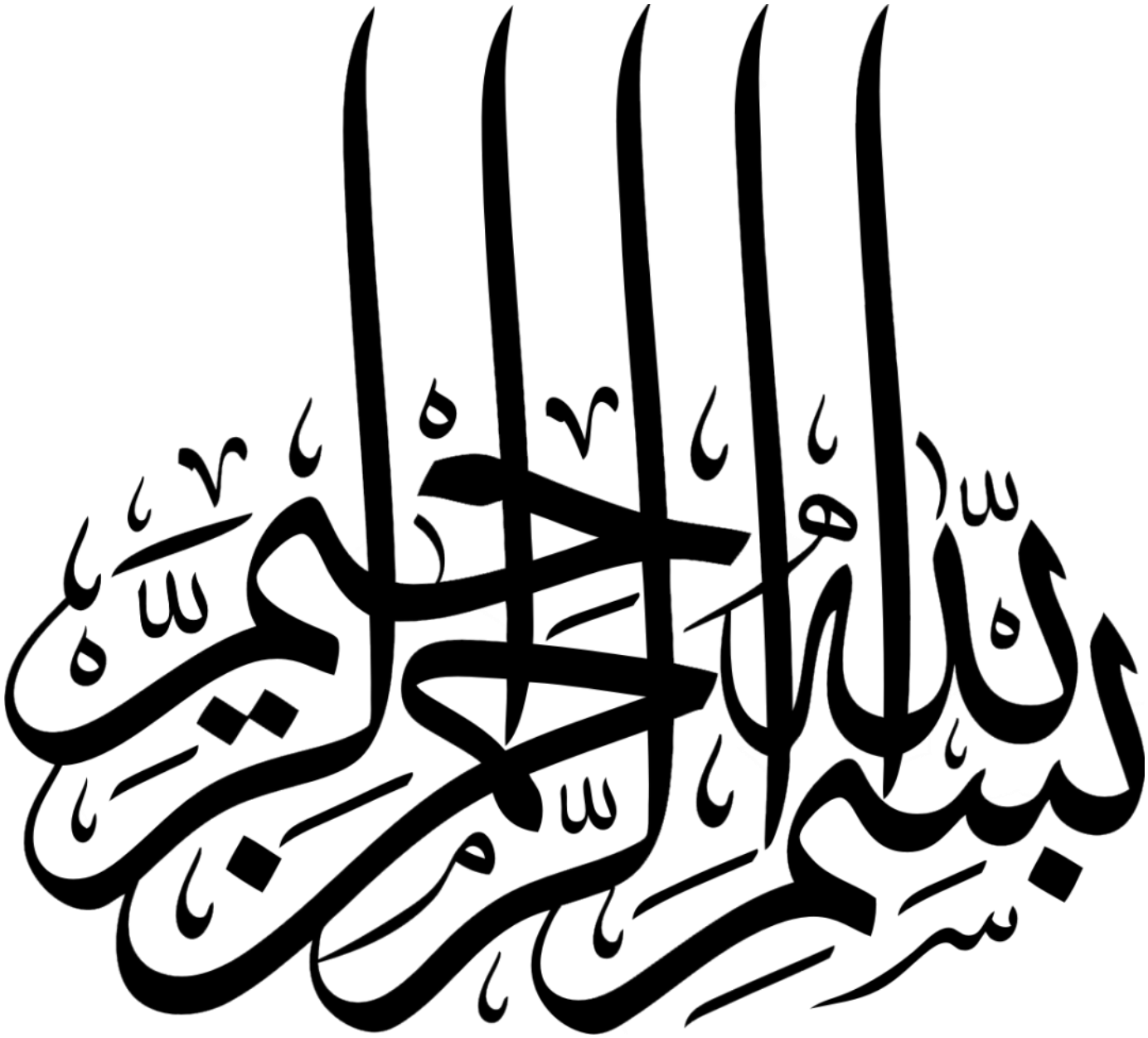

بسم الله الرحمن الرحيم

کتاب الکترونیکی کوتاه و کاربردی از Nmap برای تست نفوذ

تهیه شده توسط

احسان نیک آور

عضو تیم Esecurity.ir

مقدمه

با عرض سلام و ادب خدمت کلیه دوستان عزیز، این کتاب به عنوان یک راهنمای کوچک ولی کاربردی برای آشنایی هر چه بهتر و استفاده مناسب از ابزار کاربردی Nmap است.

