

## Capítulo

# 1

## Introdução ao Pentest e Técnicas de Intrusão

Jean Carlos Martins Miguel e Rafael Menezes Barboza

### *Resumo*

*O minicurso Introdução ao Pentest e Técnicas de Intrusão, em nível intermediário, consiste em apresentar os procedimentos para a execução da técnica de Pentest em um ambiente controlado e isolado por máquinas virtuais vulneráveis de sistemas operacionais Linux e Windows, simulando um ambiente empresarial comum em muitas empresas. Abordam-se neste curso, técnicas de reconhecimento de alvo com utilização de ferramentas e técnicas como NMAP, Netcat, e exploração de vulnerabilidades com uso da ferramenta Metasploit.*

### **1.1. Informações gerais**

Para a realização deste minicurso recomenda-se que o candidato tenha conhecimentos prévios nas áreas de Segurança da Informação, Redes de Computadores, Sistemas Operacionais e afinidade com o sistema operacional Linux. Estes requisitos são necessários pois o curso tem como principal base conexões remotas através de endereços IPs e portas TCP/UDP, além disso, o sistema operacional usado para realizar os ataques é o Kali-Linux, distribuição baseada em GNU Linux. O nível de profundidade do minicurso é intermediário.

### **1.2. Equipe ministrante**

O minicurso proposto é ministrado por alunos do curso de Ciência da Computação da Universidade Tecnológica Federal do Paraná - câmpus Campo Mourão.

- **Jean Carlos Martins Miguel** - Acadêmico do curso de Ciência da Computação da UTFPR - Campo Mourão e membro do grupo de cibersegurança desde 2017. Recentemente desenvolveu tutoriais em Segurança da Informação, o qual objetivou-se a sistematização de ataques e vulnerabilidades, testes de intrusão em sistemas para estudo de diversos tipos de ataques e de vulnerabilidades, para futuramente serem desenvolvidos mecanismos e ferramentas para a prevenção e detecção de ataques similares.

- **Rafael Menezes Barboza** - Acadêmico do curso de Ciência da Computação da UTFPR - Campo Mourão e membro do grupo de cibersegurança desde 2018. Desenvolve um projeto de Iniciação Tecnológica e Inovação sobre “Estudo de casos de ataques cibernéticos à sistemas a industriais” junto à Fundação Parque Tecnológico Itaipu - Brasil.

O Grupo de Pesquisa em Cibersegurança da UTFPR campus Campo Mourão é um grupo composto por professores, alunos e colaboradores externos (professores de outras instituições, egressos da UTFPR, profissionais) que tem o interesse em desenvolver projetos científicos e de extensão na área de Cibersegurança. O grupo investiga técnicas e ferramentas de segurança, como também ataques e ameaças cibernéticas, com o intuito de desenvolver novas técnicas e ferramentas computacionais para a proteção de redes de computadores, sistemas computacionais e de dados. Também atua na conscientização de usuários por meio de seminários e palestras, tanto de caráter técnico como informativo, visando disseminar a cultura de Segurança da Informação (InfoSec) para a comunidade acadêmica e externa.

### **1.3. Infraestrutura e materiais**

Com intuito de trazer uma melhor experiência para os alunos durante o minicurso será necessário utilizar um laboratório, por exemplo, laboratório - E101, contendo aparelho projetor e computadores que suportam no mínimo duas máquinas virtuais executando simultaneamente. Isso é necessário pois grande parte do minicurso é baseada em atividades práticas individuais, seguindo as instruções passadas pelos ministrantes do minicurso.

Os requisitos de infraestrutura são:

- Aparelho projetor.
- Um computador por aluno matriculado.
- Os computadores devem conter o software VirtualBox para virtualizar os sistemas:
  - Kali Linux 64 Bits
  - Windows 7 SP1 64 Bits

Os sistemas operacionais usados nas máquinas virtuais sendo eles "Kali Linux Light x64 e Windows 7 SP1 x64" serão disponibilizados para a equipe organizadora do evento pelos próprios autores do minicurso. As ferramentas necessárias para conduzir o curso serão previamente instaladas na máquinas virtuais distribuídas.

