Universidade Paulista - UNIP

William De Freitas Campos

ESTUDO E ANALISE DE PACOTES E DE DADOS EM ATAQUES DE NEGAÇÃO DE SERVIÇO

Limeira
2021

Universidade Paulista - UNIP

William De Freitas Campos

ESTUDO E ANALISE DE PACOTES E DE DADOS EM ATAQUES DE NEGAÇÃO DE SERVIÇO

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da computação sob a orientação do professor Me.Sergio Eduardo Nunes.

Limeira
2021

William De Freitas Campos

ESTUDO E ANALISE DE PACOTES E DE DADOS EM ATAQUES DE NEGAÇÃO DE SERVIÇO

Trabalho de conclusão de curso apresentado à banca examinadora da Faculdade UNIP, como requisito parcial à obtenção do Bacharelado em ciência da Computação sob a orientação do professor Me. Sergio Eduardo Nunes.

Aprovada em XX de XXXXX de 201X.

BANCA EXAMINADORA

_____

Prof. Dr. Nome completo

_____

Prof. Me. Nome completo

_____

Prof. Esp. Nome completo

DEDICATÓRIA

Dedico este trabalho a todos que acreditaram em mim e me ajudaram dando um apoio incondicional; A meu professor orientador Me. Sergio Eduardo Nunes pelos ensinamentos e orientações.

“Seja paciente.tudo chegara a você no momento certo”.

(Sidarta Gautama - Buddha)

RESUMO

Os ataques de negação de serviço *DDOS* são uma das grandes ameaças aos sites da internet e estão entre os problemas de segurança mais graves atualmente. Esses ataques são preocupantes em particular por causa do grande impacto que eles causam sem nenhum aviso prévio da noite para o dia.Um ataque de *ddos* pode facilmente acabar com os recursos de computação e comunicação da vítima em curto período de tempo.

Este trabalho irá apresentar de forma simples como funciona o ataque de *DDO S*em um ambiente controlado, e também mostrará como podemos nos proteger do mesmo,também será mostrado características importantes de cada tipo de ataque e defesa e as vantagens e desvantagens do procedimento de defesa. O princípio do trabalho é simplificar o entendimento do senso comum de como funciona, para então ter uma melhor compreensão sobre esse tipo em particular de ataque, e assim possa ser alcançada uma melhor e mais eficiente técnica de defesa.

Palavra-Chave: até cinco palavras, separadas por ponto-e-vírgula.

ABSTRACT

Text...

Key Words: ...

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

SUMÁRIO

1. INTRODUÇÃO

Quando um usuário acessa um determinado site sendo ele o Google, Netflix ou realiza a venda de uma mercadoria na qual é necessário a emissão de um cupom fiscal via SAT,esses serviços precisam estar acessíveis on-line.Explicando de forma simplificada, o usuário faz a solicitação e esta requisição precisa se conectar a um servidor central onde é feita a troca de informações, a mesma é retornada ao usuário, tornando o serviço disponível.....

.....O que antes era quase inexistente devido a capacidade limitada de processamento e lentidão no acesso a internet, hoje já são em sua grande maioria um custo enorme a empresas e serviços de aplicativo devido aos ataques de crackers e empresas concorrentes. Um dos métodos mais comuns dessa ameaça é o ataque de DDOS ou ataque de negação de serviço, que consistem em agrupar uma enorme quantidade de hosts zumbis direcionados a um alvo específico, enviando solicitações de acesso a este site simultaneamente assim inviabilizando seu acesso aos demais usuários.....

1.1 Objetivo

Este trabalho tem o objetivo analisar o tráfego de pacotes e dados mais comuns durante um ataque de negação de serviço através de um comparativo entre dois programas: T50 e Inundator .esses softwares que servirão de ferramenta de simulação para ataque a uma rede local de forma isolada.

Para que este objetivo seja demonstrado com sucesso, será necessário inicialmente abordar temas como o funcionamento da internet, a construção de uma rede local, e criação de host, além disso será abordado tipos de ataques e defesas que são os mais comuns da internet para facilitar o entendimento sobre essa área em específico.

Será mostrado como foi desenvolvido a rede local a qual sofrerá o ataque com os programas e serão coletados dados por meio de um programa de análise trafico de rede o IPERF. Com os dados obtidos será possível realizar análises das

conseqüências desses ataques ao sistema e o impacto que pode causar em um servidor ou a um serviço que esteja em execução.

Com à analise aprofundada das conseqüências dessa simulação de ataque no sistema, será possível mensurar os efeitos que a maquina (servidor) a qual foi atacada sofreu na questão de trafego de rede, memória e CPU e na parte do cliente (host) no sentido de lentidão de sistema entre outras, com essas informações será traçado um caminho para poder mitigar e se proteger de uma ameaça de ataque de negação de serviço.

1.2 Justificativa

Está cada vez mais comum noticias envolvendo ataques de negação de serviço. Quase 59.8% da população do ano de 2021 são usuários da internet e trabalham por meio de computadores, uma boa parcela dos principais usuários desta maquina são os profissionais da área TI e empresas dos mais diversos ramos a mercê e podem ser atacados a qualquer momento.

A cada ano que passa a humanidade com seu avanço acelerado é mais dependente da tecnologia, e se transforma para suprir nossas necessidades e juntamente expandir todo nosso potencial, esse crescimento chega a ser quase exponencial a cada geração (como diria a Lei de Moore) e, portanto suas ameaças o acompanham.

Tanto os cursos de informática quanto os demais apenas mencionam esse tema de forma superficial o tornando escasso, sendo necessário um estudo que adentre efetivamente na solução dos atentados à segurança. É um nicho defasado que este trabalho visa elucidar de onde advém um ataque DDOS desde sua criação a sua correção.

[1] xxxxxx

[2] xxxxxx

1.3 Metodologia

A fundamentação dessa metodologia dá-se por meio da síntese das pesquisas bibliográficas consultadas, isso proporciona aos caminhos desenvolvidos uma nova base de estudo estruturada, sendo assim, aprofundando o conhecimento a cerca dos ataques de negação de serviço sem que haja algum tipo de informação fragmentada. Portanto esse trabalho visa abordar o ataque de negação de forma linear explorando possibilidades de ataque e defesa e contribuindo para a segurança de usuários e embasando trabalhos futuros.

O trabalho será divido em 3 partes, em que a primeira consiste em abordar detalhadamente o que é um ataque de negação de serviço explorando seus componentes, os aspectos que necessitam ser desenvolvidos individualmente para que haja a execução de um ataque com a união de suas funções, abordado os tipos de ataque direto e refletor.

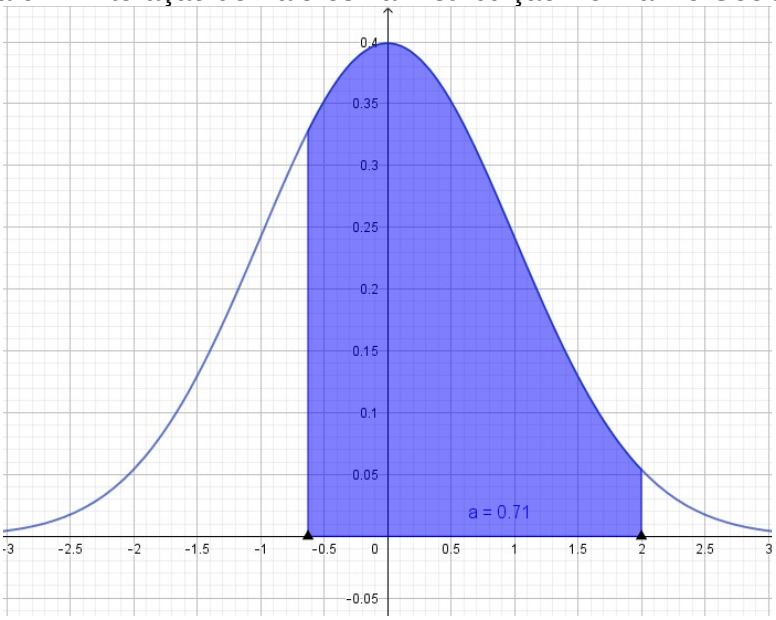
Elucidado o que é um ataque é importante ressaltar que é uma estrutura para variados meios para o objetivo da negação de serviço, a segunda parte do trabalho consiste no detalhamento dos tipos de ameaça na internet e as diferenças das varias ferramentas de ataque de negação de serviço.Também abordará tópicos sobre segurança da informação e alguns meios de defesa e mitigação.

A ultima parte será a proposta prática, onde será desenvolvido o sistema em si, a criação da rede, para isso iremos criar duas máquinas virtuais simulando máquinas físicas do mundo real. Esta rede servirá de ambiente para simular o ataque de DOS (ataque de negação de serviço), será possível observar como os recursos do servidor se tornarão quase indisponíveis devido à alta demanda de requisições de acesso que o ataque irá realizar, indisponibilizando um site para o usuário comum, e através desse experimento, com a ferramenta IPERF, serão capturados os dados necessários para uma analise dos pacotes e dados mais comuns.

2. PRIMEIRO NÍvEL

Texto...

Figura 01 – Interação de Valores na Distribuição Normal no GeoGebra



Fonte: Elaborado pelo autor, print software GeoGebra.

2.1 Segundo Nível

3. Texto...

2.1.1Terceiro nível

Texto...