در این کتاب، همانند کتب دیگر ما از نصب ابزار Nmap بر روی ویندوز یا لینوکس و ... شروع نخواهیم کرد. چرا که در کتاب های مشابه این امر توضیح داده شده است. البته این ابزار در سیستم عامل کالی لینوکس موجود است و ما از این سیستم عامل استفاده می کنیم.

این کتاب مرجعی سریع برای علاقمندان به امنیت شبکه و تست نفوذ می باشد که با زبانی ساده و به صورت کوتاه تهیه شده است که استفاده از آن آسان باشد و وقت زیادی از شما نگیرد.

این کتاب در هفت بخش تهیه شده است که در هر بخش مطالب کاربردی جهت استفاده از ابزار قدرتمند Nmap مطرح شده است.

پس پیشنهاد می کنیم تا انتهای این کتاب با ما همراه باشید.

هر کتاب و مطلبی قطعا کامل نیست و دارای نواقصی می باشد. به همین منظور هر گونه انتقاد، پیشنهاد و نظرات شما دوستان گرامی که این مطلب را مطالعه می نمایند، راه گشای ما برای تهیه کتاب ها و مطالب بعدی خواهد بود.

لذا کلیه از شما خواهشمند هستیم تا نظرات خود را به ایمیل info@esecurity.ir با موضوع Nmap ارسال نمایید.

بسیار ممنون می شوم که اگر این کتاب را مفید دانستید، آن را با دوستان خود به اشتراک بگذارید تا از این کتاب استفاده نمایند.

احسان نیک آور

بخش اول

Nmap در چه بخشی از تست نفوذ کاربرد دارد؟

مطابق با استاندارد شرکت Eccouncil که یکی از شرکت های بزرگ در زمینه امنیت شبکه و اطلاعات می باشد، مراحل تست نفوذ و یا اصطلاحاً Hacking Phase به پنج مرحله تقسیم می شود.

این پنج مراحل عبارتند از:

- جمع آوری اطلاعات
- اسکن یا پویش (که شامل اسکن شبکه، پورت و آسیب پذیری می باشد)
- به دست آوردن دسترسی اولیه
- ارتقاء و نگه داری دسترسی
- پاک کردن ردپا

ابزار قدرتمند Nmap در مراحل اول و دوم بسیار کاربرد دارد ولی کاربرد اصلی آن که شناخته شدن Nmap بر این اساس است، مرحله دوم یا اسکن می باشد.

در این کتاب هم ما بر روی مرحله اسکن با استفاده از Nmap تمرکز خواهیم داشت.

همانطور که اشاره شد، مرحله اسکن شامل اسکن شبکه، پورت و آسیب پذیری می باشد.

در اسکن شبکه، بازه یک شبکه و رنج آدرس های IP شناسایی می شوند.

در اسکن پورت، پورت های باز بر روی سیستم ها و سرویس های موجود بر روی آن ها شناسایی می گردد.

در اسکن آسیب پذیری، آسیب پذیری موجود بر روی سیستم مورد ارزیابی قرار خواهد گرفت.

بخش دوم

تعریف هدف برای Nmap

در اولین مرحله برای آشنایی با Nmap ما نیاز به تعریف هدف خود داریم که در واقع آدرس سیستم مورد نظر است. نحوه تعریف هدف به اشکال زیر امکان پذیر است:

nmap 10.0.0.1

در اولین و ساده ترین حالت، آدرس IP سیستم هدف را بعد از عبارت Nmap قرار می دهیم.

nmap 10.0.0.1,2,3

حالت دیگر جدا سازی آدرس ها با علامت کاما می باشد. (در صورت پشت سر هم بودن آدرس ها)

nmap 10.0.0.1-100

مشخص کردن بازه ای از آدرس ها که از ۱ تا ۱۰۰ در این مثال است.

nmap 10.0.0.0/24

مشخص کردن یک بازه ای از شبکه که به صورت Subnet مشخص شده است. در این مثال آدرس های ۱۰,۰,۰,۱تا آدرس ۱۰,۰,۰,۲۵۴ هدف ما می باشد.

nmap -iL list.txt

در این مثال با استفاده از سوییچ iL– یک فایل که حاوی آدرس های IP می باشد، مورد نظر می باشد.

nmap 10.0.0.0/24 --exclude 10.0.0.12

اگر قصد داشته باشید که از یک بازه آدرس IP یک آدرس خاص را استثناء نمایید بعد از تعریف بازه آدرس از عبارد excloude-- استفاده نموده و آدرس مورد نظر که نباید اسکن شود را وارد می کنید.

nmap 10.0.0.0/24 --excludefile list.txt

اگر قصد دارید تا بازه ای از آدرس ها را استثناء نمایید از دستور excludefile-- در ادامه معرفی آدرس استفاده نموده و بعد از این عبارت، لیست حاوی آدرس ها را معرفی می نمایید.

nmap -6 IPv6

تا به این جا آدرس های IPv4 مد نظر ما بود. در صورتی که قصد دارید تا آدرس های IPv6 را اسکن نمایید می توانید مطابق مثال بالا عمل نمایید.

