MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

INSTITUTO MILITAR DE ENGENHARIA

CURSO DE GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

Ten VINÍCIUS MAIA SENNA DELGADO

Alu WALTER MACAMBIRA OLLIVEIRA SANTTOS

ESTUDOS DE TESTES DE PENETRAÇÃO

Rio de Janeiro

2011

INSTITUTO MILITAR DE ENGENHARIA

Ten VINÍCIUS MAIA SENNA DELGADO

Alu WALTER MACAMBIRA OLLIVEIRA SANTTOS

ESTUDOS DE TESTES DE PENETRAÇÃO

Iniciação à Pesquisa apresentada ao Curso de Graduação de Engenharia de Computação como requisito parcial para a obtenção do título de Engenheiro.

Orientador: Anderson Fernandes P. dos Santos – D. Sc.

INSTITUTO MILITAR DE ENGENHARIA
Praça General Tibúrcio, 80 – Praia Vermelha
Rio de Janeiro – RJ CEP: 22290-270

621.317 Delgado, Vinícius Maia Senna
D352 Estudos de Testes de Penetração / Vinícius Maia Senna Delgado, Walter Macambira Olliveira Santtos – Rio de Janeiro: Instituto Militar de Engenharia, 2011.

72 p.

Iniciação à Pesquisa – Instituto Militar de Engenharia – Rio de Janeiro, 2011.

1. Engenharia de Computação. Iniciação à Pesquisa. 2. Sistemas de Controle. 3. Sistemas de Comunicação. I - Delgado, Vinícius Maia Senna. II – Santtos, Walter Macambira Olliveira. III – Título. IV – Instituto Militar de Engenharia.

CDD 621.317

INSTITUTO MILITAR DE ENGENHARIA

Ten VINÍCIUS MAIA SENNA DELGADO

Alu WALTER MACAMBIRA OLLIVEIRA SANTTOS

ESTUDOS DE TESTES DE PENETRAÇÃO

Relatório parcial de Iniciação à Pesquisa apresentada ao Curso de Graduação de Engenharia de Computação como requisito parcial para a obtenção do título de Engenheiro.

Orientador: Anderson Fernandes P. dos Santos - D. Sc.

Aprovado em 08 de junho de 2011 pela seguinte Banca Examinadora:

Anderson Fernandes P. dos Santos – D. Sc.

Julio Cesar Duarte – D. Sc.

Sérgio dos Santos Cardoso Silva – M. Sc.

Rio de Janeiro

2011

AGRADECIMENTOS

Dedicamos o referido trabalho às nossas famílias, que sempre estiveram presentes em nossa formação e nos incentivaram a prosseguir em nossos projetos. Aos nossos colegas de turma, com os quais não compartilhamos somente alegrias, mas dificuldades das quais nunca nos escusamos. E, principalmente, ao Maj Anderson, nosso orientador, pelo constante entusiasmo com o projeto e pela prontidão em sempre nos auxiliar no curso desta pesquisa.

Sumário

LISTA DE SIGLAS

Sigla	Significado
ABNT	Associação Brasileira de Normas Técnicas
ACL	*Access Control List*
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI	*Common Gateway Interface*
CRT	*Cathode Ray Tube*
CSIS	*Center for Strategic and International Studies*
DDoS	*Distributed Denial of Service*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
DoS	*Denial of Service*
FEOIS	*Federal Office for Information Security* – BSI
FTP	*File Transfer Protocol*
GCHQ	*Government Communications Headquarters*
HTML	*HyperText Markup Language*
HTTP	*Hypertext Transfer Protocol*
IDS	*Intrusion Detection System*
IETF	*Internet Engineering Task Force*
IM	*Instant Messenger*
IP	*Internet Protocol*
IRC	*Internet Relay System*
LCD	*Liquid Crystal Display*
NAT	*Network Address Translation*
NDA	*Non-Disclosure Agreement*
NIST	*National Institute of Standards And Technology*
P2P	*Peer to peer*
RFID	*Radio Frequency Identifier*
SMS	*Short Message Service*
SO	Sistema Operacional
SQL	*Structured Query Language*
SSI	*Server Side Include*
TCP/IP	*Transmission Control Protocol/Internet Protocol*
TI	Tecnologia da Informação
TTL	*Time-To-Live*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*

LISTA DE FIGURAS

RESUMO

Devido à atual complexidade dos sistemas de comunicação e falta de controle sobre a segurança, configurações indevidas ou, até mesmo, falhas de software e hardware proporcionam vulnerabilidades que podem resultar em acesso não autorizado ao sistema. A mitigação de riscos desta natureza é de grande interesse para qualquer organização que preste serviços que necessitem de confiabilidade em seus sistemas.

Um teste de penetração é uma tentativa controlada de invadir esses sistemas a partir do ponto de vista externo ou interno, com o propósito de detectar suas vulnerabilidades e evitar as consequências de um ataque real.

O presente trabalho trata da padronização para a realização de testes de penetração em sistemas de informação. Inicialmente, aborda-se o assunto de maneira genérica, com a pretensão de se estabelecer bases jurídicas, éticas e metodológicas de como realizar o teste de maneira que seja resistente às evoluções de software e de hardware. Posteriormente, são detalhados os procedimentos realizados, incluindo uma lista com as ferramentas utilizadas e suas respectivas configurações.

ABSTRACT

Due to the complexity of the current information systems, the lack of control over information security, misconfigurations or even software and hardware failures create vulnerabilities that can lead into a non-authorized system access. The mitigation of risks of this kind is of great value for any organization that provides services that need reliable systems.

A penetration test is a controlled attempt at penetrating those systems from outside, with the purpose of detecting their vulnerabilities, avoiding the drastic consequences of a real attack.

This study is aimed at the standardization for performing penetration tests in information systems. Initially, this issue is addressed in a generic way, with the intention of establishing juridical, ethical and methodological basis of how to perform a penetration test in a way of making it resistant to software and hardware evolution. Later, procedures performed are detailed, including a list of the tools used and their configurations.

1 INTRODUÇÃO

A preocupação com a segurança dos sistemas de informação tem crescido significativamente com a informatização das organizações. Apesar dos grandes benefícios trazidos, as vulnerabilidades inerentes a um sistema informatizado representam um grande risco de prejuízo financeiro.

Deste modo, com a finalidade de mitigar possíveis falhas de segurança e, por consequência, eventuais ônus oriundos de um acesso não autorizado, a necessidade de testes para avaliar um sistema de informação se tornou de grande interesse das organizações. Neste contexto, surgem os testes de penetração (*pentests*), uma maneira controlada para detectar e explorar as vulnerabilidades desses sistemas.

1.1 Contextualização

O relatório "Sob fogo cruzado: infraestruturas críticas na era da ciberguerra", encomendado pela McAfee e de autoria do *Center for Strategic and International Studies* (CSIS, 2010), mostra o crescente risco da guerra cibernética, transformando-a em fator constate do atual cenário mundial. Segundo Iain Lobban, diretor da agência britânica *Government Communications Headquarters* (GCHQ), diversos países já estão utilizando técnicas de guerra cibernética para executar ataques entre si por motivações políticas explícitas, demandando, assim, a necessidade de proteger e vigiar sistemas críticos de computadores.

Em junho de 2010, o vírus *Stuxnet*, sob suspeita de ter sido criado por algum Estado, afetou usinas nucleares secretas no Irã e indústrias fundamentais na China. Casos recentes como este aumentam a preocupação das nações com a segurança cibernética.

No Brasil, apesar das estatísticas do ano de 2010 e de 2011, os incidentes de rede têm crescido quase exponencialmente, causando receio aos usuários quanto à segurança de serviços informatizados. Este medo se justifica ao observar os dados registrados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) na Figura 1.1.

Frente a este cenário, o tema guerra cibernética recebeu a devida atenção do Governo Federal, originando, como consequência desta preocupação, a Estratégia Nacional de Defesa. Esta estratégia, ademais de seus outros objetivos, entrega a missão dos estudos sobre guerra cibernética ao Exército Brasileiro.

Desta forma, alinhado com as determinações da Estratégia Nacional de Defesa, o IME, como elemento principal do desenvolvimento científico e tecnológico do Exército

Brasileiro, propõe, através de um projeto de Iniciação à Pesquisa, o corrente tema Estudos de Teste de Penetração.

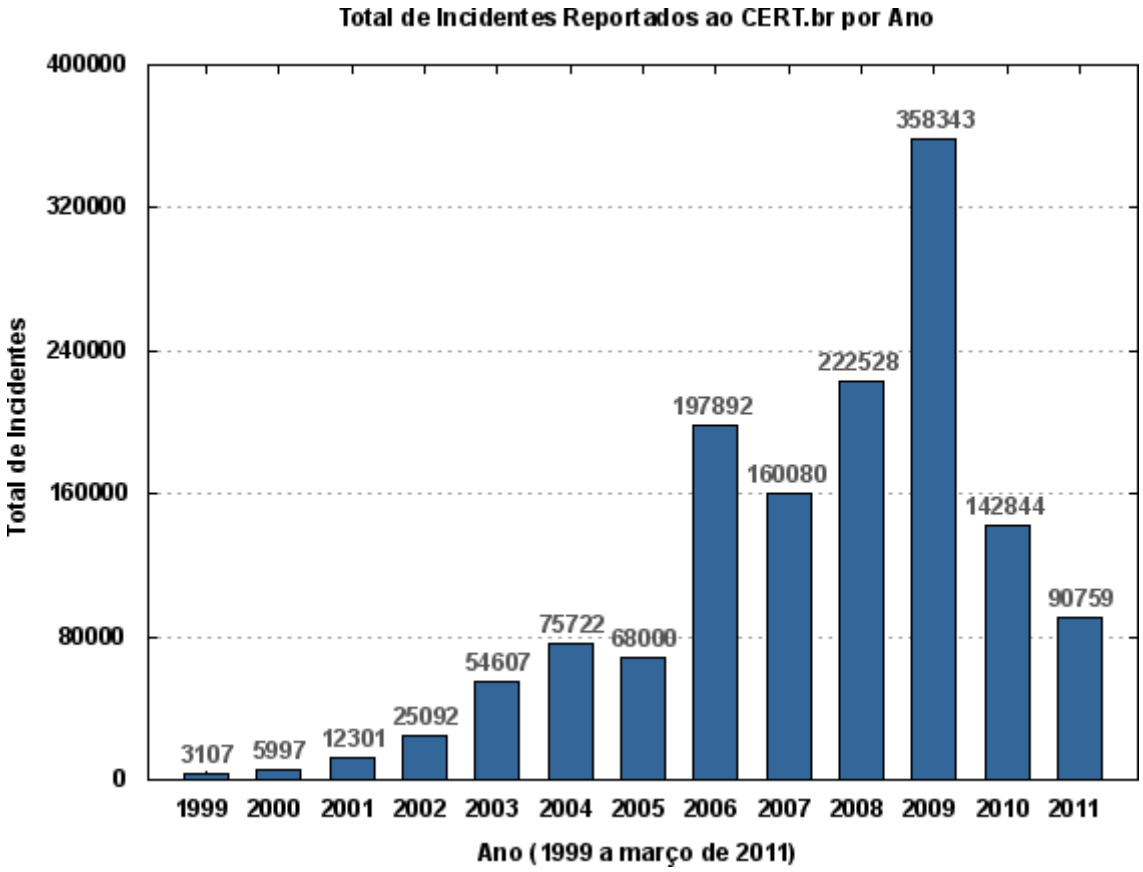

Figura 1.1 - Taxa de Incidentes de Rede Por Ano (CERT.br)

1.2 Relevância deste trabalho

Os resultados de um teste de penetração dependem da infraestrutura do sistema de informação. Além da constante evolução do hardware e do software, a eficácia de um teste varia muito com a criatividade e a experiência de quem o realiza, pois não existem padrões rígidos a serem seguidos. Deste modo, este trabalho busca consolidar bases sobre a realização de um teste de penetração, abordando, principalmente, os princípios envolvidos.

1.3 Objetivo

O objetivo geral desta iniciação à pesquisa é concentrar, de modo didático, informações sobre testes de penetração, abordando conceitos teóricos e definindo

termos relacionados ao assunto. Almeja-se a sugestão, no âmbito de instituições de ensino como o IME, de uma metologia específica e o estabelecimento de procedimentos abrangentes resistentes à evolução tecnológica. Desta forma, não se especificam detalhes sobre as ferramentas utilizadas ou sobre a infraestrutura analisada.

Após essa consolidação teórica, este trabalho tem como objetivo específico detalhar módulos para a realização do teste de penetração. Esta tarefa será feita através da revisão das principais obras da literatura relacionada, abordando não só as ferramentes utilizadas para cada atividade, mas também as informações básicas necessárias para a execução de cada uma.

1.4 Organização da Monografia

Seguindo o modelo definido pelo *Federal Office for Information Security* (FEOIS, 2003), tratar-se-á inicialmente de uma introdução na qual se estabelecem definições básicas e o público alvo. Deve-se, ainda, introduzir conceitos de segurança da informação e suas ameaças e definir, em linhas gerais, o teste de penetração.

Posteriormente, procura-se diferenciar testes de penetração e auditorias de segurança da informação, ainda delimitando os objetivos do teste, suas limitações e suas classificações. Deve-se abordar, superficialmente, aspectos legais e éticos da aplicação do teste, pois essas questões dizem respeito à legislação de cada país.

Após isso, será detalhada a metodologia e a aplicação do teste de penetração em termos um pouco mais técnicos e avançados. Nesta fase, serão condensadas informações de diversas normas internacionais a fim de estabelecer módulos. Cada módulo é uma unidade de uma sequência mais abrangente de procedimentos que compõe o *pentest*.

Em seguida, serão relacionadas e descritas as principais ferramentas utilizadas para a execução dos módulos a partir da bibliografia disponível. Por fim, dar-se-á atenção ao tratamento dos resultados obtidos com o teste de penetração e como eles podem se tornar úteis para a melhoria da segurança da informação de uma organização.

2 SEGURANÇA DA INFORMAÇÃO

2.1 Sistemas de Informação

Sistema de informação é o conjunto de pessoas, máquinas e métodos organizados para coletar, processar transmitir e disseminar dados que representem informação de modo a apoiar as funções ou processos de uma organização.

2.2 Segurança da Informação

Segurança da informação é a proteção de informações de um indivíduo ou organização seja em seu armazenamento em diversas mídias ou em seu transito. São características básicas da segurança da informação a confidencialidade, integridade, disponibilidade e autenticidade (ABNT, 2005).

2.3 Ameaça

Ameaça é causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT, 2005, apud ISO/IEC 13335-1:2004).

