CICAD.II.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

IMPLEMENTAÇÃO DE TESTES DE INVASÃO EM APOIO À PROTEÇÃO CIBERNÉTICA DE REDES E SISTEMAS DE INTERESSE DA DEFESA

Luiz Henrique Filadelfo Cardoso[1], Lucas Maurício Alves Zigunow[2]

Pós-graduado em Gestão de Segurança da Informação[1], Mestrando em Gestão dos Sistemas de Informação e das Redes[2]

RESUMO: Este trabalho tem como principal objetivo apresentar aspectos fundamentais sobre Testes de Invasão e sobre a sua implementação em apoio à proteção cibernética de redes e sistemas de interesse da Defesa. Buscou-se neste artigo apresentar o atual cenário de proteção, dominado por técnicas e ferramentas de caráter passivo, assim como defender que o apoio da segurança ofensiva, em específico do processo de pentesting, pode ser relevante para o estabelecimento de uma consciência situacional mais equilibrada sobre os ativos de Defesa que se deseja proteger. Para isso, realizou-se uma pesquisa bibliográfica em busca de conceitos consistentes sobre Teste de Invasão, principais modalidades, metodologias aplicáveis e de características que o afastem em entendimento de outras modalidades de avaliações de segurança como Auditoria de Segurança e Análise de Vulnerabilidades. Na sequência, discorreu-se sobre a dinâmica presente nos Testes de Invasão, identificando procedimentos e correlações entre cada fase interdependente e como cada estágio influencia no resultado final de tais testes. Por fim, foram feitas considerações a respeito da implementação do pentesting no contexto militar, apontando caminhos de caráter estrutural, de treinamento e formação de equipes para que os benefícios advindos da adoção de tal prática não se restrinjam apenas a complementar a proteção dos ativos de Defesa, como inicialmente proposto, mas que vá além e contribua também de maneira relevante para formação e adestramento do combatente cibernético brasileiro.

Palavras-chave: Teste de invasão. Segurança ofensiva. Proteção cibernética. Defesa cibernética. Defesa nacional.

INTRODUÇÃO

Em um mundo cada vez mais complexo e interconectado, proteger-se contra a exploração de vulnerabilidades por elaboradas ameaças consiste em diferencial de grande valia para Estados e organizações que desejam permanecer ativos e operacionais, principalmente a partir do ciberespaço.

Nesse contexto, o uso de métodos, técnicas, ferramentas e procedimentos adequados de segurança, aliado ao pleno entendimento sobre eventuais vulnerabilidades identificadas (e do potencial impacto caso sejam exploradas), é competência que os responsáveis pela proteção cibernética de sistemas e redes de interesse da Defesa Nacional devem se valer durante 24 horas por dia, 7 dias por semana.

Porém, ainda que estes profissionais sigam políticas, melhores práticas e recomendações de segurança, assim como monitorem a infraestrutura sob sua responsabilidade de maneira ininterrupta, tradicionalmente não há a presença do olhar ofensivo, com viés do invasor, na detecção de vulnerabilidades, o que efetivamente traria uma consciência situacional mais adequada do ambiente a ser protegido. Ou seja, há a primazia da ótica defensiva com ênfase na reação (ação após incidentes e configuração de soluções de caráter passivo), em detrimento de uma visão expandida na qual também teria espaço a mimetização do mindset proativo do hacker na percepção de ameaças e proposição de medidas de segurança customizadas. A fim de reduzir essa lacuna e cumprir a máxima de que “Para pegar o invasor, deve-se pensar igual a ele”, emerge como disciplina complementar a Segurança Ofensiva.

Segurança Ofensiva pode ser definida como o conjunto de ações proativas que visa

descobrir brechas de segurança, por meio da aplicação de técnicas e ferramentas usualmente utilizadas por criminosos cibernéticos, com o intuito de analisar a extensão e impacto de eventuais ataques antes que vulnerabilidades sejam exploradas pelos referidos atores ou outros agentes adversos. Posto isto, o processo baseado em metodologia específica e técnicas avançadas que melhor se coaduna ao atendimento dos objetivos supramencionados é o Teste de Invasão.

