
DICIONÁRIO HACKER
Nível: Básico
The Cybers Team
A pior falha do sistema é ser criado pelo ser humano!

# Sumário:

Sobre: O projeto surgiu através de uma livestream do youtuber "MC Hackudão", em que foi criado um podcast onde os inscritos e audientes que houvessem dúvidas em significados de palavras ou contextos, comentavam e assim eram respondidas no decorrer da stream . A iniciativa tende ao público iniciante no qual poderá ser discutido idealidades de significados a partir de cada opinião formalizada de ideal.


Autores:
Mitiny / offset


**Participação especial:**

**Ghost Dork**
**R3act0r**
**Grosche**
**Hacker Chapadão**
**Hacking @Root**
**Heisenberg**
**Lucky Wolf**
**Lysider**
**Paulo Henrique**
**Thiago Duarte**

Nota: o Dicionário está de forma bem resumida e contendo poucas **palavras, pois como na capa mesmo condiz é o básico , fizemos assim pois pensamos em lançar outras futuras versões dependendo do rendimento e avaliação dessa inicialização.**

**Foi catalogado com as seguintes cores para categorizar cada tópico:**

- De finalidades de intenção maléfica ou prejudicial.
- De Finalidades de intenção benéfica ou benéfico.
- De Finalidades de intenção neutra.

Atenção: Este book poderá passar por atualizações e evolução, portanto verifique qual a última data de atualização neste link: http://pastebin.com/uF1ixfLV

**Qualquer dúvida ou questionamento de respostas entre em contato que para próxima edição será deixado seu determinado crédito, e será efetuado tal correção.**

**A formatação de páginas está de forma de impressão, então qualquer bug visual no Pdf poderá ser corrigido a partir da impressão.**

# A

**Adware:** O termo (Ad) vem de adsense e (Ware) de malware. Como o próprio nome condiz, é um malware que tem como principal função exibir propaganda indesejada a sua vítima, seja em forma de pop-up ou unclosable window, para que o atacante ganhe dinheiro com os anúncios.

**AES:** A sigla AES é uma abreviação do termo Advanced Encryption Standard, que traduzido para o português significa Padrão de Criptografia Avançada Ele é um algoritmo utilizado para a criptografia de chave simétrica ou outros algoritmos que seguem o padrão de criptografia de segurança em transmissão e armazenamento de dados.

**Anti-Spyware:** São programas para remover adwares, spywares,, keyloggers, trojans, ou outros malwares.

**Aprovar:** Foi originado pela seguinte frase: "Sua Compra Foi Aprovada", que foi bem recebida pela área cyber criminosa (carder), sendo assim, sempre que o cracker conseguir efetuar uma compra de forma ilícita dará como "Compra Aprovada".

**Arbitrary Code Execution:** é um termo utilizado para referenciar uma falha de segurança que permite o atacante executar um código arbitrário.

**Assembly:** É uma linguagem de baixo nível, ou seja, próxima daquela que as máquinas "entendem". Para utilizá-la é necessário conhecer não só a própria linguagem como também as características de funcionamento da máquina, ela é utilizada para programar códigos entendidos por dispositivos computacionais como microprocessadores e microcontroladores.

**Autoit:** É uma linguagem de automação no qual tem como principal atuação em manutenção e instalação de softwares, pela sua facilidade de criação e

utilização. Muitos hackers aproveitaram a sua utilidade de ação e tiraram proveito, levando como um complemento para seus malwares.

# B

**Backdoor:** É um recurso no qual comandos não-autorizados são executados remotamente, para possibilitar entrada posterior no sistema, pode-se criar tal função(s) por via de malwares.

**Big Data:** É um termo que descreve o imenso volume de dados estruturados ou não estruturados que podem ser utilizados por empresas de forma que lhes convém.

**Black Hat:** É a subcategoria de hackers no qual se segue o ideal do benefício a si próprio sem se preocupar com os danos causados ao próximo. Muitas dessas pessoas seguem como principal alvo de atuação o carder ou a área de Infect.

**Bot:** É a classe de robôs no qual tende como principal ação em funções de repetição e aplicação, pode-se se considerar um Bot tudo a qual se redige a função sequencial feita em forma massiva não pelo homem.

