ESTGF | POLITÉCNICO DO PORTO

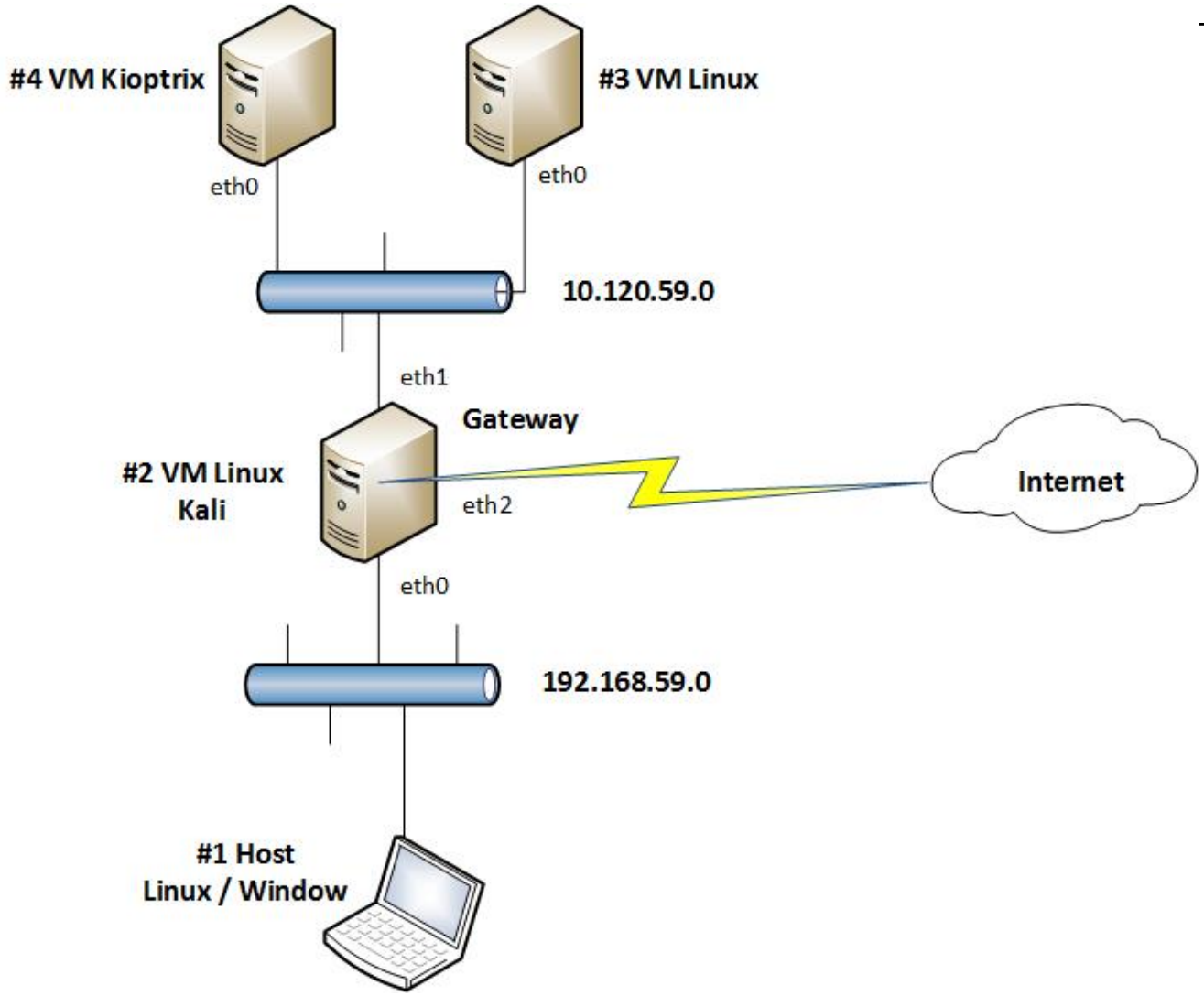
LICENCIATURA EM SEGURANÇA INFORMÁTICA EM REDES DE COMPUTADORES

SEGURANÇA DE REDES

Trabalho Prático 1

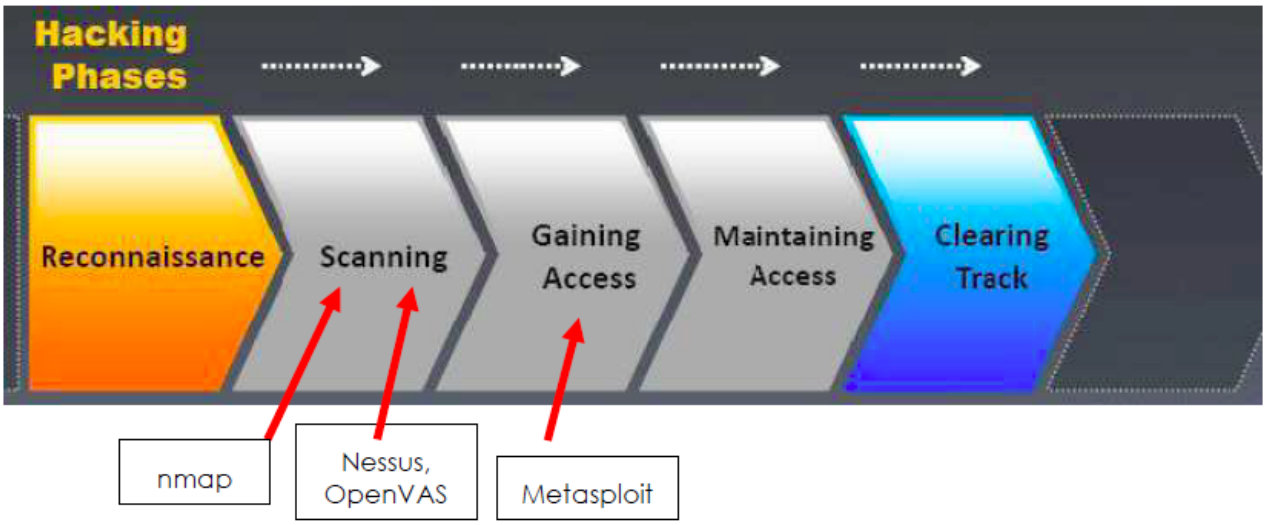
Análise de Vulnerabilidades

Construção de laboratório de Testes



1) Montar o cenário indicado.
2) Validar e documentar conectividades entre todas as máquinas.
   a) Comandos uteis.
      i) route add xx.xx.xx.xx mask xx.xx.xx.xx xx.xx.xx.xx
      ii) route add -net xx.xx.xx.xx/xx gw xx.xx.xx.xx
      iii) ifconfig eth0 xx.xx.xx.xx netmask xx.xx.xx.xx up
      iv) apt-get install <nome>.
      v) cat /proc/sys/net/ipv4/ip_forward
      vi) echo 1 > /proc/sys/net/ipv4/ip_forward
3) Validar e garantir funcionamento da gateway, incluindo o acesso à internet das máquinas #3 e #4.

4) Usando a máquina #2, analise o tráfego.
   a) Use o tcpdump, ou wireshark.
   b) Comprove a conectividade entra as várias máquinas usando um dos sniffers. Documente.
   c) Instale o serviço ftp na máquina #3 e use o serviço a partir da máquina #1. Detecte o user e a password a partir da máquina #2.
   d) Valide a existência do serviço ssh e telnet na maquina #3.
   e) Verifique e documente todo o fluxo de dados de uma ligação telnet e ssh.
   f) Determine as diferenças entre esses dois serviços.
   g) A partir de uma máquina com acesso à internet valide e documente a diferença entre um acesso http e acesso https.