2.4 Incidentes de Segurança

Segundo o CERT.br (2011), incidentes de segurança são eventos adversos ao sistema computacional ou à rede de computadores. São considerados incidentes as atividades sob suspeita e as confirmadas. Os exemplos mais comuns de incidentes de segurança são:

i. Tentativas de ganhar acesso ilegal ao sistema,
ii. Ataques de negação de serviço e
iii. Modificações ilícitas no sistema alvo.

Esses incidentes podem ser entendidos como a exploração das vulnerabilidades de um sistema com intuito de causar dano ou operar sobre esse sistema de forma ilícita.

2.5 Diferença entre Auditoria de TI e Teste de Penetração

Conforme o documento do NIST (2008), a diferença entre uma auditoria em segurança da informação e um teste de penetração consiste no enfoque do serviço.

As auditorias são voltadas à metodologia e à aplicação das técnicas de segurança da informação, é uma mudança de comportamento da empresa e seus integrantes, examinando a infraestrutura em termos de padronização, eficiência, efetividade e outros aspectos, ou seja, não necessariamente detectam ativamente pontos de vulnerabilidade.

O teste de penetração se aprofunda na parte técnica e sugere mudanças na metodologia e aplicação das medidas de segurança da informação, realizando a análise dos sistemas de informação de uma organização buscando e explorando vulnerabilidades lógicas e físicas.

2.6 Tipos de Invasores

Segundo o FEOIS, existem três tipos básicos de invasores:

i. *Script Kiddies*: antigamente chamados "*lamer's*", são invasores que não tem conhecimento sólido sobre o assunto, fazendo o uso de ferramentas desenvolvidas por terceiros.
ii. *Hackers*: invasores com grande conhecimento sobre o assunto que realizam as invasões com objetivo meramente técnico.
iii. *Crackers*: sua diferença para os hackers é o objetivo das invasões, pois procuram ilegalmente obter lucro, fama ou respeito. Quando um *cracker* possui informações privilegiadas sobre o sistema que está atacando, ele é denominado um *insider* (normalmente, um antigo funcionário insatisfeito com a empresa). Os riscos oferecidos pelo *insider* são maiores devido à sua familiarização com o sistema invadido e com suas falhas.

Pode-se ainda falar em espionagem industrial, onde empresas buscam ganhar vantagem sobre as demais obtendo informações confidenciais por meio de invasões.

2.7 Métodos de Invasão

Os métodos de ataque são divididos em três grandes tipos de acordo com a FEOIS. Primeiramente, existem os ataques baseados na rede, que exploram falhas nos componentes de hardware e de software da rede. O segundo tipo são os ataques de

engenharia social, que procuram agir no usuário do sistema de modo que esse revele informações intencionalmente ou não, incluindo a dissimulação para obter informações privilegiadas ou até mesmo a extorsão. E, finalmente, existem os ataques por fraude dos sistemas físicos de segurança, que se aproveitam da fragilidade da segurança no acesso aos meios físicos do sistema.

3 TESTE DE PENETRAÇÃO

3.1 Introdução

3.1.1 Procedimentos para um Teste de Penetração

O primeiro passo é recolher informações sobre o sistema alvo através de bancos de dados gratuitamente disponíveis que contém informações sobre os blocos de IP associados à determinada organização. Com a lista dos endereços, deve-se escaneá-los em busca de portas abertas, procurando os serviços oferecidos pelo sistema alvo.

Posteriormente, identificam-se os nomes e as versões dos sistemas e dos aplicativos por meio de *fingerprinting*. Com estas informações, pesquisam-se as vulnerabilidades existentes no sistema alvo e, em seguida, explorando estas vulnerabilidades.

A qualidade de um teste de penetração, entretanto, não pode ser descrita apenas nestes procedimentos, dependendo muito mais do quanto é possível se aproximar da realidade do alvo. A criatividade para esta aproximação, reflexo da experiência do realizador do teste, representa um dos elementos cruciais para seu sucesso.

3.1.2 Objetivos de um Teste de Penetração

Os principais objetivos do teste de penetração são: melhorar a segurança do sistema físico, identificar vulnerabilidades, obter uma segurança da informação reconhecida por terceiros (certificações diversas de organismos reguladores da segurança da informação) e melhorar a infraestrutura organizacional e pessoal.

É interessante lembrar que os testes de penetração são limitados, eles não garantem uma segurança total do sistema e nem previnem o mesmo de futuros ataques, porém os testes reduzem significativamente a probabilidade de um ataque bem sucedido. Devido ao constante surgimento de novas ferramentas e descobertas de falhas de segurança, testes de penetração se tornam ultrapassados rapidamente e, desse modo, devem ser modernizados e realizados periodicamente.

Um teste de penetração não substitui outras medidas padrões de segurança da informação, como as auditorias.

3.1.3 Requisitos para um Teste de Penetração

i. Requisitos Organizacionais

Deve-se considerar, antes de realizar um teste de penetração, quem, além do cliente, será afetado direto ou indiretamente, incluindo os sistemas terceirizados. Nesta consideração, inclui-se a total ciência das implicações legais que podem ser originadas.

O horário de realização e a duração dos testes devem ser acertados entre ambas as partes, a fim de reduzir o prejuízo ao sistema. Da mesma maneira, planos para caso de falhas precisam ser estabelecidos previamente.

ii. Requisitos de Pessoal

Os testes devem ser personalizados de acordo com o cliente e, por isso, só devem ser feitos por pessoas com experiência na área de segurança em TI. Para um bom desempenho, os seguintes conhecimentos são necessários: administração de sistemas, sistemas operacionais, TCP/IP e outros protocolos de comunicação, linguagens de programação, produtos de segurança, ferramentas de *hackers* e de varredura de vulnerabilidade, aplicativos do sistema, criatividade dentre outros.

iii. Requisitos Técnicos

Visto que a maioria dos ataques é realizada sobre redes públicas, o sistema alvo deve ter acesso a elas. Outro requisito importante é uma banda elevada o suficiente para suportar o tráfego causado pelas ferramentas de varredura.

Ferramentas de auditoria adequadas devem estar disponíveis, assim como uma rede local para testes.

3.1.4 Questões Éticas

Deve ser especificado até que ponto pode se utilizar a engenharia social. Também deve ser discutido se as vulnerabilidades descobertas precisam ou podem ser exploradas.

As partes envolvidas devem estar de comum acordo, ou seja, qualquer comportamento proativo será considerado um ataque e deve ser rejeitado.

i. Engenharia Social

Existem polêmicas sobre o uso de engenharia social, pois envolvem diretamente os membros da organização que concordam com a realização do teste de penetração. Deste modo, esta técnica deve ser restringida aos casos onde as exigências de segurança são muito altas.

O cliente deve ser sempre informado das possíveis consequências da engenharia social e que a probabilidade de sucesso é maior quando funcionários não são treinados. Os efeitos colaterais que podem ser causados nos funcionários precisam ser explicitados e registrados.

ii. Explorando Vulnerabilidades

Às vezes, apenas a detecção de uma vulnerabilidade é suficiente para a eficiência do teste de penetração. Deste modo, é importante analisar os riscos de se explorar a vulnerabilidade, ou seja, pesar a necessidade da exploração para atingir o objetivo definido para o teste.

3.2 Metodologia do Teste de Penetração

3.2.1 Classificação do Teste de Penetração

A realização de um teste de penetração deve condizer com a realidade da organização alvo e com os resultados esperados. Para tanto, é necessário fazer uma classificação da abordagem adotada para o teste.

Os documentos 800-42 (NIST, 2003) e 800-115 (NIST, 2008) preconizam a divisão em testes quanto à aproximação (dissimulado ou ostensivo), ao ponto inicial (interno ou externo) e ao sobreaviso da equipe de segurança da organização em relação à existência do teste em andamento. Enquanto isso, o OSSTMM considera a relação entre o nível de conhecimento da equipe de teste sobre o sistema alvo e o de sobreaviso da equipe de segurança da organização alvo.

O FEOIS (2003) possui critérios mais detalhados, portanto a sua classificação, unida ao critério de sobreaviso da equipe de segurança, será adotada no presente trabalho. Desta forma, classificar-se-á um teste de penetração de acordo com o seguinte:

1. Conhecimento Inicial: o que se sabe inicialmente sobre o alvo.

    1.1 *Black-box*: as informações são adquiridas por pesquisa própria de quem ataca, ou seja, não possui conhecimento prévio sobre o sistema.
    1.2 *White-box*: possui informações detalhadas sobre algumas partes ou totalidade do sistema.

2. Agressividade: quão agressivo o teste será.

    2.1 Passivo: as vulnerabilidades detectadas não são exploradas.
    2.2 Cauteloso: explora somente as vulnerabilidades onde o sistema testado não sofrerá algum resultado.
    2.3 Calculado: testa vulnerabilidades que podem causar falhas no sistema, porém a possibilidade de sucesso e a seriedade das consequências são analisadas antes.
    2.4 Agressivo: utiliza as potenciais vulnerabilidades em todos os sistemas independentemente das informações a respeito dos mesmos. Devem ser levadas em conta as possíveis consequências nos sistemas relacionados.

3. Escopo: quais sistemas serão testados.

    3.1 Específico.
    3.2 Limitado.
    3.3 Completo.

4. Aproximação: qual a visibilidade, durante o teste, de quem ataca.

    4.1 Dissimulado: apenas métodos que não podem ser identificados como uma tentativa de invasão são utilizados. Devido aos custos associados à discrição do teste, esta abordagem é menos utilizada.
    4.2 Ostensivo: não se preocupa em ser identificado ou não pela equipe de segurança da organização alvo.

5. Sobreaviso da equipe de segurança.

    5.1 *Red Teaming*: a equipe de segurança desconhece que o teste ocorrerá, enquanto um gerente hierarquicamente superior possui conhecimento detalhado sobre o teste a ser realizado. A vantagem deste método é a possibilidade de se testar a resposta da equipe aos incidentes de segurança

percebidos, verificando, inclusive, o conhecimento desta a respeito da política de segurança da organização.

5.2 *Blue Teaming*: o teste é realizado com o consentimento e conhecimento da equipe de segurança da organização alvo.

6. Técnica: quais as técnicas empregadas.

   6.1 Baseado na rede (TCP/IP).
   6.2 Outras redes de comunicação (telefone, Bluetooth, etc.).
   6.3 Ataque presencial: quem ataca tem contato físico com o equipamento atacado.
   6.4 Engenharia Social.

7. Ponto Inicial.

   7.1 Interno: o realizador do teste parte de um ponto interno à rede da organização alvo, portanto possui certo nível de acesso e conhecimento sobre a rede.
   7.2 Externo: neste caso, o realizador do teste parte de um ponto externo à rede da organização alvo, portanto seu acesso inicial é normalmente limitado. No caso dos dois pontos de vista serem escolhidos, o primeiro ponto de partida a ser executado é o interno.

É interessante, para minimizar os riscos ao sistema, combinar diferentes abordagens de ataque. Apesar das inúmeras combinações possíveis, deve haver coerência na escolha dos critérios, por exemplo, não é aconselhável empregar técnicas agressivas em um teste dissimulado.

Um teste de penetração pode trazer efeitos indesejáveis ao sistema, pois alguns de seus procedimentos podem gerar sobrecarga, chegando até a causar um dano permanente. Por esta razão, sua realização deve ser feita com cautela.

3.2.2 Sugestão Para Fases do Teste de Penetração

O teste de penetração é dividido em fases. Esta divisão não ocorre de maneira igual na literatura, porém, apesar destas pequenas diferenças, três fases principais são comuns e serão utilizadas para estabelecer uma sequência de fases para este trabalho. A Figura 3.1 assinala as equivalências entre três dos diversos documentos analisados:

<table>
<tr><th>FEOIS</th><th>NIST</th><th>Empresas do Ramo</th></tr>
<tr><td>Preparação</td><td>Planejamento</td><td>Planejamento e Preparação</td></tr>
<tr><td>Reconhecimento</td><td>Reconhecimento</td><td>Avaliação</td></tr>
<tr><td>Análise de informações</td><td>Ataque</td><td rowspan="3">Documentação e Relatório</td></tr>
<tr><td>Execução</td><td rowspan="2">Documentação</td></tr>
<tr><td>Análise Final</td></tr>
</table>

Figura 3.1 – Equivalência Entre as Fases do Teste de Penetração

Considerando as equivalências acima, sugere-se a seguinte divisão de fases:

- Fase 1 – Planejamento e Preparação – Os testes de penetração têm seu escopo definido em contrato entre o prestador de serviço e o cliente, normalmente, as questões de custo-benefício ditam o escopo, a abrangência e a classificação (conforme Seção 3.2.1). Trata-se do acordo entre cliente e prestador de serviço para definir custos e limites. Deve ser levado em conta todas as responsabilidades legais advindas da realização do teste e todos os riscos para os sistemas do cliente.

- Fase 2 – Reconhecimento e Execução – Nesta fase, o teste é efetivamente aplicado através de uma sequência de módulos, que são conjuntos de procedimentos que definem atividades de reconhecimento e execução (exploração das vulnerabilidades encontradas). Cada módulo normalmente possui pré-requisitos e gera resultados que podem ser empregados nos outros módulos.

- Fase 3 – Conclusões – Trata-se da geração de um relatório final contendo, detalhadamente, vulnerabilidades encontradas, riscos potenciais e recomendações para melhoria. Deve-se utilizar como auxílio toda a documentação gerada nas outras fases do teste.

A documentação deve ser desenvolvida durante as três fases, garantindo que o teste de penetração fique claro e possível de ser executado novamente de maneira idêntica. A Figura 3.2 ilustra a abordagem de cada fase e em paralelo especifica a documentação a ser redigida nas mesmas.