Quadro 01 – Tipos de Distribuição Estatística

Distribuições Contínuas	Distribuições Discretas
Normal	Poisson
Uniforme	Uniforme discreta
Triangular	*****
Exponencial	*****
Weibull	*****

Fonte: Adaptado Filho (2001, p. 173)

4. PROPOSTA PRATICA

Para a criação da rede interna foi necessário realizar a instalação de dois sistemas operacionais dentro da maquina virtual, e para isso foi utilizado a VM VirtualBox 6.0.24..Os sistemas operacionais utilizados foram o kalilinux e o Windows 7 . Já para o ataque de negação de serviço foram utilizadas duas ferramentas para a simulação de ataque de negação de serviço, a 1º ferramenta foi a T50 e a 2ª Inundator

4.1 Desenvolvimento Do Sistema

Para a criação de rede isolada foi utilizado a VM VirtualBox 6.0.24, que permite a criação de vários ambientes virtuais em uma só maquina.

https://download.virtualbox.org/virtualbox/6.0.24/VirtualBox-6.0.24-139119-Win.exe

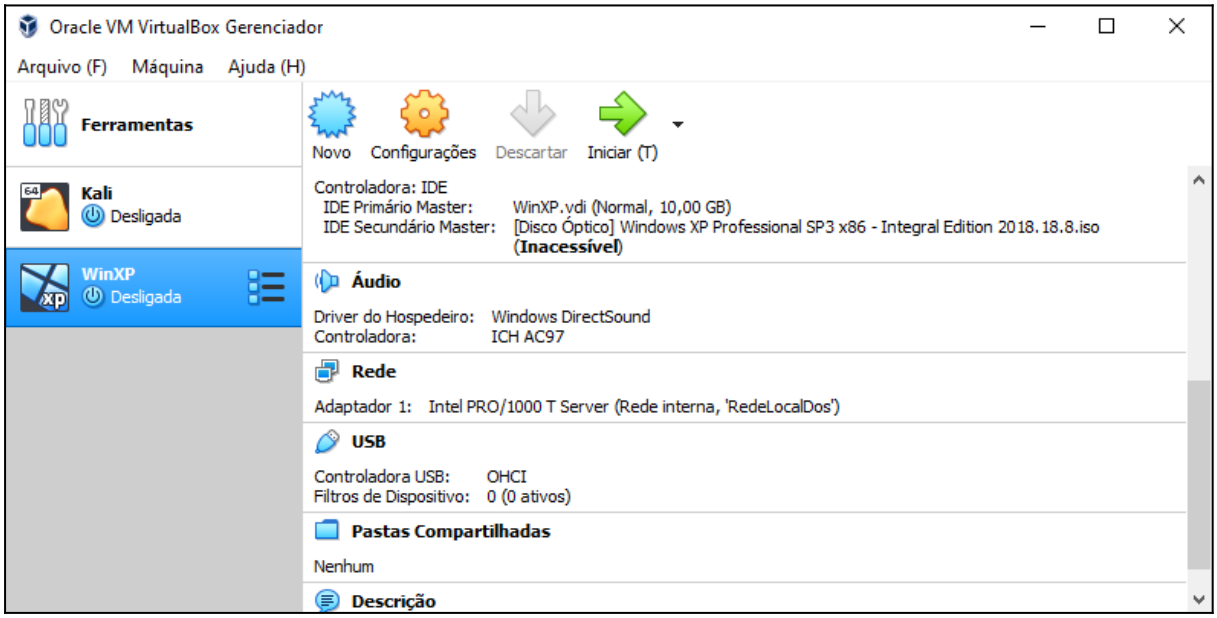
para configuração do sistema e instalação do sistema operacional Kali clique em novo

Ao criar será necessário nomear e escolher a pasta da maquina, no tipo selecione a opção Linux e na versão Other Linux (64-bit) e clique em next

