disponibilidade de 99,44% por mês. Para as medidas de Desempenho, uma taxa máxima de utilização de CPU e Memória em 60%. Para Segurança, solicitou-se um Serviço de Proteção contra Anti-DDoS, a partir da sinalização remota de *black hole* em anúncios BGP, utilização de *blacklist* para bloqueio de tráfego.

TRT da 18ª. Região [10] foi solicitada a Disponibilidade de 99,60% por mês. Solicitou que as medidas de Desempenho tivessem taxa máxima de utilização de CPU e Memória em 70%. O único item de Segurança solicitado foi a utilização de DNSSEC (*Domain Name System Security Extensions)* para os domínios já registrados no DNS primário do TRT18.

2.2. Análise das Licitações

Podemos resumir os editais: todos consideram os requisitos de Disponibilidade e Segurança, entretanto, apenas dois (Câmara dos Deputados e TRT18) consideram Desempenho.

Cabe ressaltar que apesar dos requisitos de Segurança constarem em todos os editais, os mesmos não possuem padrão algum. Esta ocorre em função das múltiplas tendências tecnológicas que são lançadas no mercado [11].

Outros motivos para a falta de padrão seria a inexistência de um escritório central no Governo Federal, que direcione a contratação. Assim temos vários órgãos gerando documentos de boas práticas e manuais com informações que se sobrepõem dentro das diversas esferas de Governo (Federal, Estadual e Municipal).

Existe uma relação direta entre os aspectos de Segurança, Disponibilidade e Desempenho. A inexistência ou falha de um destes fatores nos itens de uma Licitação, passa a ser um risco. O tamanho da solução também é outro fator que deveria ser levado em consideração.

Demonstraremos tal relação através de testes de sobrecarga. Estes nos possibilitam estabelecer medidas para identificar futuros ataques e estabelecer limites para as plataformas. Nosso intuito, a partir de cenários pré-estabelecidos e resultados obtidos, é mensurar e configurar as aplicações de rede, de forma que no futuro tenhamos um padrão de configuração que possa aguentar nossos testes.

3. TESTES PARA VERIFICAÇÃO DE REQUISITOS

Para demonstrar a relação entre Disponibilidade e Desempenho, montamos um ambiente de redes de computadores, onde utilizamos ferramentas e dispositivos para simular testes de sobrecarga e ataques. Nas próximas seções os descreveremos.

3.1. Ambiente

Em nosso ambiente de testes temos três dispositivos: um computador (atacante) conectado a uma rede local através de um switch gerando testes de sobrecarga a outro computador com um servidor HTTP em LINUX (atacado), conectado ao mesmo switch.

3.2. Ferramentas

Selecionamos o T50 [12] como simulador para testes de sobrecarga. Suas principais características são: suporte a vários protocolos de rede incluindo TCP, UDP e ICMP; simulação de mais de 1.000.000 de pacotes por segundo em redes *Gigabit*; simulação de testes de sobrecarga e ataques com esgotamento de recursos e inundação e facilidade de parametrização.

As ferramentas para coleta e disponibilização de resultados utilizadas em nossos testes foram: NMON [13] que é um monitor de desempenho e deve ser compilado no computador que vai receber os testes de sobrecarga e; NMONCHART [14] que é um script que converte os arquivos coletados pelo NMON em arquivos HTML. Permite-nos ver pelo menos 53 gráficos de recursos e configuração dos sistemas operacionais LINUX e AIX.

3.3. Resultados

O T50 afetou a CPU atacada e durante o período da simulação a sua utilização ficou superior a 50%, conforme a figura 1.

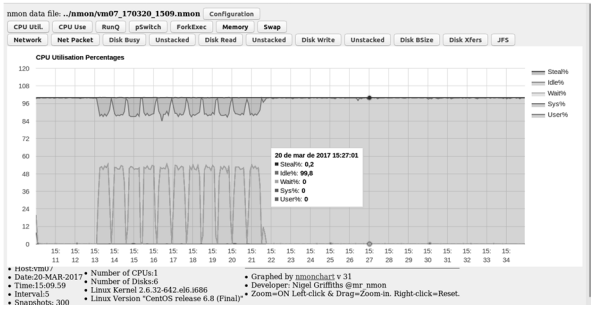

Figura 1 - Medição de CPU.

O T50 afetou a Memória e durante o período da simulação a memória livre estava em 79,9 MB passou para 68,8 MB, conforme a figura 2.