Importante ainda expor que, para esse trabalho, o entendimento de redes e sistemas de interesse da Defesa correlaciona-se às infraestruturas de Tecnologia da Informação e Comunicação (TIC), inclusive infraestruturas críticas, que sejam essenciais para os interesses do Ministério da Defesa, cumprimento da missão das Forças Singulares e para a continuidade da sociedade da informação, conforme depreendido de Brasil (2014).

Sendo assim, este artigo foi organizado da seguinte forma: Seção I apresenta definição de Teste de Invasão, principais tipos, metodologias aplicáveis e sua distinção em relação a outras modalidades de avaliações de segurança como auditoria de segurança e análise de vulnerabilidades; na Seção II serão detalhadas as fases presentes em um Teste de Invasão, com base no recomendado pela metodologia PTES; já na Seção III discorre-se sobre a implementação do Teste de Invasão no contexto militar; e por fim são tecidas as conclusões sobre o estudo realizado.

1 TESTE DE INVASÃO

Em consonância ao apresentado por Weidman (2014, p.30), Teste de Invasão (ou Pentesting) pode ser interpretado como uma simulação de ataques reais destinada a avaliar os riscos e impactos associados a brechas de seguranças identificadas (caso sejam exploradas). A referida autora também acrescenta que diferente de auditoria de segurança e de análise de vulnerabilidades, onde aquela visa checar o cumprimento de controles previamente definidos e esta a identificar e analisar vulnerabilidades sem necessariamente explorá-las, a finalidade de um teste de invasão vai além ao utilizar métodos e técnicas de um atacante para não somente identificar brechas de segurança, mas para também analisá-las profundamente, explorando-as quando viável, a fim de avaliar o que pretensos invasores poderiam obter após uma exploração bem sucedida das vulnerabilidades encontradas.

Em uma outra definição, esta advinda da empresa de segurança Ec-Council extraída de seu curso Certified Ethical Hacker V.9, depreende-se que:

> Teste de invasão é um método de avaliação de segurança voltado a um sistema de informação ou rede por meio da simulação de um ataque para encontrar vulnerabilidades que atacantes poderiam explorar; [e que] um teste de invasão não apenas descobre vulnerabilidades, mas também documenta como elas podem ser exploradas (CEH, 2017, mod.1, p.59).

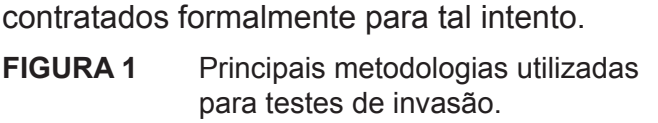
Testes de invasão são ainda subdivididos em três tipos básicos em relação ao conhecimento sobre da infraestrutura a ser testada, quais sejam: black-box - quando não há conhecimento prévio da infraestrutura a ser testada; gray-box - conhecimento parcial da infraestrutura que necessita ser testada; e white-box - quando há total conhecimento sobre a infraestrutura objeto de testes (CEH, 2017).

É importante destacar que o escopo do pentesting não se restringe apenas a testes na esfera lógica de redes e sistemas, mas também o foco da verificação pode ser estendido para testar controles físicos de acesso e avaliação do nível de conscientização de segurança dos colaboradores de uma organização. Alguns especialistas defendem ainda uma outra subdivisão voltada a origem do teste de invasão em: teste de invasão externo - no qual os ataques simulados partiriam de “fora para dentro” da organização, por exemplo via Internet e (ou) via engenharia social; e teste de invasão interno - no qual, por exemplo, simular-se-ia um colaborador descontente com intenções maliciosas

dentro da organização com acesso a sistemas, redes, salas, documentos etc, objetivando-se verificar o grau de segurança de tais ativos e as eventuais consequências danosas caso se confirme o cenário testado (WEIDMAN, 2014).