### **1.4. Importância da Segurança Cibernética**

Defesas e métodos de segurança contra ataques cibernéticos no início da era virtual eram mínimas ou inexistentes. Um aluno do ensino médio ou um hacker inexperiente obtinham acesso aos sistemas e redes sem muito esforço. Porém, os índices de ataques e invasões foram crescendo à medida que cada vez mais informações importantes e confidenciais eram gerenciadas pelos meios tecnológicos modernos. Logo, o interesse de hackers, ativistas e nações em deter informações e controle sobre sistemas e dados foram aumentando.

Países do mundo todo tornaram-se mais conscientes da ameaça de ataques cibernéticos. As ameaças impostas por ataques cibernéticos agora encabeçam a lista das maiores ameaças à segurança nacional e econômica na maioria dos países, sinalizando a importância da cibersegurança e salientando o seu crescimento.

Além da segurança nacional, empresas, indústrias e usuários comuns também são alvos de ataques e podem sofrer com o cibercrime. Para mitigar essas situações é interessante que todos tenham o básico de conhecimento sobre segurança cibernética e os riscos que os cibercriminosos podem oferecer. Tendo noção dos perigos cibernéticos, os usuários de dispositivos tecnológicos tornam-se mais conscientes e seguros diante dos riscos que podem enfrentar. Logo trabalhos de pesquisa e iniciativas educacionais como este minicurso são maneiras de conscientizar os usuários e partilhar o conhecimento sobre a área.

Diante do cenário atual, o profissional Pentester e empresas de segurança cibernética passam a ser muito requisitados na busca por vulnerabilidades e potenciais ameaças que podem comprometer os usuários ou clientes envolvidos com sistemas e informações.

### **1.5. O PenTest**

O termo PenTest é derivado de Penetration Test, em português a melhor tradução seria Testes de Intrusão ou de Invasão é um conjunto de técnicas e ferramentas utilizadas para identificar falhas de segurança em sistemas e redes corporativas. Através dessas técnicas, o profissional Pentester irá identificar as vulnerabilidades existentes na arquitetura da empresa, explorá-las e entregar um relatório à empresa, que deverá então tomar as devidas ações para corrigir as falhas de segurança.

Apesar de ser uma simulação de um ataque hacker, é importante mencionar que o PenTest é uma atividade profissional e sobretudo ética. Uma empresa contrata esses serviços para ter seus sistemas analisados por uma empresa ou profissional qualificado.

### **1.6. Profissão**

Um Pentester é um profissional com elevados conhecimentos em diversas áreas da computação, principalmente em sistemas operacionais, redes de computadores e segurança da informação. Ele faz uso de aplicativos e ferramentas para explorar vulnerabilidades e busca identificar quais tipos de informações podem ser obtidas por meio dessa falha. Esse Profissional também é chamado de Auditor Pentest e até mesmo de Ethical Hacker (hacker ético).

As empresas que contratam o serviço de pentest podem escolher diferentes tipos de análise que são White Box, Black Box e Gray Box. Cada tipo de análise possui suas características e podem ser aplicadas de acordo com a estratégia e o objetivo da análise pentest.

Na análise White box o profissional ou empresa responsável pelo pentest recebem dos contratantes as informações e acessos privilegiados como versões de aplicativos, mapa da rede, acesso físico e lógico aos sistemas e rede alvos.

O Black box é uma estratégia totalmente oposta ao White Box, onde o Pentes-

ter não recebe nenhuma informação ou acesso privilegiado do alvo tornando a tarefa de descobrir vulnerabilidades e pontos de acesso mais realista e próximo de um real ataque hacker. Algumas empresas usam esta abordagem para validar sua própria resposta a incidentes de segurança.

