Hacking

- ## Hypertext Transfer Protocol

  O Hypertext Transfer Protocol, sigla HTTP é um protocolo de comunicação utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web. Hipertexto é o texto estruturado que utiliza ligações lógicas entre nós contendo texto.

  Exemplos de códigos HTTP:

  200 OK - O recurso foi encontrado com sucesso
  301 Moved Permanently - Redirecionamento para outra URL
  302 Found - O recurso está temporariamente sobre outra URL
  403 Forbidden = falta privilégios suficientes
  404 Not Found - O servidor não encontrou o recurso buscado
  500 Internal Server Error - O servidor não suporta essa funcionalidade

- ## Métodos de acessar um servidor

  nc -v site.com 80 # conecta com o servidor
  GET / HTTP/1.0 # retorna o código fonte do site
  HEAD / HTTP/1.0 # traz o head
  GET /simon /HTTP/1.0 # verificar se tem essa página no servidor

Protocolos de Redes

Porta de serviço/protocolo:

- **23 Telnet**
- **25 SMTP**
- **53 DNS**
- **69 TFTO**
- **80 HTTP**
- **110 POP3**
- **137, 138, 139 NetBIOS**
- **143 IMAP**
- **161/162 SNMP**
- **443 HTTPS**
- **445 SMB**
- **989/990 FTPS**
- **1,812 RADIUS**
- **3389 RDP**

O SSH usa a porta TCP 22. Todos os protocolos criptografados pela SSH, incluindo SFTP, SHTTP, SCP e SExec também usam a porta TCP 22.

Trivial File Transfer Protocol (TFTP) requer autenticação e opera usando UDP porta 69.

Terminal Access Controller Access-Control System (TACACS) é um protocolo de autenticação remota usado para comunicação com servidores de autenticação, comumente em redes UNIX. RFC 1492 TCP/UDP porta padrão 49

O **Diameter** é um protocolo baseado no RADIUS, que tenta consertar as deficiências apresentadas no mesmo.

O **Network-based intrusion prevention system** (NIPS) monitora toda a rede para tráfego suspeito, por análise de protocolos.

Segurança em rede WIFI

WIFI Segura com WPA2 CCMP.
O CCMP usa criptografia AES de 128 bits com um vetor de inicialização de 48 bits
Este vetor de inicialização torna o cracking um pouco mais difícil.

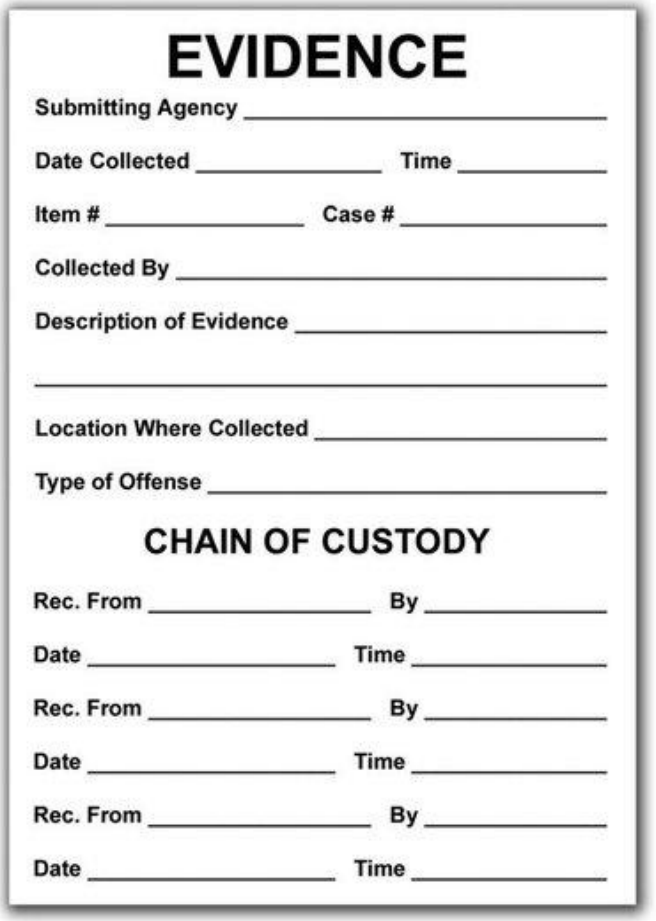
Honeynet é uma coleção de Honeypots que é um computador ou sistema preparado como se fosse uma armadilha e assim ajudar a entender como funcionam os ataques.