Por demandar um caráter multidisciplinar dos profissionais que realizam tais testes (pentester), é mandatório que eles sejam organizados em equipes formadas de acordo com os conhecimentos requeridos no escopo do teste (forense computacional, desenvolvimento web, análise de malwares, criptografia, redes Wi-Fi, administração de redes e servidores etc). Uma outra questão reside no vínculo dos integrantes das equipes de pentesting com a organização a ser testada, pois não há a obrigatoriedade de que os pentesters pertençam exclusivamente ao quadro de colaboradores da organização (ainda que seja oportuno), desta forma é plausível também que profissionais externos a organização procedam tais ações, devendo tão somente estarem autorizados ou contratados formalmente para tal intento.

FIGURA 1 Principais metodologias utilizadas para testes de invasão.



Fonte: OPTRASECURITY, 2018.

No que tange as principais metodologias empregadas na estruturação de um teste de invasão, destacam-se, conforme apresentado na Figura 1: Penetration Testing Execution Standard (PTES), Open Source Security Testing Methodology Manual (OSSTMM), OWASP Testing Guide e National Institute of Standards and Technology (NIST) guidelines. Dentre as listadas acima, apenas a metodologia PTES foi desenvolvida com o intuito específico de servir como modelo para conformação de testes de invasão. Enquanto a OWASP possui um escopo dedicado a testes em serviços e aplicações web, NIST e OSSTMM possuem escopo mais amplo e voltado a testes de segurança em geral, ainda que customizáveis para a configuração de um pentesting (BERTOGLIO; ZORZO, 2015).

2 FASES DE UM TESTE DE INVASÃO

Com o firme entendimento do que vem a ser Teste de Invasão, torna-se necessário conhecer e entender a sua dinâmica, desde o esboço até a entrega dos resultados ao solicitante do referido teste. A seguir, serão detalhadas as fases presentes em um teste de invasão, com base no recomendado pela metodologia PTES, as quais se resumem em: preparação, coleta de informações, análise de vulnerabilidades, exploração de falhas, pós-exploração de falhas e geração de relatórios.

2.1 PREPARAÇÃO

Antes do início do teste de invasão, os pentesters devem interagir com o solicitante (Cliente) do teste em busca de definir claramente os objetivos e as eventuais restrições para sua realização. Neste momento determina-se, tal qual recomendado por Weidman (2014):

a) escopo do teste: nesta etapa defini-se a extensão e parâmetros do teste, as redes, sistemas e ativos que serão testados, assim como detalham-se quais ações serão realizadas em sistemas que sejam críticos para o negócio da organização, a fim de evitar indisponibilidades. Por exemplo, nesta etapa deve-se fazer algumas das seguintes perguntas: quais sistemas ou faixa de endereços IP serão testados? Será permitido engenharia social nos colaboradores? O solicitante autoriza o uso de exploit ou de uma simples varredura (scan) em seus sistemas críticos?

b) janela de testes: estipula-se, com base no negócio da organização e devidamente acordado com o solicitante, a duração estimada e o horário em que será procedido os testes para que não ocorram descontinuidades em processos importantes de negócio. Por exemplo, sistemas de

email ou web corporativos apenas serem testados fora do horário comercial.

c) contato de responsável da organização para coordenação: é importante definir uma contraparte na organização a ser testada, geralmente o gestor de mais alto nível de TIC, a fim de que o chefe da equipe de pentesters possa contatá-lo caso a equipe faça uma descoberta grave ou outra coordenação relevante durante a realização do teste de invasão.

d) autorização formal para execução do teste: após reuniões entre as partes, nas quais são definidos limites, objetivos, responsabilidades e acordos de confidencialidade, assim como o escopo dos sistemas, redes e processos a serem testados, o produto final de como será conformado o teste de invasão será resumido a um contrato. Este instrumento não é só imprescindível para a organização solicitante resguardar o seu negócio, mas sobretudo é a permissão formal e o passe "fora da prisão" da equipe de pentesters para executar ações invasivas em ativos alheios, ainda que sob teste.