5) Instalar a ferramenta nmap (http://nmap.org/man/pt_PT)
   a) Procure as portas abertas em todas as máquinas.
   b) Use o nmap para tentar detetar os sistemas operativos das máquinas.
6) Nessus (http://www.tenable.com): é uma ferramenta de análise de vulnerabilidades bastante interessante e de baixo custo que permite realizar uma análise de segurança a máquinas remotas (desde activos de rede a servidores e desktops). Outra referência é o SAINT (http://www.saintcorporation.com/), mas apenas existe em versão comercial. O Nessus agora é uma ferramenta paga, mas no momento em que a versão grátis deixou de existir apareceu uma ferramenta derivada (fork) do Nessus chamada de OpenVAS (http://www.openvas.org/) sendo indicado que a ultima versão realiza mais de 20000 testes.
   a) Ler a documentação sobre a ferramenta de scanning de vulnerabilidades Open VAS,

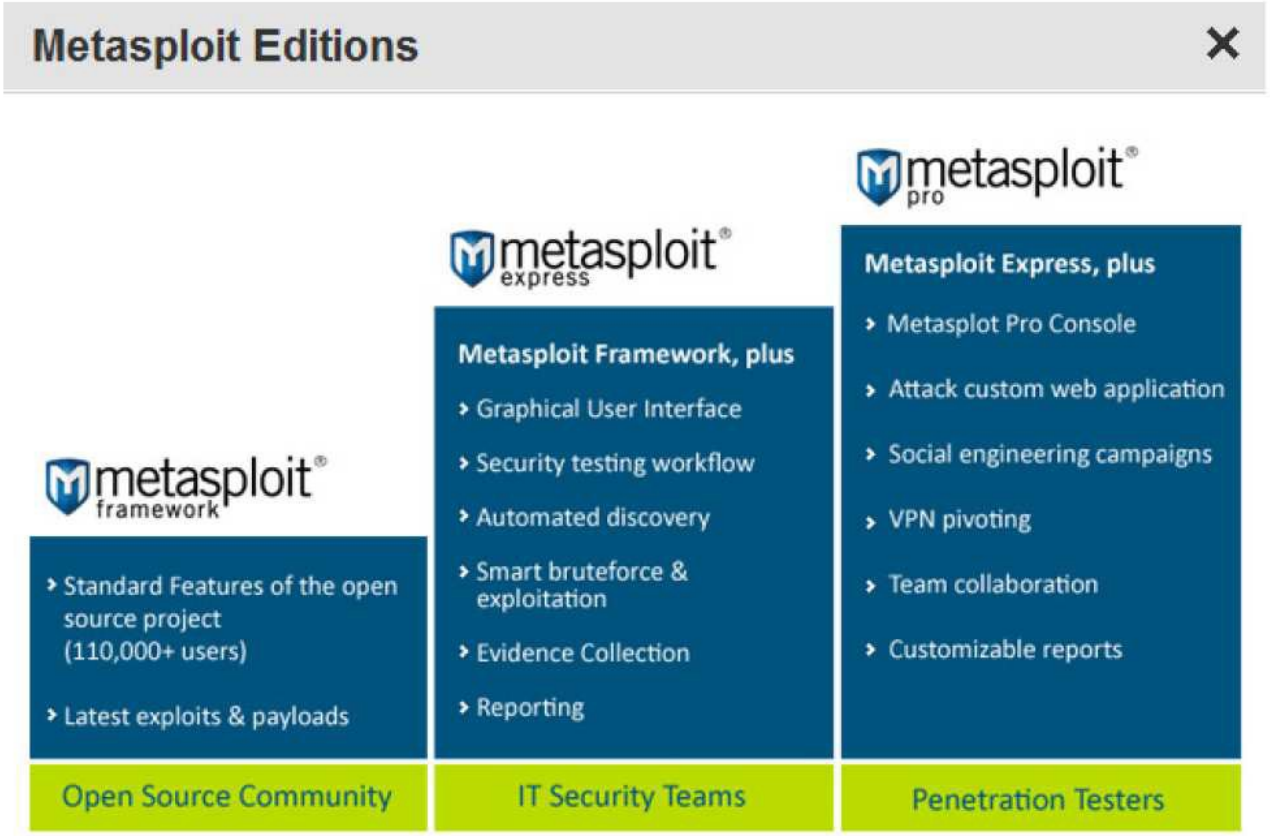
b) Documentar como instalar no nosso ambiente de laboratório.

c) Instalar.

d) Usar ferramenta nas máquinas do lab.

e) Elaborar documento com resultados de vulnerabilidades.

