HÖGSKOLAN VÄST

Datum: 2025-05-08

# Case 3 (Nmap)

Mahmoud Azar
Basir muse

***Lista flera tjänster som körs på minst tre datorer i 193.10.236.0/24 nätet. Specifiera vilken server som kör vad.***

grp60-serv1.grp60.lab.hv.se (193.10.236.246):

Hypertext transfer protocol (Http port 80) : **Open**
Hypertext transfer protocol secure (Https port 443): **Open**
Cisco skinny call control protocol (Cisco-sccp port 2000): **Open**
Session initiation protocol (Sip port 5060): **Open**
programvarupaket (xmpp port 8010): **Open**

grp60-serv2.grp60.lab.hv.se (193.10.236.247):

Hypertext transfer protocol (Http port 80) : **Open**
Hypertext transfer protocol secure (Https port 443): **Open**
Cisco skinny call control protocol (Cisco-sccp port 2000): **Open**
Session initiation protocol (Sip port 5060): **Open**
programvarupaket (xmpp port 8010): **Open**

grp61-serv1.grp61.lab.hv.se (193.10.236.248):

Hypertext transfer protocol (Http port 80) : **Open**
Hypertext transfer protocol secure (Https port 443): **Open**
Cisco skinny call control protocol (Cisco-sccp port 2000): **Open**
Session initiation protocol (Sip port 5060): **Open**
programvarupaket (xmpp port 8010): **Open**

***2. Kan Nmap identifiera vilket operativsystem som körs på varje system? Finns det någon Nmap-funktion som kan användas för att gissa värdens operativsystem? Förklara ditt svar. Med hjälp av de öppna portarna och de möjliga tjänsterna som körs på dessa portar ta fram vilka operativsystem som körs på dessa datorerna (var för sig). Förklara ditt svar.***

Man kan identifiera operativsystem med hjälp av Nmap, den har en inbyggd funktion som gör det möjligt att identifiera vilket typ av operativsystem som körs på varje system. Denna funktion kallas för OS-fingerprinting och används med flaggan -O
Kommandot nmap -O [IP address].
Det funkar så att namp skickar ett specialdesignat paket (TCP, Syn) till målet och sedan analyseras och jämförs svaren mot en databas med signatur för olika operativsystem.
Baserat på sekvensnummer , svarstid och felmeddelande försöker namp att avgöra vilket operativsystem som mest används på värden.
Om till exempel port 80 är öppen och operativsystem svarar med ett tcp värde som matchar linux kernel så kommer namp att rapportera att operativsystemet är linux.
Med hjälp av öppna portar och tjänster kan man också göra gissningar om vilket operativsystem som körs även om fingerprinting inte fungerar eller ger otydliga svar.

När man kör kommandot nmap -O 193.10.236.246:
Device type visar att operativsystemet är linux 3.X | 2.6.X (89%)
Aggressive OS guesses visar att linux 3.2 - 3.8 (89%)  och linux 2.6.32 - 2.6.39 (86%)
Det innebär att systemet körs på linux och versionen är kernel 3.X eller 2.6.X och procent anger hur säker namp är på sin gissning (enligt bild 1, 2, 3).