Por fim, a estratégia Gray box é uma mistura das duas estratégias citadas acima (White Box e Black Box), em que o Pentester possui algumas mas não todas informações e acessos. Na grande maioria das vezes essas informações recebidas são afirmadas durante a contratação do serviço.

## 1.7. Fases do Pentest

A análise Pentest é dividido em fases. Esta seção aborda as principais fases para a realização de pentest.

**Reconhecimento:** Nesta fase a equipe de Pen Testers realizam o levantamento detalhado de informações possíveis sobre a empresa analisada. São documentadas algumas informações, como por exemplo : ramo de atuação, existência de filiais ou empresa associadas a ela, serviços prestados, endereço físico (se houver), além de nome e e-mails de profissionais que ocupam cargos altos, como gerentes e diretores. . Essas informações ajudarão o Pentester a observar em quais locais e serviços ele deve focar para encontrar vulnerabilidades.

**Varredura:** Nesta fase é realizada uma varredura do que está presente na rede. Por exemplo, a faixa de IPs, quais os servidores existentes, os sistemas operacionais utilizados, as portas abertas, entre outros.

**Obtenção de Acesso e Exploração:** Com base no que foi identificado na fase de varredura, nesta fase cada item deverá ser analisado e explorado, isto é, efetivamente identificar e explorar as vulnerabilidades existentes. Utilizando técnicas e ferramentas identifica-se os serviços vulneráveis e que tipo de informação, falhas ou controles podem ser obtidos através daquele serviço.

**Obtenção de Evidências e Reporte:** As evidências de todas as falhas e vulnerabilidades identificadas são coletadas pela equipe. Com base nessas informações, através de um relatório, a equipe irá mostrar todos os possíveis prejuízos que a empresa pode ter com cada tipo de vulnerabilidade.

## 1.8. Vulnerabilidades

Vulnerabilidades são descritas como qualquer fraqueza ou brecha em sistemas, redes, processos que podem ser explorados e comprometerem de alguma forma o estado natural das coisas ou violarem regras/políticas de segurança. As vulnerabilidades podem ser encontradas em software, hardware e também em pessoas, que podem ser influenciadas pelo atacante a realizarem ações que contribuam para um ataque através de engenharia social.

Quando uma vulnerabilidade encontrada não é de conhecimento do fornecedor do hardware ou do software esta é rotulada como vulnerabilidade **zero-day**. Na maioria das vezes a vulnerabilidade é explorada por um longo tempo podendo até ser comercializada

por empresas fachadas e grupos de interesses no mercado negro.

Até que a organização e a equipe de desenvolvedores atuem no desenvolvimento de um solução para a vulnerabilidade, esta pode ser explorada por qualquer um que detenha da informação e do código de exploração (exploit). Mesmo após lançado a solução para a vulnerabilidade, muitos usuários optam por não atualizaram e receberem a correção, ficando vulneráveis a ataques.

Indústrias e setores empresariais estão entre os principais usuários de software desatualizados. Como esses grupos de usuários devem manter suas máquinas e sistemas sempre operando acabam por não realização os patches (atualizações de software), pois geralmente são frequentes e demoradas, além de que mudanças podem ocasionar o mal funcionamento de algo. Por essas razões as empresas costumam não atualizar os software tornando-se mais suscetíveis a ataques.

Durante o minicurso será explicado e demonstrado vulnerabilidades presentes em softwares comuns e usuais como por exemplo às vulnerabilidades presentes no software Adobe Reader v9.3.4 (*CVE-2010-2862 e CVE-2010-1240*) e em sistemas operacionais como no caso da vulnerabilidade (*CVE-2017-0144*) presente no protocolo SMB (*Server Message Block*) do Windows e precursor do famoso ataque Wannacry.

Também será relacionado vulnerabilidades com ataques famosos a indústria e aos usuários de computadores no geral. Enfatizando como pequenas vulnerabilidades podem afetar um grande número de usuários e causar danos a estruturas críticas essenciais a uma sociedade.