**Booters:** É uma subcategoria hacker no qual tem como principal atuação programar funções massivas usando como protótipos de Bots, vítimas de botnets, muitas das vezes em projetos publicitários abrindo involuntariamente diversas de propagandas em suas vítimas .

**Botnet:** É uma rede de computadores infectados por malwares de acesso ou controle de rede no qual é amplamente utilizado em ataques de negação de serviço.

**Brute force:** traduzido como força bruta, é um algoritmo que faz várias tentativas de solução para algum problema, por exemplo descobrir a senha de usuário, ou quebrar uma criptografia. Um dos usos mais populares são servidores de e-mails, servidores com Telnet ativo, FTP, HTTP com autenticação, painel administrativo, etc.

**Buffer Overflow:** É um ataque que consiste em um transbordamento de dados ou estouro de buffer (região de memória). É uma anomalia onde um programa se aproveita da entrada de dados não filtrada para escrever dados em um buffer, ultrapassando o seu limite para sobrescrever a memória adjacente.

# C

**Carder:** É uma subcategoria do hacking que atua na área de cibercrimes e situa-se em pequenas fraudes e até mesmo o estelionato. As metodologias de um carder efetuar seu crime, inicia-se na escolha de dados dentro de um site como cartão de crédito, e-mails, senhas, finalizando em uma compra com tais informações.

**CEH:** É umas das principais certificações internacionais voltada a profissionais da área de segurança da informação, com ênfase naqueles que demandem conhecimentos na área de auditorias e teste de invasão.

**Cloud Computing:** É a capacidade de computação infinitamente disponível e flexível. A nuvem é tudo aquilo que fica por trás da conexão. As preocupações com a largura de banda, espaço de armazenamento, poder de processamento, confiabilidade e segurança, são postas à parte.

**Consulta (Query):** Vem da função de consulta ao banco de dados, que assim como o termo aprovação foi recentemente bem recebido pelo carder, definindo a operação de selecionar (SELECT) os dados pessoais de algum alvo, tendo informações pessoais dadas como Nome Completo, CPF, RG entre outras informações sensíveis.

**Compilador:** O compilador é o programa que analisa e gera o executável do código fonte (source code). Ele pega um texto compreensível por humanos (o que o programador escreveu) e transforma em código compreensível pela máquina (código binário) que possui instruções que o processador deve executar.

**CTF:** Significa Capture the Flag. No âmbito da informática, são competições que envolvem diversas competências dos profissionais/estudantes/entusiastas para a resolução de desafios relacionados à infosec (segurança da informação), com o objetivo de capturar a bandeira (normalmente um código) e pontuar no placar.

# D

**Database:** É um conjunto de arquivos relacionados entre si, amplamente utilizado em desenvolvimento de softwares, para fazer a persistência de dados, como usuários, logins, conteúdo dinâmico do site, etc.

**DDoS:** Tem como objetivo tornar um servidor, um serviço ou uma infraestrutura indisponíveis ao sobrecarregar a largura banda ou fazendo uso dos seus recursos até que estes se esgotem. O atacante utiliza outras redes (ex: BOTNETs e Shells).

**Deface:** É toda e qualquer tipo de alteração ou "pichação" de páginas web, muitas das vezes tende a ser feita por hacktivista deixando alguma frase de protesto ou grupos de hackers satirizando algum tipo de falha.

**Decrypt:** É a operação inversa ao Encoder, é utilizado para descriptografar informações encriptografadas.

**Dork:** É a metodologia de busca avançada, bastante utilizada no cenário hacker. Sua principal utilidade é buscar informações de forma mais precisa.

**DoS (ataque):** É um ataque de negação de serviço em que deixa processos sem respostas, o ataque tem como alvo principal servidores web, no qual é facilmente sobrecarregado por solicitação massiva de informação, sobrecarregando o sistema.

**Directory Traversal Attack:** consiste em explorar campos de nome de arquivos sem filtro em uma aplicação web para acessar arquivos de sistema.

**Dns:** É um sistema de gerenciamento de nomes hierárquico e distribuído operando segundo duas definições: Examinar e atualizar seu banco de dados; Resolver nomes de domínios em endereços de rede (IP).