بخش سوم

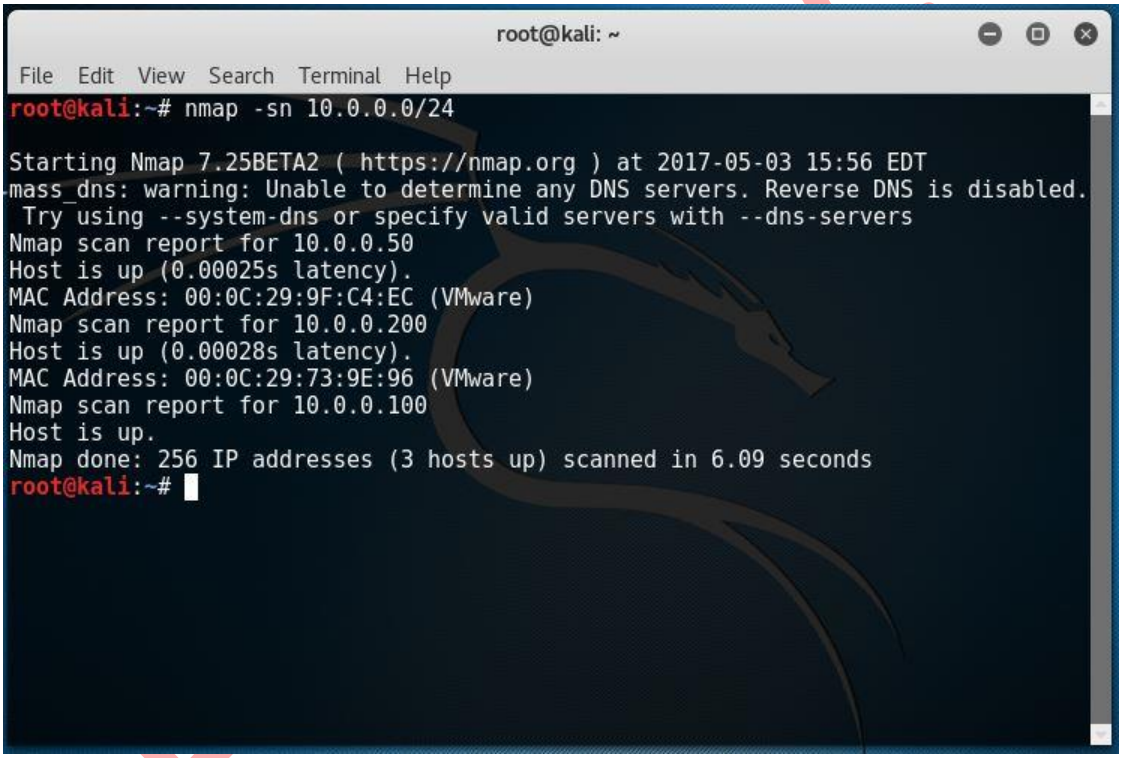
شناسایی سیستم های روشن در شبکه و اسکن با ICMP

یکی از موارد استفاده ابزار Nmap شناسایی سیستم های روشن در شبکه است که اصطلاحاً به آن Check for Live System یا Host Discovery گفته می شود.

برای این منظور می توان از دستور زیر استفاده نمود.

nmap –sn IP

در این دستور به جای عبارت IP می توان از حالات مختلفی که در بخش اول به آن اشاره کرد استفاده نمود تا از سیستم های روشن درون شبکه اطلاع حاصل نمود.



روش دیگری که برای شناسایی سیستم های روشن از آن استفاده می شود تکنیک Ping Sweep است. در این روش یک بسته ICMP حاوی ECHO Request به آدرس مورد نظر ارسال شده و در صورت بازگشت یک جواب ECHO Reply، سیستم هدف روشن در نظر گرفته می شود.

