

Aluno: Cássio de Albuquerque
Curso : Técnico em Redes de Computadores

SA2 - Atividade 4 - Presencial - Instalar a ferramenta Ntop na máquina virtual Linux (Ubuntu Server)

Introdução:

Foi nos proposto efetuar a instalação da ferramenta Ntop, utilizada para monitoramento de redes médias e mais robustas.

Acredito que simplesmente efetuar a instalação do software mecanicamente não adicionaria conteúdo relevante à atividade. Por isso, optei por realizar um pequeno resumo sobre as características dessa ferramenta, mais robusta que o MRTG, que auxilia o Adm. de redes em sua tomada de decisão no dia a dia.

Ntop

O ntopng foi desenvolvido na Universidade de Pisa, Itália. É um software de código aberto e pode ser baixado na internet através de seu repositório no site github.

O NTop monitora e gera relatórios sobre o tráfego e suporte dos hosts pelos seguintes protocolos:

TCP/UDP/ICMP,

(R)ARP,

IPX,

DLC,

DECnet,

AppleTalk,

Netbios

TCP/UDP

Diferentemente do MRTG que apenas gera estatísticas através do protocolo snmp, o Ntop é capaz de analisar o tráfego e propor ações de segurança com base nos dados da rede que coletou, utilizando, também o snmp.

Além disso, o Ntop pode ser utilizado em parceria com o Wireshark, coletando seus dados para gerar relatórios.

Por fim, o Ntop é compatível com a tecnologia Netflow dos equipamentos Cisco.

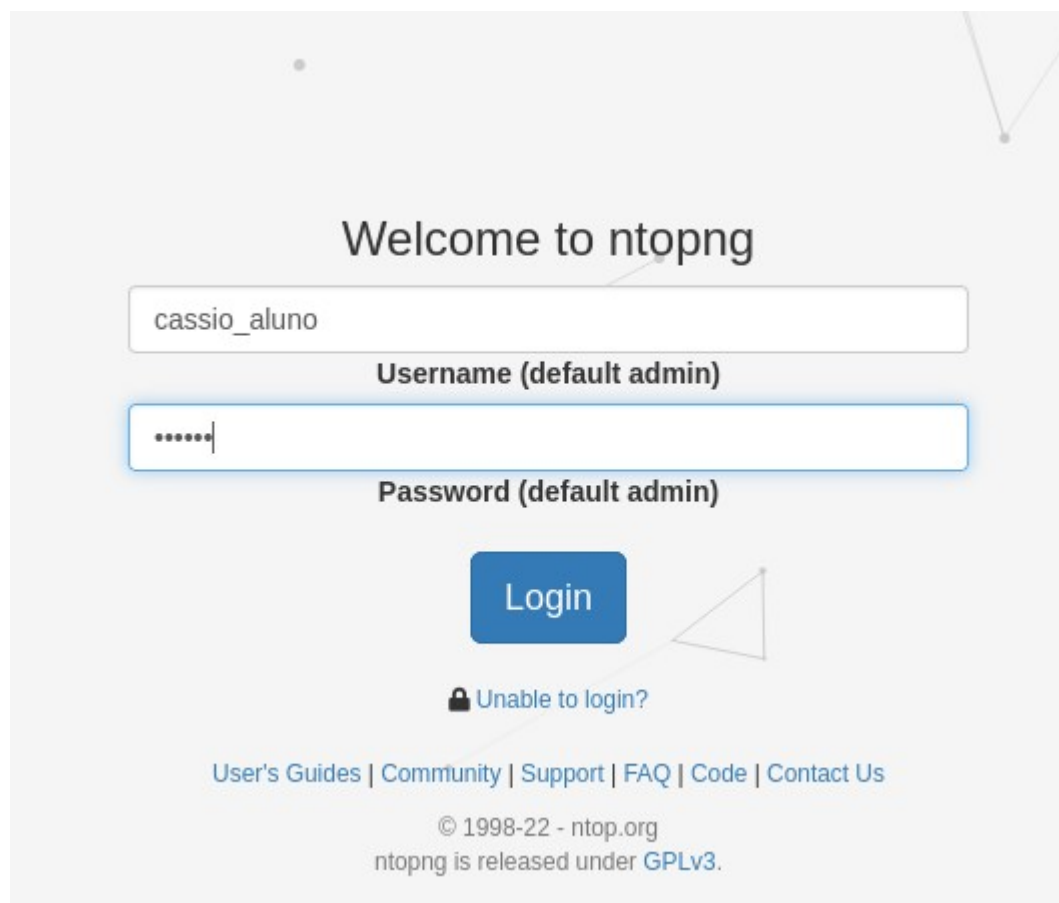
Diante do exposto, fica claro que o ntop é uma boa ferramenta para o gerenciamento de uma rede e que, aliado a outras, pode nos ajudar a tornar nossa rede mais eficiente, segura e escalável.