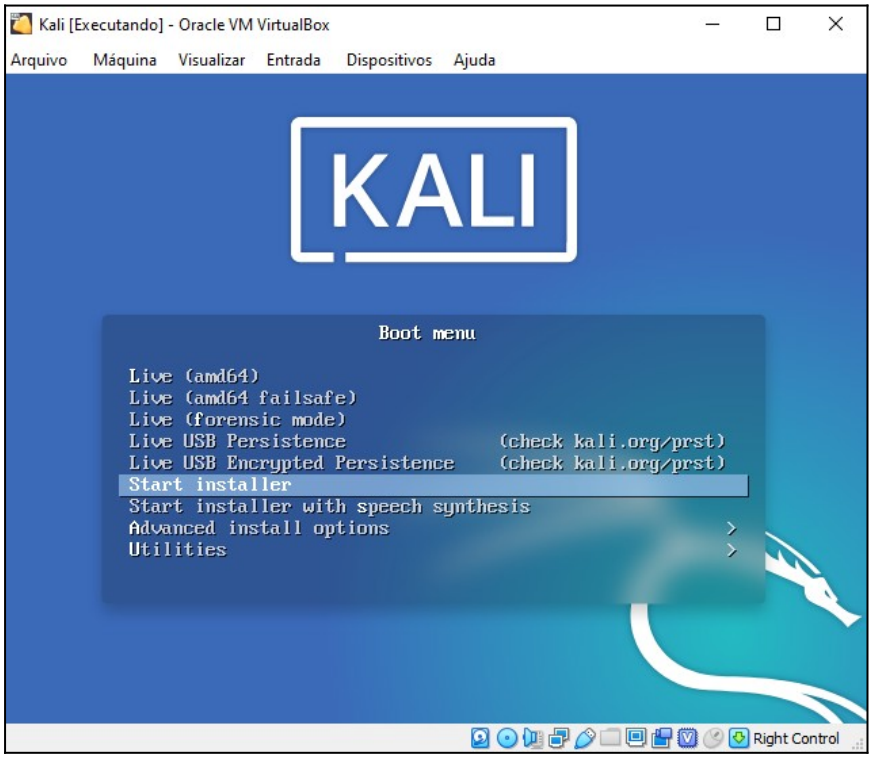
selecione o tamanho da memória

Escolha a opção criar um novo disco virtual

Após configurado clique em iniciar para instalar o sistema kali



ao iniciar será necessário selecionar a imagem iso e clique em iniciar

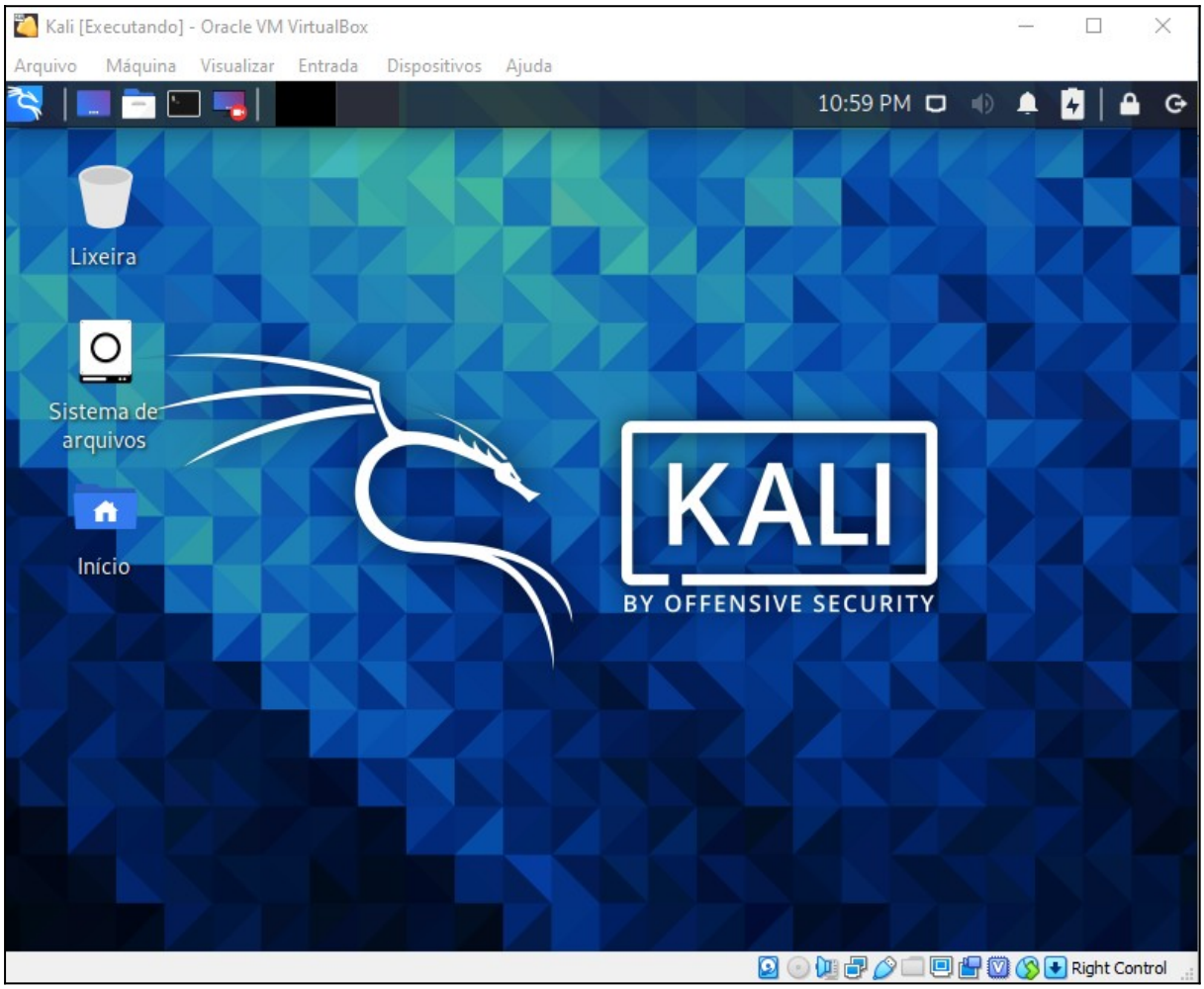


e seguir com o procedimento de instalação padrão do sistema operacional

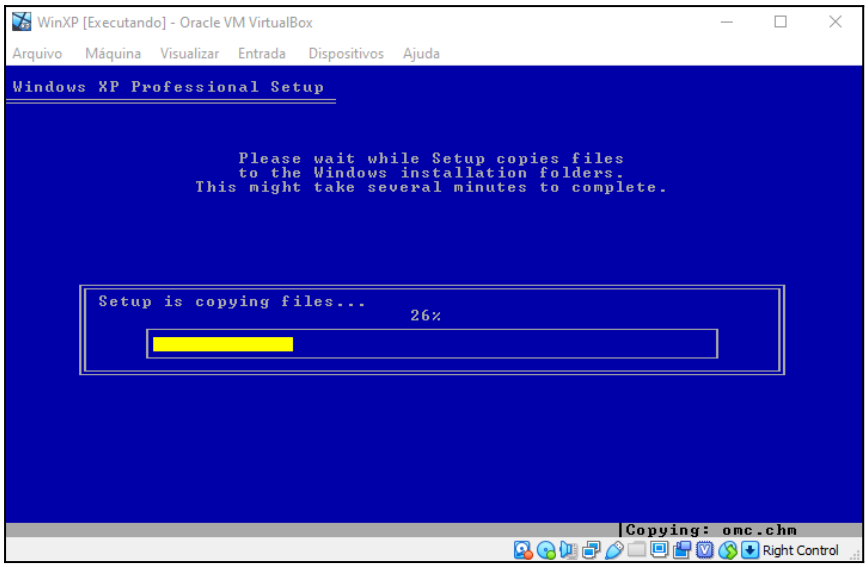
Usuário:Kali2021

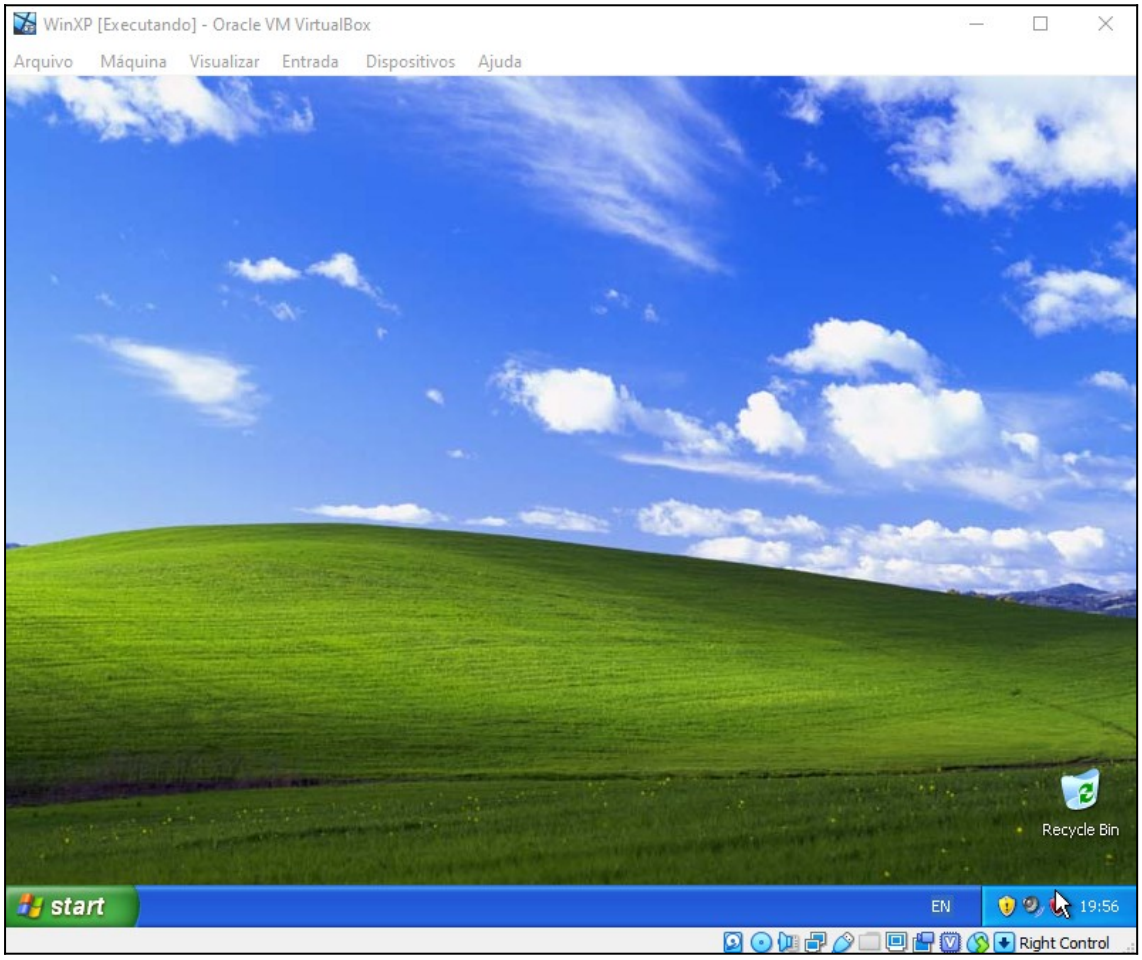
Senha:Kali2021

Após a instalação a maquina deverá ser iniciada normalmente

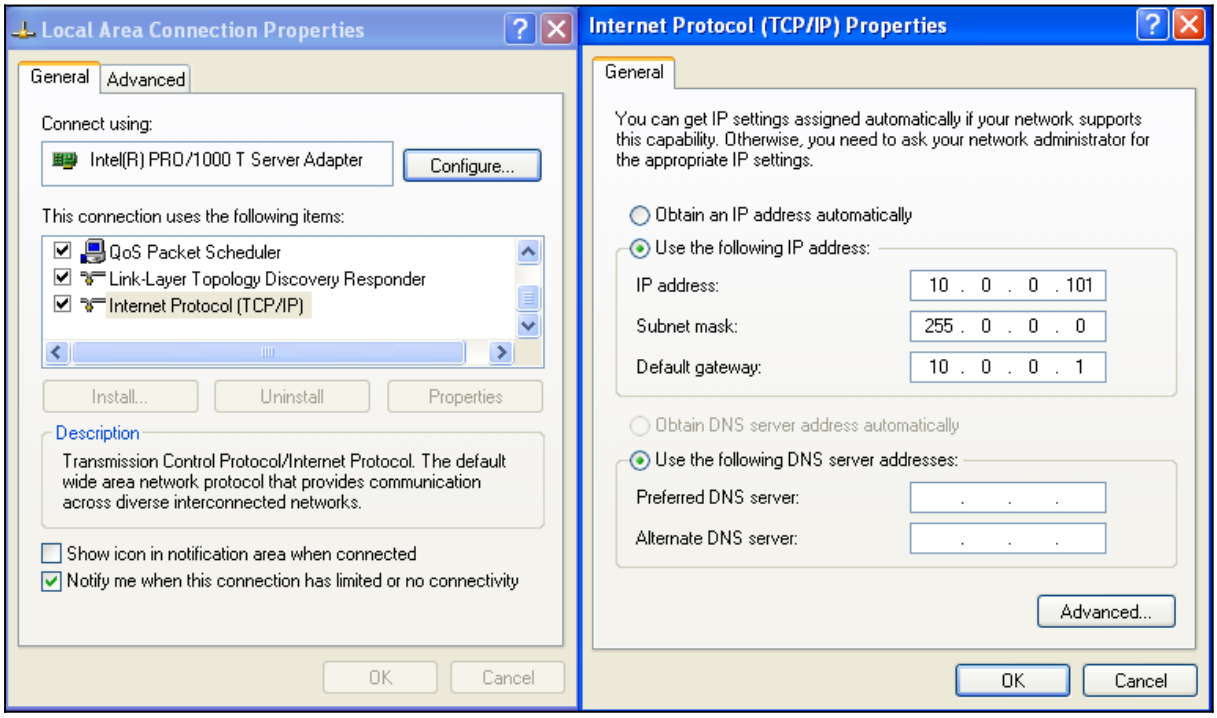


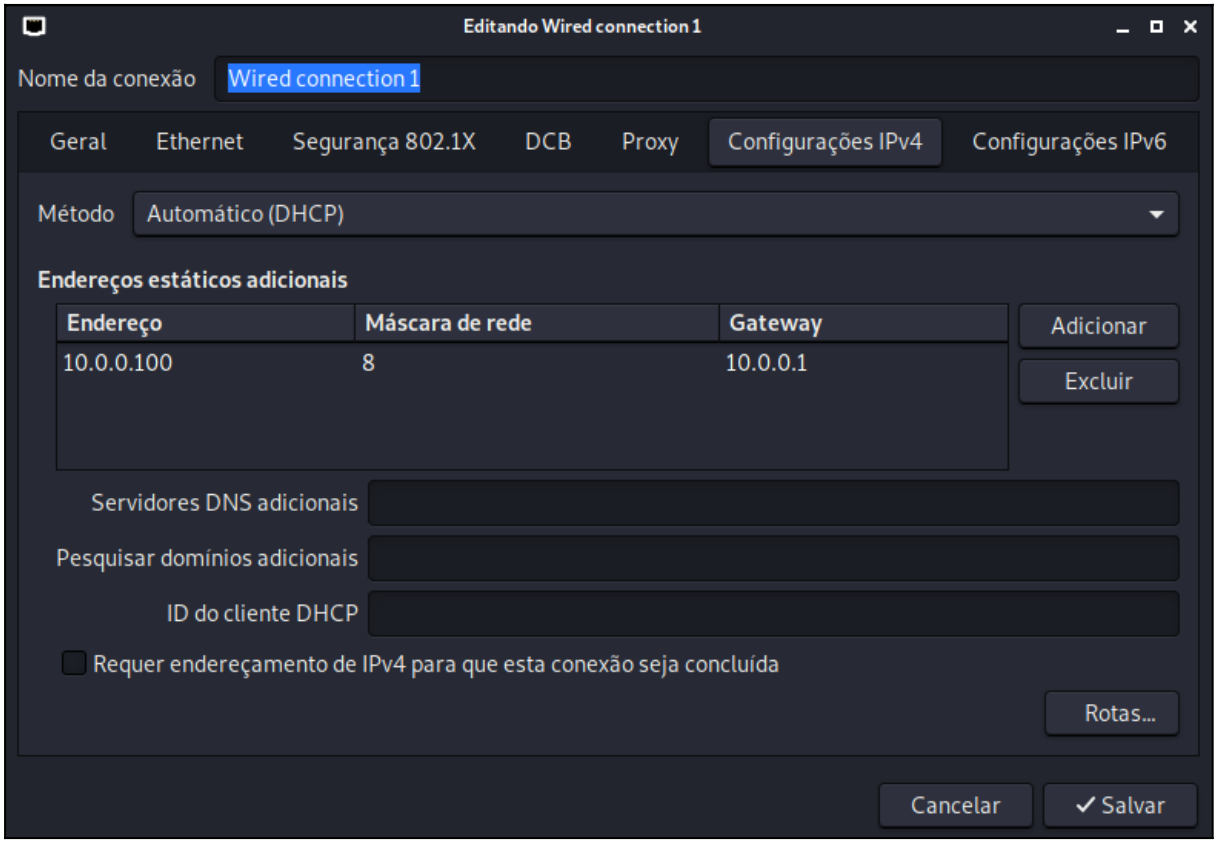
Para a maquina que servira de host também foi realizado o mesmo procedimento de criação