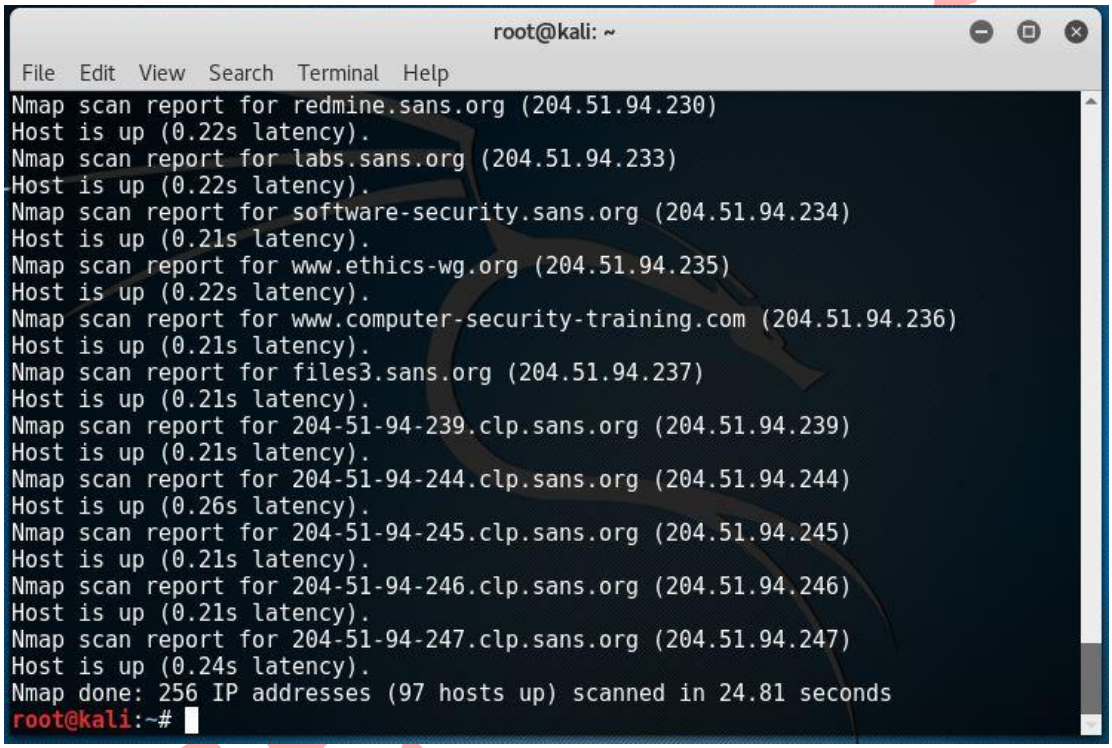
از دستور زیر برای اسکن به روش Ping Sweep استفاده می گردد.

nmap -sP 10.0.0.0/24

در دستور بالا Subnet مورد نظر اسکن شده و در صورت روشن بودن هر سیستم، گزارش آن نمایش داده می شود. خروجی این دستور مشابه سوییچ sn– می باشد.

همچنین شما می توانید به جای آدرس IP از نام هاست نیز استفاده نمایید.

Nmap -sP esecurity.ir/24



تصویر بالا بخشی از خروجی دستور Nmap –sP sans.org/24 می باشد.

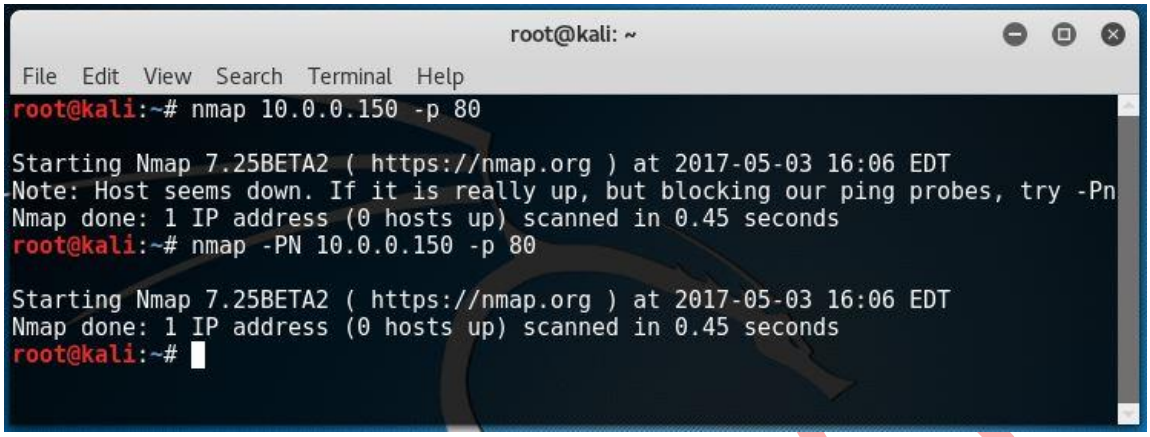
نکته: چون Nmap ابتدا Host Discovery انجام می دهد اگر فایروال بسته های ICMP را مسدود کرده باشد اسکن پورت انجام نمی شود. (در این حالت باید از سوییچ PN- استفاده گردد تا عملیات Host Discoveryصورت نگیرد.)