Abaixo segue a instalação e configuração do software.

1 Instalação ferramenta Ntop no Linux Ubuntu

```
root@ubuntu-VirtualBox: /home/ubuntu# apt-get install ntopng
Lendo listas de pacotes... Pronto
Construindo árvore de dependências... Pronto
Lendo informação de estado... Pronto
Os pacotes adicionais seguintes serão instalados:
 fonts-font-awesome fonts-glyphicons-halflings javascript-common libatomic1 libdbi1 libhiredis0.14 libjemalloc2
 libjs-bootstrap libjs-d3 libjs-jquery libjs-jquery-form libjs-jquery-metadata libjs-jquery-tablesorter
 libjs-jquery-ui libjs-rickshaw liblua5.1-0 liblua5.3-0 liblzfl1 libmysqlclient21 libndpi4.2 libnorm1 libpgm-5.3-0
 librrd8 libwireshark-data libzmq5 lua-bitop lua-cjson mysql-common node-html5shiv ntopng-data redis-server
 redis-tools
Pacotes sugeridos:
 apache2 | lighttpd | httpd libjs-jquery-ui-docs geoipupdate geoip-database geoip-database-extra libjs-leaflet
 libjs-leaflet.markercluster snmp-mibs-downloader nodejs ruby-redis
Os NOVOS pacotes a seguir serão instalados:
 fonts-font-awesome fonts-glyphicons-halflings javascript-common libatomic1 libdbi1 libhiredis0.14 libjemalloc2
 libjs-bootstrap libjs-d3 libjs-jquery libjs-jquery-form libjs-jquery-metadata libjs-jquery-tablesorter
 libjs-jquery-ui libjs-rickshaw liblua5.1-0 liblua5.3-0 liblzfl1 libmysqlclient21 libndpi4.2 libnorm1 libpgm-5.3-0
 librrd8 libwireshark-data libzmq5 lua-bitop lua-cjson mysql-common node-html5shiv ntopng ntopng-data redis-server
 redis-tools
0 pacotes atualizados, 33 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 18,6 MB de arquivos.
Depois desta operação, 86,5 MB adicionais de espaço em disco serão usados.
```

2- Configuração de Usuário e senha




3- Alterando Senha

Change Password

Default admin password must be changed.
Please enter a new password below.

Language

 Portuguese ▼

Change Password

[Logout](#)

© 1998-22 - ntop.org
ntopng is released under [GPLv3](#).

4- Monitoramento ativo:

Ativo Fluxos

?

10 ▾ Hosts ▾ Status ▾ Severity ▾ Direção ▾ Aplicações ▾ Categorias ▾ DSCP ▾ Pool de host ▾ Networks ▾ Versão IP ▾

Protocol ▾

	Aplicação	Protocolo	Cliente	Servidora	Duração	Demolir	Thpt real	Total de Bytes	Info
	TLS.AmazonAW...	TCP	ev00008882.sp.local :36618	52.85.213.67 :https	02:00		0 bps ▾	16.61 KB ▾	conte
	TLS.AmazonAW...	TCP	ev00008882.sp.local :43758	52.85.213.70 :https	00:01 sec		0 bps ▾	16.13 KB ▾	firefo
	HTTP	TCP	ev00008882.sp.local :33758	34.107.221.82 :http	03:33		0 bps ▾	14.38 KB ▾	detec
	HTTP	TCP	ev00008882.sp.local :33762	34.107.221.82 :http	03:33		0 bps ▾	13.2 KB ▾	detec
	TLS	TCP	ev00008882.sp.local :49472	34.117.237.239 :https	01:26		0 bps ▾	9.43 KB ▾	contil

Ativa Pausado

Contribute to the project by sending encrypted, anonymous telemetry data to [ntop.org](#).

enp0s3 [08:00:27:A0:50:3B]

Família

pcap

1518 Bytes

Rapidez

1 Gbit/s

9.0% 0.0%
Local->Remote Other

91.0%
Remote->Local

0.1%
Other

99.9%
IPv4

Local Hosts Anomalies

0 ▾

Remote Hosts Anomalies

0 ▾

248.2 KB [491 Pkts] ▾

Pacotes Soltos

0 Pkts ▾

18 KB [220 Pkts] ▾

Tráfego recebido

230.2 KB [271 Pkts] ▾

1 min

pcap baixar