**Dump:** É baixar toda informação contida em determinada(s) tabela(s) ou até mesmo de um banco de dados inteiro. Em outras palavras seria um "Backup" de uma determinada base de dados/tabela/coluna/linha.

# E

**Encrypt:** É todo tipo de sistema de encriptação no qual sua função primária é dificultar o acesso a informação contida, muito das vezes é usado esse tipo de sistema para proteger senhas ou informações de nível sensível.

**Engenharia social:** É um método onde o atacante tende a manipular pessoas de forma em que é adquirido seus objetivos. Uma forma de engenharia social é adquirir confiança da vítima para obter dados pessoais como nome, e-mail ou até mesmo senhas de locais específicos ou sistemas. Pode ser feito através de ferramentas avançadas ou até mesmo uma simples de conversação.

**Enumeration:** É uma lista completa de itens, pode ser de usuários, banco de dados, serviços, plugins de extensões ou complementos de um sistema.

**Exploit:** É toda função de metodologia no qual é tirado proveito de uma vulnerabilidade fazendo assim uma exploração, o termo Exploit traduzido significa explorar vulnerabilidade.

**Exposed:** É toda e qualquer exposição de dados pessoais como nome completo, CPF, informações sensíveis como endereço ou telefone.

**Eye View:** É um script pouco conhecido que muda e depura em, hexadecimal, ou assembly softwares, com claves de copyright sem corromper a integridade e autenticidade. A pouco tempo ele foi exposto por uma equipe de hackers noruegueses abrindo as permissões de diretório e visando todas as portas abertas pela empresa de antivírus Baidu.

# F

**Firewall:** É a segurança padrão de sistemas, ele constitui em ser a linha de frente de defesa de rede com principal objetivo aplicar políticas de segurança padronizada ou selecionada pelo usuário.

**Firmware:** É um conjunto de programações operacionais na parte hardware, são informações armazenada em circuito integrado como memória de hardware.

**Footprint:** É uma etapa onde se coleta o máximo de informação sobre o alvo sem ser detectado, como visitar o site da empresa e coletar dados relevantes para um futuro ataque.

**Forense:** É catalogada como área de análise ou investigação, sua principal atuação é interpretar e desvendar crimes, mas também pode-se atuar no cotidiano, investigando e mitigando problemas em perícia informatizada.

**FTP:** É um protocolo de transferência de arquivos, utilizado por desenvolvedores para publicar os arquivos do site no servidor para serem acessíveis na internet.

# G

**Gateway:** É uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos.

**Git:** É um sistema de controle de versão de arquivos. Através deles podemos desenvolver projetos na qual diversas pessoas podem contribuir simultaneamente, muito utilizado em projetos open source, ou em repositório privado de uma determinada empresa.

**Gnome:** É um sistema desktop usado em muitas distros como Ubuntu, Debian e outras. O Linux em si, é apenas o núcleo do sistema operacional e o gnome é um ambiente gráfico que roda sobre esse núcleo, assim como o KDE e XFEC4.

# H

**Hackerativismo:** Invadir para promover ideologia política - promovendo expressão política, liberdade de expressão, direitos humanos ou informação ética.

**Hacker Ético:** É o novo perfil do hacker white hat, que segue como ideal os parâmetros da ética, aplicando o seu conhecimento de forma autoral e autêntica seguindo os padrões de regras ou termos constitucionais legais.

**Hardening:** É um processo de mapeamento de ameaças tende a sua principal atuação localizar, catalogar e mitigar problemas de segurança em toda sua infraestrutura empresarial.

**Hexadecimal:** O sistema hexadecimal é um sistema de numeração posicional que representa os números em base 16, possuindo números (de 0 à 9) e letras (de A à F), portanto empregando 16 caracteres.

**Hijacking:** É uma categoria de malwares no qual tende como principal função alterar registros de informações, a tradução dele tende ao significado "sequestrador" mas a explicação de atuação não é bem o que o nome significa, ele é bem associado de complemento ou extensão ao Adware pois tende a mudar registros e adicionar propagandas para associar redirecionamento de paginas .

**Http:** É sigla de HyperText Transfer Protocol, que significa "Protocolo de Transferência de Hipertexto". É um protocolo de comunicação entre sistemas de informação que permite a transferência de dados entre redes de computadores, principalmente na internet.

