PENDÊNCIAS E ADAPTAÇÕES A SEREM REALIZADAS NO CADERNO DE TESTES DA EMPRESA TRACENET - LOTE 5

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 - Item atendido

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 - Item atendido

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

OK - Item atendido

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 - Item atendido

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

Item 4.2 - OK - Item atendido

Pendente. Item 4.3. Favor citar os comandos e procedimentos que serão utilizados para gerar os hashes.

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.

Pendente. Item 4.5. Favor citar os comandos e procedimentos que serão utilizados para gerar os hashes.

Item 4.6 - OK - Item atendido

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 - Item atendido

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.

Pendente – a empresa deve apresentar uma topologia de rede bem detalhada, com a indicação dos equipamentos na topologia, bem como indicação de todos os endereços IP de todos os equipamentos, interfaces e sub redes que farão parte do escopo do teste. Em suma, a figura que ilustra a topologia não deve ser genérica da forma como apresentada pela empresa.

Verificação dos procedimentos de testes contidos nos itens 5.1.5 a 5.1.11 no caderno de testes enviado pela empresa – OK – Itens atendidos

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.

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 - por uma questão de equidade com os outros lotes, obrigatoriamente, a lista deve ser apresentada pelo menos para IPS e aplicações identificadas pelo equipamento. A única exceção é a filtragem de URL's, que tem potencialmente milhões de URL's categorizadas e várias categorias. Neste caso, pode ser apresentado o número de categorias e o número de URL's na base. Favor atender a demanda.

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 – Itens atendidos

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.

Pendente – favor citar os comandos e procedimentos que serão utilizados para gerar os hashes.

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

OK – Item atendido

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 – Item atendido

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 – Item atendido

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 – Item atendido no item 4.5 do caderno de testes enviado pela empresa

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

Pendente. Favor citar os comandos e procedimentos que serão utilizados para gerar os hashes.

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

OK – Item atendido

d) Descrição dos procedimentos e comandos que serão executados no firewall da amostra para zerar contadores e apagar configurações, de forma a atender o item 5.3.8.5 do Anexo E.

OK – Item atendido

e) 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 – Item atendido

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 – Item atendido no item 4.5 do caderno de testes enviado pela empresa

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

OK – Item atendido

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 – Item atendido

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 – Item atendido

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.

i. 2.1.29. Possuir proteção e suporte a protocolos de Real Time, contemplando no mínimo: Real Time Transport Protocol (RTP), H323 e SIP sobre os protocolos IPV4 ou IPV6.

   OK – Item atendido

   Observação: não ficou claro na lista divulgada pela empresa, proteção e suporte ao RTP. Assim, ressaltamos que obrigatoriamente deverá ser comprovado o suporte ao referido protocolo durante os testes.

ii. 2.3.3. Decodificar múltiplos formatos de Unicode

   OK – Item atendido

iii. 3.3.4 Suportar fragmentação e desfragmentação IP

   OK – Item atendido

iv. 3.3.5 Detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão

   OK – Item atendido

v. 3.3.6 Detectar e Proteger contra, no mínimo, ataques de RPC (Remote Procedure Call), Windows ou NetBios, SMTP (Simple Message Transfer Protocol), IMAP (Internet Message Access Protocol), Sendmail ou POP (Post Of ice Protocol), DNS (Domain Name System), FTP, SSH, Telnet, ICMP (Internet Control Message Protocol), SIP, SNMP, SSDP ou CHARGEN, RDP (Remote Desktop Protocol), DoS (Denial of Service) e ataques com assinaturas complexas, tais como ataques TCP hijacking.

   OK – Item atendido

   Observação: ressalta-se que a referida lista de ataques será auferida durante os testes.

vi. 3.3.7 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 (buf er 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 Plug-ins/Add-nos.

OK – Item atendido

Observação: espera-se que o procedimento citado no passo 3 – "testar resultados" corresponda ao ato de direcionar o gerador de tráfego e ataques para produzir os ataques citados no item.

vii. 2.3 .13 . Deve resistir a técnicas de evasão ou ataques direcionados ao próprio equipamento, suportando, no mínimo, as técnicas: IP Packet Fragmentation, Stream Segmentation, RPC Fragmentation, URL Obfuscation, HTML Obfuscation, Payload Encoding, FTP Evasion e Layered Evasions.

OK – Item atendido

Observação: ressalta-se que a referida lista de ataques será auferida durante os testes.

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.

OK – Item atendido

Observação: espera-se que o procedimento citado no passo 3 – "testar resultados" corresponda ao ato de gerar o tráfego no gerador e auferir o resultado nas categorizações da caixa.

ix. 2.5.16. Suportar e forçar pesquisas seguras em pelo menos dois sistemas de buscas, contemplando Google e/ou Bing e/ou Yahoo.

OK – Item atendido

x. 3.29.1.2 Possuir, no mínimo, o throughput de 10 Gbps 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.

OK – Item atendido

xi. 3.29.1.5 Possuir a capacidade mínima de 2 (dois) discos, sendo rígidos ou SSD de 240 GB em RAID 1 para armazenamento de logs

Pendente – na especificação apresentada, a empresa está referenciando a solução de guarda e gerenciamento centralizado de logs, mas o objetivo deste teste complementar é testar a especificação do item 3.29.1.5 do Anexo E do Termo de Referência quanto à presença e capacidade de discos em RAID1 no *EQUIPAMENTO FIREWALL.* Favor indicar o procedimento que irá ilustrar a comprovação deste ponto.

9. ESCLARECIMENTOS DIVERSOS

Cabe esclarecer ainda que o documento apresentado pela Tracenet não seguiu a estrutura mínima proposta no Anexo E do Edital de Pregão em epígrafe. Dessa forma, sugere-se que a empresa siga a estrutura mínima de testes apontada no referido anexo e também o indicado na avaliação apresentada.

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.