UNIVERSIDADE DO ESTADO DE MATO GROSSO
CAMPUS UNIVERSITÁRIO DEP. EST. RENÊ BARBOUR
FACULDADE DE CIÊNCIAS EXATAS E TECNOLÓGICAS
CURSO DE CIÊNCIA DA COMPUTAÇÃO

ArchScan - Scan Port TCP / UDP

Discentes:

Karan Luciano Silva

Douglas Teles de Oliveiras

Hevelyn Hespanhol Câmara

Docente:

Me. Diógenes Antônio Marques José

Roteiro

- Resumo
- Objetivo
- Contextualização
- Metodologia
- Descrição da Proposta
- Resultados
- Dificuldades
- Conclusões
- Bibliografia

Resumo

- O escaneamento de portas em sistemas distribuídos faz uso de sockets com e sem conexão.
- Linguagem de Programação Python.
- O aplicativo foi testado em um testbed com quatro computadores.
- Pode ser usado como auxílio no estudo de sistemas distribuídos uma vez que ele possibilita visualizar na prática os conceitos teóricos de socktes.
- Os resultados mostram que o software encontrou corretamente as portas abertas e fechadas na rede.

Objetivo

- Desenvolver um software com interface gráfica que permite escanear portas de serviços TCP/UDP e demonstrar sua eficácia em comparação a outros programas que realizam as mesmas funções.

Contextualização

- Sistemas distribuídos
- Auditoria e segurança de rede
- Nmap - Linux
- Zenmap - Windows
- Hosts estão disponíveis na rede
- serviços (nome do aplicativo e versão)
- sistemas operacionais (e versões do SO)
- Tipo de protocolo

Metodologia

- **Pesquisa:**
  - Revisão Bibliográfica;
- **Sofware Utilizados:**
  - Python 2.7;
  - Geany;
  - Nmap;
  - ZenMap;
  - Pscan;
  - Wireshark;
  - Gimp;
- **Sistema Operacional:**
  - Arch Linux x86_64;
  - Ubuntu x86_64;
  - Windows 7 x86_64;
- **Tipo de Socket:**
  - TCP e UDP;
- **Hardware para desenvolvimento:**
  - Intel i3 e i7;
  - GeForce GT 425M;
  - 8GB RAM;
  - SSD 128GB + HD 500GB;

Metodologia

- **Hardware do ambiente de teste:**
  - Intel Pentium;
  - 4GB RAM;
  - HD 160GB;
- **Testes Realizados:**
  - Testebed;
  - 3 Computadores;
  - Rede Local;
  - Classe C 192.168.0.0/24;
- **Comparação:**
  - Nmap;
  - Wireshark;

Descrição da Proposta

- Python;
- De fluxo → SOCK_STREAM;
- De pacotes → SOCK_DEGRAM;
- Threads;

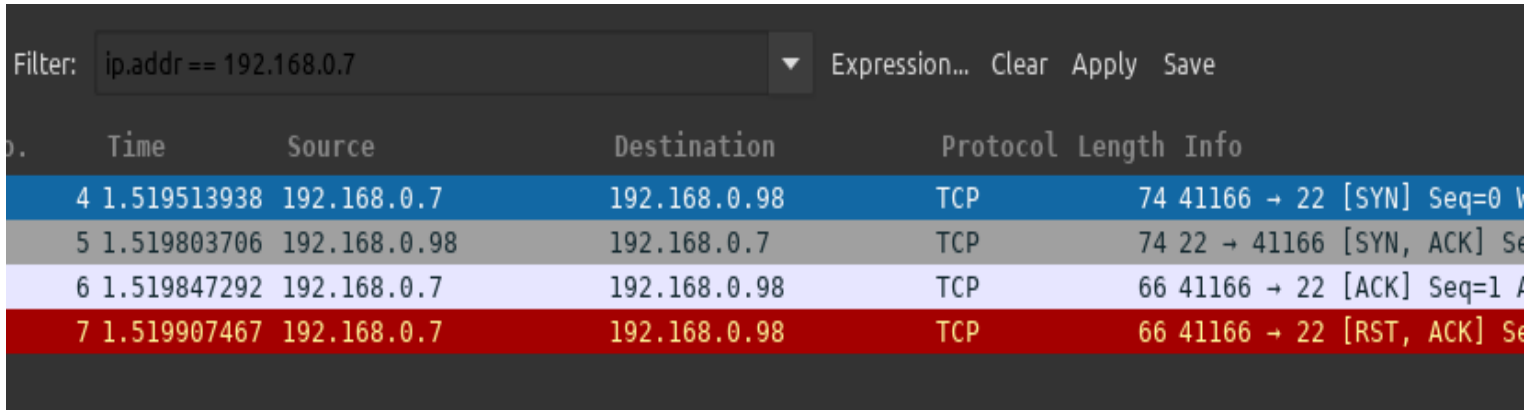
Resultados


```
root@karan-ubuntu:/home/karan/Desktop/ArchScan# nmap -sT -p 22 192.168.0.7

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-08 10:32 -03
Nmap scan report for 192.168.0.7
Host is up (0.00034s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 78:DD:08:BA:E2:12 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 13.40 seconds
root@karan-ubuntu:/home/karan/Desktop/ArchScan#
```