**Https:** É sigla de HyperText Transfer Protocol Secure, que significa "Protocolo de Transferência de Hipertexto Seguro", onde é adicionado uma camada de criptografía SSL/TLS para proteger o tráfego de dados.

# I

**ICMP:** É um protocolo para transportar mensagens para os dispositivos de rede, para que através do tipo e código do seu cabeçalho sejam passadas informações sobre o funcionamento do dispositivo.

**IDS:** (Intrusion Detection System), ou sistema de detecção de intrusão. É um sistema que tem por função detectar e prevenir os acessos não autorizados às redes ou hosts de uma ou mais redes de modo passivo.

**Input:** Se refere a um campo de entrada de dados para um sistema web, desktop ou shell. Pode fazer a leitura através dos periféricos como teclado, touch ou mouse para o humano se comunicar com a máquina ou programa.

**IP:** Internet Protocol é um protocolo de comunicação para encaminhar os dados entre as máquinas da rede. Ele tende a ser unitário e pode ser alterado periodicamente para se adaptar a sua forma lógica.

**IP logger:** São formas de obter uma lista de endereços de IP das pessoas que acessaram uma determinada URL de um site. Geralmente é enviado um link com algo interessante e aparentemente nocivo para a vítima, a fim de pegar o seu IP.

**IPV4:** É um endereço IP constituído por 4 octetos tendo no total 32 bits. É a identificação que todo computador ou dispositivo precisa para se conectar à Internet. Esta identificação deve ser única se usado como IP público, e a maneira usada hoje para escrevê-la chamada IPv4 (IP versão 4) que permite a internet ter apenas 4.294.967.296 endereços.

**IPV6:** É um protocolo de internet da próxima geração, criado para substituir o protocolo de internet atual IPV4. Para estabelecer comunicação através da internet, os computadores e outros dispositivos devem possuir endereços de remetente e destinatário.

**Kali Linux:** É uma distro Linux baseada no Debian, voltada para o pentest. Foi criada pela empresa Offensive Security para substituir a antiga distribuição conhecida como Backtrack.

**Kernel:** É o núcleo do sistema operacional, com o intuito de conectar o software ao hardware, estabelecendo uma comunicação eficaz entre os recursos do sistema.

**Keygen:** O Termo "Key" vem de chave, e "gen" de gerador, e assim como o próprio significado diz, a funcionalidade dele é gerar keys, geralmente é usado para gerar números de séries para ativar programas de forma ilegal.

**Keylogger:** É uma categoria de malware que tende como principal função pegar tudo que foi escrito pelo infectado, uma boa explicação de como isso ocorre é simular um bloco de notas invisível que grava tudo o que a vítima digita.

**Lammer:** É um termo utilizado para as pessoas que não possuem nenhum ou pouco conhecimento sobre hack e utilizam ferramentas desenvolvidas por outros para realizarem seus ataques sem entender como tudo realmente funciona.

**LFI:** (Local File Include), é uma falha de segurança em aplicações web que permite a inclusão de arquivos sensíveis de qualquer diretório do site ou até mesmo do sistema operacional. Também pode explorar técnicas de upload de shell.

**Linux:** Também conhecido como GNU/Linux, é um sistema operacional open source, O Kernel foi criado pelo Linus Torvalds e por isso é conhecido apenas por Linux que é a junção do seu nome com o antigo sistema Unix.

**Lock Picking:** É o estudo de como funcionam as fechaduras normalmente utilizadas em portas e cadeados, incluindo como utilizar diversas ferramentas para abrir e testar a real segurança das mesmas.

**Log:** É o histórico de registro e eventos em um sistema, ele tende como principal função descrever o que foi feito pelos usuários para que possam ser analisados.

# M

**Mac Address:** O Endereço MAC (Media Access Control) é o Endereçamento de Camada 2 do Modelo OSI que permite o Controle de Acesso ao meio. Esse tipo de Endereçamento é gravado de forma física na memória ROM das Placas. O MAC Address da Placa de Rede, como é mais conhecido, é um endereço de 12 Dígitos Hexadecimais totalizando 48 bits.

**Mailing:** É um segmento de envio de emails de propaganda as famosas malas diretas, ela consiste em um banco de dados com informações do usuário tais como email, nome completo, telefone entre outras, com finalidade promover seu produto em forma de propaganda.

