eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Varreduras Intrusivas**
  - ✓ Principais comandos do Nmap
    - ✓ Traçando roteamento
    - ✓ Selecionando interfaces
    - ✓ Gerando relatórios
    - ✓ Alvos Randômicos
    - ✓ Buscas específicas
    - ✓ Lista de alvos
  - ✓ Tipos de varreduras sob outros protocolos
  - ✓ Entendo protocolo SCTP
  - ✓ Entendendo protocolo ICMP
  - ✓ Arquitetura do protocolo ICMP
  - ✓ Exercício – Gerando relatório com auxilio de Bash Script

Conhecendo o Nmap

Principais comandos

Principais comandos NMAP:

-T

Timing Template (0-5): Você pode setar a velocidade da varredura, quanto maior o número, mais rápido:

Nmap –T1 192.168.1.1
Nmap –T4 192.168.1.0/24
Nmap –T5 192.168.1.1

-v

Verbosity Level: Você pode obter em tela, tudo o que o Nmap está fazendo.
A opção –vv traz mais detalhes

Nmap –v 192.168.1.1
Nmap –vv 192.168.1.0/24

Principais comandos

-F

Fast Mode: Scaneia menos portas que o padrão, geralmente procura por portas conhecidas.

Nmap –F 192.168.1.1

Nmap –F 192.168.1.0/24

--open

Open Ports: Verifica apenas as portas abertas ou possivelmente abertas.

Nmap –-open 192.168.1.1

Nmap --open 192.168.1.0/24

--packet-trace

Packet Trace: Apresenta em tela todos os pacotes enviados e recebidos

Nmap –-packet-trace 192.168.1.1

Nmap –-packet-trace 192.168.1.0/24

Principais comandos

--iflist
Interface List: Apresenta em tela as interfaces do atacante e o roteador.
Nmap --iflist

-e
Specified Interface: Você pode utilizar interfaces específicas para varredura
Nmap -e eth0 192.168.1.1
Nmap -e eth1 192.168.1.0/24

-oN | -oX | -oS| -oG <arquivo>
Output File: É possível gerar relatório de diversas maneiras no Nmap, conforme as opções: -oN (Normal), -oX (XML), -oS (Script Kiddie) e –oG (Grepável)
Nmap -oN relatório.txt 192.168.1.1
Nmap –oS relatório.txt 192.168.1.0/24

Principais comandos

-iL

Input List: Você poderá varrer máquinas de uma determinada lista.

Nmap -iL lista_maquinas.txt

-iR

Randon Targets: Esta opção escolhe alvos aleatoriamente em uma rede. No exemplo abaixo, ele escolherá 5 máquinas aleatórias na rede.

Nmap -iR 5 192.168.1.0/24

--dns-server

DNS Server: Você pode utilizar determinados servidores DNSs para resolver nomes de máquinas específicas

Nmap --dns-server 8.8.8.8,8.8.4.4 www.pudim.com.br

Principais comandos

--version-intensity <0-9>
Version Intensity: Aumente a intensidade da varredura em busca de versionamento de serviços na máquina alvo.
Nmap --version-intensity 9 192.168.2.1

--send-ip
Send IP: Requisições ARP são realizadas para efetuar varredura no modo padrão, você pode enviar pacotes IP ao invés de ARP.
Nmap -send-ip 192.168.1.0/24

--privileged
Privileged: Envia os pacotes informando que o utilizados possui os privilégios necessários
Nmap --privileged www.pudim.com.br

Principais comandos

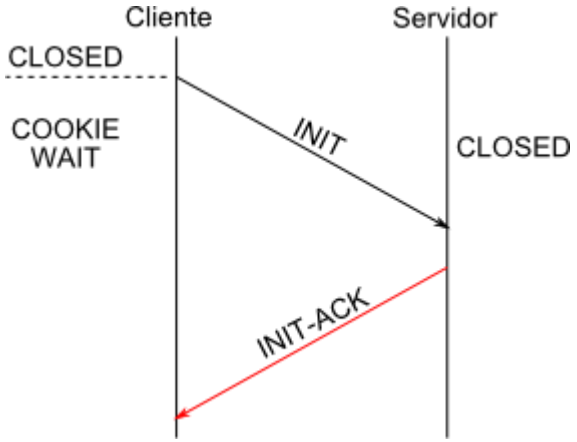
--traceroute

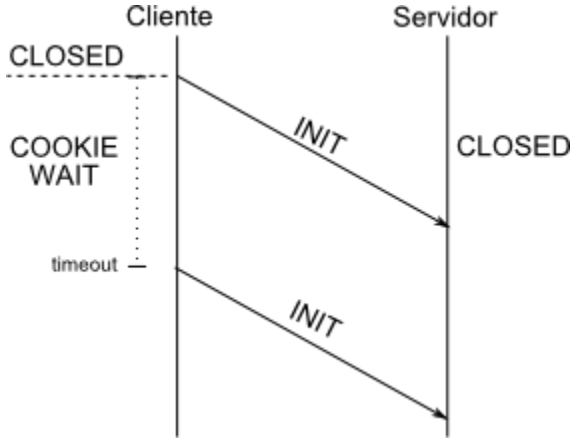
Trace Route: Determina a rota ao qual o pacote irá percorrer, é importante para determinar quantos saltos o alvo está de você.