## **1.9. Ferramentas**

Nesta seção são abordadas algumas das principais ferramentas utilizadas pelos profissionais de Pentest no teste de intrusão, e que também serão usadas durante o minicurso.

### **1.9.1. Nmap**

O Nmap ou (Network Mapper) é uma ferramenta de licença aberta para mapear e auditar redes utilizando pacotes IP e determinar quais hosts estão disponíveis na rede, quais serviços (nome do aplicativo e versão) esses hosts estão oferecendo, quais sistemas operacionais (e versões do sistema operacional) estão executando, entre outras funcionalidades. Esse procedimento é mais conhecido como varredura ou scanning.

É comum os profissionais que utilizam a ferramenta Nmap usarem o modo "linha de comando" para trabalhar, portanto é a forma que abordada durante o minicurso. Há uma interface gráfica para a ferramenta Nmap chamada "Zenmap" que pode também ser utilizada com o mesmo propósito.

A ferramenta Nmap disponibiliza várias maneiras de realizar varreduras de portas, que variam de acordo com o nível de detalhamento necessário para a coleta de informações. Quanto maior o nível de detalhamento desejado mais são as chances da busca ser identificada e bloqueada.

Esta ferramenta pode ser muito útil para identificar quais recursos estão ativos e com portas abertas e então protegê-las ou elaborar ou utilizar um exploit para realizar a

exploração na tentativa de conseguir ter acesso ao alvo.

*Principais comandos:*

- nmap 192.168.2.2 = Análise de um host.
- nmap -p 80 192.168.2.2 = Análise de um host na porta 80.
- nmap teste.com = Análise de um domínio.
- nmap -v 192.168.2.0/24 = Análise de uma rede de 255 endereços com método verbose.
- nmap -O 192.168.2.2 = Detecta o sistema operacional do alvo.
- nmap -sv 192.168.2.2 = Analisa as versões dos serviços que estão disponíveis nas portas abertas.

### **1.9.2. NetCat**

O Netcat é uma ferramenta de licença aberta que lê e envia dados através de conexões de rede, usando o protocolo TCP/IP. Sua função é proporcionar um ambiente de conexão com serviços via texto.

Com o netcat é possível se conectar a qualquer endereço IP e Porta que estejam abertos e aceitem conexão e assim podendo enviar para o serviço em questão, comandos via texto. Se os comandos passados fazem parte do protocolo que o serviço opera as informações enviadas são interpretadas e executadas assim ocorrendo a comunicação. Hackers e profissionais da área de segurança costumam chamar a ferramenta netcat de canivete suíço diante das infinidades de formas de uso e funcionalidades que cooperar em uma análise ou ataque.

A sua principal interface é por linha de comando. Existem versões da ferramenta para todos os principais sistemas operacionais (Windows, Linux, Mac OS), tornando o uso da ferramenta mais acessível a diversidade de cenários.

*Principais Comandos:*

- netcat host port = Conectar a um host/domínio na porta especificada.
- netcat -l 4444 = Escutar conexões TCP na porta 4444.

### **1.9.3. Metasploit Framework:**

É um projeto de Segurança da Informação com a finalidade de análise de vulnerabilidades de segurança em plataformas, servidores e em sistemas operacionais, além de facilitar testes de invasão (pentests) e no desenvolvimento de assinaturas para Sistemas de Detecção de Intrusão (IDS).

Com o Metasploit é possível realizar testes de invasão (pentests). É possível fazer desde uma varredura mais simples até uma análise ou invasão mais completa, explorando vulnerabilidades em programas instalados.

Possui duas versões: uma comercial e outra gratuita. Utilizaremos a versão gratuita instalada por padrão no Kali Linux.

Quase todas as interações feitas com o Metasploit são através de módulos, que são pequenos softwares que podem ser usados pelos metasploit.

