Port scan

#Full Port Scan

nmap -p- --open -vvv <victim_ip> -vvv -oN fullportscan

#Script & Version Scan

nmap -p 80,445 -sV -sC -vvv <victim_ip> -vvv -O -oN versionscan

#No Ping Scan

nmap -Pn <victim_IP> -vvv -oN nopingscan

#Vuln Scan

nmap -p 445 -T4 -Pn -A --script smb-vuln* <victim_ip> -vvv -oN vulnscan

#No DNS Resolution

nmap -n <victim_IP> -vvv -oN nodnsresolutionscan

#UDP Scan

nmap -sU --open -vvv <victim_ip> -oN udpscan

#Script

https://github.com/21y4d/nmapAutomator

- **********

nmap –script “all” 10.0.0.1
nmap –script “./custom_scripts” 172.16.0.0/28
nmap –script “/tmp/scripts,/usr/share/nmap/scripts” 10.0.0.0/24

Vulnerabilidades:

nmap --script http-proxy-brute -p 8080 <host>
nmap --script http-brute 80 <host>
nmap --script http-rfi-spider -p80 <host>
nmap --script http-default-accounts host/ip
nmap -p445 --script smb-vuln-ms17-010 <IP ALVO>
nmap --script ssh-brute --script-args userdb=/home/kali/userlist.txt,passdb=/home/kali/passlist.txt,ssh-brute.timeout=2s -p 22 <IP ALVO>
nmap -sT -sV -O -p8080
sudo nmap --min-rate 10000 -p- -Pn -sU
sudo nmap -sU -sV -O -p53

Top strings bounty

nmap -sS -sV -vv -n -Pn -T5 192.168.1.1-255 -p80 -oG - | grep 'open'
nmap -sS -sV -vv -n -Pn -T5 192.168.1.1-255 -p80 -oG - | grep 'open'| grep -v 'tcpwrapped'
sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.11.214
sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.129.70.118 -oG allPorts

O script http-waf-detect foi projetado para nos ajudar a conhecer a presença de um firewall de aplicativo da web. Ele examinará o servidor da Web de destino com várias solicitações.
nmap -p80,443 --script http-waf-detect --script-args="http-waf-detect.aggro,http-waf-detect.detectBodyChanges" targetWebsite.com

Estou usando o argumento http-waf-detect.aggro , que instrui o Nmap a testar todos os seus vetores de ataque internos para acionar os servidores WAF.

Também está habilitado o argumento http-waf-detect.detectBodyChanges , que procura alterações no corpo das solicitações HTTP e aumenta ainda mais a probabilidade de detecção.

O script Nmap de impressão digital http-waf foi projetado para nos ajudar a identificar em um servidor da Web de destino o firewall do aplicativo Web em uso exato. Ele também tentará identificar seu tipo e número de versão exato
nmap -p80,443 --script http-waf-fingerprint targetWebsite.com

Podemos melhorar ainda mais a capacidade do Nmap de detectar tipos e versões de WAF usando o argumento http-waf-fingerprint.intensive . Isso prolongará o tempo de verificação e também aumentará a quantidade de ruído (tráfego da web) gerado pelo script.
nmap -p80,443 --script http-waf-fingerprint --script-args http-waf-fingerprint.intensive=1 targetWebsite

Encontrar erros HTTP

nmap -p80,443 --script http-errors targetWebsite.com

Acima, o Nmap detectou um status 403, o que sugere que as permissões de arquivo dos servidores estão mal configuradas e os visitantes não possuem acesso ao recurso solicitado.

Abaixo está um comando mais refinado que inclui vários argumentos de script.

nmap -vv -p80,443 --script http-errors --script-args "httpspider.url=/docs/,httpspider.maxpag

O script dns-brute embutido no Nmap foi projetado para enumerar subdomínios e seus endereços IP do servidor correspondente.

nmap -p80,443 --script dns-brute targetWebsite.com

Abaixo está um comando dns-brute que apresenta vários –script-args .

nmap -p80,443 --script dns-brute --script-args dns-brute.threads=25,dns-brute.hostlist=/root/Desktop/custom-subdomain-wordlist.txt targetWebsite.com

O script http-exif-spider do Nmap pode ser usado para extrair dados EXIF interessantes de fotos encontradas em sites. Tal script não é útil contra sites comuns como Instagram, Twitter e Facebook.

nmap -p80,443 --script http-exif-spider targetWebsite.com

Podemos ver que o objetivo acima é usar um telefone Android e uma variedade de câmeras digitais. Podemos agora gerar uma payload específico do Android e enviá-la ao alvo para comprometer ainda mais seus dispositivos.

Ao tentar extrair dados EXIF de fotos grandes, o Nmap pode enviar uma mensagem de erro “O tamanho do cache HTTP atual excede o tamanho máximo”. Este um aviso que a foto é muito grande e está excedendo o valor padrão máximo do tamanho do arquivo. Use o argumento http.max-cache-size e aumente o valor conforme necessário. Abaixo eu o configurei para um número arbitrariamente alto.

nmap -p80,443 --script http-exif-spider --script-args="http.max-cache-size=99999999" targetWebsite.com