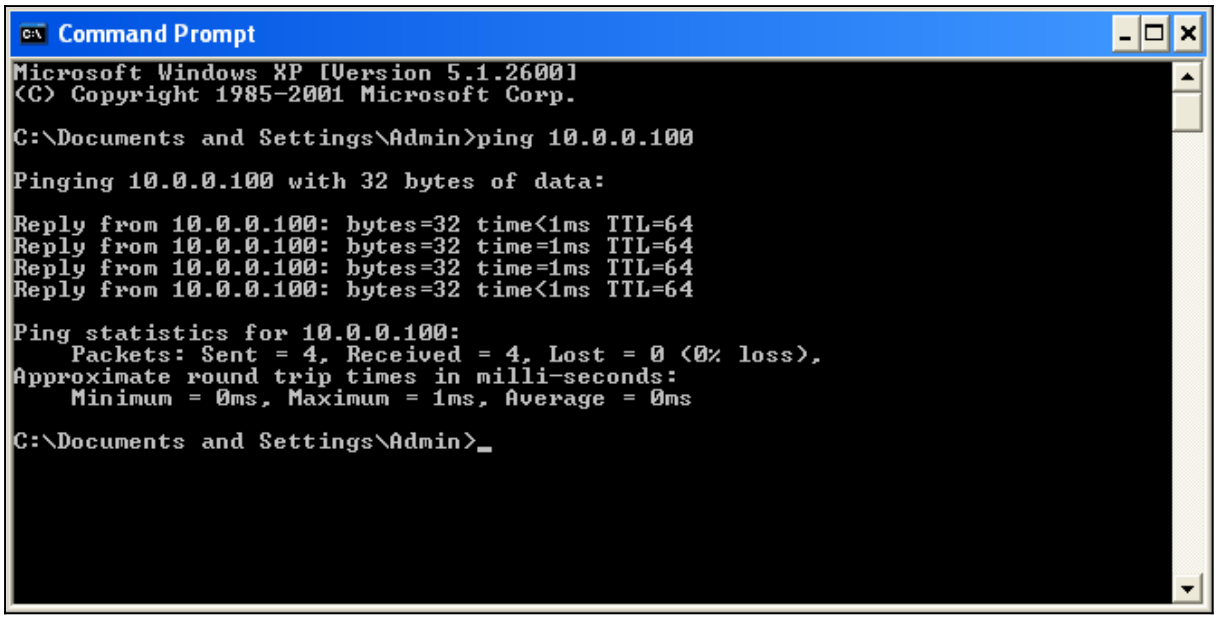

WinXP [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Windows XP Professional Setup
Please wait while Setup copies files
to the Windows installation folders.
This might take several minutes to complete.
Setup is copying files...
26%
Copying: omc.chm
Right Control

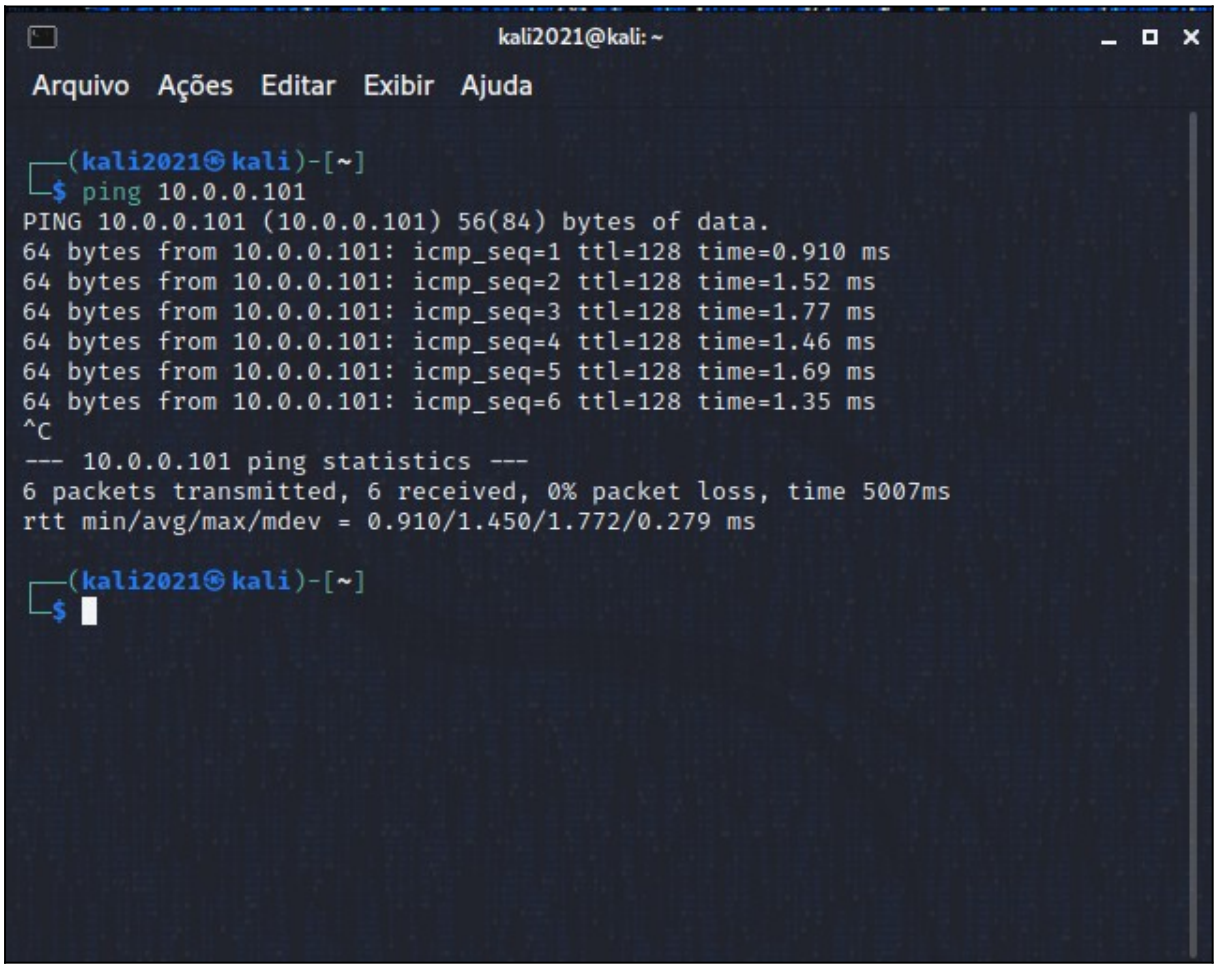

WinXP [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
Recycle Bin
start
EN
19:56
Right Control

Para criar a rede interna, será necessário configurar as maquinas virtuais e também atribuir uma faixa de IP as maquinas,