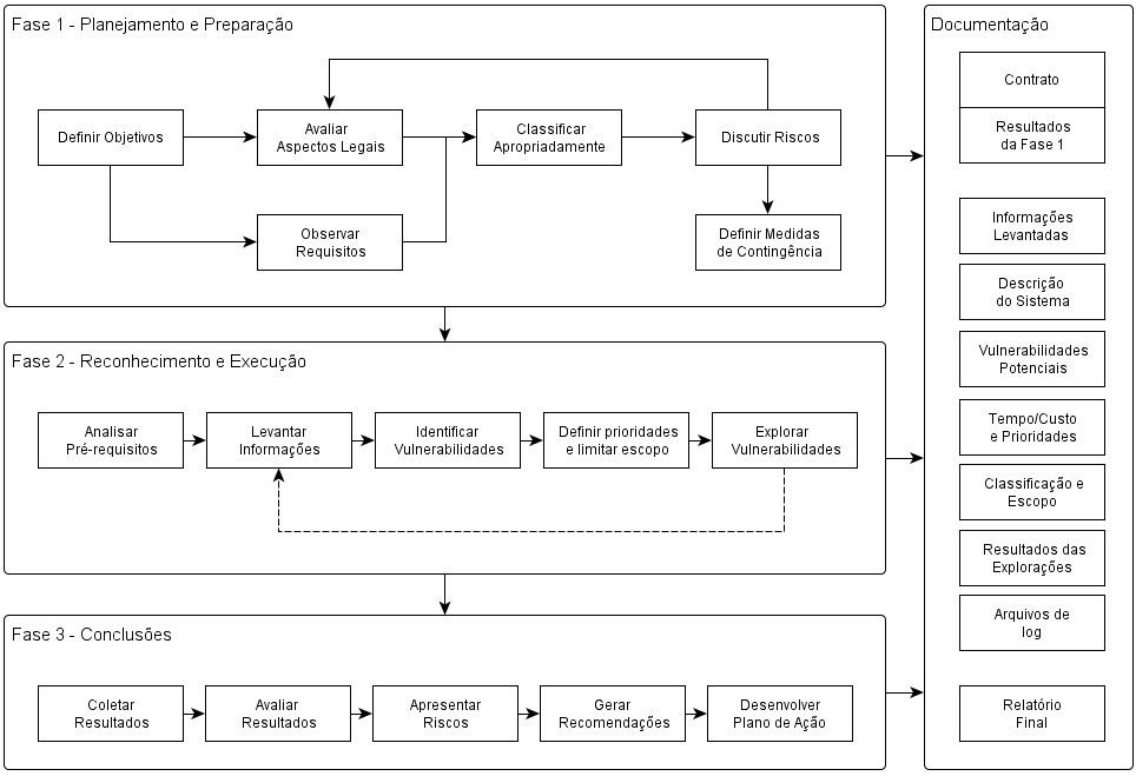

Figura 3.2– Fases do Teste de Penetração e o Processo de Documentação

3.2.3 Módulos Para Teste de Penetração

Segundo o OSSTMM 2.2 (2006), durante a definição da metodologia do teste, é importante não limitar a criatividade do realizador do teste com a introdução de padrões demasiadamente formais e inflexíveis, reduzindo a qualidade do teste de penetração. Assim como é importante deixar as tarefas abertas a algum tipo de interpretação, pois definições exatas fazem a metodologia frágil à evolução tecnológica.

Desta forma, por meio da comparação da bibliografia consultada, pôde-se determinar uma sequência comum de atividades que abordam de forma genérica os procedimentos de um teste de penetração. Para fins de organização, estas atividades são subdivididas em módulos, que, por sua vez, possuem pré-requisitos, objetivos e tarefas. Os módulos não são mutuamente excludentes, podendo alguns possuir trechos em comum.

Os módulos serão descritos posteriormente e são os seguintes:

- Análise de Informações Públicas
- Identificação da Estrutura da Rede
- Varredura de Portas
- Análise e Verificação de Vulnerabilidades

- Teste de Aplicações e Serviços
- Captura e Quebra de Senhas
- Teste de Roteadores
- Teste de Firewall
- Teste de Sistemas Confiáveis (*Trusted Systems*)
- Teste do Sistema de Detecção de Intrusos
- Teste das Medidas de Contingência
- Teste de Negação de Serviço
- Teste do Sistema de Comunicação por Telefonia
- Teste de Dispositivos Sem-fio
- Teste da Segurança Física
- Engenharia Social

3.3 Fases do Teste de Penetração

3.3.1 Fase de Planejamento e Preparação

Esta fase se inicia com o entendimento comum entre cliente e o executor do teste sobre os objetivos do teste de penetração. De acordo com o que foi combinado, os quesitos legais e todos os requisitos são discutidos entres ambas as partes.

Com o auxilio da classificação, o teste apropriado é determinado utilizando os sete critérios vistos na Seção 3.2.1. No caso de ser a primeira vez que se realiza um teste de penetração no sistema, deve-se englobar todas as possibilidades. O tempo levado na execução do teste é um fator importante e deve ser decidido de acordo com as prioridades definidas.

Os riscos para o cliente aumentam de acordo com a abordagem da classificação estabelecida. O cliente e o realizador do teste devem discutir o que pode decorrer dos riscos ao qual o sistema será exposto, traçando medidas de contingência e os responsáveis pelas mesmas.

Havendo a conclusão de que riscos inaceitáveis estão envolvidos na realização do teste, uma classificação diferente deverá ser escolhida, ou alterações devem ser feitas no escopo original. Se for necessário, os aspectos legais e organizacionais são discutidos novamente neste estágio.

Depois de acertado todos esses detalhes, tudo deverá ser registrado em um relatório e assinado por ambas as partes. A extensão do relatório final é acertada nesta fase, sendo grande o suficiente para permitir que o teste seja refeito de maneira idêntica.

A fase de preparação encerra-se com o planejamento detalhado definindo com precisão quando cada componente será penetrado e com que nível de intensidade, além dos equipamentos e recursos necessários para o teste. Medidas de contingência devem ser definidas para os sistemas sensíveis. Os horários de realização do teste devem ser bem definidos para não acarretar ônus aos usuários de um serviço, por exemplo.

Por fim, antes de prosseguir para a próxima fase do teste, deve estar claro como os resultados do teste serão tratados, assim como sua confidencialidade. Normalmente, isso é feito através da assinatura do NDA (*Non-Disclosure Agreement*), ou seja, do Termo de Confidencialidade.

3.3.2 Fase de Avaliação e Execução

Na fase de Avaliação e Execução, serão empregados os módulos. Inicialmente, adquirem-se informações sobre o sistema alvo, analisando-o como um todo, definindo os objetivos a serem atingidos e verificando os riscos da realização do teste no sistema. O tempo desprendido para o teste também deve ser considerado.

Deve-se ainda descobrir as vulnerabilidades do sistema. Com estes dados, pode-se executar as tentativas de ataque ao sistema, determinando, finalmente, se a vulnerabilidades detectadas representam um risco. Durante essa exploração, é normal encontrar novas vulnerabilidades, sendo necessário reavaliar os procedimentos realizados incluindo essas novas variáveis no teste de penetração.

Como a realização de alguns procedimentos do teste de penetração proporciona riscos à organização, devem-se, previamente, analisar as suas possíveis consequências. Toda e qualquer ação tomada pelo realizador do teste deve estar prevista ou amparada pelo contrato.

A documentação desta fase deve conter as informações previstas como resultado de cada módulo. Devem também ser armazenados detalhes suficientes para a reconstituição do teste pelo cliente em outra oportunidade. Isso inclui os registros obtidos com o uso das ferramentas, gerando uma garantia de que as operações feitas pelo realizador do teste não ultrapassam as determinações estabelecidas no contrato.

3.3.3 Fase de Conclusões

A fase de conclusões trata da transformação dos resultados parciais do teste de penetração em informação útil de inteligência e segurança. A interpretação e análise dos

dados obtidos e documentados nos diversos módulos irão determinar a origem, as causas e as possíveis soluções das vulnerabilidades descobertas.

Em termos práticos, a fase de conclusões resume-se a reunir toda a equipe que aplicou o teste para realizar um estudo sobre as vulnerabilidades descobertas. Após esse estudo, é gerado o relatório final abordando os resultados encontrados. Esse texto é produzido de modo que os funcionários de gerência da organização alvo, não necessariamente da área de TI, consigam entender os problemas de seu sistema. As informações contidas no relatório final serão tratadas na seção de documentação (Seção 5).

A documentação parcial obtida nos módulos também é entregue ao cliente sob a forma de um anexo ao relatório final ou de um documento separado chamado relatório técnico. A documentação técnica deve conter todas as informações sobre o teste de forma que a equipe de TI da organização alvo consiga reconstituir os resultados obtidos. Os resultados inconclusivos não devem ser omitidos dos relatórios técnicos e da análise final, pois é importante que esse tipo de resultado seja registrado para futuros estudos.

Os relatórios parciais devem ser feitos pela equipe que aplicou o módulo em questão, sob o risco de redução do detalhamento desejado se delegada essa atribuição a terceiros. O relatório final deve ser elaborado a partir dos relatórios parciais e do estudo do cenário completo das vulnerabilidades. A equipe que irá redigir esse documento deve ser experiente e ocupar cargos de supervisão, de forma que possam melhor acompanhar a realização da maioria dos módulos.

3.4 Descrição dos Módulos

3.4.1 Análise de Informações Públicas

i. Descrição

Antes de qualquer etapa é fundamental que se levantem informações preliminares sobre a organização a ser testada. Elas visam dar uma ideia inicial da forma e conteúdo do sistema a ser testado, das informações divulgadas oficialmente pela organização bem como meios de comunicações diversos e outras fontes não oficiais.

Esse levantamento se dá pelo agrupamento do maior número de informações possíveis. A estrutura física da organização, estrutura funcional, o esquema logístico, esquema de comunicações, histórico em noticiários e outros portais de comunicação com o público, interface com os usuários estão entre os principais alvos. Toda e qualquer informação sobre o alvo deve ser levantada para posterior análise.

As ferramentas utilizadas para esse módulo são as mais diversas possíveis e variam com a criatividade do técnico que irá testar o sistema, normalmente são usados sites de pesquisa, sites da organização-alvo, sites das organizações associadas, sites de listas telefônicas, sites de redes sociais, sites noticiários, blogs e outros.

ii. Objetivos

Os objetivos desse módulo são:

- Perfil da organização.
- Quadro organizacional de funcionários.
- Organizações parceiras.
- Tamanho e escopo da presença do alvo na internet.
- Listagem endereços de funcionários, inclusive e-mail.
- Listagem das disparidades entre políticas de segurança divulgadas e praticadas.
- Pesquisa sobre o sistema utilizado e tecnologia de segurança.

iii. Pré-requisitos

O único pré-requisito para esse módulo é que a fase de planejamento e preparação do teste esteja terminada, ou seja, devem estar estabelecidos o escopo do teste e o amparo legal.

iv. Tarefas

- Levantamento de informações no(s) site(s) da organização como, por exemplo, tipo de banco de dados, informação coletada pela empresa, tipo de *cookie*, tempo de expiração do *cookie*, entre outras.
- Pesquisa em bancos de informações públicos.
- Pesquisa de informações em noticiários.
- Levantamento de informações de pessoal.
- Listagem de e-mails funcionais.
- Pesquisa de organizações parceiras na área de TI bem como de profissionais da área contratados ou demitidos.
- Verificação de ferramentas e procedimentos adotados na interação com o usuário.
- Verificar material de TI vendido pela organização, principalmente dispositivos de armazenamento de informações.

v. Considerações

É importante enfatizar que esse módulo tem um caráter eminentemente passivo, ou seja, não é necessário nem desejável que a organização alvo identifique que informações estão sendo levantadas. O levantamento ostensivo de informações se dará nos módulos seguintes conforme a necessidade do teste e conforme o prescrito em contrato.

A maioria dos resultados desse módulo visa utilizar direta ou indiretamente de informações levantadas em módulos posteriores. Trata-se de um reconhecimento das atividades da organização bem como seus profissionais em uma tentativa de definir qual o nível de segurança e importância do sistema de informações da organização.

Este módulo deve ser realizado em paralelo com a etapa de levantamento de informações do módulo de Teste de Segurança Física, pois muitas informações podem ser obtidas através de uma visita à organização e com as tarefas descritas naquele módulo.

3.4.2 Identificação da Estrutura da Rede

i. Descrição

A identificação da estrutura de uma rede utiliza uma grande variedade de métodos ativos e passivos para descobrir servidores ativos em uma rede e como ela opera. A identificação passiva é feita sem realizar o envio um pacote sequer através da monitoração do tráfego da rede a partir de um ponto interno. Desta maneira, esta abordagem consome muito mais tempo que uma abordagem ativa, correndo o risco ainda de não detectar servidores que não enviem ou recebam tráfego durante o período de monitoramento.

A identificação ativa envia, através normalmente de uma ferramenta, vários tipos de pacotes para a rede numa tentativa de solicitar resposta dos servidores. Estas ferramentas de descoberta de rede obtêm as informações de diversas maneiras por meio de varreduras. Desta maneira, como as organizações comumente possuem firewalls e sistemas de detecção de intrusos (IDS - *Intrusion Detection System*), é essencial que não se escolham métodos de varredura suspeitos (como o SYN/FIN e NULL *scan*) que podem despertar a atenção dos administradores do sistema alvo. Isto conduz à escolha de varreduras menos agressivas como, por exemplo, em velocidades menores e originadas de uma maior variedade de endereços IP. Além destas preocupações, alguns tipos de varreduras podem causar falhas em sistemas antigos ou cuja segurança é fraca, devendo este risco ser levado em conta.

Apesar da redução do tempo necessário e da possibilidade de ser executada de um ponto externo à rede, a identificação ativa pode causar latência na rede devido à sua interferência no tráfego normal.

As redes sem-fio existentes também devem ser analisadas. Sua grande facilidade de instalação e a inobservância de aspectos relacionados à segurança abrem margens para torná-las portas de entrada para outras redes mais importantes.

Neste módulo, nenhuma invasão está sendo realizada diretamente nos sistemas alvos senão nos domínios considerados semi-públicos, ou seja, acessíveis a qualquer um, mas com possibilidade de controle de acesso ou monitoramento.

ii. Objetivos

Os objetivos deste módulo são:

- Nomes de domínios.
- Faixas de endereçamento IP.
- Nome dos servidores.
- Endereços IP.
- Descrição das funções do servidor.
- Informação sobre o ISP / ASP.
- Endereços IP dos roteadores.
- Funções dos roteadores na rede.
- Sistema operacional, fabricante e modelo do roteador.
- Acesso das redes sem-fio disponíveis.
- Mapa da rede.
- Donos dos sistemas e dos serviços.
- Possíveis limitações do teste.

iii. Pré-requisitos

Para a execução deste módulo, fazem-se necessários os endereços IP dos sistemas alvo, a faixa de endereços IP ou os nomes dos domínios/servidores. A descoberta das informações sobre os roteadores podem ser obtidas com o auxílio de informações descobertas durante a realização deste e do próximo (Varredura de Portas) módulos.

iv. Tarefas

- Realizar buscas em bases de dados públicas.
- Solicitar aos servidores os clientes e subdomínios.
- Realizar buscas dos nomes dos servidores.
- Realizar uma varredura na faixa de endereços IP através de *pings*, em endereços IP vizinhos e em nomes comuns dos servidores.
- Traçar múltiplas rotas para o *gateway* para descobrir a parte externa da rede e os roteadores.
- Analisar os pacotes IP roteados.
- Explorar as vulnerabilidades das redes sem-fio detectadas.
- Tentar obter acesso às redes sem-fio.
- Tentar acessar dados das redes sem-fio.
- Examinar informações em cabeçalhos de e-mail.
- Verificar o código HTML das páginas atrás de *links* externos ou comentários.
- Verificar grupos de notícias atrás de postagens dos empregados da

organização alvo, assim como a ocorrência de ataques anteriores.

