INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 01: *Portscan* com Nmap

Olá turma, hoje iremos ter a nossa primeira aula prática da Disciplina. Inicialmente iremos conhecer um *software* de varredura de portas, chamado de nmap, que pode ser obtido gratuitamente em: `http://nmap.org`. Na sequência, iremos conhecer melhor a nossa rede através do Nmap.

Ferramenta Nmap

Em máquinas com o protocolo TCP/IP instalado, serviços estão associados a portas, por exemplo, a Web funciona na porta 80 e Web seguro (HTTPS) funciona na porta 443. O *Portscan* é o processo de verificação da existência de algum serviço em uma porta. Para fazer isso, o atacante tenta basicamente se conectar (efetuar um "*three-way-handshake*" do protocolo TCP/IP em cada porta. Dependendo do tipo de resposta, sabemos se a porta está aberta (funcionando e atendendo a requisições) ou não.

Entre as muitas ferramentas existentes para esse fim, o Nmap (`http://nmap.org`) é uma das mais completas ferramentas, funcionando em diversos Sistemas Operacionais. O Nmap possui funções que permiti a identificação do Sistema Operacional alvo, assim como modelo e versão dos serviços testados. Conta com diversas técnicas, explorando ao máximo os protocolos vinculados ao IP. Atualmente possui inclusive a capacidade de *scripts*, podendo efetuar tarefas automatizadas. O ZeNmap é uma interface gráfica do Nmap e auxilia em algumas tarefas.

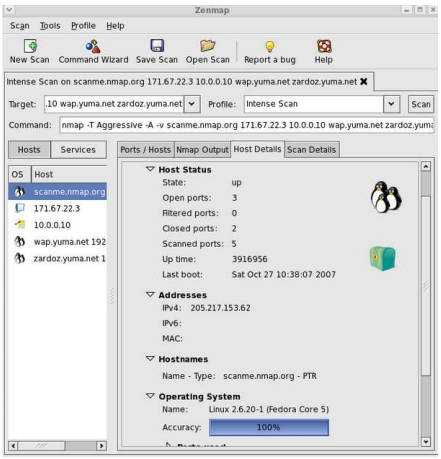

Figura 1: Janela Principal do ZeNmap

O Nmap é utilizado, por muitos administradores de rede, para tarefas de inventário de rede, gerenciar o escalonamento de *upgrade* de serviços e monitoramento de *hosts*. Por exemplo,

- Que computadores estão ligados na rede local?
- Que ips se encontram na rede?
- Qual o sistema operativo do alvo?
- Que portas tem o alvo abertas?
- Descobrir se o sistema está infectado com vírus ou malware.
- Pesquisar por computadores ou serviços não autorizados na rede.

Entretanto, o Nmap também pode ser utilizado para atividade maliciosa de reconhecimento que descobre serviços ativos na máquina. Os atacantes, primeira descobre vulnerabilidades em serviços para depois explora-las. Entretanto, o *portscan* pode ser detectável via logs: servidor, firewall e IDS.

Sintaxe de Uso

```
nmap [<Scan Type>...] [<Options>]
    {<target specification>}
```

Onde o <target> é o endereço IP do alvo (*host*) ou rede que se deseja escanear. Caso exista uma forma de resolver nomes, como um DNS configurado, você pode usar o nome do *host* ao invés do IP.

Os parâmetros para <Scan Type> são ajustados de acordo com o que se deseja obter, os principais são:

- -sT: escaneamento através de tentativas de conexão TCP. Essa forma é muito fácil de ser identificada por *firewalls* e IDS;
- -sS: utiliza pacotes TCP com a flag SYN ligada, ou seja, como apenas uma requisição de conexão. Essa técnica dificulta um pouco a detecção;
- -sP: usa pacotes ICMP *echo request*. Verifica apenas se o *host* está ativo;

- -sU: envia pacotes UDP com 0 *byte* para determinar o estado dessas portas;
- -sO: é usado para tentar determinar os protocolos suportados pelo *host*;
- -O: é feito uma tentativa de determinar o sistema operacional de um *host* (no sentido de ser atacado).
- -p: utilizado para especificar portas ou faixas (*ranges*) de portas para análise.

Exemplos de Uso

01 Análise a um IP:

```
nmap 127.0.0.1
```

02. Análise de um domínio:

```
nmap ifrn.edu.br
```

03. Análise de uma rede:

```
nmap 192.168.0.0/24
```

04. Mais informações do alvo:

```
nmap -sT -n -P0 10.0.0.1
```

Onde:

- -sT: faz a varredura completa de portas TCP;
- -n: não resolver nomes via DNS;
- -P0: não realizar teste para verificar se o servidor alto está ativo (icmp Request e ack na porta 80);
- 10.0.0.1: representa seu IP.

05. Tentar detectar o Sistema Operativo e a sua versão:

```
nmap -A -T4 10.0.0.1
```

06. Descobrir se o alvo é protegido por uma *firewall*:

```
nmap -sA facebook.com
```

07. Analisar uma porta específica (80):

```
nmap -p 80 192.168.2.2
```

08. Analisar que programas e versão correm nas portas abertas:

```
nmap -sv 192.168.2.2
```

Atividade

01. Façam grupos de três componentes e descubra o máximo de informações sobre a rede IFRN Acadêmica São Gonçalo do Amarante (10.225.0.0/16). Descubra, os computadores, portas abertas/fechadas/filtradas, topologia, versões de Sistema Operacionais e de serviços. Ao final faça um relatório e envie para jose.macedo@ifrn.edu.br até a segunda 25/03.