**Malware:** O termo (mal) vem de maléfico e (Ware) de software. Como o próprio nome condiz, ele é um software mal intencionado, ele pode variar em várias subcategorias tendo várias funções / utilidades mas todas com um propósito de prejudicar ou tirar proveito de suas vítimas.

**Man In The Middle:** É um termo que se refere quando um atacante intercepta os dados de outras pessoas sem que as vítimas venham a perceber, ou seja, a informação é interceptada, e retransmitida pelo atacante.

**Mass Deface:** É quando um invasor consegue acesso root a um servidor que possui vários sites hospedados ou subdomínios para fazer um deface em todos eles de uma só vez.

**MetaSploit:** é um framework que contém vários recursos e módulos para profissionais de segurança. Foi desenvolvido em ruby e hoje em dia contém diversos exploits, payloads, e encoders. Também disponibiliza uma api para que qualquer usuário possa criar novos exploits em ruby e importar para poder utilizar.

**Modelo OSI:** O Modelo OSI é constituído por 7 camadas sendo elas: "Física, Enlace, Rede, Transporte, Sessão, Apresentação, Aplicação".As camadas 1,5,6 não contém protocolos de rede e todas essas camadas são utilizadas para estabelecer toda conexão da rede.

**Mysql:** É um sistema gerenciador de banco de dados relacional de código aberto usado na maioria das aplicações gratuitas para gerir suas bases de dados.

# N

**NAT:** O NAT (Network Address Translation) é um protocolo que faz a tradução dos endereços IP ("Local") ex: 192.168.1.2 para um IP ("Externo") ex: 172.217.29.23. O mesmo ocorre com o servidor acessado.

**Netcat:** É um utilitário de rede que ganhou o apelido de canivete suíço, pode ser usado como uma ferramenta de fingerprinting ou como um servidor e cliente. Geralmente é utilizado para se conectar a uma shell reversa para enviar comandos ou transferência de arquivos.

**Network:** É uma coleção de computadores, servidores, mainframes, dispositivos de rede, periféricos ou outros dispositivos conectados entre si para permitir o compartilhamento de dados.

**NFS:** É um protocolo de sistema de arquivos que permite um usuário em um computador cliente acessar os arquivos em uma rede de computador. O NFS baseia-se o sistema ONC RPC (Open Network Computing Remote Procedure Call) permitindo que qualquer pessoa implementar o protocolo.

**Noob:** É diferente de newb (ou newbie) que significa "aprendiz" ou "inexperiente", designando um iniciante numa atividade ou profissão. É alguém que pode cometer erros por não saber como executar uma determinada tarefa, mas o objetivo é aprender e evoluir.

# O

**Osstmm:** É uma metodologia de testes de segurança de um ambiente, com testes meticulosos e análises minuciosas, seguindo essa metodologia é possível testar se seu ambiente está seguro.

**OWASP:** É o projeto aberto de segurança em aplicações web, uma comunidade online que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web.

# P

**Phishing:** São formas de tentar adquirir acesso a informações super sensíveis tais como senhas, cartões de créditos, entre milhares de outras informações do tipo. Ele é bem conhecido também como "bait" pois é criado por alguma engenharia social e enviada a sua vítima se passando de algo de seu interesse para tentar pegar seus determinados objetivos.

**Payload:** É um conjunto de instruções para desviar o fluxo de um software para fazer com que seja realizado atividades maliciosas e até mesmo trazer uma bind shell ou reverse shell ao atacante.

**Pentest:** Penetration Test, ou teste de intrusão, é uma metodologia quanto aos procedimentos e processos realizados pelo pentester para burlar as proteções de um sistema e gerar um relatório para que a empresa fique ciente das falhas encontradas e possam tomar medidas para correção das mesmas.

**PooP-UP:** É uma janela que abre no navegador quando acessa determinados sites, muitas das vezes contém propagandas ou Phishing ou até mesmo com adwares que são adicionados como extensão sem a vítima notar.

**Port:** É um número de 16 bits também conhecido como número da porta, utilizado para identificar os serviços que estão associados a um endereço de IP. É utilizado pelos protocolos TCP e UDP e funcionam na camada de transporte do Modelo OSI.