- Extrair informações sobre o ambiente de TI da organização alvo através das vagas de empregos oferecidas por ela.
- Realizar buscas em serviços *Peer to peer* (P2P) por conexões na rede alvo e por dados sobre a organização alvo.

v. Considerações

Sob o ponto de vista legal, antes de qualquer tentativa de identificar a estrutura da rede, é recomendável definir contratualmente exatamente quais sistemas devem ser testados. Isso objetiva encontrar o número de sistemas alcançáveis a serem testados sem causar a infração da lei com o teste de outros sistemas. De acordo com as necessidades do cliente, pode-se, então, ser fornecida uma lista dos endereços IP que podem ser testados.

A identificação pode ser prejudicada por segmentos protegidos da rede e por técnicas e dispositivos de segurança de perímetro como, por exemplo, um ambiente que utiliza NAT (*Network Address Translation*) não revela seus endereços IP internos, traduzindo-os sempre, ao sair da rede, em endereços públicos dedicados ao tráfego externo. Além disto, informações erradas podem ser geradas devido ao tráfego ter sido estimulado pela ferramenta de varredura.

De modo geral, as informações obtidas pelos dois tipos abordagem raramente são completamente precisas, sendo necessário realizar varreduras periodicamente para obter resultados mais precisos. Deve-se valer ainda da opinião de um realizador experiente de testes de penetração baseada na análise das informações obtidas.

Deve-se manter em mente que, quase sempre, mais servidores serão descobertos durante o teste de penetração, havendo necessidade de testá-los do mesmo modo que os descobertos inicialmente.

3.4.3 Varredura de Portas

i. Descrição

A varredura de portas é uma sondagem das portas e seus protocolos da camada de redes e da camada de transportes. O modelo TCP/IP possui 65.536 portas, através das quais diversas aplicações estabelecem conexões fim-a-fim para comunicação. Existem diversas portas com funções pré-estabelecidas, no entanto o sistema quase nunca escuta todas as portas.

A varredura de portas é um importante passo na identificação de vulnerabilidades do sistema. As portas utilizadas sugerem informações sobre o sistema operacional utilizado bem como aplicações e protocolos de comunicação. Além disso, as portas abertas podem fornecer informações adicionais sobre a estrutura da rede

devido a características dos próprios protocolos.

ii. Objetivos

Os objetivos desse módulo são:

- Identificação das portas abertas, fechadas e as com filtro.
- Informações sobre os serviços oferecidos pelo dispositivo alvo.
- Identificação de protocolos de tunelamento, encapsulamento e roteamento disponíveis na rede.
- Obter informações sobre o sistema operacional.
- Complementar o módulo de identificação da estrutura da rede identificando endereços de IP e endereços da rede interna.

iii. Pré-requisitos

Para a execução desse teste é necessário que o módulo de identificação da estrutura da rede obtenha resultados expressivos. São necessários endereços IP de o maior número possível de máquinas envolvidas no sistema.

iv. Tarefas

- Examinar os pacotes IP em busca de informações sobre protocolos utilizados.
- Medir o tempo de retorno de pacotes.
- Medir a taxa de aceitação e resposta de pacotes.
- Medir quantidade de pacotes perdidos e de negação de conexões.
- Coletar transmissões em *broadcast* da rede.
- Testar o *firewall* com pacotes TTLs (*Time-To-Live*) para todos os endereços IP.
- Fazer a varredura de portas utilizando ferramentas próprias, identificando as abertas, fechadas e filtradas.
- Tentar fazer conexões DNS com todos os servidores.

v. Considerações

O módulo de varredura de portas não possui muitas tarefas, pois, em sua maioria, os testes são feitos através de softwares que se baseiam em detalhes sobre sistemas operacionais e protocolos de comunicação. Como esses fatores são sujeitos a atualizações e evoluções não é interessante descrever quais portas devem ser testadas e através de qual protocolo.

Devido à variedade de ferramentas disponíveis e a constante evolução de sistemas operacionais, *firewalls* e protocolos de comunicação, a equipe de teste tem papel chave na aplicação deste módulo. É importante que os membros da equipe

estejam atualizados e cientes de todas as mudanças nos fatores que influenciam a varredura de portas, pois muitas vezes é a experiência e criatividade da equipe irá detectar possíveis vulnerabilidades no sistema.

A varredura de portas geralmente utiliza diversos pacotes IP modificados para obter respostas do sistema alvo. A utilização destes pacotes pode ser confundida com um ataque de negação de serviço, por isso é interessante que a varredura de portas seja conduzida em horários de baixo tráfego na rede.

A utilização de ferramentas mais agressivas em ambiente interno à rede não gera melhorias significativas à qualidade do teste se comparadas ao risco de danos ao sistema.

O módulo de varredura de portas é um complemento ao módulo de Identificação da estrutura de redes. O resultado de ambos combinados será usado posteriormente em quase todos os módulos.

3.4.4 Análise e Verificação de Vulnerabilidades

i. Descrição

Indo além da interpretação humana das informações sobre os servidores e seus atributos, a análise e verificação de vulnerabilidades, que pode utilizar como entrada para reduzir seu esforço as informações obtidas nos módulos anteriores, realiza a identificação e verificação de *softwares* desatualizados, correções não instaladas, debilidades do sistema, falhas de configuração e cumprimento ou não da política de segurança de uma organização.

Os padrões de ataque enviados por uma ferramenta de varredura de vulnerabilidades geram, em um sistema, comportamentos específicos e saídas. Estas respostas do sistema alvo são comparadas com informações de bases de dados na tentativa de caracterizar assinaturas de vulnerabilidades conhecidas. Além deste mecanismo baseado na assinatura do sistema, algumas ferramentas tentam simular padrões de ataque para testar outras falhas. Deve-se manter em mente que esta base de dados deve estar sempre atualizada para uma melhor eficiência do teste de penetração, além de que outros meios de informação, como IRC, grupos de notícias e sites FTP do submundo, devem ser consultados.

Apesar de ser uma maneira rápida de quantificar a exposição de uma organização a vulnerabilidades de superfície, ou seja, falhas que ocorrem isoladamente independentes de outras, uma ferramenta varredura de vulnerabilidades é incapaz de detectar falhas mais graves resultantes das inúmeras combinações entre pequenas vulnerabilidades. Deste modo, a criatividade e a experiência do realizador do teste de penetração se tornam fundamental para a obtenção de resultados corretos.

Quando as credenciais necessárias para realizar uma varredura de vulnerabilidades nos servidores não são conhecidas, esta varredura se limita a descobrir

vulnerabilidades relacionadas à estrutura da rede e às portas abertas. Uma varredura partindo de um ponto interno normalmente revela mais vulnerabilidades do que uma que se origina externamente, porém, como dispositivos de segurança do perímetro influenciam no que consegue trafegar de fora para dentro da rede e vice-versa, os dois pontos de vista são importantes.

Uma varredura partindo de um ponto interno, por utilizar acesso local e uma conta com privilégios elevados, detecta vulnerabilidades (exploráveis tanto localmente como pela rede) com um maior nível de detalhamento. Quando se parte de um ponto externo, a varredura enfrenta uma série de limitações. Uma delas é o fato se restringir aos sistemas ativos, encobrindo vulnerabilidades de superfície e sendo incapazes de estimar o nível de risco real em uma rede. Ainda se pode falar em uma elevada taxa de falsos-positivos que devem ser submetidos a uma análise manual mais crítica. Como ocorre no módulo de Identificação da Rede, o uso da rede para a descoberta e verificação de vulnerabilidades causa um excesso de tráfego, podendo ocasionar latência, detecção da varredura ou, até mesmo, a falha de sistemas mais frágeis.

A política de segurança da organização alvo delineia procedimentos a serem seguidos pelos seus membros a fim de evitar maiores riscos à segurança dos sistemas. Desta maneira, em posse desse documento, o realizador do teste possui mais um ponto de partida para busca de vulnerabilidades do sistema. Esta busca pode se iniciar pela observação tanto do descumprimento dessa política pelos membros da organização como das determinações delineadas na mesma.

ii. Objetivos

Os objetivos deste módulo são:

- Lista de potenciais vulnerabilidades.
- Lista das vulnerabilidades confirmadas.
- Lista de vulnerabilidades que não conseguiram ser testadas.
- Listas das possíveis vulnerabilidades de negação de serviço.
- Lista dos níveis de correção do sistema e das aplicações.
- Listas de DMZ.
- Lista de áreas protegidas por acesso obscuro ou visível.
- Mapa da rede

iii. Pré-requisitos

Na fase de verificação das vulnerabilidades, faz-se necessário ter conhecimento profundo sobre portas abertas, serviços oferecidos, aplicações e sistemas operacionais utilizados. A lista das potenciais vulnerabilidades geradas neste primeiro momento servirá como base para a fase de verificação.

iv. Tarefas

- Incluir as ferramentas populares de varredura nos testes.
- Avaliar a organização alvo com as ferramentas populares de varredura.
- Determinar vulnerabilidades pelo sistema e pelo tipo de aplicação.
- Determinar as vulnerabilidades dos serviços.
- Determinar o tipo de aplicação e o serviço pela vulnerabilidade.
- Realizar testes redundantes com pelo menos duas ferramentas de varredura.
- Identificar todas as vulnerabilidades de acordo com: aplicações e sistemas operacionais.
- Identificar todas as vulnerabilidades de sistemas similares que possam afetar os sistemas alvo.
- Verificar a existências de falso-positivos e falso-negativos em todas as vulnerabilidades encontradas durante a fase de identificação.
- Verificar, respeitando as limitações contratuais, todas as vulnerabilidades reais.
- Revisar a política de segurança da organização alvo.

v. Considerações

As dificuldades encontradas pelo realizador do teste no módulo de Identificação da Estrutura da Rede também são aplicáveis a uma varredura de vulnerabilidades que parte de um ponto externo à rede. Deste modo, pode ser solicitado ao administrador da rede que forneça condições de acesso externo da rede que garantam a eficiência do teste de penetração.

Pelo fato das ferramentas de varredura de vulnerabilidades possuírem soluções comumente proprietárias, a comparação entre resultados obtidos por diversas ferramentas se torna subjetivo. Além disto, os níveis de risco considerados por uma ferramenta pode não refletir o risco real para uma organização. Desta maneira, mais uma vez a criatividade e a experiência do realizador do teste são fundamentais.

A escolha da profundidade avaliada por uma ferramenta de varredura de vulnerabilidades é uma tarefa do realizador do teste. Um nível mais abrangente pode detectar um maior número de vulnerabilidades com um custo associado de duração mais elevado, enquanto um teste mais simples consumiria menos tempo abrangendo somente vulnerabilidades mais comuns.

A análise de vulnerabilidades é uma atividade que consome muito esforço de uma equipe que realiza um teste de penetração, exigindo grande envolvimento dos integrantes para interpretar os resultados corretamente. Outro ponto importante desta atividade é que ela não se encerra após ser executada, visto que a descoberta de vulnerabilidades é um processo iterativo que pode evoluir durante a realização de outras etapas do teste de penetração.

3.4.5 Teste de Aplicações e Serviços

i. Descrição

Esse módulo visa identificar e testar as aplicações e serviços oferecidos pelo sistema da organização alvo. As plataformas sobre as quais os sistemas se baseiam podem conter vulnerabilidades e erros conhecidos, por isso é essencial que se identifiquem quais as aplicações envolvidas no sistema, qual a plataforma provê suporte e quais interfaces o sistema possui com outras aplicações.

Em certos casos, mais de uma aplicação coexiste por trás do serviço prestado pelo sistema. Geralmente uma aplicação é a interface enquanto as outras são componentes do sistema como um todo que lhe dão suporte.

Nesse cenário o sistema operacional (SO) sobre o qual o sistema alvo está depositado também pode ser encarado como um componente que oferece suporte à aplicação. A identificação de um sistema operacional é conhecida como *fingerprinting*, ou seja, uma investigação de indícios que indiquem qual SO está sendo utilizado.

Após a identificação das aplicações e serviços alvos, o módulo busca listar, identificar e explorar suas vulnerabilidades.

ii. Objetivos

Os objetivos desse módulo são:

- Lista de aplicações do sistema.
- Identificar componentes da aplicação.
- Identificação do Sistema Operacional.
- Identificar o nível de *patch* das aplicações, serviços e sistema operacional.
- Identificar interfaces entre aplicações.
- Complementar o mapa da estrutura da rede.
- Lista e descrição de vulnerabilidades das aplicações.

iii. Pré-requisitos

Para esse módulo são necessários os resultados dos módulos de análise das informações públicas, identificação da estrutura de rede e da varredura de portas.

iv. Tarefas

- Combinar os resultados da varredura de portas com os protocolos utilizados na porta a fim de obter informações sobre o serviço ou aplicação envolvida.
- Examinar respostas do sistema pra identificar aplicações e o sistema operacional.