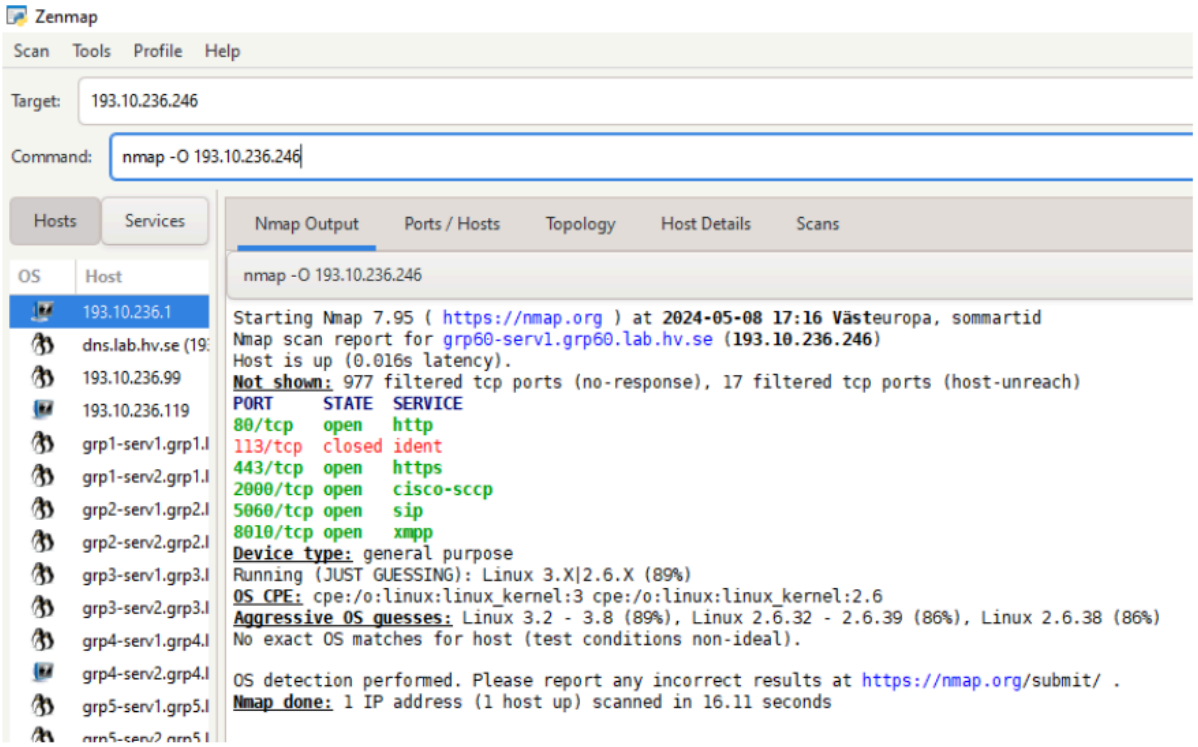



Bild 1. Resultat av kommandot nmap -O 193.10.236.246


Bild 2. Resultat av kommandot nmap -O 193.10.236.248

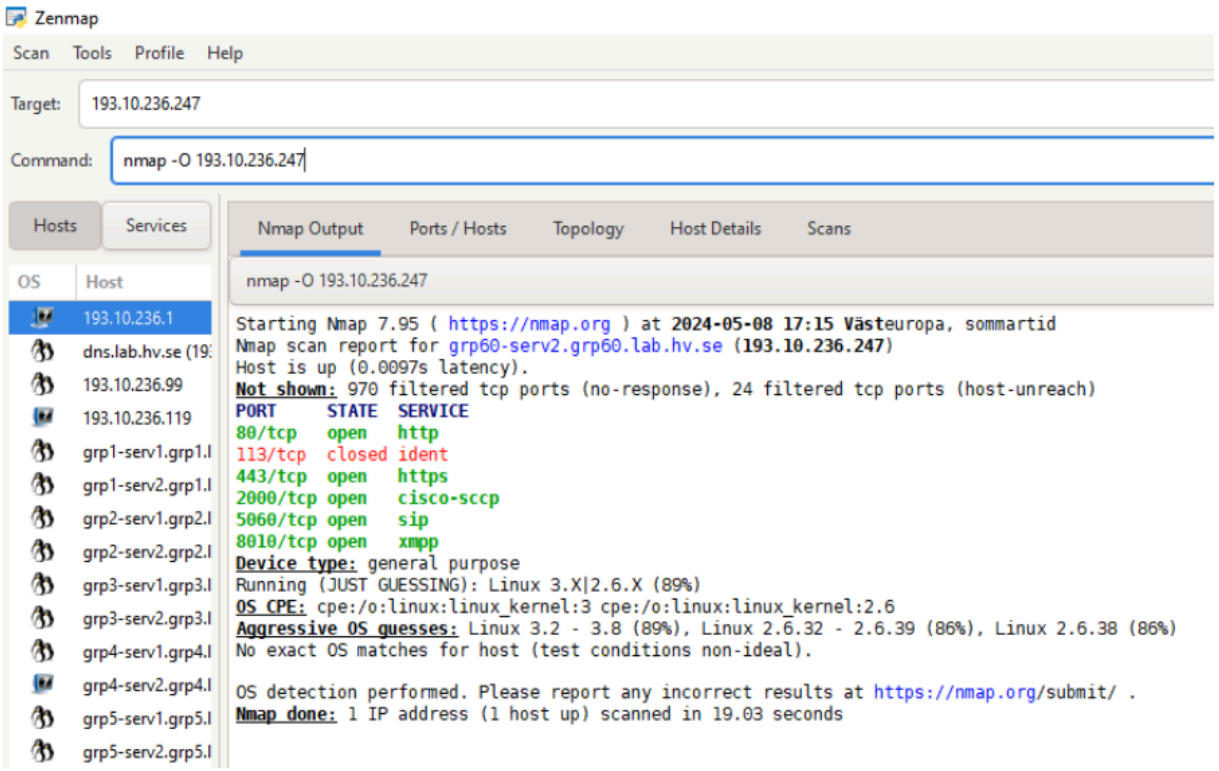



Bild 3. Resultat av kommandot nmap -O 193.10.236.247

***3. Vilken dator tycker du verkar mest säker? Minst säker? Förklara dina svar.***

Alla tre maskiner verkar lika säkra eftersom de har identisk konfiguration vad gäller öppna portar och tjänster. För att avgöra säkerhetsnivå krävs djupare testning av konfiguration och eventuella sårbarheter i de tjänster som körs.

***4. Beskriv flera viktiga användningsområden för Nmap.***

Nmap är ett kraftfullt verktyg det används framför allt för att skanna nätverk, det vill säga att ta reda på vad som finns där ute, vad som är öppet, och vad som kanske borde ha varit stängt. Man börjar ofta med en så kallad host discovery, där man helt enkelt försöker lista ut vilka enheter som faktiskt är aktiva på nätverket. Det görs genom att skicka olika sorters ping förfrågningar eller TCP SYN paket och se vilka som svarar.
När man väl vet vilka maskiner som är igång, kan man gå vidare till att skanna deras portar. Här visar Nmap sin styrka. Det kollar vilka portar som är öppna, stängda eller filtrerade, vilket i sin tur avslöjar vilka tjänster som är tillgängliga.