Existe hoje em dia um elevado número de ferramentas e sistemas que pretendem fornecer segurança. Alguns exemplos são os detectores de intrusões, os antivírus, firewalls, filtros AntiSpam, fuzzers, analisadores de código etc.

Segurança da Informação

As políticas de uso aceitáveis [Acceptable use policies (AUPs)] descrevem como os funcionários de uma organização podem usar sistemas e recursos da empresa, tanto software como hardware.

Sobre análise forense - Cadeia de custódia trata de como a evidência está segura, onde ela é armazenada e quem tem acesso a ela.



EVIDENCE

Submitting Agency _____

Date Collected _____ Time _____

Item # _____ Case # _____

Collected By _____

Description of Evidence _____

_____

Location Where Collected _____

Type of Offense _____

CHAIN OF CUSTODY

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

Rec. From _____ By _____

Date _____ Time _____

De que lado?

Há uma discussão na área sobre qual chapéu um profissional da segurança está usando, ou seja, de que lado moral o profissional age com o conhecimento de técnicas de penetração. Normalmente, são definidos em White Hat, Black Hat e Grey Hat.

WHITE HAT:
Os hackers WHITE HAT optam por usar seus poderes para o bem. Também conhecidos como "hackers éticos", estes às vezes podem ser empregados pagos ou contratados trabalhando para empresas como especialistas em segurança que tentam encontrar buracos de segurança através de técnicas de invasão. Os WHITE HAT empregam os mesmos métodos de hacking que os BLACK HAT, com uma exceção - eles

fazem isso com a permissão do proprietário do sistema, o que torna o processo completamente legal. Os hackers WHITE HAT realizam testes de penetração, testam os sistemas de segurança no local e realizam avaliações de vulnerabilidade para as empresas.

BLACK HAT:
Como todos os hackers, os BLACK HAT geralmente têm um amplo conhecimento sobre a invasão de redes de computadores e a ignorância de protocolos de segurança. Eles também são responsáveis por escreverem malwares, que é um método usado para obter acesso a esses sistemas. Sua principal motivação é, geralmente, para ganhos pessoais ou financeiros, mas eles também podem estar envolvidos em espionagem cibernética, hacktivismo ou talvez sejam apenas viciados na emoção do cibercrime. Os BLACK HAT podem variar de amadores, ao espalhar malwares, e hackers experientes que visam roubar dados, especificamente informações financeiras, informações pessoais e credenciais de login. Eles não só procuram roubar dados, mas também procuram modificar ou destruir dados.

GREY HAT:
Como na vida, há áreas cinzentas que não são nem preto nem branco. Os hackers GREY HAT são uma mistura de atividades de BLACK HAT e WHITE HAT. Muitas vezes os hackers GREY HAT procurarão vulnerabilidades em um sistema sem a permissão ou o conhecimento do proprietário. Se os problemas forem encontrados, eles os denunciaram ao proprietário, às vezes solicitando uma pequena taxa para corrigir o problema. Se o proprietário não responde ou cumpre, as vezes os hackers GREY HAT publicarão a descoberta recentemente encontrada online para o mundo ver. Esses tipos de hackers não são inerentemente maliciosos com suas intenções, eles estão procurando tirar algum proveito de suas descobertas por si mesmos. Geralmente, esses hackers não vão explorar as vulnerabilidades encontradas. No entanto, esse tipo de hacking ainda é considerado ilegal, porque o hacker não recebeu permissão do proprietário antes de tentar atacar o sistema.

Coleta de Informação

OSINT

Utilizado por empresas de segurança/cibersegurança e agências de inteligência governamentais como **FBI, NSA, CIA, MI6, ABIN, CDCiber, Mossad, BND** e entre outras, o termo **OSINT** nada mais é do que a coleta, análise e processamento de informações.

Para aplicar-se o OSINT devemos obter **informações relevantes** em diversas fontes como:

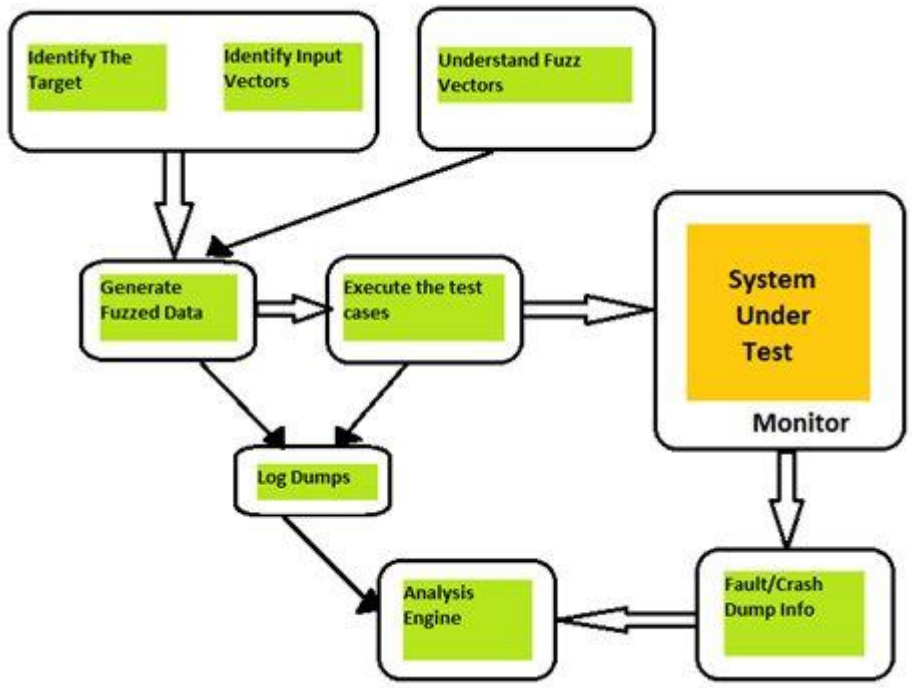
- Internet: sites de busca, redes sociais, blogs, wikis, fóruns e até mesmo na Deep Web.
- Mídia: jornais, televisão, revistas e rádio.
- Informações públicas de fontes governamentais.
- Eventos, conferências, trabalhos e até bibliotecas.

OSINT pode ser usado em diversos meios de atuação como por exemplo: combate aos ataques terroristas, recrutamento, propriedade intelectual, e até mesmo por empresas de marketing.

Os processos principais na aplicação do OSINT (**Open Source Intelligence**) são: reconhecimento –> fontes de informação –> coleta de dados –> processamento de dados –> análise de dados –> inteligência.

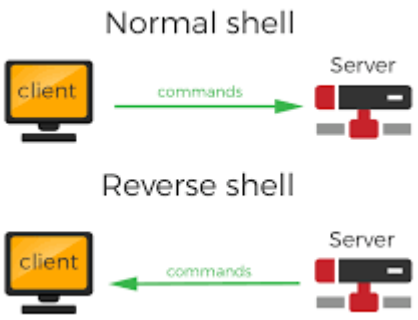
Técnicas

Fuzzing é uma técnica de teste de software que envolve o prover dados inválidos, inesperados ou aleatórios como entrada. O programa é então monitorado para exceções, como falhas ou falhas na validação, ou vazamentos de memória.



Shell Shoveling

Shell shoveling, em segurança de rede, se refere ao ato de redirecionar a entrada e a saída de um shell para um serviço de modo que ele possa ser acessado remotamente. Na computação, o método mais básico de interface com o sistema operacional é o shell.



Backdoor

Backdoor é um método, geralmente secreto, de escapar de uma autenticação ou criptografia normais em um sistema computacional, um produto ou um dispositivo embarcado.

Exploit

Um exploit é um pedaço de software, um pedaço de dados ou uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento acidental ou imprevisto a ocorrer no software ou hardware de um computador ou em algum eletrônico.

Proxy

Em redes de computadores, um servidor proxy é um aplicativo de servidor que atua como intermediário entre um cliente que solicita um recurso e o servidor que fornece esse recurso.

Ataque de negação de serviço - DDoS

Um ataque de negação de serviço, é uma tentativa de tornar os recursos de um sistema indisponíveis para os seus utilizadores. Alvos típicos são servidores web, e o ataque procura tornar as páginas hospedadas indisponíveis na rede. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga.

Existem várias técnicas de invasão, estou mostrando algumas aqui.

Google Hacking

Google hacking, também chamado de Google dorking, é uma técnica hacker que usa o Google Busca e outras aplicações do Google para encontrar brechas de segurança na configuração ou nos códigos utilizados pelos sítios web. Google dorking também pode ser usado para OSINT.

Vou deixar algumas dorks aqui para vocês testarem:

cache: www.site.com
==========
linux -ubuntu
==========
python filetype: pdf (txt, exe, py)
==========
site:dedsecurity.com
==========
intitle: login
==========
inurl: /wp-admin
==========
intext:tecnologia
==========
2017...2019:
==========
link:google.coom
==========
info:dedsecurity.com
==========
iphone "11"
==========
iphone -11
==========
dedsecurity inurl:robots.txt
==========
site:pastebin.com password
==========
site:.gov.br intitle: login
==========
site:.gov.br filetype:.txt password
==========
intitle:”NetCamXL*”
==========
intitle:phpmyadmin
==========

site:.gov.br inurl: /admin
==========
intitle:”index of” inurl:ftp
==========
intext: cpf + nome + rg + conta site:.com.br
==========
find all subdomains
site:*.dedsecurity.com -www

Nmap

Nmap é um software livre que realiza port scan desenvolvido pelo Gordon Lyon, autoproclamado hacker "Fyodor". É muito utilizado para avaliar a segurança dos computadores, e para descobrir serviços ou servidores em uma rede de computadores.