Nmap -PN 10.0.0.10 -p 80 ➔ No Ping

در دستور بالا با استفاده از سوییچ PN– عملیات Host Discovery صورت نمی گیرد تنها پورت ۸۰ از آدرس مورد نظر اسکن می شود. (به مبحث اسکن پورت در ادامه پرداخته می شود.)

نکته

ابزار Nmap به حروف کوچک و بزرگ حساس می باشد.



در تصویر بالا اولین بار دستور بدون PN- تست شد که در خروجی ملاحظه می نمایید که به ما می گوید:

"به نظر می رسد که هاست خاموش باشد اگر مطمئن هستید که این هاست فعال است اما توسط فایروال، بسته های Ping و ICMP مسدود شده است، با سوییچ PN- تست را انجام دهید."

در دومین مرتبه که انجام شد با سوییچ PN- تست انجام شد که مشخص گردید هاست وجود ندارد و یا خاموش است.

بنابراین اگر سیستم هدف روشن باشد و توسط فایروال، بسته های ICMP مسدود شده باشد، اگر دستورات Nmap را بدون PN- وارد کنیم، ممکن است پاسخ تست دچار چالش شده و باعث نتیجه نادرست گردد.

نکته:

در Nmap تفاوتی میان Pn- و PN- و P0- وجود ندارد.

بخش چهارم

اسکن پورت

در ساختار شبکه، دو نوع پورت وجود دارد که شامل پورت سخت افزاری و نرم افزاری یا مجازی می باشد. پورت های سخت افزاری شامل پورتUSB ، ۲PS، Serial، VGAو از این دست می باشد. به طور کلی پورت های سخت افزاری به صورت فیزیکی قابل رویت بوده و تعداد آنها محدود می باشد.

پورت های نرم افزاری یا مجازی بر خلاف پورت های سخت افزاری قابل مشاهده نیستند و تعداد آنها از یک تا ۶۵۵۳۵ می باشد. البته این تعداد هم برای TCP و هم برای UDP می باشد. این پورت ها به سه دسته تقسیم بندی می شوند.

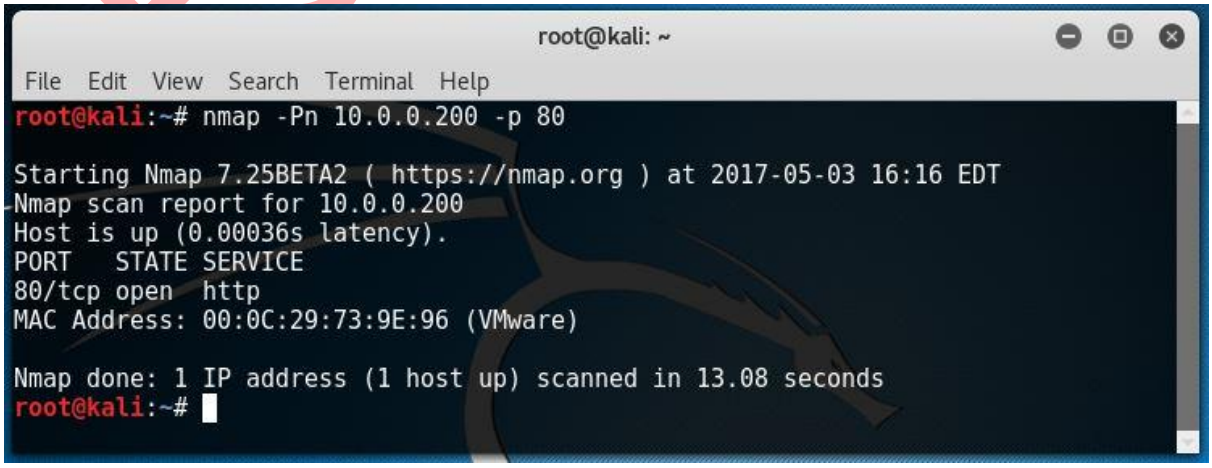
۱-۱۰۲۴ پورت های مربوط به سرویس های خاص شبکه که به آن ها پورت های شناخته شده یا Well-known ports نیز گفته می شود.