Det handlar alltså inte bara om att se att port 80 är öppen. Nmap kan även lista ut att det är en Apache server som körs där, och exakt vilken version. Den typen av information är guld värd när man letar efter sårbarheter.
Nmap kan också göra något som kallas OS-fingerprinting, det vill säga försöka gissa vilket operativsystem målet kör, baserat på hur det svarar på särskilt utformade paket. Det är inte hundra procent exakt varje gång, men ofta tillräckligt nära för att det ska vara användbart.
En annan användbart funktion är Nmap Scripting Engine (NSE). Det är en kraftfull funktion som gör det möjligt att köra skript för allt från att leta efter kända sårbarheter, till att brute-force lösenord eller analysera nätverkskonfigurationer. Det vill säga en passiv informationsinsamling med en aktiv testning.
Det gör Nmap till ett verktyg som funkar lika bra för systemadministratörer som vill dubbelkolla sin setup, som för penetrationstestare.
Man kan även använda Nmap för att testa hur brandväggar reagerar på olika typer av trafik. Genom att simulera attacker eller köra stealth scans kan man se vad som släpps igenom, vad som blockeras, och hur bra ens IDS eller IPS verkligen fungerar.
Nmap är ett analysverktyg, ett sårbarhets sökande instrument, och ibland ett verktyg för upptäckta faror och sårbarhet.