*Os tipos de módulo são:*

- Exploits (“modules/exploits”) = São definidos como módulos que utilizam payloads.
- Auxiliares (“modules/auxiliary”) = Incluem port scanners, fuzzers, sniffers e outros.
- Payloads (“modules/”) = Consiste em um código que executa remotamente.
- Encoders (“modules/encoders”) = Garantem que payloads cheguem ao seus destinos intactos.
- Nops (“modules/nops”) = Mantém o tamanho dos payloads consistente.

*Principais Comandos:*

- msfconsole = Inicializar o Metasploit em modo console.
- search = Buscar por um exploit, vulnerabilidade (CVE), Sistemas Operacionais.
- show = Utilizado para mostrar as opções, este comando pode ser utilizado com outros parâmetros, por exemplo:
  - show options = Mostrar as opções disponíveis a partir de um exploit definido.
  - show targets = Mostrar os alvos vulneráveis a partir de um exploit definido .
- set LHOST = Definir o Domínio/Máquina Local (IP\_Atacante).
- set LHOST = Definir a Máquina Remota (IP\_Vítima).
- use = Comando para utilizar um exploit, por exemplo:
  - use auxiliary/scanner/smb/smb\_ms17\_010.
- run ou exploit = Executa um exploit definido .
- help = Mostra uma lista dos comandos principais do metasploit e suas descrições.
- msfupdate = É utilizado para atualizar o Metasploit com as últimas versões dos exploits.
- search name:”module name” type:”module type” = Utilizado para procurar módulos dentro do Metasploit. Ex:msf > search name:microsoft type:exploit

- info “module path” = Mostra as informações sobre um módulo específico. Ex: info auxiliary/admin/http/iis\_uth\_bypass

**Exploit:** Os Exploits são um subconjunto de programas maliciosos (*malwares*). Programas maliciosos com dados ou códigos executáveis capazes de aproveitar as vulnerabilidades de sistemas em um computador local ou remoto.

**Ativos:** Exploram um host específico, executam até completar e então saem.

**Passivos:** Aguardam pela entrada de hosts e os exploram assim que eles se conectam. Na maioria das vezes focados em clientes como browsers, clientes FTP, etc.

**Payload:** São scripts utilizados para interagir com o sistema invadido. São divididos em três grupos.

**Singles:** Realizam uma tarefa simples no sistema invadido, como por exemplo, abrir um programa, criar um arquivo. Ex.: “windows/shell bind tcp”

**Stagers:** Configuram uma conexão de rede entre o atacante e a vítima. Ex.: “windows/shell/bind tcp”

**Stages:** São componentes transferidos pelos Stagers que podem proporcionar recursos avançados ao atacante. Ex.: Meterpreter, VPNInjection. Ex.: “windows/shell/bind tcp”

**Meterpreter:** Meterpreter é um payload que utiliza stagers de injeção de DLL na memória. Ele se comunica através do socket do stager e fornece uma API client-side Ruby.

## 1.10. Prática e exploração de vulnerabilidades

Nesta seção apresenta-se na prática como utilizar as ferramentas de Pentest para explorar algumas vulnerabilidades. Essas práticas objetivam conscientizar sobre alguns perigos das vulnerabilidades e da importância do estudo de segurança cibernética para prevenir ataques.

### 1.10.1. Exploração de Vulnerabilidades em Sistemas Operacionais

Para demonstrar como ocorre uma exploração de vulnerabilidades em Sistemas Operacionais é utilizado o sistema operacional Windows 7 Home Premium SP1 que possui uma vulnerabilidade crítica no protocolo de comunicação e compartilhamento de arquivos remoto SMB (Server Message Block).

O código de exploração (exploit) EternalBlue é elemento de um conjunto de programas secretos revelados pelo grupo Shadow Brokers em 14 de abril de 2017 e foi utilizado no ciberataque mundial com o ransomware WannaCry e o malware Adylkuzz. O código explora uma vulnerabilidade do Microsoft Windows, mais precisamente na implantação do protocolo Server Message Block, que permite compartilhamento de arquivos que quando relacionado a ataques malware, pode ajudar na disseminação do malware entre as máquinas da rede.