7) Metasploit: é um Framework para testes de penetração em redes informáticas. Esta ferramenta, com variante gratuita, é uma referência na análise de vulnerabilidades. A grande diferença em termos funcionais para as anteriores é que permite também a exploração das vulnerabilidades encontradas.



Nota: Consultar site http://nmap.org, onde existe uma lista exaustiva de ferramentas de segurança para todas fases já mencionadas e links úteis para download.

Info adicional sabre ferramentas:

Function	Tool	TorunonOS	Cost	Download from
Network Scanning	SuperScan	Windows	Eval is Ftee	http:l!www.foundstone.com/rdlabsltennsofuse.php?filenam e=sul!erscan.exe
	Nmap	Linux	Free	http://www.nmap.o
	NmapNT	Windows	Free	htt :l/www.
	Pinger	Windo'W!:	Free	hU.Q:/fvicu:Ucoft.ne-Mnai1.nt/Qin@./
	Netcat	Linux!Windows	Free	http://www.packetstormsecurity.org/ >search for netcat
	Strobe	Linux!Windows	Free	http:l!www.luyer.nel lsoftware/strobe -classb/
	Nessus	Linux!Windows	Free	httn:l/www.nessus.or
	udpflooder	windows	Free	http:l!www.foundstone.cotnlknowledge/tennsofuse.hbnl? fl1 enarne=udpflood.zip
	Netcat	Linux!Windows	Free	htt:l/www.atstake.com!research/tools/ncl l0.tgo http:l!www.atstake.com/resea rcMools/ncll nt.zip
Routing	NeoTrace	Windows	Eva!is free	htt :l/www.neoworx.com/downloadldownload.asl!?eroduct =Neo Trace
	Visual Route	Windows	Eva!is free	httn:llwww.vi sua!route.com/
Network Sniffers	Network Monitor	Windows	Builht	Included inNT4/2000 (full version in SMS 2.0)
	SMS2.0	Windows	Eva!is *$14.95*	htt :l!ww
	Tcpdump	Linux	Free	htt :l/www.
	Windump + WinPc3p	Windows	Free	http:l!netgroup -serv.pol&o.iVwindump/instalVdefault.htm
Password	LOphtLC3	Windows	Eva!is free	htt :l/www.
	Crack5.0	Linux	Free	ft :l/sunsite.cnlab switch.chlmirror/OpenBSD/snapshots/packages/i386/crack
	John the Ripper	Linux!Windows /DOS	Free	htte:l/www.oeenwall.com/jo hn
	Snadboy	Windows	Free	htt :l/www.
Trojans	Netbus	Windows	Free	htto:llhome.t- online.delhome/TschiTschiln etbus.htm
	SubSeven	Windows	Free	htto:llwww.sub7.*orflf*
Forensics	NTFSDOS Read-only	MSDOSboot disk	Eva!is free	htte:Jlwww.s sintemals.
KeyBoard Logging	Keylogger	Hardware (any OS)	$139 (one per class only)	htt :l/www.
	Keyboard Logger	Hardware (any OS)	$189 (one per class only)	htt :llwww.
	Klogger	Windows	Free	htt :llntsecuritj1.nultoolboYJklogger/
Inttusi.on Detection	Internet Scanner6	Windo	Ft'ee	Included with the WindoW!: 2000 Server Re::ource Kit
	Snort	Linux!Windows	Free	htto:llwww.snort.orf!/
	IDScenter	Windows	Free	htto:llnet-securitv.orf!/csti.binlfile.c2i?idscenter.:tio
Fitt:l'WC:ills	Ch•t.:kPuinL Firewall-!	NT 4.0 3t< v'" with SP4 min.	$14 00 apprux. (one per class only)	*hLLp.flwww*.cuttuuk.cum - tCUUJUlt!!U.lt:d. fut Checkpoint, chooseCPFW -F1G *-250,* obtain license for 172.17.10.1 (Inakuot.or Ma.ohino1).
	!SA Server onnn	Windows 2000 "D1	Eva!is Free	http:llwww.microsoft.comlisaserver/evaluatiollltrial/default.