

## **PENDÊNCIAS E ADAPTAÇÕES A SEREM SANADAS NO CADERNO DE TESTES DA EMPRESA Blockbit – LOTE 1**

### **1. CONSIDERAÇÕES INICIAIS**

Além das informações já apresentadas na primeira versão do Caderno de Testes, a empresa deve estruturar o caderno de testes de acordo com o modelo e premissas listadas abaixo, as quais estão de acordo com o preconizado no Anexo E, que fornece orientações gerais para a elaboração do caderno de testes.

Ressalta-se que o caderno de testes será utilizado como apoio principal, contudo, na execução dos testes, a empresa deve se atentar a todos os requisitos elencados no Anexo E – Caderno de Testes do Termo de Referência do Pregão nº 05/2017. Desta forma, o Caderno de Testes deve refletir a documentação mínima de informações para que os testes sejam executados. Entretanto, os testes poderão ser ajustados conforme dispostos nos itens 2.16 e 2.17 do Anexo E do termo de referência do Edital de Pregão nº 05/2017.

A empresa deve também colocar ou referenciar nos cadernos de testes comandos e procedimentos a nível de sessão / capítulo do caderno, a fim de deixar o caderno de teste e a realização dos testes mais transparentes.

Os *scripts*, ou seja, a automação da criação das configurações, devem ser apresentados antes da realização dos testes para avaliação do grupo técnico, pelo menos com 10 dias corridos de antecedência da data dos testes marcada pela pregoeira. Deve-se destacar que esse procedimento destina-se apenas a averiguação prévia de configuração dos equipamentos a fim de informar em maiores detalhes a equipe técnica.

E ainda, a empresa deve passar a listagem dos *malwares*, ataques e aplicações que o equipamento de teste é capaz de gerar, bem como a listagem dos malwares, ataques, aplicações e URLs que a empresa pretende ativar no equipamento de testes durante os testes de assertividade.

Por fim, deve-se indicar que, quando couber, os cadernos de testes apresentados deverão ser complementados ao que foi inicialmente proposto. Essa complementação deve ser conforme a estrutura indicada no Anexo E, os pontos aqui levantados a seguir e as observações apontadas neste documento.

### **2. DISPOSIÇÕES GERAIS**

a) Descrição dos objetivos gerais do teste de bancada para cada item testado.

**OK. Premissa atendida no tópico 1 do Caderno de Testes enviado pela Blockbit.**

b) Descrição de todos os equipamentos acompanhados de seus modelos, incluindo o gerador de tráfego, além de todas as versões de firmwares que serão utilizadas nos testes.

**OK. Premissa atendida no tópico 2 do Caderno de Testes enviado pela Blockbit.**

c) Indicação da equipe técnica que irá acompanhar os testes, de acordo com item 2.13 do Anexo E, informando, no mínimo, nome e e-mail.

**OK. Premissa atendida no tópico 3 do Caderno de Testes enviado pela Blockbit.**

### **3. PREPARAÇÃO INICIAL**

a) Descrição dos comandos a serem utilizados para limpeza e exclusão de dados de forma a zerar configurações, conforme o item 4.1 do Anexo E.

**OK. Premissa atendida no tópico 4 do Caderno de Testes enviado pela Blockbit.**

b) Descrever procedimentos para verificação dos itens 4.2 e 4.3 do Anexo E.

**OK. Premissa atendida no tópico 4 do Caderno de Testes enviado pela Blockbit.**

c) Descrever o procedimento e comandos que serão executados para criar o backup após configuração inicial, indicando em qual mídia o backup será salvo, de forma a atender o item 4.5 e 4.6 do Anexo E.

**OK. Premissa atendida no tópico 4 do Caderno de Testes enviado pela Blockbit.**

#### **4. CONFIGURAÇÃO DE TESTES E TOPOLOGIA**

a) Descrição dos procedimentos que serão executados para comprovar que todas as funcionalidades indicadas no item 5.1.1 do Anexo E estão ativas.

**OK. Premissa atendida no tópico 6 do Caderno de Testes enviado pela Blockbit.**

b) Apresentação da topologia de rede esquematizada e com legenda, de forma que possa ser possível identificar todos os objetos, redes, equipamentos e interfaces que farão parte do escopo do teste, compatíveis e de acordo com o preconizado nos itens 5.1.5 a 5.1.11 do Anexo E.

**OK. Premissa atendida no tópico 6 do Caderno de Testes enviado pela Blockbit.**

c) Apresentação da lista (que pode ser editada em planilha anexa) de todos os ataques, ameaças, site e aplicações, de forma a atender o item 5.1.2.1 do Anexo E.