2.2 COLETA DE INFORMAÇÕES

Nesta fase, conforme exposto por Weidman (2014, p. 31), "o pentester procura informações disponíveis sobre o cliente e identifica maneiras em potencial de conectar-se com seus sistemas". Tal coleta pode ocorrer por meio de fontes cibernéticas, humanas ou aberta. Por exemplo, coleta em redes sociais online e websites da organização e de seus funcionários, uso de scanners de porta a fim de identificar serviços, versões e portas abertas em sistemas-alvo e faixas IP de interesse (tal qual exposto abaixo na Figura 2), coleta e análise do lixo da organização, observação da rotina laboral e comportamental de colaboradores de interesse.

FIGURA 2 Resultado de um scanner (Nmap) para descobrir portas, versões e serviços ativos em sistema-alvo.

```
Starting Nmap 5.21 ( http://nmap.org ) at 2010-04-01 11:19 IDT
Nmap scan report for Scanme.Nmap.Org (64.13.134.52)
Host is up (0.18s latency).
rDNS record for 64.13.134.52: scanme.nmap.org
Not shown: 993 filtered ports
PORT      STATE  SERVICE
25/tcp    closed smtp
53/tcp    open   domain
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed auth
8009/tcp  open   ajp13
31337/tcp closed Elite
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.15 - 2.6.26
```

Fonte: Tosch, 2011.

É importante que a fase de coleta de informações seja a mais extensa e metódica possível, uma vez que "os achados" serão determinantes para formulação do melhor caminho para acessar os ativos em teste, conforme será visto a seguir, principalmente na fase de modelagem de ameaças.

2.3 MODELAGEM DE AMEAÇAS

De acordo com os dados e informações colhidos na fase anterior em relação aos ativos, sistemas e redes a serem testados, o pentester irá definir um adequado plano de ataque, com base em procedimentos, ferramentas e métodos específicos para o ativo a ser testado. Ou seja, com base no conhecimento obtido serão definidas estratégias para explorar os sistemas, redes e controles sob teste. Nessa fase também é usual a priorização de cada descoberta por ordem de severidade com base no risco de exploração e o seu eventual impacto danoso (ELEARNSECURITY, 2015).

2.4 ANÁLISE DE VULNERABILIDADES

Após os pentesters colherem informações (serviços e versões de sistemas, faixa de endereços IP de interesse, informações sobre hierarquia, colaboradores e setores-chave da organização etc.) e definirem caminhos e estratégias, priorizando quais ações são mais relevantes, chega o momento de descobrir ativamente as vulnerabilidades existentes com a finalidade de se determinar até que ponto suas

estratégias de exploração poderão ser bem-sucedidas (WEIDMAN, 2014).

Nessa fase, os profissionais fazem tentativas para encontrar brechas de segurança nos controles, sistemas, redes e ativos, no intuito de caracterizá-los como vulneráveis, e por consequência, passíveis de serem explorados. A título de exemplo, executar scanners de vulnerabilidades como SqlMap, Nessus, Nikto, OpenVas ou identificar sistemas, serviços, aplicações carentes de atualizações de segurança são algumas das ações realizadas na fase de análise de vulnerabilidades. Um procedimento comum também nessa fase é a consulta ao banco de vulnerabilidades CVE (Common Vulnerabilities and Exposures), o qual concentra a descrição das principais vulnerabilidades identificadas, com a finalidade de, ao se comparar com as versões de serviços ou aplicações testadas, verificar a existência de códigos (exploits), softwares, técnicas ou procedimentos capazes de explorar os ativos sob análise (ROHR, 2017).

2.5 EXPLORAÇÃO DE FALHAS

Para a grande maioria, essa é a fase mais divertida e interessante em um teste de invasão (WEIDMAN, 2014). No entanto, ela apenas será efetiva se as fases anteriores foram realizadas com detalhamento e produziram dados ou inoformações de valor.

Assim, já com as vulnerabilidades encontradas, listadas e analisadas, o próximo passo é ganhar acesso (de preferência com privilégios de administrador) nos ativos sob teste, sempre objetivando não ser detectado e sem deixar rastros.

O uso de email malicioso (phishing), injeção e manipulação de código SQL malicioso, malwares, credenciais padrão, técnicas de engenharia social e exploração por exploits são os vetores mais comuns de exploração de sistemas, a variar apenas sua escolha, de acordo com o perfil do sistema e usuário almejados (CARDOSO, 2017). Uma plataforma comumente utilizada para dar suporte a este intento é o framework Metasploit, nativo da distribuição Kali Linux, voltada especificamente para segurança ofensiva.

2.6 PÓS-EXPLORAÇÃO DE FALHAS

Com acesso ao sistema ou ativo de interesse, na fase de pós-exploração de falhas, são realizados levantamentos a fim de se aferir o que é possível realizar ou extrair com o acesso conquistado ao sistema.

Elevação de privilégios, instalação de códigos maliciosos para manutenção de acesso, possibilidade de movimento lateral para outras máquinas na mesma rede (ou para outras redes), limpeza de rastro e alteração de logs, busca por arquivos e informações sensíveis, extração de credenciais que possam dar acesso a outros ativos são algumas das ações que os pentesters devem tentar nessa fase para compor o relatório final. Essas ações proporcionarão mensurar o eventual impacto caso um agente adverso venha a ter acesso ao ativo sob teste.

2.7 GERAÇÃO DE RELATÓRIOS

Por fim, na fase de geração de relatórios, os pentesters compilam em documento formal as descobertas tanto para os profissionais executivos (alta direção) quanto para o corpo técnico (responsáveis na “linha de frente” pela gestão e manutenção dos ativos sob análise) da organização. Conforme depreende-se de eLearnSecurity (2015, p.6), “o mais importante ao se confeccionar relatórios é evitar fazer uso de jargões ou termos que possam prejudicar a inteligibilidade por parte do público-alvo”.

Esse documento contemplará, ordenadamente e por seções, a dinâmica do teste de invasão realizado: escopo do teste, apontamentos sobre o que é feito de correto, o que está incorreto e pode ser melhorado, vulnerabilidades encontradas, como o acesso foi conseguido, o que foi descoberto, o risco e impacto para o negócio e como corrigir os problemas encontrados (WEIDMAN, 2014, p. 35). Desta forma, se todos os dados e informações foram

colhidos e organizados adequadamente durante o teste, escrever o relatório mostra-se como uma tarefa meramente de síntese em relação às descobertas e recomendações aplicáveis para corrigir as vulnerabilidades identificadas.

Ainda cabe destacar que o recomendável é que a equipe envolvida no teste proceda, com base no relatório final, uma apresentação oral na organização testada com a presença do corpo técnico e de representantes da alta direção, a fim de que para os técnicos sejam elucidadas eventuais dúvidas e para a direção seja salientada a necessidade de resolução das vulnerabilidades encontradas e a importância de suporte à equipe de técnicos para o êxito da correção. Esta exposição deve ser pautada por maturidade e objetividade (e não como um "caça as bruxas" e busca por culpados) tanto por parte do interlocutor, quanto pelos ouvintes (ELEARNSECURITY, 2015).

3 CONSIDERAÇÕES SOBRE A IMPLEMENTAÇÃO DE TESTES DE INVASÃO NO CONTEXTO MILITAR

Ainda que no cenário empresarial a busca por profissionais e a realização de testes de invasão cada vez seja mais requerida, sobretudo em organizações que possuem dados sensíveis e são obrigadas por força de Lei ou por Estatutos a dar respostas a seus sócios, acionistas, mercado e clientes quanto ao grau de segurança cibernética do seu negócio, no contexto militar ainda não é a realidade e instrumento usual tal prática de sergurança (SERPRO, 2018).

De acordo com a Estratégia Nacional de Defesa (BRASIL, 2008), que definiu o desenvolvimento do setor cibernético sob responsabilidade do Exército Brasileiro, o que demandou entre outras ações a criação do Centro de Defesa Cibernética (CDCiber) em 2012 como órgão operacional e o Comando de Defesa Cibernética (ComDCiber) em 2014 como órgão coordenador e gestor da atividade em âmbito nacional, a tarefa de se realizar testes de invasão em redes e sistemas de interesse da Defesa pertenceria - sob autorização e supervisão normativa do ComDCiber - naturalmente ao braço operacional, qual seja o CDCiber.

Porém, devido à restrição quantitativa de pessoal para o escopo amplo e complexo

de testes que se apresenta: universo normativo e tecnológico heterogêneo, unidades militares distribuídas geograficamente, entre o próprio Exército Brasileiro, Marinha do Brasil e o Comando da Aeronáutica; uma proposta alternativa seria transferir parte dessa responsabilidade executiva de realização de testes de invasão, de maneira similar ao que já ocorre com a proteção cibernética nos moldes atuais para cada Força Armada.

Nesse cenário, ficaria a cargo do CD-Ciber: a execução de testes de invasão nas redes e sistemas de interesse do Ministério da Defesa (eventualmente em outros órgãos da Administração Pública Federal e nas forças militares singulares), a preparação de pessoal dedicado para ações de Estado no tocante à Defesa Cibernética e treinamento do pessoal militar (equipes de pentesting) do Exército, Marinha e Aeronáutica para execução de tais testes (por meio da Escola Nacional de Defesa Cibernética - ENaDCiber), respectivamente, no âmbito de cada Força. O ComDCiber seria o órgão responsável por emitir normas basilares (e outras diretivas) sobre a realização de testes de invasão no âmbito da Defesa, sobre a forma e a dinâmica de solicitação e responsabilidades, padronização, desenvolvimento, doutrina, entrega de relatórios e apresentação dos resultados após os testes realizados. Desta forma, cada Força Armada recepcionaria em seu âmbito os pedidos internos de pentesting, assim como definiria o processo de como devem ser executados tais testes em suas redes e sistemas, tornando-os efetivamente um instrumento complementar para prover a proteção cibernética desejada aos ativos sob sua responsabilidade, de maneira oportuna, tempestiva e especializada ao seu contexto e realidade particular.

Outro aspecto que deve ser levado em conta é o treinamento e a estruturação das equipes de pentesting. Diferente do contexto civil em que as equipes são formadas com primazia pela aptidão e especialização de seus integrantes e pouco pelo tempo “de casa” ou hierarquia funcional; no meio militar a estruturação das equipes pode vir a sofrer influência em maior grau pela hierarquia do que pela especialização e aptidão do pentester.

Uma solução equilibrada pode ser considerar tanto na escolha da trilha de formação quanto na estruturação das equipes, o viés

da aptidão, habilidade reconhecida e da experiência anterior, fazendo uso da hierarquia funcional apenas para a posição de gerência ou coordenador de equipe. Por exemplo, em uma equipe formada por três integrantes, o de maior precedência ficaria responsável por coordenar os trabalhos e organização e formalizaçao dos resultados do teste de invasão, os outros dois por sua execução (caso necessário, também com apoio do integrante de maior precedência). Importante ainda acrescentar que a participação regular em exercícios cibernéticos simulados (red team vs blue team), cursos, treinamentos na área, desafios na modalidade CTF (Capture the Flag) e outros eventos nos quais sejam simulados ambientes e situações encontradas também em testes de invasão, contribuem de maneira determinante para a identificação de afinidades e habilidades aproveitáveis no pessoal a ser escolhido para a composição de equipes de pentesting, assim como para o seu devido adestramento e preparo contínuo (LOSPINOSO, 2018).

CONCLUSÕES

Por crer no aforismo de Sun Tzu, o chefe militar mais conhecido da antiguidade, quando este afirma que "conhecer o modo de agir de um oponente é fator preponderante para a vitória", este trabalho buscou apresentar a modalidade teste de invasão, que visa mimetizar métodos, técnicas e ferramentas usadas por criminosos cibernéticos, não para obter vantagens ilícitas, mas sim para complementar a proteção de redes, sistemas e outros ativos de interesse da Defesa.

O artigo definiu o que vem a ser testes de invasão, sua distinção em relação a auditoria de segurança e análise de vulnerabilidades, suas principais abordagens e características.

Também foi exposta a dinâmica presente nas fases de um teste de invasão desde o seu esboço até a geração de relatórios pós-teste a serem apresentados e entregues aos solicitantes. Neste momento cabe frisar: para que o artigo não se tornasse extenso em demasia, estes autores optaram por apresentar a estruturação do teste e não o detalhamento minuncioso das ferramentas a serem utilizadas em cada etapa, deixando tal aprofundamento como possibilidade em trabalhos futuros.

Na sequência, foram tecidas considerações sobre a adoção de testes de invasão no contexto militar, principalmente no que tange aos aspectos normativos e configuração de equipes de pentesting.

Por fim, em um olhar aproximado, vislumbra-se como benefícios imediatos da implementação de tais testes no meio militar, não só o reforço substancial da proteção cibernética dos ativos de Defesa, mas também a identificação e adestramento de pessoal especializado para atuar no ciberespaço (não só como defensores) ativamente como combatentes cibernéticos iniciados e adaptados nos três tipos de ações cibernéticas básicas demandadas pela Doutrina Militar de Defesa Cibernética brasileira (BRASIL, 2014), quais sejam: ataque cibernético, exploração cibernética e proteção cibernética.

IMPLEMENTATION OF PENTESTS IN SUPPORT TO THE CYBER PROTECTION OF SYSTEMS AND NETWORKS OF INTEREST OF DEFENSE

ABSTRACT: This work has as main objective to present fundamental aspects of Pentests and its implementation in support to the cyber protection of networks and systems of interest to the Defense. In this article we present the current protection scenario, dominated by passive techniques and tools, as well as to defend that the support of offensive security, specific to the pentesting process, may be relevant to the establishment of a more balanced situational awareness about the assets of Defense that one wishes to protect .In order to do this, a bibliographical research was carried out in search of consistent concepts about pentesting, main modalities, applicable methodologies and of characteristics that distance it in understanding of other modalities of security evaluations such as Security Audit and Vulnerability Assessment. Afterwards, we have analyzed the dynamics present in the Pentests, identifying procedures and correlations between each interdependent phase and how each stage influences the result of such tests. Finally, considerations were made regarding the implementation of pentesting in

THE MILITARY CONTEXT, POINTING OUT STRUCTURAL, TRAINING AND TEAM BUILDING PATHS SO THAT THE BENEFITS ARISING FROM THE ADOPTION OF SUCH PRACTICE WOULD NOT BE LIMITED TO COMPLEMENTING THE PROTECTION OF DEFENSE ASSETS, AS INITIALLY PROPOSED, BUT ALSO TO CONTRIBUTE IN A RELEVANT WAY TO THE TRAINING OF THE BRAZILIAN CYBER COMBATANT.

KEYWORD: PENTEST. OFFENSIVE SECURITY. CYBER PROTECTION. CYBER DEFENSE. BRAZILIAN DEFENSE.

REFERÊNCIAS

BERTOGLIO, D. D.; ZORZO, A. F. Um mapeamento sistemático sobre Testes de Penetração. Porto Alegre: FACIN/PUCRS, 2015.

