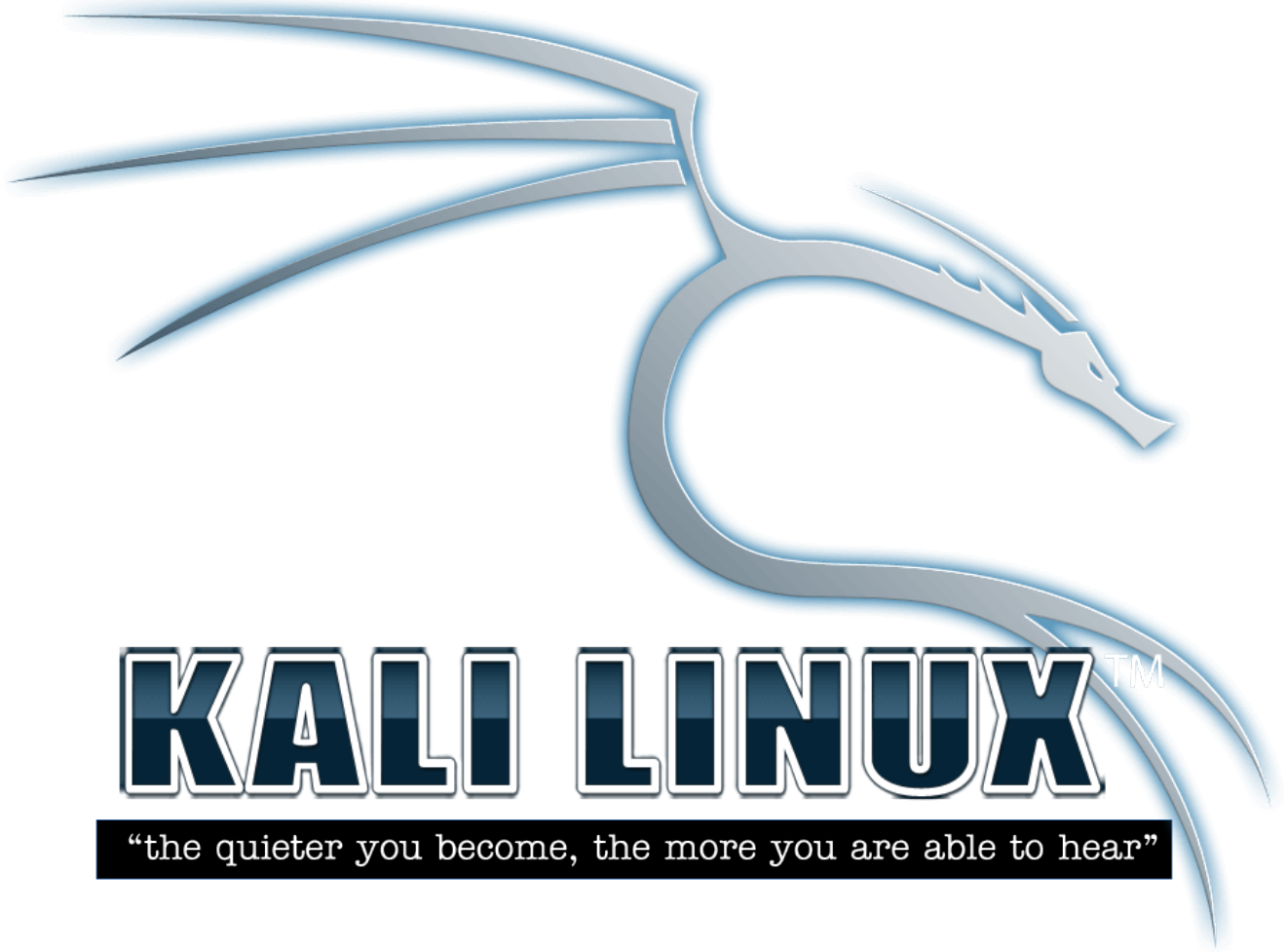
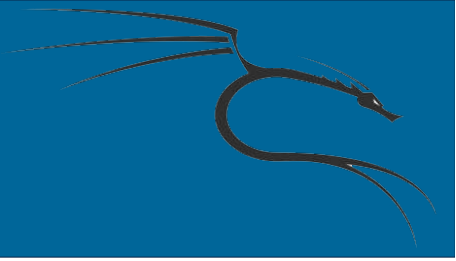
Pentest com Kali Linux





