



Domínios & Infraestruturas

A arte de buscar por phishing's

Monitoramento de marca
usando fontes públicas. Part-1

SOBRE MIM

Sou o Júlio César AKA GreenMind.

- Família, jogos e esportes radicais
- Compartilhar conhecimento
- OSINT Village



SUMARIO

01

ANTES DE COMEÇAR

Apresentação do curso,
sobre mim, antes de começar
e a história do OSINT

02

criando laboratório

A importância da criação de
um laboratório, VMS
Windows, Linux e Android

03

EVIDENCIANDO PROCESSOS

A importância das evidências,
criando lista de visibilidade e
gerando evidências.

04

INTRODUÇÃO

Introdução ao OSINT,
conceitos básicos, soluções
automatizadas e comunidades

05

DOMÍNIOS e REDES SOCIAIS

Buscando por domínios e
páginas suspeitas.

06

CONCLUSÃO e CTF

Aqui iremos conversar um
pouco sobre o tema e iniciar
o Capture the Flag

MONTANDO INFRAESTRUTURA LABORATÓRIO

A IMPORTÂNCIA DO LAB

A importância do lab, evitando corromper evidências e sua segurança

KALI

Kali será usado para realizar essa análise

01

02

03

04

WINDOWS

Validar informações em ambientes Windows

ANDROID

Alguns phishings só estão disponíveis para mobile e o Genymotion nos ajuda nisso

A IMPORTÂNCIA DO LABORATORIO

Diariamente realizamos análises de phishings, páginas suspeitas e aplicativos. Devido a isso é de suma importância a criação de laboratórios, seja para máquinas virtuais Linux com o Kali, Android com o Genymotion e laboratório windows com máquinas atualizadas.



EVITANDO CORROMPER EVIDÊNCIAS

Para uma melhor análise é recomendado que sempre use um laboratório limpo, sem cache e sem estar prejudicado. Isso é recomendado para evitar corromper possíveis evidências.



SUA SEGURANÇA

É recomendado usar laboratórios via rede NAT, assim damos uma camada a mais de segurança evitando que a máquina host seja comprometida e a sua rede local.



KALI

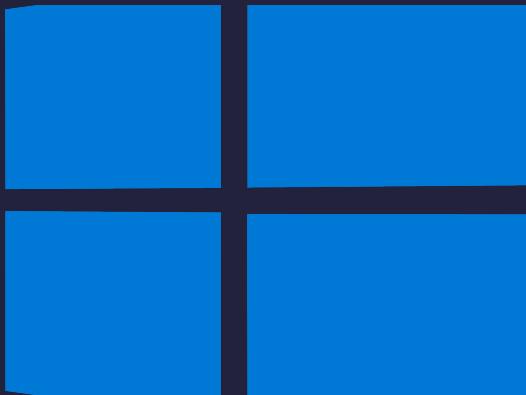
O Kali Linux é baseado no Debian, contém diversas de ferramentas voltadas para diversas tarefas de segurança da informação, como pentesters, computação forense e engenharia reversa. Iremos utilizar ela para buscar e validar informações encontradas.



LAB WINDOWS

O Windows será usado para testar phishings e possíveis malwares no ambiente microsoft. Assim como o Linux e Android o Windows também será usado em laboratórios.

Como ele podemos usar diversas versões, os respectivos aplicativos disponíveis e usar de forma virtualizada sem a necessidade de ter diversos dispositivos físicos.



LAB ANDROID E O GENYMOTION

O Genymotion é um projeto que tem como objetivo a emulação gratuita de sistemas operacionais Android.

Como ele podemos usar diversas versões, os respectivos aplicativos disponíveis e usar de forma virtualizada sem a necessidade de ter diversos dispositivos físicos.



Como ele pode nos ajudar ?

Com o Genymotion podemos realizar diversas ações, por exemplo:

- Emular um dispositivo Android;
- Obter root no dispositivo;
- Realizar download do APK.



criando lista de visibilidade

criando nossa lista

Precisamos ter a visibilidade do que precisa ser monitorado, urls, redes sociais, imagens e etc

AFINAL O QUE É ?

Documento que possui todas as informações que desejamos ver

01

02

03

04

QUAIS OS BENEFÍCIOS

Guia os times, empresas parceiras são beneficiadas e visibilidade total do escopo

INFORMAÇÕES IMPORTANTES

Logo, domínios, urls, ips, bloco de IPS, aplicativos oficiais e palavras chaves

TLD's

- Entendendo o que são domínios
- Conhecendo o TLD's
- Quais são os mais conhecidos
- Site com todos os TLD's
- Criando nossa lista de TLD's



criando domínios - gratuitos

Domínios gratuitos:

- Dot.tk
 - .tk
 - .ml
 - .ga
 - .cf
 - .gq



criando domínios - pagos

Domínios pagos:

- Godaddy.com
- Superdominios.org



CYBERSQUATTING

ADIÇÃO

Nesse ataque é realizada a adição de um carácter.