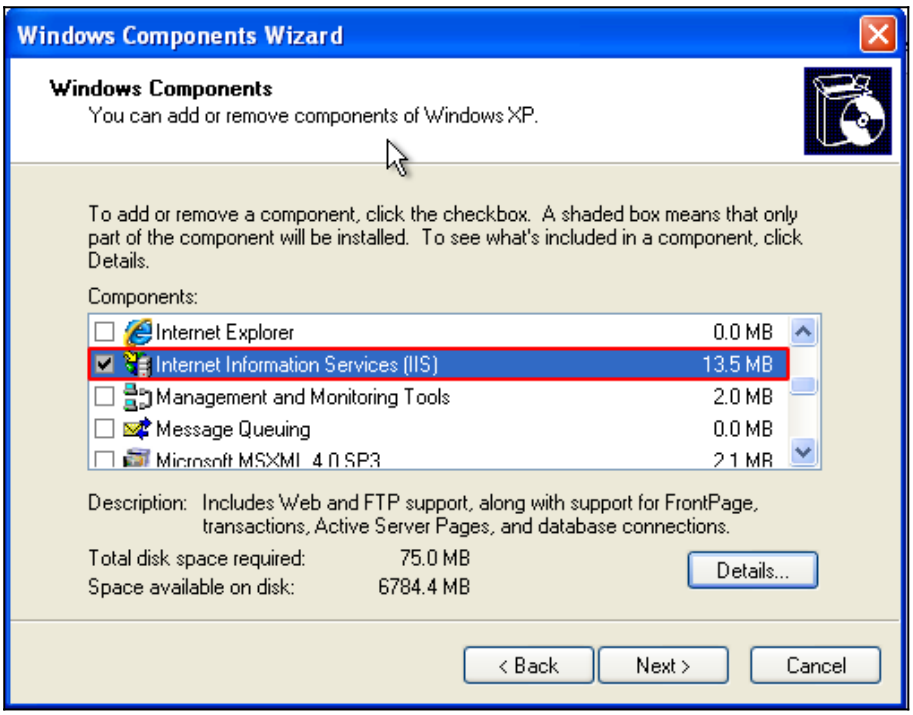


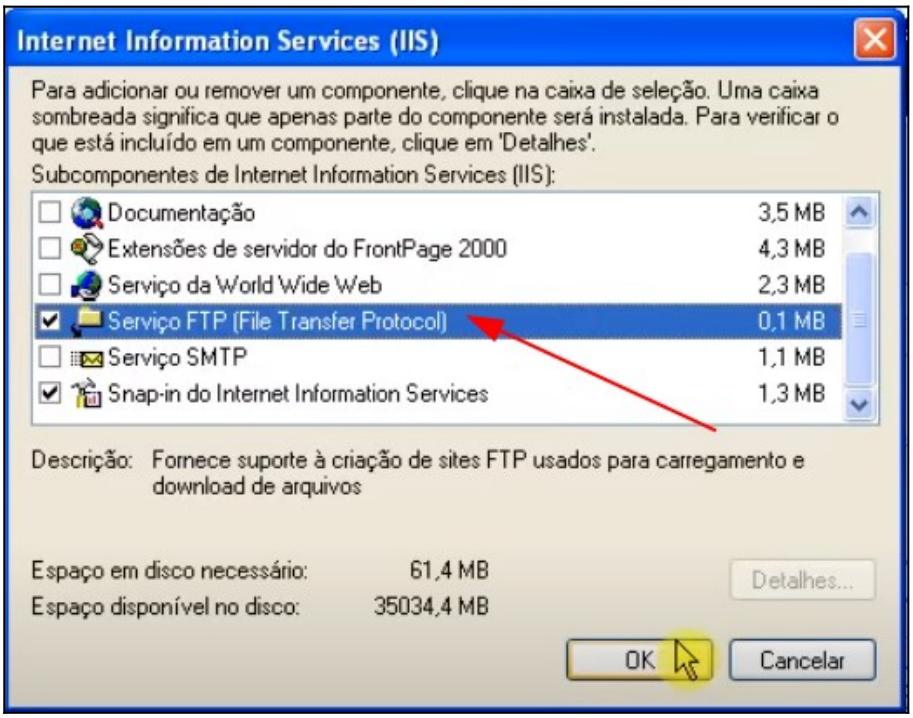

Command Prompt
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\Admin>ping 10.0.0.100
Pinging 10.0.0.100 with 32 bytes of data:
Reply from 10.0.0.100: bytes=32 time<1ms TTL=64
Reply from 10.0.0.100: bytes=32 time=1ms TTL=64
Reply from 10.0.0.100: bytes=32 time=1ms TTL=64
Reply from 10.0.0.100: bytes=32 time<1ms TTL=64
Ping statistics for 10.0.0.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Documents and Settings\Admin>


kali2021@kali: ~
Arquivo Ações Editar Exibir Ajuda
(kali2021㉿kali)-[~]
$ ping 10.0.0.101
PING 10.0.0.101 (10.0.0.101) 56(84) bytes of data.
64 bytes from 10.0.0.101: icmp_seq=1 ttl=128 time=0.910 ms
64 bytes from 10.0.0.101: icmp_seq=2 ttl=128 time=1.52 ms
64 bytes from 10.0.0.101: icmp_seq=3 ttl=128 time=1.77 ms
64 bytes from 10.0.0.101: icmp_seq=4 ttl=128 time=1.46 ms
64 bytes from 10.0.0.101: icmp_seq=5 ttl=128 time=1.69 ms
64 bytes from 10.0.0.101: icmp_seq=6 ttl=128 time=1.35 ms
^C
--- 10.0.0.101 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 0.910/1.450/1.772/0.279 ms
(kali2021㉿kali)-[~]
$

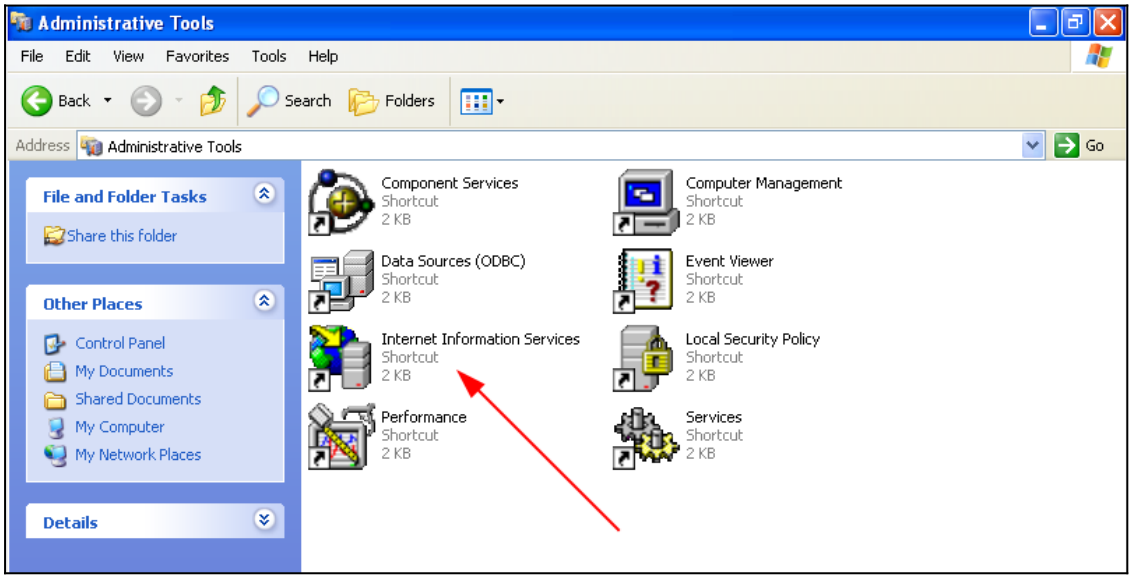
Servidor FTP

O Windows XP possui uma ferramenta própria para criação de servidores FTP. Essa ferramenta se chama Internet Information Services (IIs).para poder utiliza-la basta apenas configurar utilizando o Windows Components Wizard.

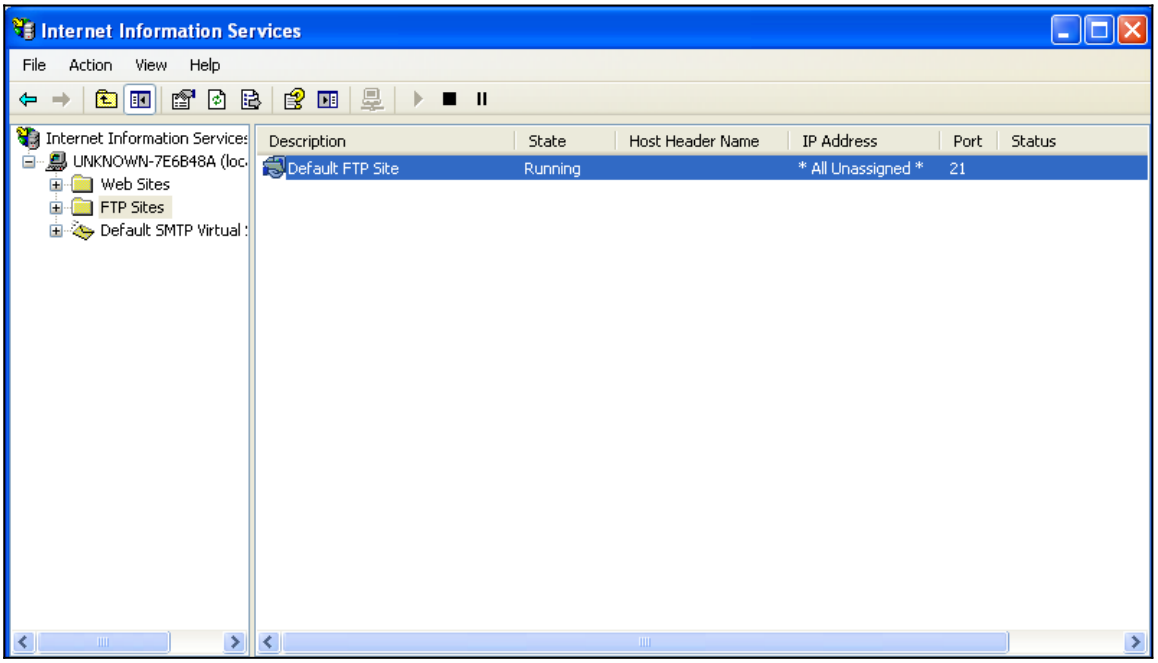




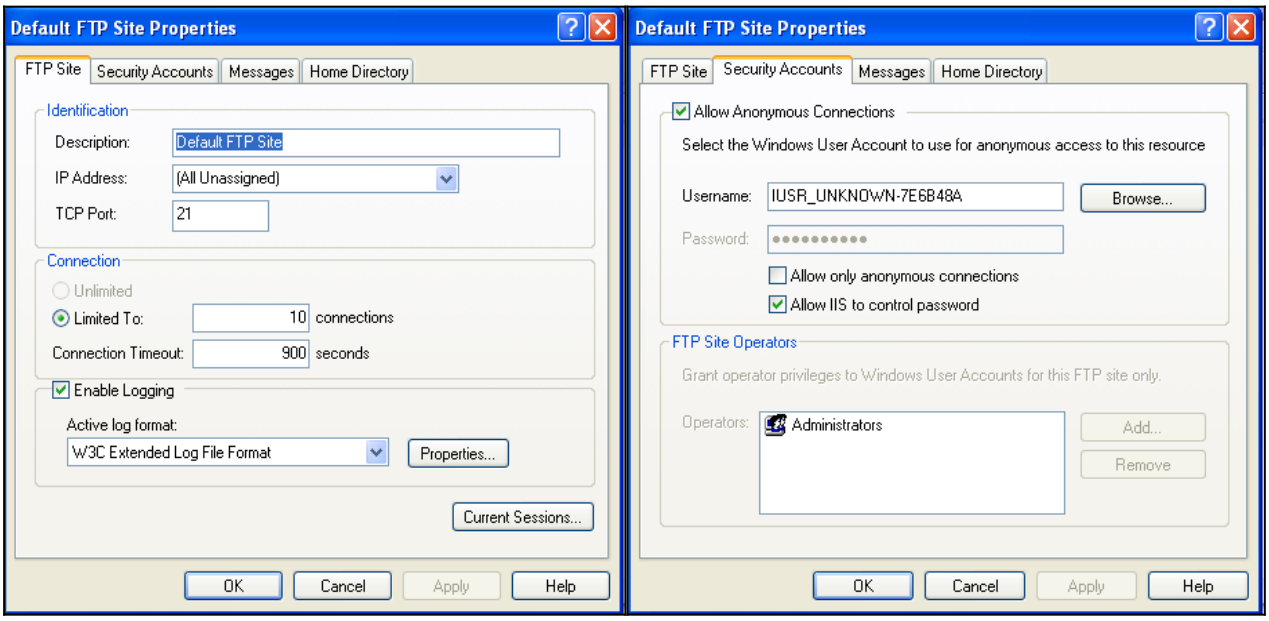
Após realizada a configuração basta acessa-la pelo menu Painel de controle>Ferramentas Administrativas> Internet Information Services (IIs).



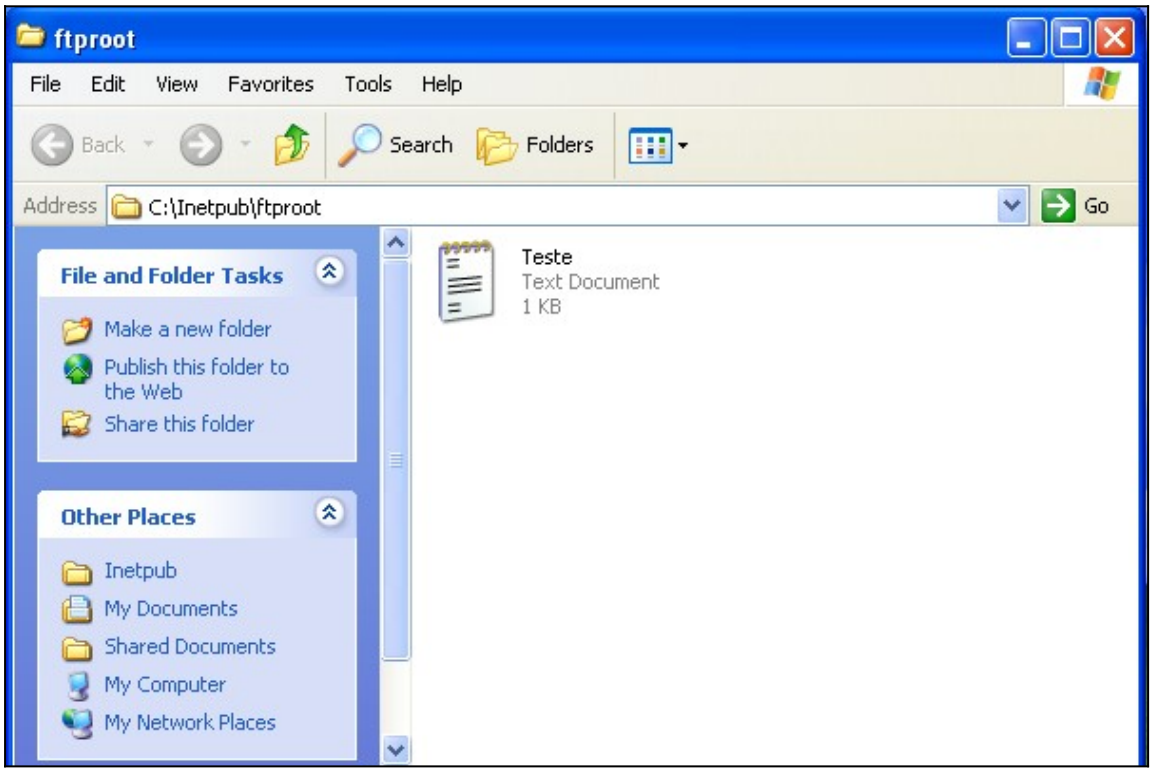
e como se pode ver o serviço FTP esta em execução.



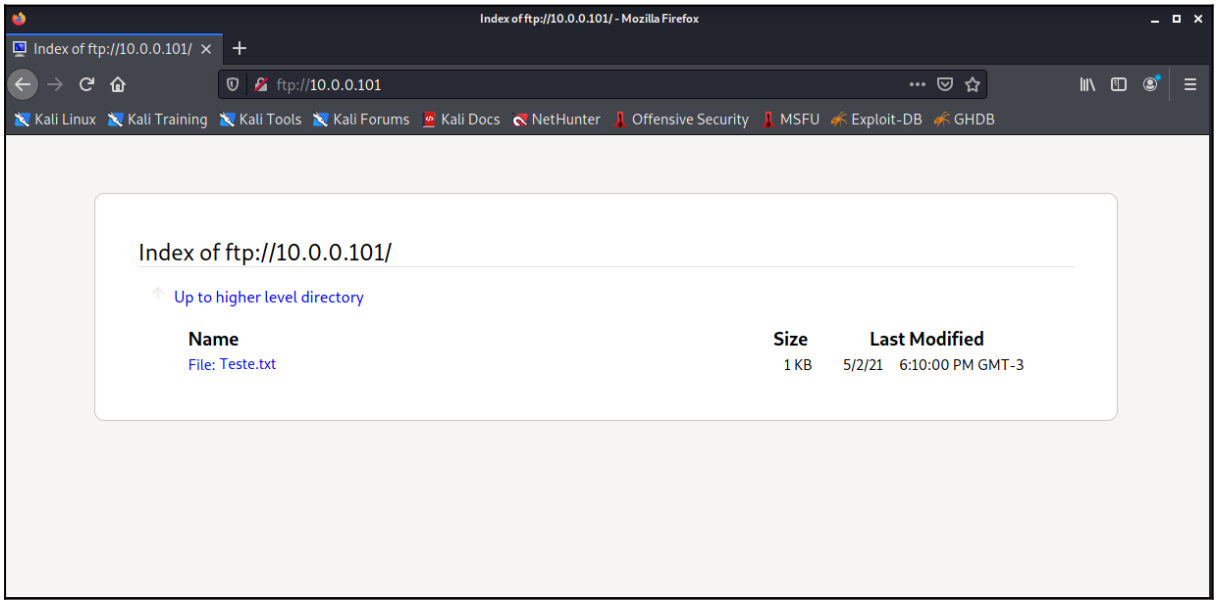
Após realizada configuração será necessário configurar o domínio e as portas desse servidor. E para isso basta clicar em cima do xxx e configurar como mostra a imagem x e y



Para fazer o upload de arquivos basta acessar o disco local C\Inetpub\ftproot, uma vez acessado basta copiar os arquivos dentro desse diretório.