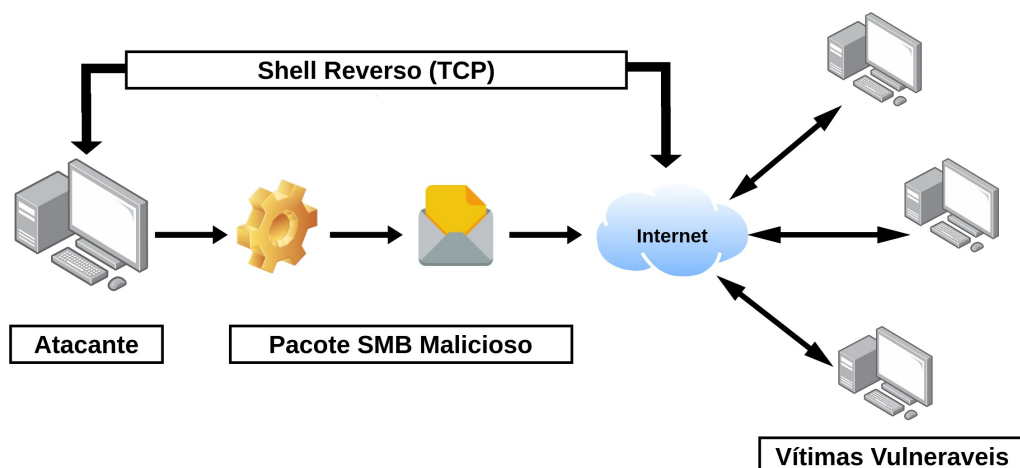
A vulnerabilidade foi categorizada como CVE-2017-0144 e está presente em várias versões do sistema operacional Windows. Sua exploração consiste no envio de um pacote malicioso especialmente criado e não autenticado ao servidor SMBv1 alvo. A atualização de segurança resolve a vulnerabilidade, corrigindo a maneira como o SMBv1



lida com essas solicitações.

CVE-2017-0144: O servidor SMBv1 no Microsoft Windows Vista SP2; Windows Server 2008 SP2 e R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold e R2; Windows RT 8.1; e Windows 10 Gold, 1511 e 1607; e o Windows Server 2016 permite que atacantes remotos executem código arbitrário por meio de pacotes criados, também conhecido como "Vulnerabilidade de execução remota de código do Windows SMB". - (MITRE)

Como já abordado a exploração desta vulnerabilidade acontece através de um arquivo PDF malicioso criado pelo atacante. A Figura 1.1 demonstra intuitivamente como acontece a exploração. A máquina atacante ou hacker manipula através da ferramenta Metasploit um pacote SMB inserindo o exploit responsável por explorar a vulnerabilidade na vítima, o pacote é enviado para a vítima na porta do serviço SMB vulnerável ocorrendo a execução do exploit e do payload "shell reverso" responsável por disponibilizar o shell da vítima na máquina atacante.



**Figura 1.1. Exploração da vulnerabilidade no protocolo SMB do Windows através de um pacote SMB malicioso.**

### 1.10.2. Exploração de Vulnerabilidades em Software

Para demonstrar como ocorre uma exploração de vulnerabilidades em softwares é utilizado o software leitor de arquivos PDF Adobe Reader versão 9.3.4 que possui duas vulnerabilidades críticas, sendo uma delas possível de realizar a exploração remota por meio de arquivos PDF maliciosos.

A fim de contextualizar os perigos presentes em vulnerabilidades de software, foi selecionado o Adobe Reader que é um dos famosos de leitores de arquivos PDF e, é amplamente utilizado por usuários de todos os tipos, inclusive em ambientes empresariais/industriais. Vulnerabilidades deste tipo, podem por em risco a segurança de computadores e redes, podendo ser o caminho perfeito para um ataque hacker.