BRASIL. Decreto-lei no 6.703, de 18 dezembro de 2008. Aprova a Estratégia Nacional de Defesa. Presidência da República. Brasília, 2008.

_____. MD31-M-07: Doutrina Militar de Defesa Cibernética. Ministério da Defesa. 1. Ed. Brasília, 2014.

CARDOSO, L.H.F. Anatomia de um ataque cibernético: conhecer e entender para melhor defender os ativos e meios de interesse da Força Aérea Brasilieira. SPECTRUM: Revista do Comando Geral de Operações Aéreas, Brasília, n.20, p.51-57, set. 2017.

CEH. Module 1: introduction to Ethical Hacking Certified Ethical Hacker Course, V.9. Ec-Council. 78p, 2017.

ELEARNSECURITY. How to become a penetration tester. Introduction to a career in IT Security. Whitepaper. 2015.

IAHN, T. S. Teste de Invasão em ambiente de governo. SERPRO. 2018. Disponível em: <http://www.serpro.gov.br/menu/noticias/noticias-2018/testes-de-invasao-em-ambientes-de-governo-1>. Acesso em 03 agosto 2018.

LOSPINOSO, Josh. Fish out of Water: How the military is an impossible place for hackers, and what to do about it. War on the Rocks. 2018. Disponível em :< https://warontherocks.com/2018/07/fish-out-of-water-how-the-military-is-an-impossible-place-for-hackers-and-what-to-do-about-it/>. Acesso em 03 agosto 2018.

OPTRASECURITY. Optra Security. 2018, Disponível em: <https://www.optrasecurity.com.br/>. Acesso em 04 agosto 2018.

ROHR, A. Como brechas em programas são classificadas pelo governo dos eua. G1: Segurança Digital. 2017. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/como-brechas-em-programas-sao-classificadas-pelo-governo-dos-eua.html>. Acesso em 02 agosto 2018.

WEIDMAN, G. Testes de Invasão. São Paulo: 1º Ed. Novatec, 2014.

TOSCH. Basic use of Nmap. Tosch Production. 2011. Disponível em: < https://toschprod.wordpress.com/2011/10/07/basic-use-of-nmap/>. Acesso em 02 agosto de 2018.

Luiz Henrique Filadelfo Cardoso é 2º Sgt especialista em Comunicações (BCO), concluiu o Curso de Formação de Sargentos pela Força Aérea Brasileira (FAB) no ano de 2007, é Bacharel em Sistemas de Informação com ênfase em Análise de Sistemas pela Faculdade de Porto Velho (2011) e pós-graduado em Gestão de Segurança da Informação (2013) e em Inteligência de Segurança (2014) pela Universidade do Sul de Santa Catarina – UNISUL. Também possui o Curso de Guerra Eletrônica pela Força Aérea Brasileira (2013) e o Curso de Guerra Cibernética para Sargentos ministrado pelo Exército Brasileiro (2016). Atualmente exerce a função de Analista de Segurança da Informação. Contato: luizlhfc@fab.mil.br

Lucas Maurício Alves Zigunow é 3º Sgt especialista em Informática (SIN), concluiu o Curso de Formação de Sargentos pela Força Aérea Brasileira (FAB) no ano de 2012, é Técnologo em Redes de Computadores pela Universidade Estácio de Sá (2017), cursando pós-graduação em Computação Forense e Perícia Digital pelo Instituto de Pós-Graduação e Graduação (IPOG) e mestrando em Segurança dos Sistemas de Informação e das Redes pela Universidade de Brasília (UnB). Também possui, Curso de Guerra Cibernética para Sargentos ministrado pelo Exército Brasileiro (2017), Certificação Ethical Hacker v9 pela EC-Council e outros cursos na área de TI. Atualmente exerce a função de Analista de Segurança da Informação. Contato: lucaslmaz@fab.mil.br