- Usar o *fingerprinting* e informações de anúncios para determinar aplicações e o sistema operacional.
- Identificar o nível de atualização das aplicações e do sistema operacional.
- Enviar requisições UDP e Cavalos de Tróia para o sistema a fim de analisar suas repostas.
- Analisar o resultado do módulo de analise de informações públicas em busca de ofertas de emprego e contratações de especialistas em determinados sistemas, aplicações e servidores a fim de identificá-los.
- Analisar os redirecionamentos ou remapeamentos do sistema a fim de localizar os provedores das aplicações e serviços.
- Decompor códigos binários, se acessíveis.
- Determinar o protocolo de comunicação cliente/servidor.
- Recompor a lógica da aplicação através de suas funcionalidades e mensagens de erro.
- Analisar as saídas da aplicação em busca de informações.
- Verificar informações contidas em comentários nos códigos fonte disponíveis.
- Aplicar algoritmos de força bruta para descobrimento de senhas em pontos de acesso às aplicações.
- Utilizar nome de usuário ou credencial válidos, normalmente obtidos em outros módulos como análise de informações públicas, quebra de senhas ou engenharia social.
- Utilizar *tokens* spoofados para tentar autenticação.
- Utilizar métodos diversos para obter acesso como entendimento da lógica de manutenção da autenticação.
- Identificar dados de gerenciamento de sessões.
- Identificar limitações da aplicação quanto à utilização de banda.
- Identificar codificação URL das aplicações se houver.
- Realizar ataques como sequestro de sessão e *Man-in-the-middle* nas aplicações para obter mais informações.
- Uma vez em posição de vantagem, enviar informações falsas para enganar a aplicação.
- Encontrar limitações nas variáveis e protocolos das aplicações tais como: *payload* do protocolo, tipo das variáveis, formato de construção e outros.
- Tentar causar *buffer overflow* excedendo as limitações encontradas.
- Injetar comandos de diversos tipos nos *inputs* da aplicação, por exemplo: comandos JavaScript, SQL, PERL e outros.
- Tentar obter acesso ao sistema de arquivos através dos *inputs* da aplicação.
- Executar comandos através do *Server Side Include* (SSI).
- Manipular a sessão ou *cookies* persistentes para enganar a lógica da aplicação no lado do servidor.
- Manipular variáveis HTML para tentar modificar a lógica e/ou enganar o

lado do servidor.

v. Considerações

O módulo de teste de aplicações é um dos principais na determinação do grau de segurança do sistema. Diversas tarefas descritas acima verificam a resistência a ataques das aplicações e serviços oferecidos pelo sistema. Normalmente procuram-se falhas de configuração ou erros que possam gerar vulnerabilidades a serem exploradas.

A execução desse módulo representa grandes riscos ao sistema e por isso deve ser aplicado por uma equipe experiente e dentro dos parâmetros estabelecidos em contrato. Todo o sistema pode parar de funcionar ao explorar uma vulnerabilidade apresentada na aplicação, bancos de dados e sistemas de arquivos podem ser alterados, informações confidenciais podem ser descobertas, por isso é importante manter os registros de todas as atividades como forma de garantir a legitimidade da aplicação do teste.

A criatividade é fundamental no decorrer deste teste, pois a aplicação geralmente é especifica para cada organização, ou seja, a execução do módulo pode variar drasticamente de uma organização para outra.

3.4.6 Captura e Quebra de Senhas

i. Descrição

A captura e quebra de senhas é o processo de obter senhas, comumente, a partir da obtenção de suas *hashes*. Este processo é muito empregado para identificar contas com senhas fracas. Normalmente, por questões de segurança, a senha que um usuário insere em um sistema não é utilizada diretamente para a autenticação, ou seja, uma *hash* dela é gerada e comparada com a *hash* armazenada que representa a senha do usuário. Quando as duas *hashes*, a gerada e a armazenada, correspondem, o usuário está autenticado. Ferramentas de monitoramento de tráfego da rede permitem a captura de pacotes que contém as *hashes*, assim como é possível obtê-las através do acesso ao sistema alvo (seja fisicamente ou com as credenciais necessárias). Uma vez capturadas, utilizam-se ferramentas de quebra de senha para gerar *hashes* até encontrar uma correspondente a *hash* capturada.

Uma senha pode ser quebrada através da exploração de fraquezas ou de falhas de implementação de um algoritmo de criptografia. A escolha de senhas fracas pelos usuários ou até o uso da mesma senha para vários sistemas diminuem a segurança da organização alvo.

Uma maneira para quebrar senhas é com o uso de dicionários, que são extensos arquivos de texto, em um ou mais idiomas, abrangendo desde palavras de um dicionário comum a nomes de celebridades ou marcas famosas. Uma ferramenta utiliza cada

palavra destes dicionários para gerar *hashes* e compará-las com a *hash* capturada. Como um aprimoramento do emprego de dicionários, o ataque híbrido adiciona caracteres especiais ou substitui algumas letras das palavras do dicionário.

A força-bruta também é uma alternativa para a quebra de senhas, comparando a *hash* capturada com as *hashes* geradas a partir de todas as combinações possíveis de caracteres até um determinado tamanho. Em tese, a força-bruta consegue quebrar qualquer senha, entretanto o tempo demandado para isso e a capacidade de processamento envolvida podem não ser condizentes com a realidade do teste de penetração sendo realizado. Apesar da possibilidade de consumir muito tempo, quebrar uma senha com o uso da força-bruta leva bem menos tempo que o recomendado pela maioria das políticas de segurança para a troca de senha.

Outra maneira de quebrar senhas é com o uso de *rainbow tables*, que são tabelas de pesquisa com *hashes* já pré-computadas. Por definição, uma função de *hashing* (responsável por gerar os *hashes*) leva valores de um conjunto muito grande (por exemplo, as palavras de um dicionário) em um conjunto menor composto pelas *hashes*, então o uso dessas *rainbow tables* diminuiria o esforço demandando para quebrar uma senha. De toda forma, além de levarem um grande tempo para serem geradas, essas tabelas podem se tornar ineficazes ou muito grandes contra uma técnica chamada *salting*. Esta técnica insere pedaços aleatórios de informações no processo de *hashing*, diminuindo a probabilidade de senhas idênticas retornarem a mesma *hash*.

A quebra de senhas realizada *off-line* produz quase nenhum impacto no sistema ou rede alvo. Pode-se, assim, validar a política de segurança para senhas da organização alvo além de verificar se a mesma está sendo seguida.

ii. Objetivos

O objetivo deste módulo é:

- Obter as *hashes* das senhas.
- Quebrar arquivos de senhas.
- Obter senhas em claro e seus respectivos usuários.
- Lista de sistemas e arquivos vulneráveis à quebra de senhas.

iii. Pré-requisitos

A fim de realizar a captura das senhas, precisa-se ter o devido acesso ao sistema alvo para instalar as ferramentas de captura ou para acessar os registros onde estão armazenadas as senhas ou *hashes*. Este acesso é normalmente obtido no módulo de Análise e Verificação de Vulnerabilidades. Para a quebra, é necessário uma lista das *hashes* capturadas ou o acesso ao sistema para realizar testes *online*.

iv. Tarefas

- Obter o devido acesso ao sistema alvo e instalar ferramentas de captura no

mesmo.

- Gravar e analisar tráfego da rede em busca de *hashes* ou senhas transmitidas.
- Verificar as *hashes* obtidas com a ferramenta adequada.
- Realizar a quebra das senhas e usuários contidos em arquivos.
- Realizar testes *online* caso não se tenha obtido nenhuma *hash*.
- Testar manualmente senhas padrões ou frequentes.

v. Considerações

Deve-se manter em mente que a instalação de ferramentas nos sistemas alvos pode causar reduções no desempenho dos mesmos, além da possibilidade de permitir o acesso de terceiros não-autorizados. Não se pode esquecer que um sistema pode acionar algum mecanismo de segurança após uma determinada quantidade de tentativas sem sucesso de se autenticar.

Como em todos os outros módulos, não se pode ultrapassar os limites legais definidos em contrato, observando sempre se alguma ação do realizador do teste foge do escopo delimitado pela a organização alvo.

3.4.7 Teste de Roteadores

i. Descrição

A organização alvo do teste pode utilizar em sua rede roteadores capazes de filtrar o tráfego externo e interno e criar um ambiente seguro na rede interna, conhecido na literatura por zona desmilitarizada (DMZ). Esses roteadores filtram a informação de acordo com as políticas de segurança da organização e as ACL's (*Access Control Lists*). O teste de roteadores busca assegurar que somente pacotes autorizados entrem ou saiam da DMZ da organização alvo.

É importante que se determine o papel dos roteadores na segurança da rede, a evolução tecnológica faz com esses equipamentos fiquem mais complexos e com novas funcionalidades desconhecidas para a equipe de teste e para a própria organização alvo. Erros de configuração ou a ignorância das funcionalidades desses equipamentos podem gerar vulnerabilidades que podem ser exploradas pela equipe de testes.

ii. Objetivos

Os objetivos desse módulo são:

- Identificar os endereços IP dos roteadores.
- Identificar o sistema de operação e fabricante dos roteadores.
- Identificar os roteadores e as funcionalidades implementadas.
- Identificar a política de segurança pelas ACL's.

- Listar os tipos de pacotes que podem entrar na rede.
- Mapear as repostas do roteador a diversos tipos de trafego.
- Complementar informações sobre a estrutura da rede identificando sistemas ativos.

iii. Pré-Requisitos

Para esse módulo é necessário um conhecimento inicial sobre a estrutura da rede e os resultados da varredura de portas.

iv. Tarefas

- Verificar rotas dos pacotes usando o comando *trace route*.
- Analisar os pacotes IP roteados.
- Verificar o tipo de roteador com informações coletadas durante os módulos anteriores.
- Verificar se o roteador está oferecendo tradução de endereços de rede (NAT).
- Verificar a entrada de pacotes com valores TTL (*Time-To-Live)* estrategicamente determinados feito no módulo de varredura de portas.
- Testar as ACL's e compará-las com os documentos de política de segurança e a regra *"Deny All"* presente nos roteadores.
- Verificar se o roteador está filtrando pacotes oriundos da rede local.
- Verificar se o roteador está detectando *spoof* de endereços.
- Verificar a penetração do *inverse scanning*.
- Verificar a saída de pacotes do roteador.
- Verificar a capacidade do roteador de lidar com pacotes muito pequenos, muito grandes e *overlapping fragments*.
- Tentar obter acesso às configurações do roteador utilizando senhas comuns e ataques de força bruta.

v. Considerações

Os roteadores são responsáveis pelo direcionamento de pacotes dentro de uma rede, toda a informação que entra e sai passa por algum roteador. Um ataque a esses dispositivos pode comprometer todo o funcionamento de um sistema, por isso é essencial que se tenha conhecimento de quais dispositivos integram a rede e quais são suas funcionalidades e vulnerabilidades.

O teste de roteadores tem como principais finalidades: detectar erros de configuração dos dispositivos e obter informações sobre as ACL's. Os roteadores também oferecem vulnerabilidade ao serem atacados através de tentativa de acesso ilegal às suas configurações através do protocolo HTTP. Ao obter acesso ao roteador, é possível obter as ACL's e ainda alterar as configurações do roteador para permitir um

ataque à rede.

O teste de roteadores deve ser executado com cuidado, pois ao alterar as configurações do dispositivo o tráfego da rede pode ficar comprometido. Organizações que utilizam a rede para realizar transações com clientes são mais sensíveis a esse tipo de alteração.

3.4.8 Teste de Firewall

i. Descrição

Um *firewall* controla o fluxo do tráfego entre a rede de uma organização, a DMZ e a internet, operando através de uma política de segurança e utilizando ACL's. Ele funciona como uma barreira de proteção que controla o tráfego de dados que entra e sai da rede, podendo ser implementado em *hardware* e/ou *software*.

Com este módulo, espera-se que o realizador do teste consiga entender, além de dados referentes ao tipo e ao modelo, a configuração do *firewall* e o mapeamento que ele desempenha entre os servidores e os serviços por trás dele. O realizador do teste tenta contornar o firewall criando uma conexão entre um ponto externo e um segmento protegido da rede.

Deve-se testar o *firewall* nos dois sentidos, ou seja, uma ferramenta localizada externamente envia pacotes para outra ferramenta localizada no interior da rede, que analisa os pacotes que conseguem chegar, e vice-versa.

ii. Objetivos

Os objetivos deste módulo são:

- Obter endereços IP e nomes DNS das componentes do *firewall*¸ incluindo componentes da configuração (roteadores internos e externos).
- Descobrir os sistemas operacionais do *firewall.*
- Modelo e nível de *patch* do *software* do *firewall.*
- Listar as regras do *firewall* que podem ser deduzidas externamente.
- Verificar as vulnerabilidades detectadas do *firewall.*
- Listar, com o máximo esforço possível, os sistemas por trás do *firewall* que podem ser alcançados.
- Listar as regras do *firewall.*
- Obter informações dos recursos implementados no *firewall.*
- Delinear a política de segurança através das ACL's.
- Listar os tipos de pacotes que conseguem entrar na rede.
- Listar os tipos de protocolos que possuem acesso dentro da rede e que conseguem acessar a rede.
- Lista de caminhos não-monitorados dentro da rede.

iii. Pré-requisitos

Para que o *firewall* seja identificado, deve-se conhecer: a estrutura da rede e os resultados da varredura de portas. O acesso da rede através um ponto atrás do *firewall* e outras informações sobre componentes utilizadas por ele são pré-requisitos da execução propriamente dita do teste, que envolve o teste do *firewall* partindo tanto de um ponto interno como de um externo.

iv. Tarefas

- Realizar um *banner lookup* das componentes do *firewall.*
- Realizar uma varredura de portas diretamente no *firewall*.
- Traçar rotas com a ferramenta adequada.
- Identificar as regras do *firewall* utilizando ferramentas adequadas (*firewalking*).
- Tentar alcançar sistemas por trás do *firewall.*
- Verificar a reação do *firewall* a pacotes fragmentados e spoofados.
- Utilizar uma ferramenta de varredura de vulnerabilidades nos servidores que possuem *firewall.*
- Testar a possibilidade de criar conexões não-autorizadas da rede interna para a internet.
- Verificar a susceptibilidade do *firewall* a ataques de negação de serviço.

v. Considerações

O acesso aos arquivos de registro do *firewall* é fundamental para entender os resultados de um teste de penetração, lembrando que estes registros não estão diretamente disponíveis para o realizador do teste.

O realizador do teste deve observar que a execução deste módulo pode comprometer o desempenho do *firewall*, além de provavelmente chamar a atenção da equipe de segurança da organização alvo.

3.4.9 Teste de Sistemas Confiáveis

i. Descrição

O teste de sistemas confiáveis busca vulnerabilidades na fronteira entre sistemas ou entre aplicações e sistemas. O cenário desse teste, muitas vezes, é mais teórico do que prático e se encontra no limite entre os testes de vulnerabilidade, de Firewall e de Roteadores.

ii. Objetivos

Os objetivos desse módulo são:

- Mapear os sistemas que dependem de outros sistemas.
- Mapear as aplicações com dependências de outros sistemas.
- Identificar os tipos de vulnerabilidades que afetam os sistemas confiáveis e as aplicações.
- Obter informação não autorizada.
- Obter acesso não autorizado aos arquivos ou sistemas.

iii. Pré-Requisitos

O principal pré-requisito para esse módulo é o teste de aplicações e serviços, porém os resultados dos testes de identificação de estrutura de redes e da análise de vulnerabilidades também são de grande valia.

iv. Tarefas

- Verificar os possíveis relacionamentos entre os resultados dos testes de aplicações e serviços, identificação de estrutura de redes.
- Testar os relacionamentos entre os vários sistemas através de *spoofing* ou *event triggering*.
- Verificar quais aplicações e sistemas são vulneráveis à técnica de *spoofing*.
- Tentar obter acesso através de parâmetros de autenticação entre sistemas.

v. Considerações

O teste de sistemas confiáveis busca verificar se as fronteiras da aplicação ou sistema alvo estão seguras e a salvo de tentativas de acesso não autorizado ou obtenção de informações privilegiadas. É importante ressaltar que os sistemas ou aplicações que estabelecem fronteira com o alvo do teste nem sempre são da mesma organização a ser testada.