**PowerShell:** É um framework da microsoft que contém uma linha de comando e linguagem de script para que o administrador possa realizar tarefas e gerenciamento de configuração local ou remoto.

**Priv8:** É um exploit ou ferramenta privada, ou seja, que após ser desenvolvido não foi publicado na internet gratuitamente, de forma que apenas pessoas que comprar ou que sejam da mesma team possam utilizar.

**Proxy:** É um tipo de servidor que realiza uma conexão indireta ao servidor acessado. Em uma conexão normal os pacotes de rede saem direto do seu computador e passam para o servidor do site que você entrou. Com um proxy ativo essa conexão é feita mandando os pacotes de rede para o servidor proxy e de lá é mandado para o site.

## Q

**Query:** É uma string com instruções SQL utilizadas para manipular informações de um banco de dados ou efetuar ações administrativas.

**QRcode:** É um código de barras bidimensional que pode ser escaneado através de uma câmera de celular para converter essas informações em texto, bem como uma mensagem, url, localização georreferenciada, e-mail, contato, etc...

## R

**Ransomware:** é o nome de um malware que utiliza alguma criptografia para tornar os dados armazenados em um equipamento indisponíveis. Após isto é solicitado um resgate(ransom) através do pagamento de um valor em bitcoins para que o atacante possa receber o dinheiro sem ser localizado.

**Rce:** (Remote Code Execution), é uma falha de segurança em aplicações web que permite o atacante executar qualquer comando no alvo escolhido sem estar fisicamente no local e ganhar acesso ao sistema.

**Rfi:** (Remote File Inclusion), é uma falha de segurança em aplicações web que permite o atacante adicionar uma url externa contendo um código para o servidor executar, também pode ser incluso o link de uma web shell em txt.

**RaspberryPi:** É um "Mini computador" que pode ser usado como servidor para hospedagem de sites e CIC Servers, para ser realizado ataques físicos, fazer máquinas de jogos, robôs, entre outras milhares de funcionalidades.

**RedHat:** A Red Hat Inc, é uma empresa dos Estados Unidos, que disponibiliza soluções baseadas no sistema operativo ou sistema operacional GNU/Linux, incluindo várias distribuições.

**Redirect:** Url redirection, é uma técnica que redireciona o usuário para uma outra url antes da página ser carregada totalmente.

**Redeface:** É quando uma pessoa ou grupo retiram uma deface feita por outra pessoa ou team e coloca a sua index. Também é considerado redface quando o site hackeado já foi notificado anteriormente no zone-h.

**Reverse Shell:** É quando a vítima se conecta ao atacante, seja por meio de um payload reverso executado na máquina da vítima, ou através de uma web shell, para permitir enviar e executar comando remotamente em uma máquina ou dispositivo.

**Rootkit:** É um tipo de software projetado para dificultar a detecção de sua existência a fim de manter o acesso privilegiado ao computador ou dispositivo. Às vezes sua remoção pode ser tão difícil que a melhor opção seria reinstalar o sistema, ou caso venha com o hardware fazer uma substituição do mesmo.

## S

**Script:** É uma sequência de código ou funções escritas para automatizar determinadas tarefas em alguma linguagem de programação.

**Shellcode:** É um payload com códigos hexadecimais dos opcodes para explorar falhas de buffer overflow a fim de obter uma shell para controlar a máquina.

**SSH:** Secure SHell, é um protocolo que permite a você acessar virtualmente o servidor como se estivesse em um terminal fisicamente.

**SSL:** É a abreviação de Secure Sockets Layer, ou seja, uma ferramenta que encripta páginas antes mesmo de serem transmitidas pela internet que identifica as partes envolvidas. É muito utilizada para pagamentos online com cartão de crédito.

**Symlink:** É um tipo especial de arquivo que contém uma referência a outro arquivo ou diretório na forma de um caminho absoluto ou relativo e que afeta a resolução do nome de caminho (pathname).

**Shell script:** É um arquivo de texto com extensão .sh que contém uma sequência de comandos para sistemas operacionais baseados em Unix, utilizado para automatizar processos de instalação, backup ou exploit.

**Sniffer:** Os sniffers são programas que, como o próprio nome diz, "farejam" o que passa pela rede, para que os dados possam ser analisados, muitas vezes utilizado para capturar senhas.