Nmap --traceroute 9 192.168.2.1

Protocolos Adicionais: SCTP

O protocolo SCTP é um protocolo de transporte confiável que opera sobre um serviço de pacotes não confiável e sem conexão, como é o caso do IP. O SCTP oferece a transferência de datagramas (mensagens) livre de erros e de duplicações através do reconhecimento de transmissões (ACKs). A detecção de corrupção, perda e duplicação de dados é obtida através de mecanismos de checksum e números sequenciais. Um mecanismo de retransmissão seletiva é usado para corrigir a perda ou a corrupção de dados.

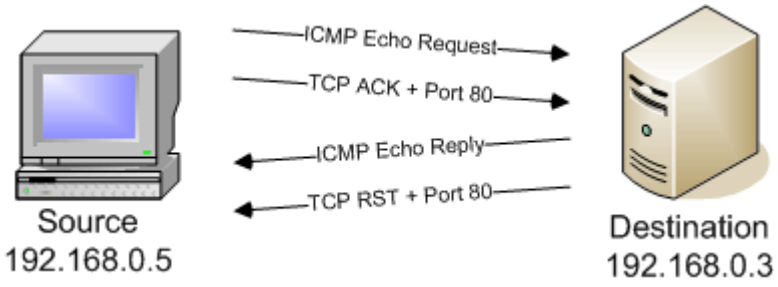




Protocolos Adicionais: ICMP

ICMP, sigla para o inglês ***Internet Control Message Protocol***, é um protocolo integrante do Protocolo IP, definido pela RFC 792, e utilizado para fornecer relatórios de erros à fonte original. Qualquer computador que utilize IP precisa aceitar as mensagens ICMP e alterar o seu comportamento de acordo com o erro relatado. Os gateways devem estar programados para enviar mensagens ICMP quando receberem datagramas que provoquem algum erro.

Como o Nmap trabalha com esse protocolo para descobrir portas:



Protocolos Adicionais: ICMP

Tipos de Tramas do protocolo ICMP

- **Echo Request / Reply**

Mensagens para funções de teste e controle da rede, caso a maquina esteja ligada ira responder com um reply e se estiver inalcançável request;
Usadas pelo comando PING

- **Destination Unreachable**

Enviado por um router que deixa fora um Datagrama;

Tipo de mensagem que é obtida quando não se consegue localizar o equipamento alvo; (nem todos os datagramas perdidos são detectados)

- **CODE** - Indica a razão da perda do datagrama
- **Timestamp Request / Reply** - Mensagens para sincronização dos relógios das máquinas

Varreduras em diversos protocolos

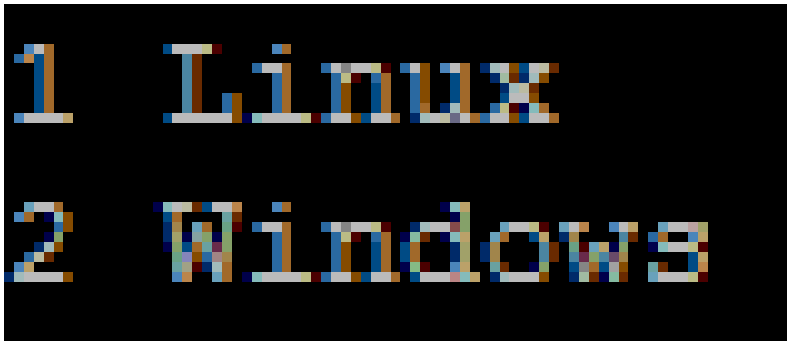
Scans utilizando protocolos diferenciados:

-PN: Não realizar Ping
-PS: Scan utilizando protocolo TCP/SYN
-PA: Scan utilizando protocolo TCP/ACK
-PU: Scan utilizando protocolo UDP
-PY: Scan utilizando protocolo SCTP
-PE: Scan utilizando protocolo ICMP Echo
-PP: Scan utilizando protocolo ICMP Timestamp
-PO: Scan utilizando o protocolo IP/Ping
-PR: Scan utilizando o protocolo ARP/Ping

Exemplo: nmap –PR www.laboratoriohacker.com.br

Nmap – Exercício

Através do NMAP, monte um script para obter a lista com o número de máquinas Windows e máquinas Linux que é possível encontrar na rede.



Nmap – Exercício: Resposta

nmap -F -O 192.168.2.1-255 | grep "Running: " > /tmp/os; echo "$(cat /tmp/os | grep Linux | wc -l) Linux"; echo "$(cat /tmp/os | grep Windows | wc -l) Windows“

-F #Fast Scan, busca apenas as principais portas
-O #Enable OS Detection, informa o nome do Sistema Operacional
|grep “Running: “ /tmp/os; # Apresenta apenas a linha onde consta essa palavra e salva no arquivo /tmp/os
$cat /tmp/os # Lê o conteúdo do arquivo
|grep Linux |wc –l # lê quantas vezes possui a palavra linux, conta e adiciona a palavra linux no final
|grep Windows |wc –l # lê quantas vezes possui a palavra linux, conta e adiciona a palavra linux no final

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker