PENDÊNCIAS E ADAPTAÇÕES A SEREM SANADAS NA SEGUNDA VERSÃO DO CADERNO DE TESTES DA EMPRESA VERT – LOTE 4

1. CONSIDERAÇÕES INICIAIS

Além das informações já apresentadas na primeira versão do Caderno de Testes e na sua segunda versão, resultante após a primeira avaliação pela equipe técnica, a empresa ainda 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.

Conforme já informado, o caderno de testes será utilizado como apoio principal, na execução dos testes e a licitante deve se atentar a todos os requisitos elencados no Anexo E – Caderno de Testes do Termo de Referência do Pregão nº 05/2017, bem como às premissas dispostas a seguir. Desta forma, o Caderno de Testes deve refletir a documentação mínima de informações para que os testes sejam executados. Ressalta-se que 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.

Conforme elucidado na ocasião da primeira revisão:

i) 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. Além disso, a empresa deve revisar as alterações

ii) 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.

iii) 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.

iv) 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.

RESULTADO DA AVALIAÇÃO DA SEGUNDA VERSÂO DO CADERNO DE TESTES – LOTE 4 – EMPRESA VERT

2. DISPOSIÇÕES GERAIS

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

Pendente. Premissa não atendida na 2ª versão do caderno de testes – item não encontrado.

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.

Pendente. Premissa atendida parcialmente no tópico 3 do Caderno de Testes enviado pela Vert – descrição dos geradores de tráfego não encontrada.

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 Vert.

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 nos tópicos 5.1.2 e 5.1.3 do Caderno de Testes enviado pela Vert.

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

OK. Premissa atendida nos tópicos 5.1.4 e 5.1.5 do Caderno de Testes enviado pela Vert.

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. Premissa atendida PARCIALMENTE no tópico 5.1.6 do Caderno de Testes enviado pela Vert – favor complementar com os comandos a serem utilizados para geração do hash do(s) arquivo(s) de backup da configuração da amostra.

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 nos tópicos 5.1.1 e 12, 13, 14 e 15 do Caderno de Testes enviado pela Vert.

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 4 do Caderno de Testes enviado pela Vert.

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.

Pendente. Premissa atendida parcialmente no tópico 5.1.5 do Caderno de Testes enviado pela Vert – lista de URL's / Categorias não encontrada (não foi encontrado no link do site informado - http://sec.huawei.com/sec/web/urlClassification.do a quantidade ou tamanho da base de URL's e categorias, apenas formulário para consulta em URL específica. Favor informar a lista ou a informação agregada.

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.

Pendente. Não foram encontradas, no caderno enviado pela empresa Vert, as informações acerca do(s) gerador(es) de tráfego. Favor informar.

- 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.
  OK. Premissa atendida no arquivo SA-SDB_Protocol_Identification.pdf enviado como anexo pela empresa Vert.

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 tópicos 5.1.1 do Caderno de Testes enviado pela Vert.

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. Premissa atendida PARCIALMENTE no tópico 5.1.6 do Caderno de Testes enviado pela Vert – favor complementar com os comandos a serem utilizados para geração do hash do(s) arquivo(s) de backup da configuração da amostra.

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

OK. Premissa atendida no tópico 16 do Caderno de Testes enviado pela Vert.

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 5.1.2 e 5.1.3 do Caderno de Testes enviado pela Vert.

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.

Pendente. Premissa atendida PARCIALMENTE no tópico 5.1.6 do Caderno de Testes enviado pela Vert – favor complementar com os comandos a serem utilizados para geração do hash do(s) arquivo(s) de backup da configuração da amostra.

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

Pendente. Premissa atendida PARCIALMENTE no tópico 5.1.6 do Caderno de Testes enviado pela Vert – favor complementar com os comandos a serem utilizados para geração do hash do(s) arquivo(s) de backup da configuração da amostra.

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

OK. Premissa atendida no tópico 17 do Caderno de Testes enviado pela Vert.

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

OK. Premissa atendida no tópico 5.1.2 e 5.1.3 do Caderno de Testes enviado pela Vert.

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. 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.

Pendente. Premissa atendida PARCIALMENTE no tópico 5.1.6 do Caderno de Testes enviado pela Vert – favor complementar com os comandos a serem utilizados para geração do hash do(s) arquivo(s) de backup da configuração da amostra.