A empresa Adobe emitiu em agosto de 2010 um boletim de segurança que reporta vulnerabilidades presentes no software Adobe Reader versão 9.3.4 e anteriores permitindo que arquivos PDF maliciosos consigam executar códigos arbitrários remotamente. As

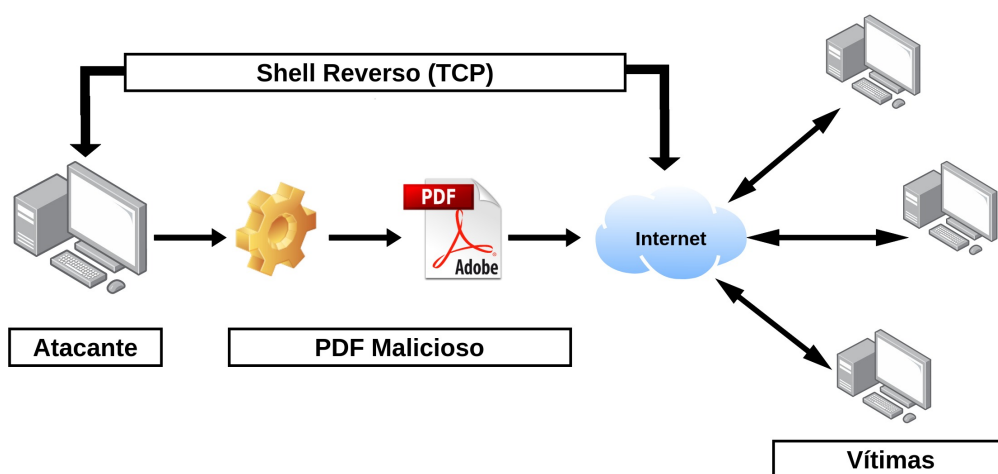
vulnerabilidades citadas foram categorizadas como CVE-2010-2862 e CVE-2010-1240, melhores descritas a seguir.

CVE-2010-2862: "Estouro de inteiro no CoolType.dll no Adobe Reader 8.2.3 e 9.3.3 e no Acrobat 9.3.3 permite que atacantes remotos executem código arbitrário por meio de uma fonte TrueType com um grande valor max Composite Points em uma tabela Maximum Profile (maxp).- (MITRE).

CVE-2010-1240: "O Adobe Reader e o Acrobat 9.x anteriores a 9.3.3 e 8.x anteriores a 8.2.3 no Windows e Mac OS X, não restringem o conteúdo de um campo de texto na caixa de diálogo de aviso Iniciar arquivo, o que facilita para os invasores remotos para induzir os usuários a executar um programa local arbitrário que foi especificado em um documento PDF, conforme demonstrado por um campo de texto que afirma que o botão Abrir permitirá que o usuário leia uma mensagem criptografada.- (MITRE)

O exploit responsável por explorar esta falha "adobe\_cooltype\_sing" já é público na Internet e incluído nas maiorias das ferramentas de exploração como o metasploit. Junto ao exploit pode ser inseridos programas como "shell reverso" ou algum executável, e programas são conhecidos como "payloads". Para a prática de exploração no minicurso será utilizado um payload muito conhecido chamado "reverse\_shell\_tcp" que abre uma conexão da máquina vítima para a máquina atacante, disponibilizando para o hacker o shell da vítima.

Como já abordado, a exploração desta vulnerabilidade acontece através de um arquivo PDF malicioso criado pelo atacante. A Figura 1.2 mostra intuitivamente como acontece a exploração. A máquina atacante ou hacker manipula através da ferramenta Metasploit um arquivo PDF inserindo o exploit responsável por explorar a vulnerabilidade na vítima, o arquivo depois de manipulado é enviado para as vítimas que ao abrirem o arquivo PDF malicioso com o software vulnerável executam o exploit e assim executam payload responsável por disponibilizar o shell da vítima na máquina atacante.