- baddbank.com.br

BITSQUATTING

Realizada troca de carácter por outro.

- bedbank.com.br

01

02

03

04

DICIONARIO

Nesse ataque é adicionado uma palavra.

- portalbadbank.com.br

HOMOGLYPH

São caracteres que aparecam ser uma letra.

- ßAdbank

CYBERSQUATTING

OMISSION

Nesse ataque é realizada a remoção de um carácter.

- bdbank.com.br

REPETIÇÃO

Realizada a repetição de carácter.

- baadbank.com.br

05

06

07

08

SUBSTITUIÇÃO

Nesse ataque é uma mudança de carácter.

- baddank.com.br

SUBDOMÍNIO

Nesse ataque é usado parte do subdomínio.

- ba.dbank.com.br

CYBERSQUATTING

TLD-SWAP

Nesse ataque é realizada a troca da TLD por outra.

- badbank.net

TRANSPOSIÇÃO

Realizada a mudança de ordem.

- bdabank.com.br

09

10

BUSCANDO POR DOMÍNIOS SUSPEITOS

DNSTWIST

O DNSTwist é um projeto incrível para nos auxiliar na busca por domínios

URLCRAZY

Solução utiliza técnicas de OSINT para buscar e gerar domínios

01

02

03

04

PHISHING CATCHER

Monitora em tempo real certificados criados e sites suspeitos

OUTROS

- dnstwist.it

HOSPEDAGENS, SERVIDORES e DNS

HOSPEDAGENS GRATUITAS

- hostinger

HOSPEDAGENS PAGAS

- Hostinger
- AWS
- Digital Ocean

01

02

03

04

AWS e DIGITAL OCEAN

- Plano gratuito
- Rotação de IPs
- Diversos países

DNS DOMÍNIO

- Cloudflare
 - Esconder IP real
 - Gerenciar domínios

MATERIAIS INDEXADOS NA INTERNET

GOOGLE DORKS

- Intitle
- Site
- inurl

REDES SOCIAIS

- Namechk
- sherlock

01

02

03

04

FACEBOOK

- site
- Inurl
- negação

INSTAGRAM

- site
- Inurl
- negação

MATERIAIS INDEXADOS NA INTERNET

TWITTER

- intitle
 - site
 - inurl

05

YOUTUBE

- intitle
 - site
 - inurl

06

07

LINKEDIN

- site
- inurl
- negação

08

OUTROS

Podemos usar esse e outros operadores para buscar por outras redes sociais

COMUNIDADES

MISP

MISP é um que nos auxilia no compartilhamento de ameaças

Phishingtank

Phishingtank é projeto que compartilha informações sobre phishing

01

02

03

04

OpenPhish

Comunidade que possui feeds informando novos endereços de phishing

Outras comunidades

Temos diversas comunidades.

- circl.lu

MISP(Malware Information Sharing Platform)

O MISP Threat Sharing é uma plataforma de inteligência de ameaças de código aberto. O projeto desenvolve utilitários e documentação para uma inteligência de ameaças mais eficaz, compartilhando indicadores de comprometimento. Existem várias organizações que executam instâncias MISP, listadas no site.

- <https://www.misp-project.org/>



Phishingtank

O Phishingtank é uma comunidade incrível onde podemos realizar a consulta de páginas de phishing, podemos ajudar adicionando páginas suspeitas e temos uma área destinada a empresas. Além disso, podemos usar a API oficial.

- <https://phishtank.org/>



OpenPhish

OpenPhish é uma plataforma independente totalmente automatizada para inteligência de phishing. Ele identifica sites de phishing e realiza análises de inteligência em tempo real, sem intervenção humana e sem usar recursos externos, como listas negras.

- <https://openphish.com/feed.txt>
- https://openphish.com/fp_feed.txt

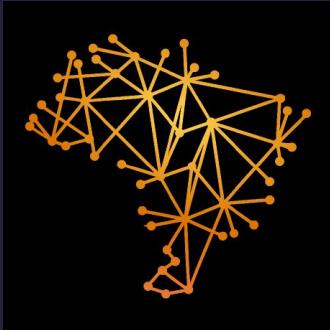


The logo consists of the word "OpenPhish" in a large, bold, blue sans-serif font, centered within a white rectangular box.

Outras comunidades

Abaixo podemos ver outras comunidades que estão ajudando a comunidade armazenando phishings e páginas suspeitas.

- CIRCL;
- Phishing database;
- OpenCTI.BR.



OBRIGADO

ATÉ A PRÓXIMA