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

Pendente. Premissa atendida PARCIALMENTE no tópico 18 do Caderno de Testes enviado pela Vert – o item 18 referência apenas os passos do segundo teste de sessões – favor indicar e referenciar no item 18 um subitem específico que trata dos passos do primeiro teste de sessões.

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 5.1.2 e 5.1.3 do Caderno de Testes enviado pela Vert.

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.”

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. Premissa atendida no tópico 19.1 do Caderno de Testes enviado pela Vert.

2.1.39 Possuir inspeção profunda de pacotes para tráfego criptografado (no mínimo em tráfego VPN e HTTPS)
OK. Premissa atendida no tópico 19.2 do Caderno de Testes enviado pela Vert.

2.1.45.6 Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoramento e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.
Pendente. Premissa atendida PARCIALMENTE no tópico 19.3 do Caderno de Testes enviado pela Vert – não foram encontradas no item 6 informações que tratem especificamente do cadastro/manipulação de objetos de rede. Favor inserir procedimentos e testes específicos, conforme requerido pelo item 2.1.45.6 do edital.

2.1.45.9 Deve suportar a geração de alertas automáticos via email, SNMP e Syslog.
OK. Premissa atendida no tópico 19.4 do Caderno de Testes enviado pela Vert.

2.1.45.12 Deve informar o número de sessões simultâneas e de novas sessões por segundo dos equipamentos gerenciados.
OK. Premissa atendida no tópico 19.5 do Caderno de Testes enviado pela Vert.

2.1.63 Suportar os protocolos de roteamento RIPv2, OSPFv2 ou OSPFv3 para as funcionalidades de VPN;
OK. Premissa atendida no tópico 19.6 do Caderno de Testes enviado pela Vert.

2.1.68 Possuir gerenciamento gráfico das funcionalidades de VPN e monitoramento de seus eventos de forma integrada tanto com a gerência local do equipamento ou do cluster quanto com a gerência centralizada da solução.
Pendente. Premissa atendida PARCIALMENTE no tópico 19.7 do Caderno de Testes enviado pela Vert – procedimentos dos testes referenciados no item 19.7 deve ser executado TAMBÉM sobre a solução de gerência centralizada (conforme especificado pelo item 2.1.68), e não somente na interface gráfica do equipamento. Favor inserir os testes para a gerência centralizada.

2.2.7 Deve possibilitar a filtragem dos logs do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.
Pendente. Premissa não atendida no tópico 19.8 do Caderno de Testes enviado pela Vert – procedimentos dos testes referenciados no item 19.8 deve ser executado sobre a solução de gerência centralizada (conforme especificado pelo item 2.2.7), e não na interface gráfica do equipamento. Favor inserir os testes para a gerência centralizada.

2.2.8 Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de sessões bloqueadas com seus destinos e serviços, os mais frequentes ataques e ameaças de segurança detectadas com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários que consumem mais banda de Internet, os sítios na Internet mais visitados.
Pendente. Premissa não atendida no tópico 19.9 do Caderno de Testes enviado pela Vert – procedimentos dos testes referenciados no item 19.9 deve ser executado sobre a solução de gerência centralizada (conforme especificado pelo item 2.2.8), e não na interface gráfica do equipamento. Favor inserir os testes para a gerência centralizada.

2.3.3 Decodificar múltiplos formatos de Unicode;
OK. Premissa atendida no tópico 19.10 do Caderno de Testes enviado pela Vert.

2.3.6 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 Office 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. Premissa atendida no tópico 19.11 do Caderno de Testes enviado pela Vert.

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 Plug-ins/Add-nos.
OK. Premissa atendida no tópico 19.12 do Caderno de Testes enviado pela Vert.

2.3.12 Permitir filtros de anomalias de protocolos, inclusive protocolos de aplicação (ex.: HTTP, SMTP, NTP, NetBIOS, HTTPS, FTP, DNS, SMB, RPC, SSH e Telnet);
OK. Premissa atendida no tópico 19.13 do Caderno de Testes enviado pela Vert.

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.
Pendente. Premissa atendida PARCIALMENTE no tópico 19.14 do Caderno de Testes enviado pela Vert – não foram encontradas no item 8, conforme apontado no procedimento do teste, informações que tratem especificamente de testes de ataques ao próprio equipamento. Favor complementar.