Instrutor:Vitor Mazuco

http://facebook.com/vitormazuco

Email:vitor.mazuco@gmail.com

WebSite:http://vmzsolutions.com.br

Tipos de dorks para buscas

Segue exemplos abaixo de alguns tipos de dorks:

Buscando senhas em arquivos de Anotações/Banco de Dados/Servidores:

- # intitle:”index of /” password.txt
- # filetype:txt + senha + com.br
- # filetype:txt intext:senha
- # intext: charset_test = email = default_persistent
- # inurl: / wwwboard / passwd.txt
- # filetype: log inurl: “password.log”

Tipos de dorks para buscas

- # filetype: conf inurl: proftpd.conf-sample
- # filetype: bak inurl: “htaccess | passwd | shadow | htusers”
- # outlook filetype: pst

Buscando backup de configurações de CMSs

- # filetype: inurl sql: wp-conten t / Backup-*
- # intext:”~~Joomla1.txt” title:”Indexof /”
- # configuration.php_ “<?phpclass Jconfig{“
- # inurl:wp-config.old
- # inurl:configuration.php.bkp

Acesso a impressora remotas

- # intitle:”Web Image Monitor” & inurl:”/mainframe.cgi”

Buscando câmeras/webcams disponíveis na internet:

- inurl:”inurl:/view.shtml”
- inurl:”inurl:ViewerFrame?Mode=”
- inurl:”intitle:”Live View / – AXIS” | inurl:view/view.shtml^”
- inurl:”inurl:ViewerFrame?Mode=Refresh”
- inurl:”inurl:axis-cgi/jpg”
- inurl:”inurl:axis-cgi/mjpg (motion-JPEG)”
- inurl:”inurl:view/indexFrame.shtml”

Buscando câmeras/webcams disponíveis na internet:

- inurl:”inurl:/view.shtml”
- inurl:”inurl:ViewerFrame?Mode=”
- inurl:”intitle:”Live View / – AXIS” | inurl:view/view.shtml^”
- inurl:”inurl:ViewerFrame?Mode=Refresh”
- inurl:”inurl:axis-cgi/jpg”
- inurl:”inurl:axis-cgi/mjpg (motion-JPEG)”
- inurl:”inurl:view/indexFrame.shtml”

Tipos de dorks para buscas

- inurl:”intitle:”Live View / – AXIS””
- inurl:”intitle:”Live View / – AXIS 206M””
- inurl:”intitle:”Live View / – AXIS 206W””
- inurl:”intitle:”Live View / – AXIS 210″”
- inurl:”inurl:indexFrame.shtml Axis”
- inurl:”inurl:”MultiCameraFrame?Mode=Motion””
- inurl:”intitle:start inurl:cgistart”

Tipos de dorks para buscas

- inurl:”intitle:”WJ-NT104 Main Page””
- inurl:”intext:”MOBOTIX M1″ intext:”Open Menu””
- inurl:”intext:”MOBOTIX M10″ intext:”Open Menu””
- inurl:”intext:”MOBOTIX D10″ intext:”Open Menu””
- inurl:”intitle:snc-z20 inurl:home/”
- inurl:”intitle:snc-cs3 inurl:home/”
- inurl:”intitle:snc-rz30 inurl:home/”
- inurl:”intitle:”netcam live image””

Tipos de dorks para buscas

- inurl:”intitle:”sony network camera snc-p1″”
- inurl:”intitle:”sony network camera snc-m1″”
- inurl:”site:.viewnetcam.com -www.viewnetcam.com”
- inurl:”intitle:”Toshiba Network Camera” user login”

Tipos de dorks para buscas

Existem diversas listas de dorks para cada tipo de serviço que verifica as vulnerabilidades diferentes, basta usar o próprio Google para encontrar o tipo de busca que deseja procurar.

Vale lembrar que: **isso não é um invasão pois os dados,** pois estão aberto para acesso, mas a forma que você utiliza essa informação (**white/black hat**) é o que vai determinar se é um crime ou não.