Resultados


```
root@karan-ubuntu:~# nmap -sU -p 140 192.168.0.7

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-08 11:35 -03
Nmap scan report for 192.168.0.7
Host is up (0.0014s latency).

PORT    STATE SERVICE
140/udp open  emfis-data
MAC Address: 78:DD:08:BA:E2:12 (Hon Hai Precision Ind.)

Nmap done: 1 IP address (1 host up) scanned in 13.67 seconds
root@karan-ubuntu:~#
```

```
root@karan-ubuntu:/home/karan/Desktop/UDP# ./socket_servidor_UDP 192.168.0.7 140
sh: 1: archscan: not found
Foi estabelecida uma conexao do endereco (192.168.0.7):
Porta do cliente é: 38609
Mensagem é: archscan
```

Dificuldades

- Linguagem Python;
- Implementação da Interface Gráfica;
- Função Scan UDP;

Conclusões

- Contato com uma nova linguagem de programação;
- Utilização do LateX;
- Auxílio a profissionais do ramo de segurança;
- Estimulo a uso de software livre;
- Desenvolvimento de atividades prática na disciplina de sistemas distribuídos;
- O software teve êxito na maioria das suas funções;

Bibliografia

- P. M. Menezes, L. M. Cardoso, F. G. Rocha**, Segurança em redes de computadores uma visão sobre o processo de pentest, Interfaces Científicas Exatas e Tecnológicas 1** (2) (2015) 85–96.
- G. Lyon, **Nmap security scanner, Nmap. org**,[En línea]. Available: http://nmap. org/.[Último acceso: 20 abril 2015].
- G. Lyon, **Nmap**, http://nmap. org/.
- Z. Durumeric, E. Wustrow, J. A. Halderman, **Zmap: Fast internet-wide scanning and its security applications.**, in: USENIX Security Symposium, Vol. 8, 2013, pp. 47–53.
- S. C. R. Giavaroto, G. R. Santos, **Backtrack linux–auditoria e teste de invasão em redes de computadores**, Rio de Janeiro: Editora Ciência Moderna.

Bibliografia

- V. Vieira, **Pscan: Uma alternativa ao nmap.**, sejalivre.org Available: https://sejalivre.org/pscan-uma-alternativa-ao-nmap/.
- G. Combs, **Wireshark**, http://www. wireshark. orgA.
- N. M. G. Farruca, **Wireshark para sistemas distribuídos**, Ph.D. thesis, FCT-UNL (2009).
- R. Chandel, **Understanding nmap scan with wireshark.**, Available: https://www.hackingarticles.in/understanding-nmap-scan-wireshark/.
- R. E. Ferreira, Linux Guia do Administrador do Sistema-2a Edição, Novatec Editora, 2008.
- W. R. Stevens, **Programação de Rede UNIX: API para soquetes de rede**, Bookman Editora, 2009.

Bibliografia

- P. Geus, E. NAKAMURA, **Segurança de redes em ambientes cooperativos** (2002).
- J. Jung, V. Paxson, A. W. Berger, H. Balakrishnan, **Fast portscan detection using sequential hypothesis testing**, in: Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, IEEE, 2004, pp. 211–225.

Bibliografia

- P. Geus, E. NAKAMURA, **Segurança de redes em ambientes cooperativos** (2002).
- J. Jung, V. Paxson, A. W. Berger, H. Balakrishnan, **Fast portscan detection using sequential hypothesis testing**, in: Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, IEEE, 2004, pp. 211–225.

Perguntas


PROCURAMOS FAZER
O POSSÍVEL PARA NÃO
PASSARMOS VERGONHA.
MUITO OBRIGADO.
TENHAM UM BOM DIA.