2.5.1 Deve possuir funcionalidades de tratamento de conteúdo web, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet web já registrados e classificados, distribuídos em, no mínimo, 40 (quarenta) categorias ou subcategorias pré-definidas;
OK. Premissa atendida no tópico 19.15 do Caderno de Testes enviado pela Vert.

2.5.9 Deve ser capaz de exibir mensagem de bloqueio customizável pelos Administradores para resposta aos usuários, na tentativa de acesso a recursos proibidos ou restringidos pela política de segurança do órgão;
Pendente. Premissa atendida PARCIALMENTE no tópico 19.16 do Caderno de Testes enviado pela Vert – não foram encontradas no item 8, conforme apontado no procedimento do teste, informações que tratem especificamente da exibição de mensagem de bloqueio customizável no acesso a recursos (URLs bloqueadas, por exemplo). Favor complementar.

2.5.10 Permitir o bloqueio de páginas web por meio da construção de filtros específicos com mecanismo de busca textual;
Pendente. Premissa atendida PARCIALMENTE no tópico 19.17 do Caderno de Testes enviado pela Vert – não foram encontradas no item 8, conforme apontado no procedimento do teste, informações que tratem especificamente do teste de construção de filtros textuais para bloqueio de páginas web. Favor complementar.

2.5.10.1 O item 2.5.10 pode ser atendido através da criação de aplicações em camada 7 customizadas.

2.5.11 Permitir o bloqueio de URLs cujo campo CN ou DN não contém um domínio válido para o certificado SSL;
OK. Premissa atendida no tópico 19.18 do Caderno de Testes enviado pela Vert.

2.5.14 Possuir categorização de sites governamentais nacionais, mesmo não tendo domínio “gov” ou “.gov.br.”
OK. Premissa atendida no tópico 19.19 do Caderno de Testes enviado pela Vert.

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.
Pendente. Premissa atendida no tópico 19.20 do Caderno de Testes enviado pela Vert, porém os procedimentos dos testes devem apontar para o item 16 – Teste de Assertividade. Favor corrigir.

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.
OK. Premissa atendida no tópico 19.21 do Caderno de Testes enviado pela Vert.

2.6.13 Identificação, bloqueio e restrição em profundidade e granularidade de aplicações, contemplando no mínimo: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Google Docs, Instagram, Twitter, LinkedIn, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR e Webex.
OK. Premissa atendida no tópico 19.22 do Caderno de Testes enviado pela Vert e pelo arquivo anexo

3.22.1.4 Possuir no mínimo 6 (seis) portas 10/100/1000 BASE-T, podendo 01 (uma) delas ser utilizada para gerência, 4 (quatro) portas 1GE SFP, com os respectivos transceivers 1000BASE-SX e padrão IEEE802.3z, e 2 (duas) portas 10GE SFP+ ou XFP, com os respectivos transceivers 10GBASE-SR e padrão IEEE802.3ae.
OK. Premissa atendida no tópico 19.23 do Caderno de Testes enviado pela Vert e pelo arquivo anexo

3.22.1.4.1 As portas elétricas podem ser entregues por meio de transceivers
OK. Premissa atendida no tópico 19.23 do Caderno de Testes enviado pela Vert e pelo arquivo anexo.

3.24.1.2 Possuir suporte para a integração com equipamentos ou serviços com a funcionalidade de APT (Advanced Persistent Threat) e Zero Day.

Pendente. Premissa atendida PARCIALMENTE no tópico 19.24 do Caderno de Testes enviado pela Vert – não foram encontradas no item 8, conforme apontado no procedimento do teste, informações que tratem especificamente da verificação do suporte e integração do equipamento com serviços de proteção à APT. Favor complementar.

3.24.1.3 A funcionalidade de APT (Advanced Persistent Threat) e Zero Day deve possuir capacidade de emular (sandbox) ataques em diferentes sistemas operacionais, tais como: Windows XP e Windows 7, assim como documentos do Windows Office. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.
Pendente. Verificar item anterior.

9. ESCLARECIMENTOS DIVERSOS

Dúvidas ou indicações adicionais foram observadas no caderno de teste apresentado pela empresa Vert. É necessário realizar nova revisão do caderno de testes a fim de gerar a versão final do documento.

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.