۱۰۲۵-۴۹۱۵۱ پورت های تصادفی یا رندوم نامیده می شوند و زمانی که قصد برقراری ارتباط به طور مثال وب در شبکه را داریم. پورتی که در مقصد باز می شود۸۰ بوده و پورت باز شده سمت ما از این دسته می باشد. به این دسته از پورت ها Registered ports نیز گفته می شود.

۴۹۱۵۲-۶۵۵۳۵ این پورت ها که آزاد نامیده می شوند، بیشتر در برنامه نویسی کاربرد دارند. به این دسته از پورت ها Dynamic or private ports گفته می شود.

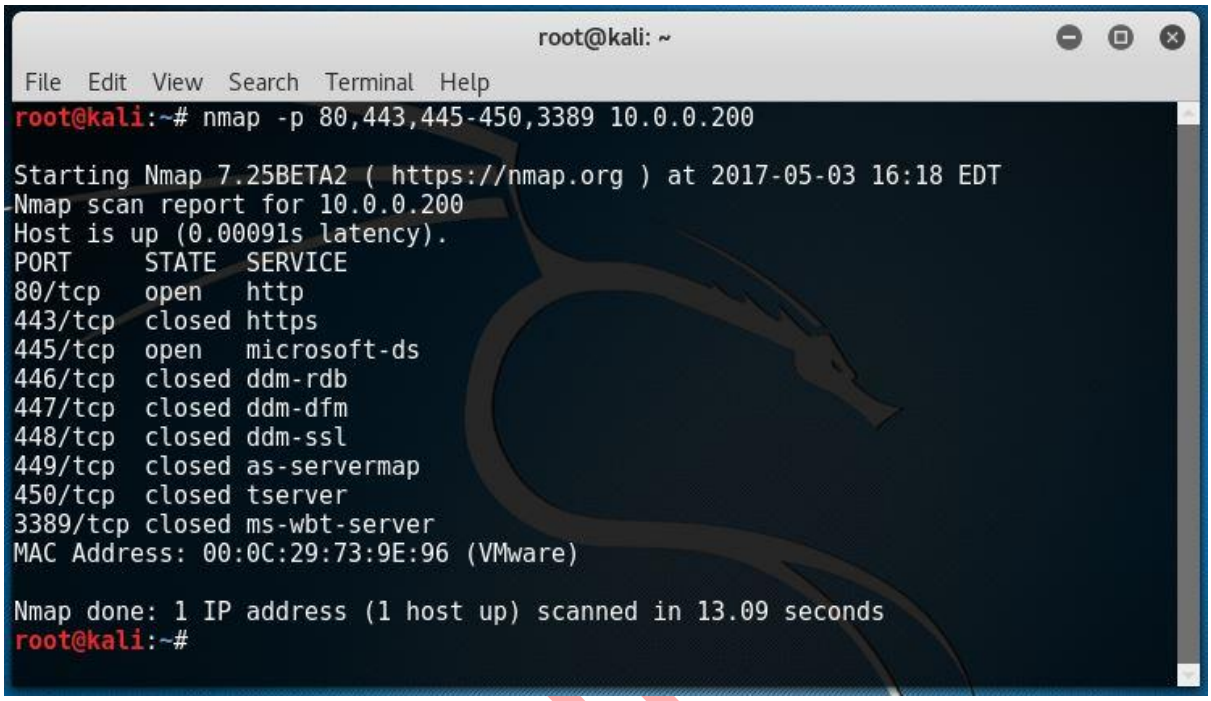
همانند تعریف آدرس IP که در بخش های قبل به آن اشاره شد، تعریف پورت برای ابزار Nmap هم دارای حالات مختلفی است که در این بخش به آن اشاره می شود.