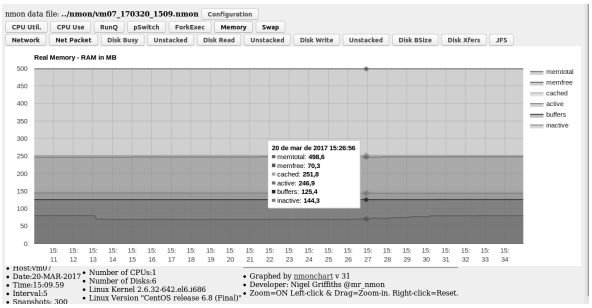

Figura 2 - Medição de Memória.

O T50 afetou o Tráfego de Rede e durante o período da simulação a interface de rede indicou um tráfego 9509,7 KB por segundo, conforme a figura 3.

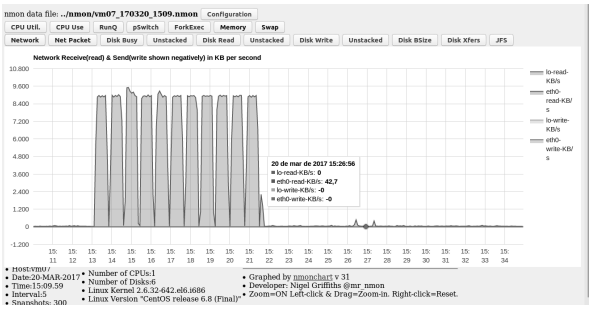

Figura 3 - Medição de Tráfego de Rede

4. CONCLUSÃO

Os resultados das simulações foram satisfatórios e podemos inferir que a Disponibilidade não foi afetada, o Desempenho, foi afetado e consequentemente a Segurança.

Sobre as Licitações analisadas, apenas a Câmara dos Deputados possui uma especificação que poderia ser menos afetada.

Um ponto importante é legitimar o tráfego de rede e diferenciar quais requisições são verdadeiras e quais são falsas, é uma das maiores dificuldades nos computadores atacados. Com nossa análise de resultados, poderemos desenvolver algoritmos que nos permitam legitimar o trafego de rede [15].

5. REFERÊNCIAS

[1] Rezende D 2008 Planejamento Estratégico para Organizações Privadas e Públicas.

[2] Sêmola M 2003 Gestão Da Segurança da Informação.

[3] Santos M T, Tarouco L, Bertholdo L, Lima F M M e Vasconcellos V 2015 Gerência de Redes de Computadores.

[4] CERT.br 2016 Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS) [acesso em 25 jul 2017]. Disponível em: https://www.cert.br/docs/whitepapers/ddos/.

[5] Somal I e Virk S 2014 Classification of distributed denial of service Attacks--Architecture, taxonomy and tools.

[6] Mirkovic J e Reiher P 2004 A taxonomy of DDoS attack and DDoS defense mechanisms. 34 **2** 39-53

[7] Edital [acesso em 25 jul 2017]. Disponível em: http://www.montecarmelo.mg.gov.br/uploads/34-Edital-Pregao-34.2017-SRP-34.2017-Contratacao-de-Internet.pdf

[8] Edital [acesso em 25 jul 2017]. Disponível em: https://www.senado.leg.br/transparencia/liccontr/licitacoes/download.asp?COD_LICITACAO=41794

[9] Edital [acesso em 25 jul 2017]. Disponível em: http://www.camara.leg.br/internet/contratos/LicitacaoArquivosDownload.asp?numSeqArquivoLicitacao=23137

[10] Edital [acesso em 25 jul 2017]. Disponível em: http://www1.trt18.jus.br/licitacao/anexos/2016PE0360002.pdf

[11] Leão M, Amaral A C P e Echeverria E L 2017 O acordo como instrumento de garantia dos serviços de tecnologia aplicados às redes de computadores. **4** 19-32

[12] Pissarra, F L T50 [acesso em 25 jul 2017]. Disponível em: http://t50.sf.net/

[13] Griffiths, N NMON [acesso em 25 jul 2017]. Disponível em: http://nmon.sourceforge.net/

[14] Griffiths, N NMONCHART [acesso em 25 jul 2017]. Disponível em: http://nmon.sourceforge.net/

[15] Braga R, Mota E e Passito A 2010 Lightweight DDoS flooding attack detection using NOX/OpenFlow. 408-415