A equipe de teste deve estar consciente que o alvo de seu teste é a aplicação/sistema do cliente e não sistemas de terceiros que porventura façam fronteiras com o alvo. Por exemplo: Uma loja virtual (cliente do teste) tem uma aplicação que faz fronteira com um sistema de cobrança através de cartão de crédito. No caso descrito, a equipe de teste deverá testar apenas a fronteira da aplicação da loja, sem afetar o sistema de cobrança.

Durante um teste de sistemas confiáveis o desempenho do sistema testado pode reduzir, portanto é interessante que se tomem medidas cabíveis para que o teste não afete o funcionamento normal do sistema.

3.4.10 Teste do Sistema de Detecção de Intrusos

i. Descrição

Este módulo verifica o desempenho e a sensibilidade do Sistema de Detecção de Intrusos (*Intrusion Detection System - IDS*). As ações tomadas pelo IDS durante um ataque nem sempre são evidentes para o invasor, sendo somente possível verificá-las por meio da análise dos arquivos de *log*. Além disso, a largura de banda de quem ataca o sistema, a distância em *hops* e a latência afetam os resultados do teste.

ii. Objetivos

Os objetivos deste módulo são:

- Obter o tipo de IDS.
- Avaliar a performance do IDS sob uma carga elevada na rede.
- Tipos de pacotes e protocolos “dropados” ou não-analisados.
- Obter o tempo e tipo de reação.
- Obter a sensibilidade.
- Obter o mapa de regras.
- Listar os falsos positivos e alarmes desapercebidos.
- Listar os caminhos de rede não-monitorados.

iii. Pré-requisitos

Para testar o IDS, deve-se possuir informações sobre o sistema alvo e os *firewalls* envolvidos. Além destas informações, é importante possuir um modo de descobrir se o IDS disparou ou não o seu alarme.

iv. Tarefas

- Verificar o tipo de IDS com as informações colhidas em outros módulos.
- Determinar a região sob ação do IDS.
- Testar os estados de alarme do IDS.
- Testar a sensibilidade a assinaturas.
- Testar as reações do IDS a diversas situações.
- Verificar a capacidade do IDS de lidar com pacotes fragmentados e com métodos específicos de ataque ao sistema.
- Testar o efeito e as reações do IDS com um único e vários endereços IP.
- Comparar os arquivos de registro e os alertas com as varreduras de vulnerabilidade e com os testes de sistemas confiáveis.

v. Considerações

A revisão dos alertas e dos arquivos de registro do IDS são especialmente importantes quando o ataque é realizado a partir de um ponto inicial externo, pois há menor visibilidade das reações e do estado do alvo. Não realizar esta revisão ignorará vários pontos potencialmente importantes para o sucesso do teste.

A avaliação do IDS demanda uma elevada porção da largura de banda, podendo impactar no desempenho da rede da organização alvo. Desta forma, o realizador do teste deverá ponderar este aspecto durante o emprego deste módulo.

3.4.11 Teste das Medidas de Contingência

i. Descrição

As medidas de contingência determinam como proceder em casos de ameaças aos sistemas de informação da organização alvo. Avaliar os mecanismos de segurança e as políticas de resposta a ameaças são o objetivo deste módulo.

ii. Objetivos

Os objetivos deste módulo são:

- Listar a capacidade de defesa anti-*trojan* e anti-vírus.
- Identificar as medidas de contingência.
- Identificar as fraquezas das medidas de contingência.
- Listar os recursos empregados.
- Verificar o funcionamento das medidas de contingência na prática.

iii. Pré-requisitos

Este módulo exige que o realizador do teste possua uma maneira de monitorar as ações tomadas diante da situação de risco criado pelo teste de penetração.

iv. Tarefas

- Analisar a adequação das ações tomadas diante da situação ocorrida.
- Medir o mínimo de recursos necessários para o funcionamento do subsistema de medidas de contingência.
- Analisar os recursos que são dispensáveis para o subsistema de medidas de contingência e os são protegidos de uso por ele.
- Analisar as medidas de detecção empregadas para a proteção desses recursos protegidos.

- Analisar as medidas de detecção empregadas para o uso incomum dos recursos necessários.
- Analisar os recursos desnecessários.
- Analisar as características do subsistema de medidas de contingência.

v. Considerações

A aplicação deste módulo pode afetar o desempenho da rede da organização alvo.

3.4.12 Teste de DoS (Denial of Service)

i. Descrição

Segundo (OSSTMM) *Denial of Service* (DoS) é uma situação ou circunstancia na qual o sistema é impedido de funcionar como o previsto. Em certos casos, o sistema pode estar funcionando exatamente como o previsto, porém ele não foi projetado para suportar a carga, escopo ou parâmetros impostos.

Ataques de negação de serviço consistem em enviar vários pacotes e requisições ao sistema alvo de forma que o processamento e memória disponíveis fiquem escassos e impeçam o sistema de executar suas funções normalmente. Esse funcionamento incorreto do sistema pode gerar vulnerabilidades não identificadas em seu estado normal.

O Ataque de *Distributed Denial of Service* (DDoS) é proibido na norma do OSSTMM pois esse tipo de ataque sempre irá causar problemas ao sistema alvo e até mesmo aos sistemas e roteadores entre a equipe de testes. As outras normas também citam o risco de se executar um DDoS e nenhuma delas recomenda a prática.

ii. Objetivos

Os objetivos desse módulo são:

- Listar sistemas suscetíveis a ataques DoS.
- Listar pontos fracos na presença na Internet inclusive pontos de acesso únicos.
- Estabelecer um padrão de base para uso regular do sistema.
- Listar comportamento do sistema sobre condições severas de uso.

iii. Pré-Requisitos

O único pré-requisito desse teste é que os sistemas a serem testados (e. g. servidores web, servidores de e-mail e outros) devem estar disponíveis no momento do

teste.

iv. Tarefas

- Verificar se a segurança de contas de administradores e o sistema de arquivos estão devidamente seguros e se o acesso é concedido de acordo com o princípio do *"Least Privilege"*.
- Verificar a exposição dos sistemas a redes não seguras.
- Verificar os padrões estabelecidos para atividade normal do sistema.
- Verificar o procedimento respondendo a atividades irregulares.
- Verificar a resposta a ataques simulados de negação de serviço.
- Testar os servidores e redes com grande volume de tráfego.

v. Considerações

Segundo a RFC (*Request For Comments*) 4732 (*Internet Engineering Task Force* - IETF, 2006) quase todos os serviços da Internet são suscetíveis a ataques de negação de serviço com escala suficiente para o serviço em questão. Todas as documentações de normatização de testes de penetração avaliadas nesse trabalho não recomendam a realização de um DDoS no sistema ou aplicação alvo, o recomendável é que se execute um DoS com proporções controladas para verificar a reação da infraestrutura de rede e dos dispositivos de prevenção como *firewalls, switches*, roteadores e outros.

3.4.13 Teste do Sistema de Comunicação por Telefonia

i. Descrição

Este módulo avaliará os seguintes sistemas de comunicação da organização alvo que empregam telefonia: PBX, FAX, correio de voz e quaisquer outros ativados por modem. Além da avaliação, deve-se tentar obter privilégios de acesso de cada um desses sistemas.

ii. Objetivos

Os objetivos deste módulo são:

- Encontrar e listar os sistemas PBX que permitem administração remota ou acesso global ao terminal de manutenção.
- Listar todos os sistemas telefônicos ativos e interativos.
- Listar as caixas de correio de voz que permitem acesso global.
- Listar os códigos de discagem e os PINs das caixas de correio de voz.

- Listar os sistemas FAX, os seus tipos e os possíveis programas que os operam.
- Obter mapa do protocolo de uso de FAX na organização.
- Listar os sistemas com modems esperando conexão, os seus tipos, os possíveis programas que os operam e os seus esquemas de autenticação.
- Listar nomes de usuário e senhas dos modems.
- Obter mapa do protocolo de uso de modems na organização.
- Listar as tentativas com sucesso de acesso através dos modems
- Listar os *"wild* modems".
- Listar as máquinas de FAX.

iii. Pré-requisitos

Para aplicar este módulo, o realizador do teste deve possuir uma faixa de números telefônicos da organização alvo.

iv. Tarefas

- Verificar se contas de administradores possuem senhas padrão ou de fácil descoberta.
- Verificar se o sistema operacional está atualizado e com os devidos *patches*.
- Verificar o acesso remoto de manutenção.
- Testar autenticação por discagem, inclusive a remota.
- Verificar o tamanho do PIN e a freqüência com a qual ele é modificado.
- Identificar, pelo correio de voz, informações sobre o usuário e a organização.
- Varrer a rede telefônica em busca de modems.
- Tentar acessar a rede através das conexões modem encontradas.
- Utilizar um *war dialer* (com componentes de detecção de sistema) na faixa de números telefônicos da organização alvo.

v. Considerações

O realizador do teste deve ter em mente que, apesar dos procedimentos serem realizados por meio da linha telefônica, existe a possibilidade de detecção do ataque pela organização alvo.

3.4.14 Teste de Dispositivos Sem-fio

i. Descrição

Esse módulo se propõe a verificar se as informações emanadas através do espectro eletromagnético estão protegidas e se os pontos de acesso à rede através desse meio estão seguros. O teste de dispositivos sem fio é um módulo que pode ser executado de modo parcial, pois muitas organizações alvo não irão necessitar de verificações tão profundas quanto as previstas em determinadas normas.

Por informações emanadas no espectro eletromagnético devemos considerar as comunicações de diversos dispositivos rádio e ainda as radiações eletromagnéticas de dispositivos que apresentam visualização de informação. Os mais comuns são:

- Redes sem fio.
- Redes *bluetooth*.
- Dispositivos de comunicação rádio.
- Telefone sem fio.
- Dispositivos de segurança sem fio.
- Dispositivos de cobrança sem fio.
- Dispositivos de identificação sem fio, *Radio Frequency Identifier* (RFID) como comandos de abertura de portões e identificação de pessoal.
- Dispositivos infravermelho.
- Dispositivos de entrada e saída sem fio (teclados, mouse, scanners, impressoras, etc...).
- Monitores CRT e LCD.

As verificações consistem em verificar se os meios de comunicação estão imunes a escutas não autorizadas, interferências e a inserções de informação não autorizada ou não pertinente.

ii. Objetivos

Os objetivos desse módulo são:

- Listar sistemas suscetíveis à interferência eletromagnética.
- Verificar se a informação emanada através do espectro é feita de modo seguro.
- Obter acesso não autorizado em pontos de acesso (rádio) através de força bruta.

iii. Pré-Requisitos

A organização que realiza o teste deve ter equipamento e pessoal adequados às verificações tendo em vista que esse módulo trata de diversas tecnologias e protocolos

da indústria.

iv. Tarefas

- Realizar escuta dos meios de comunicação escolhidos a fim de verificar se existem informações sensíveis sendo trafegas em modo não seguro.
- Verificar a capacidade do sistema em resistir a interferências e inserções de informação errônea e não autenticada através dos canais de comunicação.
- Realizar tentativas de obtenção de acesso não autorizado à rede através de dispositivos sem fio.

v. Considerações

O escopo desse módulo deve ser estabelecido em contrato, pois muitas vezes a organização alvo não terá recursos para corrigir as falhas ou então não haverá necessidade de tal nível de segurança. Outro aspecto que deve ser considerado é a capacidade da empresa que irá realizar o teste de detectar falhas de segurança nesses sistemas que muitas vezes exigem conhecimento específico e equipamento de alto custo.

3.4.15 Teste da Segurança Física

i. Descrição

Um teste de penetração não se limita a aspectos dos sistemas de computação e de comunicações. A segurança da informação só se torna completa com a garantia da inviolabilidade das instalações físicas de uma organização e de onde se encontram os seus sistemas por pessoas não autorizadas.

Este módulo abrangerá os seguintes aspectos da segurança física das instalações: perímetro, monitoramento, controle de acesso, resposta a alarmes, localização e instalações. Toda organização deve se preocupar com sua segurança física para garantir que seu sistema de informação esteja realmente protegido.

ii. Objetivos

Os objetivos deste módulo são:

- Obter o mapa do perímetro físico.
- Listar os tipos de medidas de segurança física adotadas.
- Listar áreas fracamente protegidas e desprotegidas.
- Listar todos os pontos de acesso, incluindo os monitorados (por humanos ou eletronicamente).

- Listar os tipos de monitoramento adotados.
- Listar pontos de acesso sem monitoramento a áreas comuns e privilegiadas.
- Listar localização de alarmes e seus acionadores.
- Listar os tipos de autenticação exigidos.
- Listar os tipos de alarme adotados.
- Obter o mapa do procedimento em caso de alarme.
- Obter lista das pessoas envolvidas em procedimentos em caso de alarme.
- Obter lista das medidas de contenção e precauções de segurança acionados por um alarme.
- Obter o mapa das instalações físicas e da localização.
- Listar os pontos de acesso à localização.
- Listar a localização dos acessos de terceiros.
- Listar as localizações vulneráveis.
- Listar as leis, costumes e ética locais.
- Obter acesso a áreas protegidas.

iii. Pré-requisitos

Este módulo exige que o realizador do teste possua os mapas do local e das instalações da organização alvo. Para a incursão na organização alvo, são fundamentais as informações obtidas, ao longo da execução deste módulo, sobre os sistemas de controle de acesso e de monitoramento.

iv. Tarefas

- Mapear o perímetro físico e suas medidas de segurança (grades, portões, luzes, etc.).
- Mapear as rotas e métodos de acesso.
- Mapear áreas não monitoradas.
- Listar os dispositivos de monitoramento.
- Mapear áreas monitoradas e as rotas dos seguranças.
- Testar as fraquezas e limites dos dispositivos de segurança (alarmes, dispositivos de controle de acesso), incluindo a realização de ataques de negação serviço.
- Listar as áreas de controle de acesso.
- Verificar os dispositivos de controle de acesso, seus tipos e seus níveis de privacidade e complexidade.
- Verificar os tipos de alarme existentes.
- Listar os dispositivos de alarme adotados.
- Mapear os procedimentos em caso de alarme.
- Mapear as consequências acionadas pelo alarme.
- Listar as pessoas envolvidas em procedimentos em caso de alarme.