***5. Vilken funktion hos Nmap tyckte du var mest användbar och varför?***

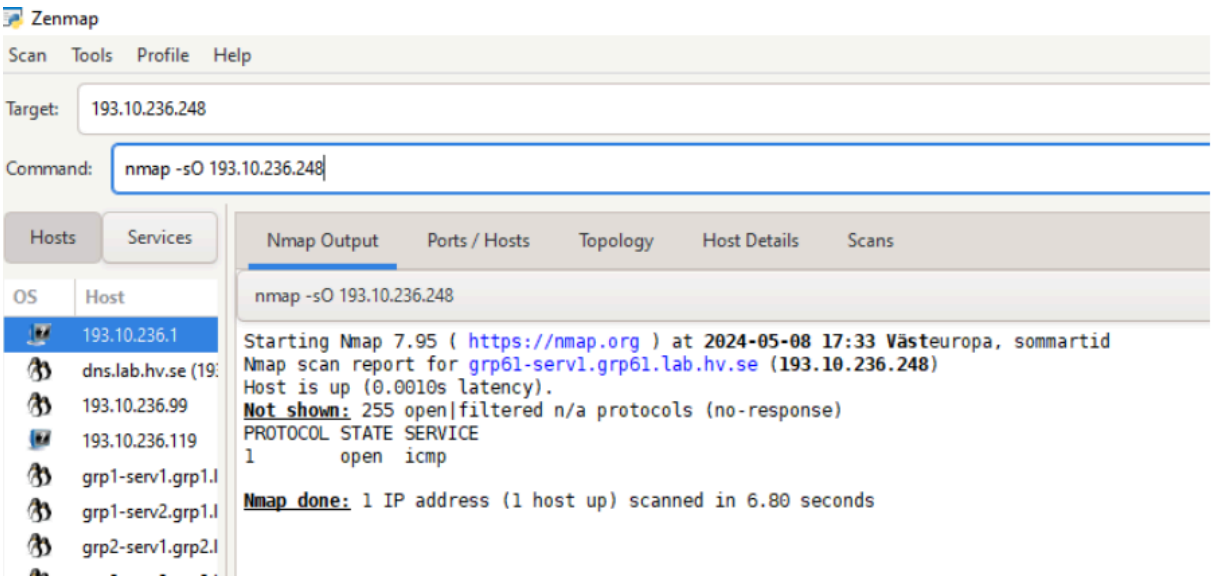
Den funktion hos Nmap som vi tyckte var mest användbar var OS-fingerprinting, som aktiveras med kommandot nmap -O [IP-adress]. Den här funktionen gör det möjligt att identifiera, eller åtminstone göra en kvalificerad gissning, om vilket operativsystem som körs på en viss host i nätverket.
Nmap skickar olika specialdesignade paket till målet, analyserar hur systemet svarar, och jämför sedan resultaten mot en omfattande databas med kända operativsystems signaturer. Genom att titta på detaljer som TCP-sekvensnummer, svarstider, TTL-värden och andra nätverks parametrar kan verktyget ofta avgöra om ett system till exempel kör en Linux-kärna av version 3.x eller en äldre Windows-version.
Den här typen av analys är mycket värdefull i allt från sårbarhetsbedömning till systemkartläggning och penetrationstestning, eftersom olika operativsystem har olika säkerhetsnivåer och kända svagheter.

***6. Vilken funktion hos Nmap tyckte du var svårast att använda och varför?***

Den funktion vi tyckte var svårast att använda var när vi försökte kombinera flera flaggor i ett enda kommando, till exempel: nmap -sS -p 21,23,53,80 -O -v 193.10.236.XX
Vi hade särskilt svårt att förstå hur flaggan -IR (Random IP Scanning) skulle inkluderas korrekt i kombination med övriga parametrar som -p, -O och -v.
Det var inte helt tydligt från dokumentationen hur -IR påverkar målet i förhållande till specifika IP-adresser.
vi tyckte det är svårt att avgöra när och hur -IR är användbart i praktiken, eftersom det går emot det vanliga arbetssättet där man själv specificerar mål och nät intervall.
Det hade behövts bättre exempel i dokumentationen för att förstå användningen i kombination med övriga funktioner.

***7. Undersök ett Nmap-kommando eller en funktion som du anser vara viktig men som inte täcks av den här labben. Beskriv dess användning och rapportera dina resultat när du kör kommandot mot ett system i labb-nätet.***

En viktig Nmap funktion som vi bestämde oss för att undersöka över är IP Protocol Scanning.
Kommandot som används är nmap -sO [IP-adress] och denna kommandot fungerar på ett annat sätt än vanliga port scanning operationer.
Nmap verktyget undersöker vilka IP-protokoll som målsystemet stöder i stället för att söka efter öppna portar.
Vi utförde testet med hjälp av IP-adressen 193.10.236.248 genom kommandot nmap -sO 193.10.236.248.
Resultatet av skanningen visade att systemet stöder tre protokoll som inkluderar ICMP (Internet Control Management Protocol), TCP (Transmission Control Protocol) och IGMP(Internet Group Management Protocol) .
Målsystemet möjliggör både traditionell TCP-kommunikation och ICMP-pinging samt IGMP multicast-funktionalitet.



Resultat av komandot nmap -sO 193.10.236.248