**Figura 1.2. Exploração da vulnerabilidade no software Adobe Reader por meio de um arquivo PDF malicioso.**

### 1.11. Pós-Exploração

Trata-se de uma técnica utilizada logo após o atacante ter acesso a máquina da vítima, e com a utilização de algumas ferramentas, pode-se ir mais a fundo e descobrir o máximo possível de informações do alvo e da rede interna, e fazer entre outras coisas na máquina alvo, como por exemplo: escrever arquivos, ver a versão do sistema operacional explorado, o IP da máquina, e muito mais coisas que vai da criatividade no caso do invasor, que pode inclusive instalar um backdoor na máquina da vítima para depois quando a mesma for desligada, o atacante ainda ter acesso total ao sistema infectado.

No minicurso iremos mostrar apenas alguns comandos utilizados através do **meterpreter** (um payload). Ele primeiro manda um pequeno executável para a vítima que será o responsável por se comunicar com a estação do atacante e pegar o resto das instruções a serem executadas.

*Principais Comandos:*

- **download:** O comando 'download' faz o download de um arquivo da máquina remota. Observe o uso das barras duplas ao fornecer o caminho do Windows. Ex:  
`download c:\boot.ini`
- **execute** = O comando 'execute' executa um comando no destino.
- **idletime** = A execução de 'idletime' exibirá o número de segundos que o usuário na máquina remota ficou ocioso.
- **ipconfig** = O comando 'ipconfig' exibe as interfaces de rede e endereços na máquina remota.
- **ls** = Como no Linux, o comando "ls" listará os arquivos no diretório remoto atual.
- **migrate** = Usando o módulo de postagem 'migrar', você pode migrar para outro processo na vítima.
- **Ps** = O comando 'ps' exibe uma lista de processos em execução no destino.
- **enumdesktops** = Mostra quantos desktops ativos a vítima tem.
- **getdesktop** = Mostra qual é o desktop atual onde o Meterpreter está sendo executado.
- **keyscan\_dump** = Mostra o que foi capturado com o keylogger.
- **keyscan\_start** = Inicia o keylogger.
- **keyscan\_stop** = Para o keylogger.
- **screenshot** = Tira uma foto do desktop remoto.
- **setdesktop** = Muda para outro desktop, se a máquina remota tiver mais que um.

### 1.11.1. Técnicas não convencionais

Muitas vezes diante de um procedimento de invasão ou exploração de vulnerabilidades o atacante não encontram maneiras convencionais de acessar remotamente um determinado dispositivo, pois nem sempre serviços como SSH, FTP ou execução de payloads estão disponíveis no nível de privilégio que o atacante se encontra. Por isso, um excelente profissional de segurança detém de várias técnicas muitas das vezes não convencionais para acessar dispositivos e ambientes.

Nesta seção aborda-se uma técnica não convencional de comunicação remota entre duas máquinas, esta tarefa terá auxílio da ferramenta Netcat realizar uma conexão entre as máquinas em uma determinada porta. O objetivo da atividade é direcionar o shell da máquina alvo para a máquina atacante (KaliLinux), podendo a máquina atacante executar comandos no shell da máquina alvo remotamente.

A Figura 1.3 mostra um exemplo de ataque não convencional utilizando a ferramenta Netcat para realizar uma conexão reversa entre máquinas envolvidas.

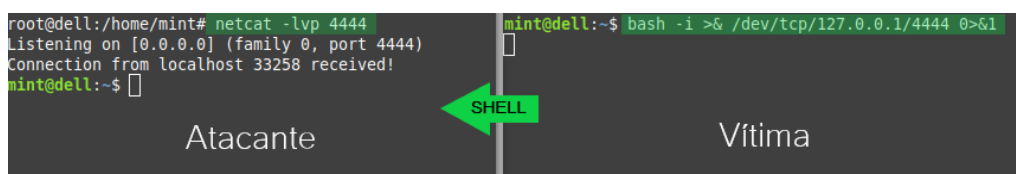


Figura 1.3. Shell Reverso com Netcat