**Spoofing:** É um ataque que tem como atuação criar uma máscara entre os pacotes de IP, ele é muito usado em ataques de engenharia social físicos no qual faz com que sua vítima acesse redes sociais em uma rede infectada para adquirir tais informações por via da sua máscara de subrede.

**SpyWare:** O termo (Spy) vem de espião e (Ware) de malware. Ele é uma subcategoria de malware que como o próprio nome condiz ele tem funções de espionar o usuário.

**Sqli:** (SQL Injection), É uma técnica usada para atacar aplicações de banco de dados, onde códigos SQL são inseridos em um campo do site ou url que não possuem filtros, e assim consegue-se fazer um dump de qualquer conteúdo do banco de dados, trazendo dados sensíveis como senhas de usuários.

# T

**TCP:** É um protocolo para envio e recebimento de dados através da internet, utilizando um handshake de três vias para estabelecer a conexão, geralmente utilizado para manter sessões.

**Trojan:** É uma subcategoria de malware que se infiltra como malware disfarçado, se passando assim como software comum.

**TOR:** É um software livre e de código aberto que proporciona o anonimato pessoal ao navegar na Internet e em atividades online.

**Tunneling:** Tunneling pseudo-interface driver. O Teredo é uma tecnologia de encapsulamento de pacotes IPv6 em pacotes IPv4, quando os dispositivos de rede não suportarem o padrão IPv6.

# U

**UDP:** É um protocolo de comunicação em rede que não é necessário estabelecer uma conexão com o handshake de três vias, apenas envia os pacotes, sem checar se foram entregues, assim possui uma velocidade de tráfego de dados mais rápida, muito utilizado em serviços de stream e jogos.

**Unix:** É um sistema operativo portável, multitarefa e multiutilizador originalmente criado por Ken Thompson, Dennis Ritchie, Douglas McIlroy e Peter Weiner, que trabalhavam nos Laboratórios Bell (Bell Labs) da AT&T.

# V

**VPN:** (Virtual Private Network) é uma forma viável de se interligar a comunicação entre determinados computadores (geralmente utilizada quando os mesmos estão separados geograficamente por longas distâncias). Ela também pode realizar um tunelamento da rede e encriptar os dados de forma com que apenas os computadores devidamente credenciados possam acessar.

# W

**Wirelles:** É a troca de informações sem a necessidade de estar conectado fisicamente, podendo ser de uma pequena distância (controle remoto de uma televisão) ou a uma longa distância (sistema de comunicação via satélite).

**Wordlist:** É um arquivo geralmente no formato .txt com uma lista grande com combinações de palavras para ser utilizado em um bruteforce.

**WAF:** Um firewall de aplicação web (WAF) é um aparelho, plugin do servidor, ou filtro que se aplica um conjunto de regras para uma conversa HTTP.

**White Hat:** Hackers bem intencionados, que não pretendem fazer mal algum a ninguém.

**WPA2:** O WPA2 é um protocolo de certificação que utiliza o AES (Advanced Encryption Standard), sistema de encriptação mais seguro e mais pesado do que o WPA original.

**WEP:** Significa Wired Equivalent Privacy, e foi introduzido na tentativa de dar segurança durante o processo de autenticação, proteção e confiabilidade na comunicação entre os dispositivos Wireless.

**Worm:** É um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar.

X

**Xss:** (Cross-site scripting), é um tipo de vulnerabilidade em aplicações web que permite o atacante injetar códigos do lado do cliente, de forma que fiquem visíveis para outros usuários .

Z

**Zone-h:** É um site no qual hackers divulgam suas defaces, nota-se que mesmo se o dono ou administrador do site tira tal deface de seus site ele ainda permanecerá com notificação ou histórico de invasão no Zone H.

# Parceiros De Divulgação:

Anarchy Ghost
BrasilBlackHat
Conhecimento Livre
Downs Hacker Oficial
Fsociety
Hacker Culture
Hacker Da Depressão
Hacker Security
InurlBrasil
KyZ Team
Lacking Faces
LulzSec Brasil
MC Hackudao
MTz Oficial
O Rei Dos Hackers
O Analista
Pr1v8
Sucuri HC
TecMundo
Uliware