- Testar os dispositivos para armar e desarmar o alarme.
- Listar as áreas visíveis.
- Listar as áreas com monitoramento de áudio.
- Testar as fraquezas e vulnerabilidades para entregadores de suprimento.
- Listar as pessoas e as empresas fornecedoras de suprimentos.
- Listar as equipes e as empresas de limpeza.
- Listar as horas e dias dos ciclos de entrega e de visitação.
- Verificar as condições para desastre natural na região.
- Verificar as condições do ambiente político.
- Identificar as fraquezas e vulnerabilidades em procedimentos de recuperação e de back-up, incluindo a possibilidade de ataques de negação de serviço.
- Comparar procedimentos operacionais com a legislação local, costumes e ética.

v. Considerações

A realização de incursões nas instalações da organização alvo pode ter consequências extremamente graves para a integridade física de quem a realiza, além da exposição do ocorrido a terceiros (mídia, vizinhança, funcionários, etc.). Desta forma, deve haver completo entendimento e definição em contrato do que poderá ser feito e de até que ponto deve ser levada uma incursão às instalações da organização alvo.

3.4.16 Engenharia Social

i. Descrição

O módulo de engenharia social visa obter informações sobre a organização alvo através de seus funcionários e prestadores de serviço. A execução desse módulo deve ser bem delimitada a fim de não interferir em questões éticas e legais.

As técnicas utilizadas nesse módulo visam obter dos funcionários informações sigilosas sobre a empresa. Como consequência, é verificado se o pessoal da empresa está seguindo os procedimentos e políticas de segurança determinados pelas empresas e se os últimos são adequados.

ii. Objetivos

Os objetivos desse módulo são:

- Obter informações de senhas e modos de acesso à empresa e ao sistema de informações.
- Listar os funcionários segundo seu grau hierárquico.
- Verificar se funcionários de níveis hierárquicos inferiores possuem acesso a

informações desnecessárias ao desempenho de suas funções.

- Verificar se as políticas e procedimentos de segurança adotados pela organização alvo são adequados e se estão sendo seguidas pelos funcionários.
- Verificar se a desmobilização do pessoal está sendo feita de forma correta.
- Listar todas as informações obtidas nos módulos a fim de utilizá-las nos demais.

iii. Pré-Requisitos

O módulo de engenharia social é considerado um módulo de reconhecimento e obtenção de informações e, portanto, deve ser um dos primeiros a ser executado. Dessa forma, considera-se o único pré-requisito para execução do módulo a delimitação contratual clara e precisa do que será executado a luz das questões éticas e legais definidas.

iv. Tarefas

- Listar os funcionários da empresa segundo seu grau hierárquico.
- Realizar contato com os funcionários através de telefone, e-mail ou fisicamente para tentar obter informações sobre a empresa.
- Realizar contato com ex-funcionários da empresa para tentar obter informações sigilosas ou detalhes sobre funcionamento e procedimentos da organização alvo.
- Verificar a política de contratações da empresa.
- Verificar a política de distribuição de informação através dos níveis hierárquicos.
- Executar *phishing* através de e-mail, correios, SMS, telefone, pessoalmente e programas de *instant messaging* (IM).
- Verificar a distribuição de informação a prestadores de serviço e parceiros de negócio.

v. Considerações

A execução do módulo de engenharia social é opcional e deve ser definida em contrato, dependendo do tamanho e das características da empresa quanto ao sigilo das informações e susceptibilidade à espionagem industrial.

Questões éticas e legais devem ser discutidas a fim de não haver excessos nas tentativas de obtenção de informação por parte da equipe de aplicação do teste. Deve-se observar também o contrato de sigilo estabelecido entre a organização alvo e a equipe de aplicação do teste de forma que a ultima não revele informações sensíveis à empresa.

A equipe de aplicação do teste deve estar em constante atualização sobre as diversas técnicas de *phishing* dado que a criatividade é essencial à esse tipo de

atividade.

4 FERRAMENTAS

As seguintes ferramentas podem ser utilizadas para a realização dos módulos acima:

Ferramenta	Aircrack
Módulos	- Captura e Quebra de Senhas - Teste de dispositivos sem fio
Descrição	Considerada a mais rápida ferramenta para quebra de senhas WEP/WPA.
Plataforma	Windows, Unix
Origem	http://www.aircrack-ng.org/

Ferramenta	Attack Tool Kit
Módulos	Todos
Descrição	Framework para realização do teste de penetração
Plataforma	Windows
Origem	http://www.computec.ch/projekte/atk/?

Ferramenta	Cain and Abel
Módulos	- Captura e Quebra de Senhas
Descrição	Possibilita a quebra de senhas do Windows.
Plataforma	Windows
Origem	http://www.oxid.it/cain.html

Ferramenta	Canvas
Módulos	- Todos
Descrição	Framework pago para a realização de testes de penetração.
Plataforma	Windows, Unix
Origem	http://www.immunitysec.com/products-canvas.shtml

Ferramenta	Cheops-ng
Módulos	Identificação da Estrutura de Rede
Descrição	Fornece uma descrição gráfica de uma rede, além de detectar os serviços e o sistema operacional dos servidores de uma rede.
Plataforma	Windows, Unix
Origem	http://cheops-ng.sourceforge.net/

Ferramenta	CIS Cisco Router Audit
Módulos	- Teste de roteadores
Descrição	Realiza teste de roteadores cisco de acordo com parâmetros da própria empresa
Plataforma	Windows

Origem	http://www.cisco.com

Ferramenta	Core Impact
Módulos	- Todos
Descrição	Framework pago para a realização de testes de penetração. Considerada a melhor e mais completa ferramenta disponível.
Plataforma	Windows, Unix
Origem	http://www.coresecurity.com/products/coreimpact/

Ferramenta	CUPP
Módulos	- Engenharia Social
Descrição	Ferramenta que auxilia a realização de engenharia social
Plataforma	Windows, Unix
Origem	http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Common_User_Passwords_Profiler_(CUPP)

Ferramenta	Dsniff
Módulos	- Identificação da Estrutura de Rede - Captura e Quebra de Senhas - Análise de informações públicas - Teste de sistemas confiáveis
Descrição	Permite a interceptação de tráfego em redes com *switch*.
Plataforma	Windows, Unix
Origem	http://www.monkey.org/~dugsong/dsniff/

Ferramenta	Firewalk
Módulos	- Identificação da Estrutura de Rede - Teste de *Firewall* - Teste de Roteadores - Teste de Varredura de Portas
Descrição	Possibilita traçar rotas, permitindo testar as regras de um *firewall*. O Hping2 consegue fornecer as mesmas funcionalidades quando devidamente configurado.
Plataforma	Unix
Origem	N/A

Ferramenta	Firewall tester
Módulos	- Teste de *Firewall* - Teste de IDS - Teste de Roteadores
Descrição	Realiza o teste de IDS e *firewall*
Plataforma	Windows, Unix
Origem	http://www.inversepath.com/ftester.html

Ferramenta	Fpipe
Módulos	- Teste de *Firewall*
Descrição	Altera a rota de conexões para outra porta e engana as regras de um *firewall*.
Plataforma	Windows
Origem	http://www.networkingfiles.com

Ferramenta	Hping2
Módulos	- Teste de *Firewall* - Teste de Roteadores
Descrição	Possibilita o teste das regras de um *firewall*.
Plataforma	Windows, Unix
Origem	http://www.hping.org/

Ferramenta	ISS Internet Scanner
Módulos	- Análise e Verificação de Vulnerabilidades - Teste de *Firewall*
Descrição	Realiza a varredura de uma rede em busca de vulnerabilidades.
Plataforma	Windows
Origem	http://www.iss.net

Ferramenta	John the Ripper
Módulos	- Captura e Quebra de Senhas
Descrição	Possibilita a quebra de *hashes* de senhas NT e Unix.
Plataforma	Unix, DOS, Windows
Origem	http://www.openwall.com/john

Ferramenta	Kismet
Módulos	- Teste de dispositivos sem fio
Descrição	Realiza o teste de dispositivos sem fio.
Plataforma	Windows, Unix
Origem	http://www.kismetwireless.net/

Ferramenta	L0pht Crack
Módulos	- Captura e Quebra de Senhas
Descrição	Possibilita a quebra de senhas Windows.
Plataforma	Windows
Origem	http://www.l0phtcrack.com/

Ferramenta	Nemesis
Módulos	- Teste de *Firewall*

	- Teste do Sistema de Detecção de Intrusos
Descrição	Possibilita a manipulação de pacotes.
Plataforma	Unix
Origem	http://the.wiretapped.net

Ferramenta	Nessus
Módulos	- Análise e Verificação de Vulnerabilidades - Teste de *Firewall*
Descrição	Realiza as mesmas funções do ISS Internet Scanner, porém com preço mais acessível.
Plataforma	Unix, Windows
Origem	http://www.nessus.org

Ferramenta	Nikto
Módulos	- Análise e Verificação de Vulnerabilidades - Teste de *Firewall*
Descrição	Procura por vulnerabilidades em servidores *Web*, incluindo *scripts* CGI (*Common Gateway Interface*). Possui código aberto, tendo o Whisker (antiga ferramenta com a mesma funcionalidade) como base.
Plataforma	Windows, Unix
Origem	http://www.cirt.net/nikto2

Ferramenta	Nmap
Módulos	- Varredura de portas - Teste de aplicações e serviços - Teste de *firewall*
Descrição	Realiza o *fingerprinting* e descoberta de aplicações
Plataforma	Windows, Mac OS X e Linux
Origem	http://nmap.org/

Ferramenta	Maltego
Módulos	- Engenharia Social
Descrição	Ferramenta que auxilia a realização de engenharia social
Plataforma	Windows, Unix
Origem	http://www.paterva.com/web5/

Ferramenta	Metasploit Framework
Módulos	- Todos
Descrição	Framework renomado e gratuito para a realização de testes de penetração.
Plataforma	Windows, Unix
Origem	http://www.metasploit.com/

Ferramenta	Paros
Módulos	- Análise de informações públicas
Descrição	Análise do tráfego web.
Plataforma	Multiplataforma (Java)
Origem	http://www.parosproxy.org

Ferramenta	Phonesweep
Módulos	- Teste do Sistema de Comunicação por Telefonia
Descrição	Exige conhecimento especializado para seu emprego.
Plataforma	Não informada.
Origem	http://sandstorm.net/products/phonesweep

Ferramenta	PWDM
Módulos	- Teste de dispositivos sem fio
Descrição	Realiza o teste de dispositivos sem fio e sugere metodologia de segurança
Plataforma	Windows, Unix
Origem	http://www.pwdm.net/

Ferramenta	RFIDIOt
Módulos	- Teste de dispositivos sem fio
Descrição	Realiza o teste de dispositivos sem fio em ampla escala de frequências.
Plataforma	Windows, Unix
Origem	http://rfidiot.org/

Ferramenta	Router Tester
Módulos	- Teste de roteadores
Descrição	Realiza identificação de roteadores para determinado servidor.
Plataforma	Windows
Origem	http://noeld.com/programs.asp?cat=dstools#rtest

Ferramenta	Saint
Módulos	- Análise e Verificação de Vulnerabilidades, - Teste de *Firewall* - Teste de sistemas confiáveis
Descrição	Realiza a varredura da rede em busca de vulnerabilidades. Diferencia-se por sua interface gráfica mais simples.
Plataforma	Unix
Origem	http://www.saintcorporation.com/

Ferramenta	Sam Spade
Módulos	- Identificação da Estrutura de Rede

Descrição	Fornece meios para obter informações (whois, DNS queries, etc.)
Plataforma	Windows
Origem	http://www.samspade.org

Ferramenta	SARA
Módulos	- Análise e Verificação de Vulnerabilidades - Teste de *Firewall* - Teste de sistemas confiáveis
Descrição	Versão gratuita do Saint, mas foi descontinuada em 2009. Originou-se do SATAN.
Plataforma	Unix
Origem	http://www-arc.com/sara/

Ferramenta	Scapy
Módulos	- Teste de *Firewall* - Teste do Sistema de Detecção de Intrusos
Descrição	Possibilita a criação e manipulação de pacotes da rede.
Plataforma	Windows
Origem	http://www.packx.net/packx

Ferramenta	Sniffit
Módulos	- Captura e Quebra de Senhas
Descrição	Específico para captura de dados de aplicações e de senhas.
Plataforma	Unix
Origem	http://reptile.rug.ac.be/~coder/sniffit/sniffit.html

Ferramenta	Snort
Módulos	- Identificação da Estrutura de Rede - Captura e Quebra de Senhas - Teste de sistemas confiáveis
Descrição	Sistema de detecção de intrusos com componente de monitoramento de tráfego.
Plataforma	Windows, Unix
Origem	http://www.snort.org/

Ferramenta	Stacheldraht
Módulos	- Teste de *Firewall* - Teste da Segurança Física - Teste de DoS
Descrição	Possibilita a realização de um ataque de negação de serviço distribuído (DDoS).
Plataforma	Unix
Origem	Indisponível

Ferramenta	Stumbler
Módulos	- Teste de dispositivos sem fio
Descrição	Realiza o teste de dispositivos sem fio.
Plataforma	Windows, Unix
Origem	http://www.stumbler.net/index.php?cat=1

Ferramenta	Tcpdump
Módulos	- Identificação da Estrutura de Rede - Captura e Quebra de Senhas - Teste de Sistemas Confiáveis
Descrição	Realiza o monitoramento de tráfego das camadas um a quatro do modelo OSI.
Plataforma	Windows, Unix
Origem	http://www.tcpdump.org

Ferramenta	TFN2000
Módulos	- Teste de *Firewall* - Teste da Segurança Física - Teste de DoS
Descrição	Possibilita a realização de um ataque de negação de serviço distribuído (DDoS).
Plataforma	Windows, Unix
Origem	Indisponível

Ferramenta	THC Amap
Módulos	- Varredura de portas - Teste de aplicações e serviços
Descrição	Realiza o *fingerprinting* e descoberta de aplicações
Plataforma	Windows
Origem	http://www.thc.org/thc-amap/

Ferramenta	THC Hydra
Módulos	- Quebra de senhas
Descrição	Realiza quebra de senhas em diversos protocolos
Plataforma	Unix
Origem	http://www.thc.org/thc-hydra/