Nmap -p 80



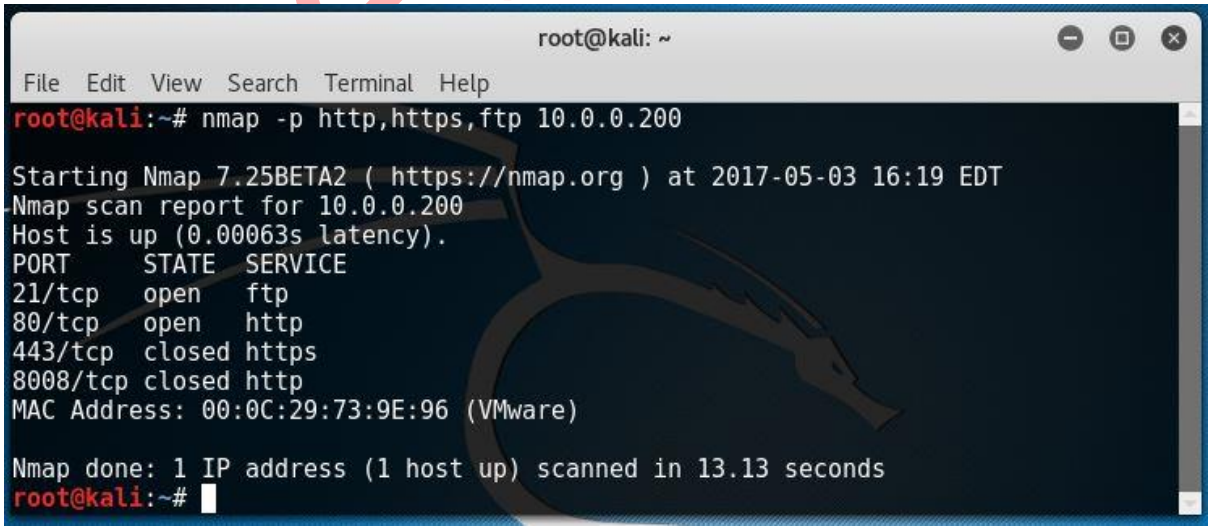
اولین و ساده ترین روش تعریف پورت به صورت بالا می باشد که با سوییچ p- و مشخص نمودن شماره پورت می باشد.

Nmap -p 80,443,445-450,3389



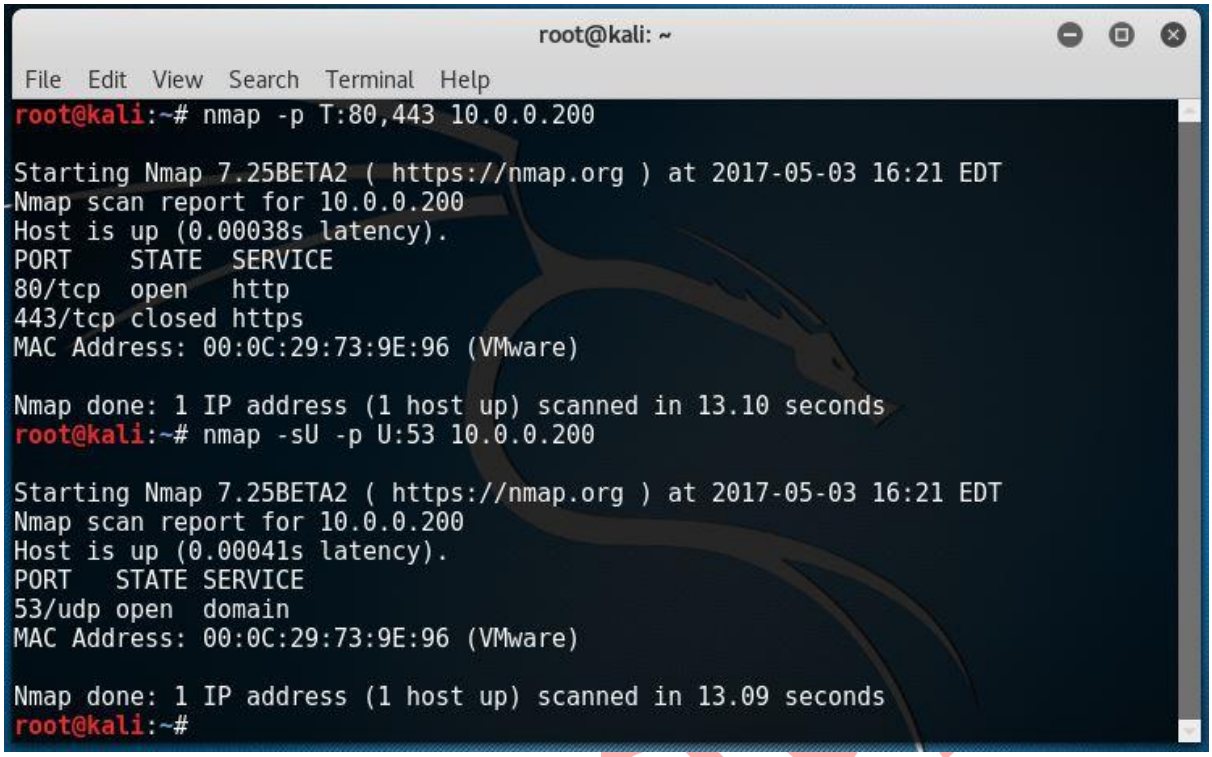
روش بعدی تعریف چندین پورت می باشد که با استفاده از کاما جداسازی می شود. البته می توان شماره پورت های پشت سرهم را به صورت ۴۵۰-۴۴۵ تعریف کرد.