Para acessar o servidor FTP basta digitar FTP://IP_SERVIDOR:PORTA



4.2.1 T50

```
root@kali:~# t50 -h
T50 Experimental Mixed Packet Injector Tool 5.4.1-rc1
Originally created by Nelson Brito <nbrito@sekure.org>
Now produced by Fernando Mercês <fernando@mentebinaria.com.br>

Usage: T50 <host> [/CIDR] [options]

Common Options:
   --threshold NUM          Threshold of packets to send     (default 1000)
   --flood                  This option supersedes the 'threshold'
   --encapsulated           Encapsulated protocol (GRE)      (default OFF)
-B,--bogus-csum             Bogus checksum                   (default OFF)
   --turbo                  Extend the performance           (default OFF)
-v,--version                Print version and exit
-h,--help                   Display this help and exit

GRE Options:
   --gre-seq-present        GRE sequence # present           (default OFF)
```

```
    --gre-key-present         GRE key present                (default OFF)
    --gre-sum-present         GRE checksum present           (default OFF)
    --gre-key NUM             GRE key                        (default RANDOM)
    --gre-sequence NUM        GRE sequence #                 (default RANDOM)
    --gre-saddr ADDR          GRE IP source IP address       (default RANDOM)
    --gre-daddr ADDR          GRE IP destination IP address  (default RANDOM)

DCCP/TCP/UDP Options:
    --sport NUM               DCCP|TCP|UDP source port       (default RANDOM)
    --dport NUM               DCCP|TCP|UDP destination port  (default RANDOM)

IP Options:
 -s,--saddr ADDR              IP source IP address           (default RANDOM)
    --tos NUM                 IP type of service             (default 0x40)
    --id NUM                  IP identification              (default RANDOM)
    --frag-offset NUM         IP fragmentation offset        (default 0)
    --ttl NUM                 IP time to live                (default 255)
    --protocol PROTO          IP protocol                    (default TCP)

ICMP Options:
    --icmp-type NUM           ICMP type                      (default 8)
    --icmp-code NUM           ICMP code                      (default 0)
    --icmp-gateway ADDR       ICMP redirect gateway          (default RANDOM)
    --icmp-id NUM             ICMP identification            (default RANDOM)
    --icmp-sequence NUM       ICMP sequence #                (default RANDOM)

IGMP Options:
    --igmp-type NUM           IGMPv1/v3 type                 (default 0x11)
    --igmp-code NUM           IGMPv1/v3 code                 (default 0)
    --igmp-group ADDR         IGMPv1/v3 address              (default RANDOM)
    --igmp-qrv NUM            IGMPv3 QRV                     (default RANDOM)
    --igmp-suppress           IGMPv3 suppress router-side    (default OFF)
    --igmp-qqic NUM           IGMPv3 QQIC                    (default RANDOM)
    --igmp-grec-type NUM      IGMPv3 group record type       (default 1)
    --igmp-sources NUM        IGMPv3 # of sources            (default 2)
    --igmp-multicast ADDR     IGMPv3 group record multicast  (default RANDOM)
    --igmp-address ADDR,...   IGMPv3 source address(es)      (default RANDOM)

TCP Options:
    --acknowledge NUM         TCP ACK sequence #             (default RANDOM)
    --sequence NUM            TCP SYN sequence #             (default RANDOM)
    --data-offset NUM         TCP data offset                (default 5)
 -F,--fin                     TCP FIN flag                   (default OFF)
 -S,--syn                     TCP SYN flag                   (default OFF)
```

```
 -R,--rst                 TCP RST flag                 (default OFF)
 -P,--psh                  TCP PSH flag                  (default OFF)
 -A,--ack                  TCP ACK flag                  (default OFF)
 -U,--urg                  TCP URG flag                  (default OFF)
 -E,--ece                  TCP ECE flag                  (default OFF)
 -C,--cwr                  TCP CWR flag                   (default OFF)
 -W,--window NUM           TCP Window size               (default NONE)
    --urg-pointer NUM      TCP URG pointer               (default NONE)
    --mss NUM              TCP Maximum Segment Size      (default NONE)
    --wscale NUM           TCP Window Scale              (default NONE)
    --tstamp NUM:NUM       TCP Timestamp (TSval:TSecr)   (default NONE)
    --sack-ok              TCP SACK-Permitted            (default OFF)
    --ttcp-cc NUM          T/TCP Connection Count (CC)   (default NONE)
    --ccnew NUM            T/TCP Connection Count (CC.NEW)  (default NONE)
    --ccecho NUM           T/TCP Connection Count (CC.ECHO) (default NONE)
    --sack NUM:NUM         TCP SACK Edges (Left:Right)   (default NONE)
    --md5-signature        TCP MD5 signature included    (default OFF)
    --authentication       TCP-AO authentication included   (default OFF)
    --auth-key-id NUM      TCP-AO authentication key ID     (default 1)
    --auth-next-key NUM    TCP-AO authentication next key   (default 1)
    --nop                  TCP No-Operation              (default EOL)

EGP Options:
    --egp-type NUM         EGP type                      (default 3)
    --egp-code NUM         EGP code                      (default 3)
    --egp-status NUM       EGP status                    (default 1)
    --egp-as NUM           EGP autonomous system         (default RANDOM)
    --egp-sequence NUM     EGP sequence #                (default RANDOM)
    --egp-hello NUM        EGP hello interval            (default RANDOM)
    --egp-poll NUM         EGP poll interval             (default RANDOM)

RIP Options:
    --rip-command NUM      RIPv1/v2 command              (default 2)
    --rip-family NUM       RIPv1/v2 address family       (default 2)
    --rip-address ADDR     RIPv1/v2 router address       (default RANDOM)
    --rip-metric NUM       RIPv1/v2 router metric        (default RANDOM)
    --rip-domain NUM       RIPv2 router domain           (default RANDOM)
    --rip-tag NUM          RIPv2 router tag              (default RANDOM)
    --rip-netmask ADDR     RIPv2 router subnet mask      (default RANDOM)
    --rip-next-hop ADDR    RIPv2 router next hop         (default RANDOM)
    --rip-authentication   RIPv2 authentication included  (default OFF)
    --rip-auth-key-id NUM  RIPv2 authentication key ID    (default 1)
    --rip-auth-sequence NUM  RIPv2 authentication sequence #  (default RANDOM)
```

```
DCCP Options:
   --dccp-data-offset NUM    DCCP data offset              (default VARY)
   --dccp-cscov NUM          DCCP checksum coverage        (default 0)
   --dccp-ccval NUM          DCCP HC-Sender CCID           (default RANDOM)
   --dccp-type NUM           DCCP type                     (default 0)
   --dccp-extended           DCCP extend for sequence #    (default OFF)
   --dccp-sequence-1 NUM     DCCP sequence #               (default RANDOM)
   --dccp-sequence-2 NUM     DCCP extended sequence #      (default RANDOM)
   --dccp-sequence-3 NUM     DCCP sequence # low           (default RANDOM)
   --dccp-service NUM        DCCP service code             (default RANDOM)
   --dccp-acknowledge-1 NUM  DCCP acknowledgment # high    (default
RANDOM)
   --dccp-acknowledge-2 NUM  DCCP acknowledgment # low     (default
RANDOM)
   --dccp-reset-code NUM     DCCP reset code               (default RANDOM)

RSVP Options:
   --rsvp-flags NUM          RSVP flags                    (default 1)
   --rsvp-type NUM           RSVP message type             (default 1)
   --rsvp-ttl NUM            RSVP time to live             (default 254)
   --rsvp-session-addr ADDR  RSVP SESSION destination address (default
RANDOM)
   --rsvp-session-proto NUM  RSVP SESSION protocol ID      (default 1)
   --rsvp-session-flags NUM  RSVP SESSION flags            (default 1)
   --rsvp-session-port NUM   RSVP SESSION destination port (default RANDOM)
   --rsvp-hop-addr ADDR      RSVP HOP neighbor address     (default RANDOM)
   --rsvp-hop-iface NUM      RSVP HOP logical interface    (default RANDOM)
   --rsvp-time-refresh NUM   RSVP TIME refresh interval    (default 360)
   --rsvp-error-addr ADDR    RSVP ERROR node address       (default RANDOM)
   --rsvp-error-flags NUM    RSVP ERROR flags              (default 2)
   --rsvp-error-code NUM     RSVP ERROR code               (default 2)
   --rsvp-error-value NUM    RSVP ERROR value              (default 8)
   --rsvp-scope NUM          RSVP SCOPE # of address(es)   (default 1)
   --rsvp-address ADDR,...   RSVP SCOPE address(es)        (default RANDOM)
   --rsvp-style-option NUM   RSVP STYLE option vector      (default 18)
   --rsvp-sender-addr ADDR   RSVP SENDER TEMPLATE address  (default
RANDOM)
   --rsvp-sender-port NUM    RSVP SENDER TEMPLATE port     (default
RANDOM)
   --rsvp-tspec-traffic      RSVP TSPEC service traffic    (default OFF)
   --rsvp-tspec-guaranteed   RSVP TSPEC service guaranteed (default OFF)
   --rsvp-tspec-r NUM        RSVP TSPEC token bucket rate  (default RANDOM)
   --rsvp-tspec-b NUM        RSVP TSPEC token bucket size  (default RANDOM)
   --rsvp-tspec-p NUM        RSVP TSPEC peak data rate     (default RANDOM)
```

```
   --rsvp-tspec-m NUM        RSVP TSPEC minimum policed unit  (default RANDOM)
   --rsvp-tspec-M NUM        RSVP TSPEC maximum packet size   (default RANDOM)
   --rsvp-adspec-ishop NUM   RSVP ADSPEC IS HOP count         (default RANDOM)
   --rsvp-adspec-path NUM    RSVP ADSPEC path b/w estimate    (default
RANDOM)
   --rsvp-adspec-m NUM       RSVP ADSPEC minimum path latency (default
RANDOM)
   --rsvp-adspec-mtu NUM     RSVP ADSPEC composed MTU         (default
RANDOM)
   --rsvp-adspec-guaranteed  RSVP ADSPEC service guaranteed   (default OFF)
   --rsvp-adspec-Ctot NUM    RSVP ADSPEC ETE composed value C (default
RANDOM)
   --rsvp-adspec-Dtot NUM    RSVP ADSPEC ETE composed value D (default
RANDOM)
   --rsvp-adspec-Csum NUM    RSVP ADSPEC SLR point composed C (default
RANDOM)
   --rsvp-adspec-Dsum NUM    RSVP ADSPEC SLR point composed D (default
RANDOM)
   --rsvp-adspec-controlled  RSVP ADSPEC service controlled   (default OFF)
   --rsvp-confirm-addr ADDR  RSVP CONFIRM receiver address    (default
RANDOM)

IPSEC Options:
   --ipsec-ah-length NUM     IPSec AH header length           (default NONE)
   --ipsec-ah-spi NUM        IPSec AH SPI                     (default RANDOM)
   --ipsec-ah-sequence NUM   IPSec AH sequence #              (default RANDOM)
   --ipsec-esp-spi NUM       IPSec ESP SPI                    (default RANDOM)
   --ipsec-esp-sequence NUM  IPSec ESP sequence #             (default RANDOM)

EIGRP Options:
   --eigrp-opcode NUM        EIGRP opcode                     (default 1)
   --eigrp-flags NUM         EIGRP flags                      (default RANDOM)
   --eigrp-sequence NUM      EIGRP sequence #                 (default RANDOM)
   --eigrp-acknowledge NUM   EIGRP acknowledgment #           (default RANDOM)
   --eigrp-as NUM            EIGRP autonomous system          (default RANDOM)
   --eigrp-type NUM          EIGRP type                       (default 258)
   --eigrp-length NUM        EIGRP length                     (default NONE)
   --eigrp-k1 NUM            EIGRP parameter K1 value         (default 1)
   --eigrp-k2 NUM            EIGRP parameter K2 value         (default 0)
   --eigrp-k3 NUM            EIGRP parameter K3 value         (default 1)
   --eigrp-k4 NUM            EIGRP parameter K4 value         (default 0)
   --eigrp-k5 NUM            EIGRP parameter K5 value         (default 0)
   --eigrp-hold NUM          EIGRP parameter hold time        (default 360)
   --eigrp-ios-ver NUM.NUM   EIGRP IOS release version        (default 12.4)
```

```
   --eigrp-rel-ver NUM.NUM   EIGRP PROTO release version      (default 1.2)
   --eigrp-next-hop ADDR     EIGRP [in|ex]ternal next-hop     (default RANDOM)
   --eigrp-delay NUM         EIGRP [in|ex]ternal delay        (default RANDOM)
   --eigrp-bandwidth NUM     EIGRP [in|ex]ternal bandwidth    (default RANDOM)
   --eigrp-mtu NUM           EIGRP [in|ex]ternal MTU          (default 1500)
   --eigrp-hop-count NUM     EIGRP [in|ex]ternal hop count    (default RANDOM)
   --eigrp-load NUM          EIGRP [in|ex]ternal load         (default RANDOM)
   --eigrp-reliability NUM   EIGRP [in|ex]ternal reliability  (default RANDOM)
   --eigrp-daddr ADDR/CIDR   EIGRP [in|ex]ternal address(es)  (default RANDOM)
   --eigrp-src-router ADDR   EIGRP external source router     (default RANDOM)
   --eigrp-src-as NUM        EIGRP external autonomous system (default RANDOM)
   --eigrp-tag NUM           EIGRP external arbitrary tag     (default RANDOM)
   --eigrp-proto-metric NUM  EIGRP external protocol metric   (default RANDOM)
   --eigrp-proto-id NUM      EIGRP external protocol ID       (default 2)
   --eigrp-ext-flags NUM     EIGRP external flags             (default RANDOM)
   --eigrp-address ADDR      EIGRP multicast sequence address (default RANDOM)
   --eigrp-multicast NUM     EIGRP multicast sequence #       (default RANDOM)
   --eigrp-authentication    EIGRP authentication included    (default OFF)
   --eigrp-auth-key-id NUM   EIGRP authentication key ID      (default 1)

OSPF Options:
   --ospf-type NUM           OSPF type                        (default 1)
   --ospf-length NUM         OSPF length                      (default NONE)
   --ospf-router-id ADDR     OSPF router ID                   (default RANDOM)
   --ospf-area-id ADDR       OSPF area ID                     (default 0.0.0.0)
 -1,--ospf-option-MT         OSPF multi-topology / TOS-based  (default RANDOM)
 -2,--ospf-option-E          OSPF external routing capability (default RANDOM)
 -3,--ospf-option-MC         OSPF multicast capable           (default RANDOM)
 -4,--ospf-option-NP         OSPF NSSA supported              (default RANDOM)
 -5,--ospf-option-L          OSPF LLS data block contained    (default RANDOM)
 -6,--ospf-option-DC         OSPF demand circuits supported   (default RANDOM)
 -7,--ospf-option-O          OSPF Opaque-LSA                  (default RANDOM)
 -8,--ospf-option-DN         OSPF DOWN bit                    (default RANDOM)
   --ospf-netmask ADDR       OSPF router subnet mask          (default RANDOM)
   --ospf-hello-interval NUM OSPF HELLO interval              (default RANDOM)
   --ospf-hello-priority NUM OSPF HELLO router priority       (default 1)
   --ospf-hello-dead NUM     OSPF HELLO router dead interval  (default 360)
   --ospf-hello-design ADDR  OSPF HELLO designated router     (default RANDOM)
   --ospf-hello-backup ADDR  OSPF HELLO backup designated     (default
RANDOM)
   --ospf-neighbor NUM       OSPF HELLO # of neighbor(s)      (default NONE)
   --ospf-address ADDR,...   OSPF HELLO neighbor address(es)  (default RANDOM)
   --ospf-dd-mtu NUM         OSPF DD MTU                      (default 1500)
   --ospf-dd-dbdesc-MS       OSPF DD master/slave bit option  (default RANDOM)
```

```
--ospf-dd-dbdesc-M        OSPF DD more bit option          (default RANDOM)
--ospf-dd-dbdesc-I        OSPF DD init bit option          (default RANDOM)
--ospf-dd-dbdesc-R        OSPF DD out-of-band resync       (default RANDOM)
--ospf-dd-sequence NUM    OSPF DD sequence #               (default RANDOM)
--ospf-dd-include-lsa     OSPF DD include LSA header       (default OFF)
--ospf-lsa-age NUM        OSPF LSA age                     (default 360)
--ospf-lsa-do-not-age     OSPF LSA do not age              (default OFF)
--ospf-lsa-type NUM       OSPF LSA type                    (default 1)
--ospf-lsa-id ADDR        OSPF LSA ID address              (default RANDOM)
--ospf-lsa-router ADDR    OSPF LSA advertising router      (default RANDOM)
--ospf-lsa-sequence NUM   OSPF LSA sequence #              (default RANDOM)
--ospf-lsa-metric NUM     OSPF LSA metric                  (default RANDOM)
--ospf-lsa-flag-B         OSPF Router-LSA border router    (default RANDOM)
--ospf-lsa-flag-E         OSPF Router-LSA external router  (default RANDOM)
--ospf-lsa-flag-V         OSPF Router-LSA virtual router   (default RANDOM)
--ospf-lsa-flag-W         OSPF Router-LSA wild router      (default RANDOM)
--ospf-lsa-flag-NT        OSPF Router-LSA NSSA translation (default RANDOM)
--ospf-lsa-link-id ADDR   OSPF Router-LSA link ID          (default RANDOM)
--ospf-lsa-link-data ADDR OSPF Router-LSA link data        (default RANDOM)
--ospf-lsa-link-type NUM  OSPF Router-LSA link type        (default 1)
--ospf-lsa-attached ADDR  OSPF Network-LSA attached router (default RANDOM)
--ospf-lsa-larger         OSPF ASBR/NSSA-LSA ext. larger   (default OFF)
--ospf-lsa-forward ADDR   OSPF ASBR/NSSA-LSA forward       (default RANDOM)
--ospf-lsa-external ADDR  OSPF ASBR/NSSA-LSA external      (default RANDOM)
--ospf-vertex-router      OSPF Group-LSA type router       (default RANDOM)
--ospf-vertex-network     OSPF Group-LSA type network      (default RANDOM)
--ospf-vertex-id ADDR     OSPF Group-LSA vertex ID         (default RANDOM)
--ospf-lls-extended-LR    OSPF LLS Extended option LR      (default OFF)
--ospf-lls-extended-RS    OSPF LLS Extended option RS      (default OFF)
--ospf-authentication     OSPF authentication included     (default OFF)
--ospf-auth-key-id NUM    OSPF authentication key ID       (default 1)
--ospf-auth-sequence NUM  OSPF authentication sequence #   (default RANDOM)
```