Detectando falhas em servidores utilizando o método de saída do tipo verbose -v
nmap -sS -v -Pn -A --open --script=vuln + IP do Alvo
(Descobre a vulnerabilidade do servidor com aquele endereço de IP especificamente)

Analisando vulnerabilidades em mais endereços de IP de uma rede
nmap -sS -v -Pn -A --open --script=vuln + IP alvo/24

Descobrindo portas abertas, versões de serviços e sistema operacional que está rodando no alvo.
nmap -v –sV -Pn -O —open + IP do alvo
(O argumento “-O” pode ser substituído pelo argumento “-A”)

Realizando pesquisas sobre alvos
nmap –script=asn-query,whois-ip,ip-geolocation-maxmind + IP do alvo

Burlando firewall
*Existem 3 maneiras diferentes de burlar um Firewall em uma rede externa:
nmap -f -sV -A + IP do alvo (Neste comando ocorre a fragmentação de pacotes que serão enviados para se conectar ao alvo)
nmap -sS -sV -A + IP do alvo (Faz varreduras do tipo SYN na rede alvo)
nmap -Pn -sV -A + IP do alvo (Não enviar pacotes ICMP para o alvo, ou seja, não pingar na rede)

Mandando um recado para o admin que está do outro lado da rede
nmap –sS www.alvo.com —verbose –data-string “Você está sendo ownado, admin!”

Buscando falhas de DDoS
nmap -sU -A -PN -n -pU:19,53,123,161 –script=ntp-monlist,dns-recursion,snmp-sysdescr + IP do alvo

Fazendo brute-force no banco de dados do alvo
nmap --script=mysql-brute + IP do alvo

Alguns comandos com Nmap em rede interna:

Analisando IP e endereços de MAC de dispositivos em uma rede
nmap 192.168.0.1/24
(IP do Gateway da rede / 24)
Como fazer menos ruídos o possível ao se fazer analise em uma rede interna para não ser banido
O fato de não se fazer muito barulho na rede deve-se ao fato de não realizar a busca de endereços do MAC e para que isso não ocorra, utilizamos o comando “–send-ip”. Exemplo:

nmap –T0 –send-ip 192.168.0.1/24 (O parâmetro “-T0” é utilizado para se fazer um Scan mais demorado na rede a ponto de não levantar tanta suspeita do alvo).

*Se o alvo estiver fora da rede, a opção “–send-ip” pode ser ignorada com segurança.

nmap -sS 192.168.1.1 => varredura SYN
nmap -sT 192.168.1.1 => varredura TCP
nmap -sU 192.168.1.1 => varredura UDP
nmap -sY 192.168.1.1 => varredura SCTP
nmap -A 192.168.1.1 => Varredura agressiva

Para realizar o uso de detecção de sistema operacional -o.