**OK. Premissa atendida nos Anexos 1, 2, 3 e 4 do Caderno de Testes enviado pela Blockbit.**

*Deve ser complementado com as observações listadas abaixo:*

- de todos os ataques, ameaças, sites e aplicações que o equipamento de geração de tráfego é capaz de gerar e que poderá ser utilizado pela equipe de apoio ao pregoeiro, de forma a atender os itens 4.8, 2.17 e relacionados.
- de todos os ataques, ameaças, site e aplicações, de forma a atender o item 5.1.2.1 do Anexo E. A lista enviada pela empresa deve ser complementada com no mínimo as seguintes aplicações: Youtube, Livestream, Skype, Viber, Whatsapp, Google+, Google Talk, Google Docs, Google Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex, Facebook-chat, Facebook-vídeo, ms-update, Netflix, Dropbox, Http-video, Apple-appstore, Instagram, Gmail, Twitter-base, Itunes-base, OpenVPN, Google update, Apple Services, Snapchat, Google Docs, One Drive, LinkedIn, Twitter, Telegram, Instagram Video, Twitter Video, Vimeo Video, Microsoft Azure e Microsoft Outlook 365.

**Pendente. Do mínimo de "aplicações" solicitadas, algumas ainda estão faltando. (itunes e TOR, dentre outras). Favor atender à solicitação.**

d) Descrição dos procedimentos e comandos que serão executados para ativar a inspeção integral de todo o tráfego, de forma a atender os itens 5.1.3 e 5.1.4 do Anexo E.

**OK. Premissa atendida no tópico 6 do Caderno de Testes enviado pela Blockbit.**

#### **5. TESTE DE ASSERTIVIDADE**

a) Descrição dos procedimentos e comandos que serão executados no firewall da Amostra para atendimento do item 5.2.2 do Anexo E.

**OK. Premissa atendida no tópico 7 do Caderno de Testes enviado pela Blockbit.**

b) Breve descrição da execução dos testes e resultados esperados.

**OK. Premissa atendida no tópico 7 do Caderno de Testes enviado pela Blockbit.**

- c) Descrição dos procedimentos e comandos que serão executados no *firewall* da Amostra para zerar contadores e apagar configurações, de forma a atender o item 5.2.7 do Anexo E.

**OK. Premissa atendida no tópico 7 do Caderno de Testes enviado pela Blockbit.**

Observação:

**A categorização contabilizada será analisada pelo grupo técnico de apoio ao pregoeiro com base nos dados gerados e obtidos pelo gerador de tráfego, sendo complementado, quando necessário, pelos dados obtidos pela amostra. Ressalta-se, que quando necessário, poderão ser apurados os *logs* tanto do gerador de tráfego quanto do firewall propriamente dito ou de sua gerência.**

- d) Inserir, ao final da descrição dos procedimentos de todos os testes a serem realizados campos para sinalizar resultados dos testes, como: "Teste OK.", "Teste com falha." e "Observação."

**OK. Premissa atendida.**

## **6. TESTE DE DESEMPENHO**

- a) Descrição dos procedimentos e comandos a serem executados para restaurar o backup executado após a configuração inicial, conforme disposto no item 4.5 do Anexo E.

**OK. Premissa atendida no tópico 8 do Caderno de Testes enviado pela Blockbit.**

- b) Descrição dos procedimentos e comandos a serem executados no *firewall* da amostra para atendimento do item 5.3.5

**OK. Premissa atendida no tópico 8 do Caderno de Testes enviado pela Blockbit.**

- c) Breve descrição da execução dos testes e resultados esperados.

**OK. Premissa atendida no tópico 8 do Caderno de Testes enviado pela Blockbit.**

- d) Inserir, ao final da descrição dos procedimentos de todos os testes a serem realizados campos para sinalizar resultados dos testes, como: "Teste OK.", "Teste com falha." e "Observação."

**OK. Premissa atendida.**

## **7. TESTE DE SESSÃO**

- a) Descrição dos procedimentos e comandos a serem executados para restaurar o backup executado após a configuração inicial, conforme disposto no item 4.5 do Anexo E.

**OK. Premissa atendida no tópico 9 do Caderno de Testes enviado pela Blockbit.**

- b) Breve descrição da execução dos testes e resultados esperados.

**OK. Premissa atendida no tópico 9 do Caderno de Testes enviado pela Blockbit.**

- c) Descrever os procedimentos e comandos que serão executados no *firewall* da Amostra para zerar contadores e apagar configurações, de forma a atender o item 5.4.2.6 do Anexo E.

**OK. Premissa atendida no tópico 9 do Caderno de Testes enviado pela Blockbit.**

- d) Inserir, ao final da descrição dos procedimentos de todos os testes a serem realizados campos para sinalizar resultados dos testes, como: “Teste OK.,” “Teste com falha.” e “Observação.”