Some considerations while running this program:

1. There is no limitation of using as many options as possible.
2. Report T50 bugs at http://t50.sf.net.
3. Some header fields with default values MUST be set to '0' for RANDOM.
4. Mandatory arguments to long options are mandatory for short options too.
5. Be nice when using T50, the author DENIES its use for DoS/DDoS purposes.
6. Running T50 with '--protocol T50' option, sends ALL protocols sequentially.

T50 Usage Example
Run a default flood test (–flood) against the destination IP (192.168.1.1):

root@kali:~# t50 --flood 192.168.1.1
entering in flood mode...
hit CTRL+C to break.
T50 5.4.1-rc1 successfully launched on May 17th 2014 10:48:51

4.2.2 Inundator

root@kali:~# inundator -h

inundator - fills ids/ips/waf logs with false positives to obfuscate an attack.
Syntax: /usr/bin/inundator [options] <target>

Options:

-a, --auth Credentials for SOCKS proxy in user:pass format.
Default: undef
-d, --delay Delay in microseconds (millionths of a second) after sending an attack.
Default: 0mus since we default to tor, and tor is slow.
-n, --no-threads Disable thread support.
Default: threads are used.
-p, --proxy Define the SOCKS proxy to use for attacks in host:port format. The use of a SOCKS proxy is mandatory for rather obvious reasons.
Default: localhost:9050 (tor)
-r, --rules Path to directory containing Snort rules files.
Default: /etc/snort/rules/
-s, --socks-version Specify SOCKS version to use (4 or 5).
Default: 5
-t, --threads Number of concurrent threads.

Default: 25

-u, --use-comments Don't ignore commented lines in Snort rules files.

Default: commented lines are ignored

--verbose Provide more information about attacks sent.

--Version Print version information and exit.

Target:

- Single host (FQDN or ip addr)
- Range of ip addrs
- Subnet in CIDR format

See 'man 1 inundator' for more information.

inundator Usage Example

Use 5 threads (-t 5) to flood the target system (192.168.1.1):

root@kali:~# inundator -t 5 192.168.1.1

[+] queuing up attacks...

[+] queuing up target(s)...

[+] detecting open ports on 192.168.1.1...

[+] child 1 now attacking.

REFERÊNCIAS BIBLIOGRÁFICAS

DE BITTENCOURT, F.; DE LUCCA, G. **MÉTODOS PARA PREVENÇÃO E DEFESA DE ATAQUES DDoS**. Revista Vincci - Periódico Científico da Faculdade SATC, v. 2, n. 1, p. 92-117, 25 abr. 2017.Disponível em:<http://revistavincci.satc.edu.br/ojs/index.php/Revista-Vincci/article/view/84/32>. Acessado em: 06 de Março de 2021,15:30.

LUIZ G. A. C.; PÉRICLES D. O. R.; SAMUEL N. D. V.; CLAUDINES T. T. **Estudo de caso de Ataques de Negação de Serviço (DDoS)**, Curso de Tecnologia em Redes de Computadores - Faculdade de Tecnologia de Bauru (FATEC) Rua Manoel Bento da Cruz, nº 30 Quadra 3 - Centro - 17.015-171 - Bauru, SP – Brasil.Disponível em:<http://www.fatecbauru.edu.br/ojs/index.php/CET/article/view/197>.Acessado em: 06 de Março de 2021,17:20.

SCHILDT, HEBERT. **C: completo e total**. 3. ed. rev. atual. São Paulo, SP: Pearson Makron Books, c1997.TOCCI.Disponível em: <https://www.inf.ufpr.br/lesoliveira/download/c-completo-total.pdf>.Acessado em: 06 de Março de 2021,16:07.