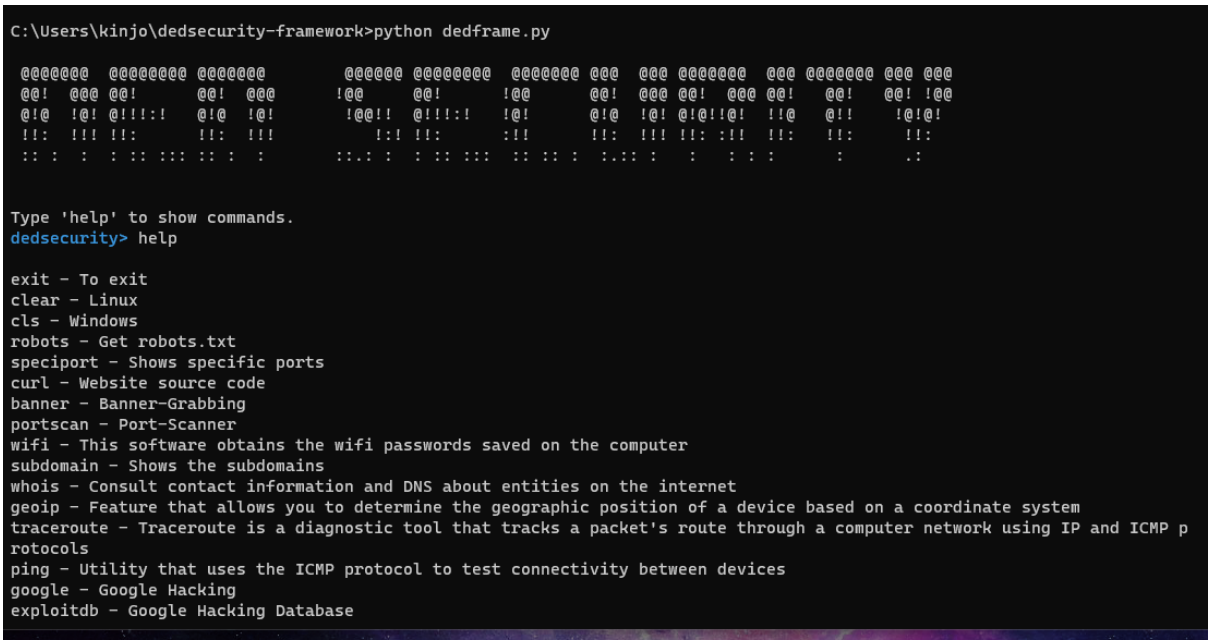
--oscan-limit = Limita a detecção de SO a alvos com pelo menos uma porta aberta e fechada, resultando em maior chance de sucesso
--fuzzy = Usado para quando o Nmap não consegue fazer uma estimativa clara, exibe a pontuação de confiança
--max-os-try = O padrão é 5, defina um número menor para acelerar a varredura.

Vulnerabilidade
nmap --script vuln 192.168.0.139
Detectando OS
nmap -O 192.168.0.139
Enable OS detection version and traceroute
nmap -A 192.168.0.139
Quem está na rede
nmap -T4 -F 192.168.0.252/24

Melhores ferramentas para hacking:

Ded Security Framework

Ded Security Framework é uma ferramenta destinada a profissionais de segurança.



Site:https://github.com/dedsecurity/dedsecurity-framework

Nmap

A mais conhecida e usada, é claro o **Nmap (Network Mapper)**, que é 100% gratuito.

Nmap é usado principalmente para a descoberta de rede e auditoria de segurança. Literalmente, milhares de sistemas de administradores em todo o mundo usam o nmap para inventário de rede, verificando se há portas abertas, gerenciando agendas de atualização de serviços e monitorando host ou uptime. Nmap, como uma ferramenta usa pacotes IP packets de forma criativa para determinar o que está disponível na rede.

Site Oficial: https://nmap.org/

Metasploit Penetration Testing

Muito conhecido também é o **Metasploit Penetration Testing,** que pode ser encontrado em sua versão gratuita e paga.

Para teste de invasão (pentest) o Metasploit é **a**mplamente utilizado por profissionais de segurança cibernética e hackers éticos esta é uma ferramenta que você tem que conhecer. Metasploit é essencialmente um projeto de segurança de computador (framework) que fornece ao usuário informações vitais sobre vulnerabilidades de segurança conhecidas e ajuda a formular planos, estratégias e metodologias para a exploração de teste de penetração e de ensaio IDS.

Site Oficial: https://www.metasploit.com/

THC Hydra

O **THC Hydra**, uma ferramenta para quebra de senhas em versão única gratuita.

Essencialmente THC Hydra é uma ferramenta rápida e estável Network Login Hacker, que vai usar dicionário de força bruta para ataques e tentar várias combinações de senha e login contra uma página. Esta ferramenta de hacking suporta um vasto conjunto de protocolos incluindo Mail (POP3, IMAP, etc.), bancos de dados, LDAP, SMB, VNC e SSH.

Pode ser encontrado aqui: http://sectools.org/tool/hydra/

Sqlmap

O sqlmap é uma ferramentas open source que permite você realizar testes automatizados em busca de falhas que permitem SQL INJECTION.

Logo ao invés de você tentar “na mão” vários tipos de injeção de SQL, você roda a ferramenta e ela faz isso para você com comandos pré-configurados e até mesmo avançados

Site Oficial: http://sqlmap.org/

Wireshark

Wireshark ferramenta de Scanners de vulnerabilidades Web muito popular em versão gratuita.

Wireshark essencialmente captura os pacotes de dados numa rede em tempo real e, em seguida, exibe os dados em formato legível (detalhado). A ferramenta (plataforma) foi altamente desenvolvida e inclui filtros, codificação de cores e outras características que permitem ao utilizador cavar fundo para o tráfego de rede e inspecionar pacotes individuais.

Site Oficial: https://www.wireshark.org/