**OK. Premissa atendida**

## 8. TESTES COMPLEMENTARES

Descrever procedimentos a serem executados para comprovação dos itens que foram indicados para verificação nos testes durante a fase de análise das propostas. (itens realçados de laranja na planilha de avaliação das propostas). Isso porque, no momento dos testes, as funcionalidades deverão ser comprovadas.

- a) Inserir, ao final da descrição dos procedimentos de todos os testes a serem realizados campos para sinalizar resultados dos testes, como: “Teste OK.,” “Teste com falha.” e “Observação.”
- i. 2.1.23.5. Deve permitir a criação de regras de acesso/bloqueio baseadas em usuários ou grupo de usuários do LDAP e do *Microsoft Active Directory*;
  - ii. 2.1.48. Deve suportar a criação de políticas de controle de uso de largura de banda, limitando ou expandido individualmente, baseadas em: porta ou protocolo, endereço IP de origem ou destino, grupo de usuários do Microsoft Active Directory e LDAP e aplicações (por exemplo, Youtube e WhatsApp).
  - iii. 2.3.7. Possuir proteção contra os ataques como, mas não restringindo-se aos mesmos : 1) Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS, Spywares, Botnets e malwares em geral; 2) Ataques e utilização de tecnologia P2P; 3) Ataques de estouro de pilha (buffer overflow); 5) Tráfego mal formado; 6) Cabeçalhos inválidos de protocolo; 6) Ataques de injeção (SQL Injection, LDAP Injection) e de Cross-Site Scripting; 7) Elevação de privilégio e 8) Exploits - Web Server, Web Browser ActiveX, JavaScript, Browser Plugins/Add-nos.
  - iv. 2.3.16. Permitir o funcionamento mínimo do engine de IPS mesmo que a comunicação com o site do fabricante esteja fora de operação;
  - v. 2.3.17. Possuir as estratégias de bloqueio e liberação selecionáveis, tanto por conjuntos de assinaturas quanto por cada assinatura;
  - vi. 2.4.4. Deve possuir serviço de atualização automática e manual de assinaturas com o fabricante
  - vii. 2.4.5. Suportar funcionamento mínimo da *engine* e antivírus e anti-malwares mesmo que a comunicação com o site do fabricante esteja fora de operação;
  - viii. 2.5.15. Categorizar as URLs com taxa de acerto mínima de 80% (oitenta por cento), não sendo consideradas neste percentual categorização genérica ou similar.
  - ix. 2.6.12. Deve ser capaz de identificar e filtrar um mínimo de 1.500 (mil e quinhentas) aplicações, contemplando no mínimo: peer to peer, streaming e download de áudio, streaming e download de vídeo, update de software, instant messaging, redes sociais, proxies, anonymizers, acesso e controle remoto, VOIP e email.

- x. 3.8.1.2. Possuir, no mínimo, o *throughput* de 250 Mbps para todas as funcionalidades dos itens 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6, ativadas simultaneamente e com inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, levando-se em consideração o perfil de tráfego descrito no ANEXO E.
- xi. 3.12.1. Atender a todos os requisitos do item 2.1.39 e do item 2.6; 3.13. LOTE 1 - item 6: Treinamento oficial para até 5 pessoas 3.13.1. Atender a tudo o que foi exposto no item 2.7.

## 9. ESCLARECIMENTOS DIVERSOS

Cabe esclarecer, ainda, que no documento apresentado pela Blockbit existe um excesso de numeração encadeadas em vários níveis. Dessa forma, observam-se 3 (três) classes de numerações (i,ii e iii) no caderno de testes. Isso dificulta a legibilidade e torna o documento confuso. Assim, para dar maior transparência, coerência, agilidade e legibilidade, sugere-se trabalhar com apenas dois níveis de numerações ao longo do caderno de testes.

## 10. CONCLUSÃO

Indique-se que atendidas as solicitações finais apontadas nesta avaliação, a empresa estará apta a seguir para a realização dos testes de conformidade de acordo com o proposto. Caso contrário, sua proposta será considerada desclassificada.

1. Com relação ao tópico 4, item c (apresentação de lista de ataques, ameaças, sites e aplicações): As listas de ameaças, aplicações, urls e categorias de assinaturas IPS/IDS foram apresentadas. Contudo, dentre o mínimo de "aplicações" solicitadas algumas ainda estão faltando. (itunes e TOR, dentre outras). Porém, deixei como "Premissa atendida" uma vez que, na primeira revisão já foi aceitado o item da mesma forma que foi enviado nesta segunda revisão.