Ferramenta	THC Orakel
Módulos	- Análise de informações públicas
Descrição	Verificação de banco de dados Oracle
Plataforma	Windows
Origem	http://www.thc.org/thc-orakel/

Ferramenta	THC Scan

Módulos	- Teste do Sistema de Comunicação por Telefonia
Descrição	Empregada como *war dialer*.
Plataforma	DOS
Origem	http://www.thehackerschoice.com

Ferramenta	THC Vmap
Módulos	- Teste de aplicações e serviços
Descrição	Verifica a versão dos aplicativos
Plataforma	Windows
Origem	http://www.thc.org

Ferramenta	Trin00
Módulos	- Teste de *Firewall* - Teste da Segurança Física - Teste de DoS
Descrição	Possibilita a realização de um ataque de negação de serviço distribuído (DDoS).
Plataforma	Unix
Origem	Indisponível

Ferramenta	Unicornscan
Módulos	-Teste de Varredura de Portas
Descrição	Realiza varredura de portas nos protocolos TCP e UDP
Plataforma	Windows, Unix
Origem	http://www.unicornscan.org/

Ferramenta	Visual Route
Módulos	- Identificação da Estrutura de Rede - Teste de *Firewall* - Teste de Roteadores
Descrição	Fornece suporte visual a rotas traçadas.
Plataforma	Unix, Windows
Origem	http://www.visualroute.com

Ferramenta	Wireshark
Módulos	- Identificação da Estrutura de Rede - Captura e Quebra de Senhas - Teste de sistemas confiáveis - Teste de dispositivos sem fio
Descrição	Além de monitorar os pacotes, consegue interpretar informações da camada de aplicação.
Plataforma	Windows, Unix
Origem	http://www.wireshark.org/

Ferramenta	WYD
Módulos	- Engenharia Social
Descrição	Ferramenta que auxilia a realização de engenharia social
Plataforma	Windows, Unix
Origem	http://www.social-engineer.org/framework/Computer_Based_Social_Engineering_Tools:_Who%27s_Your_Daddy_Password_Profiler_(WYD)

A seguir as ferramentas listadas por utilização nos módulos:

Módulos	Ferramentas
Análise de Informações Públicas	- Dsniff - Paros - THC - Orakel
Identificação da Estrutura da Rede	- Firewalk - Sam Spade - Cheops-ng - Dsniff - Wireshark - Snort - Tcpdump - Visual Route
Varredura de Portas	- THC Amap - Nmap - Unicornscan - Firewalk
Análise e Verificação de Vulnerabilidades	- ISS Internet Scanner - Nessus - Saint - SARA - Nikto
Teste de Aplicações e Serviços	- THC Amap - Nmap - THC Vmap
Captura e Quebra de Senhas	- Dsniff - Wireshark - Snort - Tcpdump - Aircrack - Cain and Abel - John the Ripper - L0pht Crack - Sniffit - THC Hydra
Teste de Roteadores	- Firewalk - Hping2 - Visual Route - CIS Cisco Router Audit

	- Router Tester - Visual Route - Firewall tester
Teste de Firewall	- ISS Internet Scanner - Nessus - Saint - SARA - Nikto - Firewalk - Hping2 - Nemesis - Stacheldraht - TFN2000 - Trin00 - Fpipe - Visual Route - Nmap - Firewall tester
Teste de Sistemas Confiáveis (*Trusted Systems*)	- Saint - SARA - Dsniff - Wireshark - Snort - Tcpdump
Teste do Sistema de Detecção de Intrusos	- Nemesis - Firewall tester
Teste das Medidas de Contingência	- Nenhuma ferramenta específica encontrada.
Teste de DoS (Denial of Service)	- Stacheldraht - TFN2000 - Trin00
Teste do Sistema de Comunicação por Telefonia	- Phonesweep - THC Scan
Teste de dispositivos sem fio	- Wireshark - Aircrack - PWDM - Kismet - Stumbler - RFIDIOt
Teste de Segurança Física	- Stacheldraht - TFN2000 - Trin00
Engenharia Social	- Maltego - CUPP - WYD
Frameworks para todos os módulos	- Metasploit Framework - Core Impact - Canvas - Attack Tool Kit

As ferramentas acima estão sujeitas à desatualização e, portanto, devem ser constantemente pesquisadas e renovadas a cada trabalho.

5 DOCUMENTAÇÃO

Para um teste de penetração, existem muitas possibilidades de classificação e de objetivos a serem atingidos. A realização de cada módulo pode divergir o suficiente para tornar o estabelecimento de um padrão de documentação impraticável em termos de complexidade. Desta forma, para não se desviar do foco desse estudo, essa seção se concentra apenas em descrever quais informações devem ser documentadas, mas não em estabelecer um formato para isto.

5.1 Relatórios Parciais

Basicamente, a documentação para cada módulo deve conter:

- Restrições.
- Descrição dos procedimentos.
- Cenário (ferramentas utilizadas e os parâmetros empregados).
- Descrição da execução.
- Arquivos de registro das ferramentas, sistemas e aplicações envolvidas.
- Resultados obtidos.

Primeiramente, são descritas as restrições contratuais impostas ao módulo, como, por exemplo: o escopo de aplicação, o ponto de partida do teste, as restrições de horário de aplicação e outras. Após a apresentação das restrições, deve-se descrever de modo sucinto quais serão os procedimentos do teste e quais os resultados são esperados após a sua execução.

As ferramentas e o ambiente em que elas são empregadas devem também ser descritas com o máximo detalhamento possível, de modo a possibilitar a reconstituição do teste. Desta forma, é interessante listar todos os parâmetros utilizados, a situação dos sistemas envolvidos, as condições da rede e as demais informações que possam interferir no resultado do teste. O conjunto destas informações comporá o cenário em que o teste foi aplicado.

A execução do teste também deve ser documentada passo-a-passo a fim de facilitar sua reconstituição. Assim, devem ser anexados ao relatório: todas as entradas e saídas devem ser descritas, os arquivos de registro e as mensagens de erro de todas as aplicações diretamente envolvidas com a execução do módulo.

Por fim, deve-se fazer uma conclusão sucinta, indicando os pontos onde houve sucessos, falhas e resultados inconclusivos. Essa última parte é fundamental para a composição do relatório final.

5.2 Relatório Final

Segundo o OSSTMM 2.2 (2006), o relatório final deve respeitar os seguintes critérios:

- Manter a privacidade dos funcionários da empresa alvo que, por ventura, tiveram participação no teste.
- Não citar nomes no relatório, apenas estatísticas.
- A equipe deverá escrever somente sobre os módulos em que esteve envolvida.
- O relatório deve ser objetivo, ou seja, não deve conter suposições.
- As recomendações devem ser válidas e práticas.
- As métricas do teste devem ser quantitativas, mas não qualitativas, ou seja, os resultados devem ser baseados em fatos e não em interpretações.
- Os relatórios devem conter os sucessos, fracassos ou resultados inconclusivos ao tentar atingir os objetivos dos módulos.
- Os meios de comunicação empregados para envio do relatório devem ser confidenciais.
- Os resultados e relatórios não devem ser usados para fins comerciais.
- Os relatórios devem apontar anomalias desconhecidas.

Segundo o NIST (2008), os resultados obtidos em um teste de penetração têm as seguintes finalidades:

- Tornar-se uma referência para uma ação corretiva.
- Definir ações a fim de mitigar vulnerabilidades.
- Comparar com resultados anteriores para apontar a evolução da empresa na área de segurança.
- Avaliar o status de implementação das recomendações de segurança.
- Analisar as relações custo-benefício para as melhorias de segurança.
- Assessorar outras atividades do ciclo de vida normal do sistema, como: análise de risco, obtenção de certificações e autorizações e esforços na melhoria de desempenho.

Respeitando esses critérios e em vista das finalidades descritas, a equipe que fez o estudo dos relatórios parciais deverá produzir o relatório final. Esse documento é feito para que pessoas leigas em TI consigam compreender os resultados e a relevância do teste de penetração para a segurança do sistema em questão. Ao contrário dos relatórios parciais, não devem ser abordados os aspectos técnicos do teste.

O relatório final é dividido em duas partes. As vulnerabilidades devem ser priorizadas e descritas na primeira parte, para isso deve-se abordar: a falha, as circunstâncias em que essa ocorre e os seus impactos para o sistema.

Na segunda parte do relatório, serão descritos os aspectos corretivos das vulnerabilidades, abordando: sua relevância, os procedimentos gerais para que as

correções sejam feitas e uma análise da relação custo-benefício para a organização alvo. Além do relatório propriamente dito, a equipe de teste deverá explanar, por meio de uma apresentação, os resultados obtidos.

Alguns autores recomendam ainda que o relatório final descreva, como sua última parte, um plano de ação para a correção dos erros, enquanto outros defendem que o teste se encerra quando as vulnerabilidades são apontadas. O principal motivo dessa divergência de abordagem se deve à complexidade do sistema alvo. Em organizações de pequeno porte, normalmente, não existe pessoal especializado em segurança da informação, sendo interessante que exista um plano de ação para as correções. Por outro lado, organizações maiores possuem departamentos de segurança da informação que têm capacidade de, avaliando o resultado do teste, desenvolver a solução mais adequada.

Verifica-se que a solução dos problemas apontados pelo teste de penetração não são triviais. Medidas, como compra de novos equipamentos e *softwares*, mudanças na política de segurança e, até mesmo, alterações no sistema alvo, podem se fazer necessárias. Assim, um plano de ação para correções dos erros extrapola os objetivos do teste de penetração, cabendo, à organização alvo, a avaliação dos resultados e a aplicação das medidas cabíveis.

O teste de penetração não se isenta completamente de apontar soluções. Procedimentos gerais para a correção das vulnerabilidades são descritos na segunda fase do relatório final, porém a aplicação dessas soluções em forma de plano deve considerar as peculiaridades da organização alvo. Por desconhecer aspectos da natureza do negócio, custos envolvidos e o impacto das correções para o funcionamento e desempenho do sistema, um plano formulado pela equipe de testes falharia em atender a todos os interesses da organização alvo.

6 CONCLUSÃO

A descoberta de vulnerabilidades envolve profundos conhecimentos do aplicador do teste nas áreas de sistemas operacionais, redes e programação. Todavia, a realização de um teste de penetração só se faz possível com uma equipe experiente e criativa. Existem muitas ferramentas disponíveis para a aplicação do teste, porém o desenvolvimento de aplicações específicas possibilita melhorias na exploração e na descoberta de vulnerabilidades.

A introdução de uma metodologia para o teste busca minimizar essa dependência do fator humano e padronizar ações para que o teste seja o mais completo possível. Apesar disso, por diversas vezes nesse trabalho, foram feitas referências à subjetividade de certos procedimentos e à recomendação de um estudo de caso por parte da equipe de aplicação do teste.

Não se pode ignorar a extensão e complexidade do assunto abordado. Devido à constante evolução dos sistemas de informação, a descrição detalhada de procedimentos para a realização do teste é impraticável. As rápidas inovações de *hardware* e *software* desatualizam as ferramentas e procedimentos adotados.

Esse trabalho é um esboço da metodologia de aplicação do teste de penetração e, portanto, é razoável que não cubra todos os seus aspectos. O resultado obtido é fruto do estudo de diversas normas internacionais e de textos relacionados ao assunto, que foram condensados de maneira a aproveitar os melhores pontos de cada abordagem.

A validação da metodologia desenvolvida se dará pela adequação do teste a uma situação real e à sua capacidade de atingir o sucesso nos objetivos propostos. Futuramente, os resultados desse trabalho poderão ser usados para desenvolver a metodologia proposta em termos práticos e corrigi-la se necessário.

GLOSSÁRIO

Fingerprinting – *Fingerprinting* da pilha TCP/IP consiste na coleta passiva de atributos de configuração de um dispositivo remoto durante a utilização da quarta camada do protocolo de comunicações em vigor. A combinação desses parâmetros pode ser usada para inferir o sistema operacional do dispositivo remoto.

Cavalo de Tróia – Cavalo de Tróia é um programa malicioso que age nas configurações da máquina atacada a fim de abrir portas de comunicação para possíveis invasões e/ou troca de informações.

Man-in-the-middle – *Man-in-the-middle* é uma técnica de ataque que consiste em interceptar a comunicação entre duas máquinas e realizar a intermediação dessa comunicação a fim de obter informações sobre as vitimas.

Hashes – *Hashes* são referencias às funções de *hash* que são funções sobrejetores que transformam seu argumento em um índice com a finalidade de facilitar a busca. As funções de hash também são usadas em criptografia para dificultar a identificação de senhas.

Firewalking – *Firewalking* é uma técnica que pode ser usada para colher informação sobre uma rede protegida por um *firewall*.

Least Privilege – O princípio do menor privilégio é o conceito abstrato de se conceder direitos de acesso mínimos aos recursos do sistema para o nível necessário ao usuário..

Phishing – *Phishing* é a técnica de obter informações da vítima induzindo-a acessar *e-mails*, páginas e *links* falsos que levem a programas ou *scripts* maliciosos.

REFERÊNCIAS BIBLIOGRÁFICAS

Federal Office For Information Security (BSI). **A Penetration Testing Model**.

HERZOG, Pete. **OSSTMM 2.2: Open-Source Security Testing Methodology Manual.**

SCARFONE, Karen; SOUPPAYA, Murugiah; CODY, Amanda; OREBAUHG, Angela. **NIST 800-115: Technical Guide to Information Security Testing and Assessment.**

WACK, John; TRACY, Miles; SOUPPAYA, Murugiah. **NIST 800-42: Guideline on Network Security Testing.**

SOARES, Rafael. **Auditoria Teste de Invasão (Pentest) – Planejamento, Preparação e Execução**. Acesso em 17/02/2011. Disponível em: http://www.seginfo.com.br/auditoria-teste-de-invasaopentest-planejamento-preparacao-e-execucao/

OWASP: The Open Web Application Security Project. **OWASP Testing Guide**. Acesso em 10/01/2011. Disponível em: http://www.owasp.org

SCAMBRAY, Joel; MCCLURE, Stuart; KURTZ, George. **Hackers Expostos**. Segunda edição. São Paulo: Makron Books, 2001.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br). **Cartilha de Segurança para Internet.**

ABNT: Associação Brasileira de Normas Técnicas. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação**. ABNT NBR ISSO/IEC 17799,2. 2005, Rio de Janeiro. Arquivo pdf.

IETF: *Internet Engineering Task Force*. **RFC 4732**. Acesso em 10/01/2011. Disponível em: http://tools.ietf.org/html/rfc4732.