Nmap -p http,https,ftp



روش دیگر استفاده از نام پروتکل یا سرویس است که مانند مثال بالا تعریف می شود.

Nmap -p T:80,443 U:53,123



همانطور در همین بخش به آن اشاره شد، ۶۵۵۳۵ پورت نرم افزاری وجود دارد که در واقع ۶۵۵۳۵ پورت TCP و ۶۵۵۳۵ پورت UDP می باشد. برای تعریف هر پورت TCP به عنوان مثال از عبارت T:80، ابتدا عبارت T و پس از آن شماره پورت قرار داده می شود.

نکته

لازم به ذکر است اگر از عبارت U برای تعریف پورت UDP استفاده نمایید، باید از سوییچ sU– استفاده کرد تا UDP Scan انجام شود.

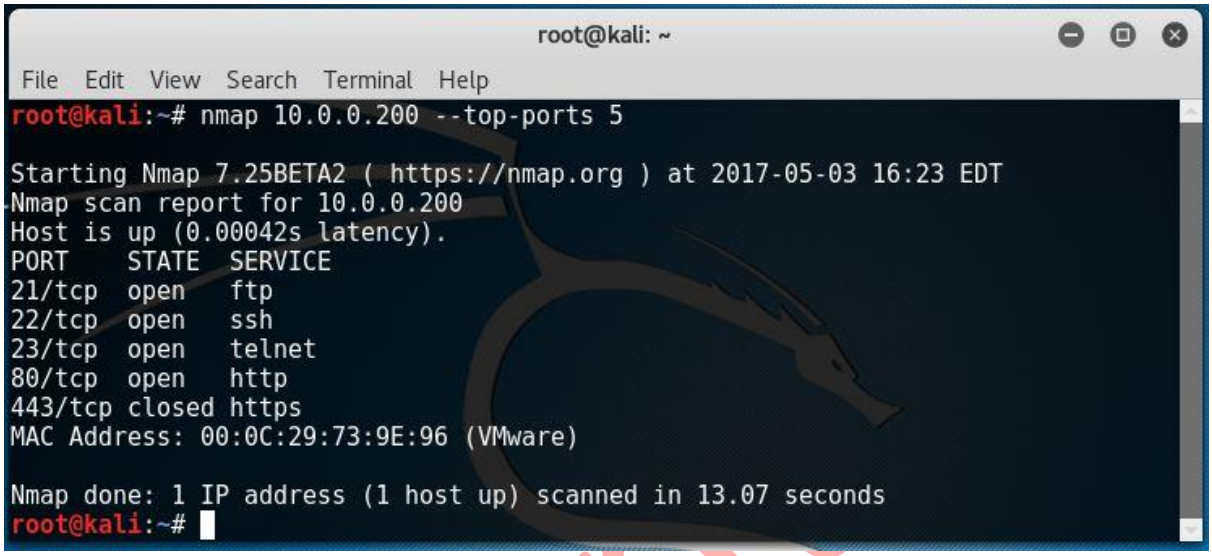
در حالت پیش فرض اسکن به صورت TCP Scan انجام می شود.

Nmap -p -1024 ➔ {1-1024}

در مثال بالا در صورتی که از خط تیره (-) استفاده شود و در ادامه آن شماره ای وارد شود، کل پورت ها تا عدد مورد نظر اسکن خواهد شد. در مثال بالا ۱۰۲۴ پورت اسکن می گردد.

Nmap --top-ports 5 ➔ 80,23,443,21,22

نوع دیگری از تعریف پورت، اسکن پورت های پر کاربرد یا top ports است. در این مثال با سوییچ --top-ports و قرار دادن عبارت ۵ بعد از آن، پنج پورت پرکاربرد اسکن می شود که این پورت ها ۸۰،۲۳،۴۴۳،۲۱،۲۲ می باشند.



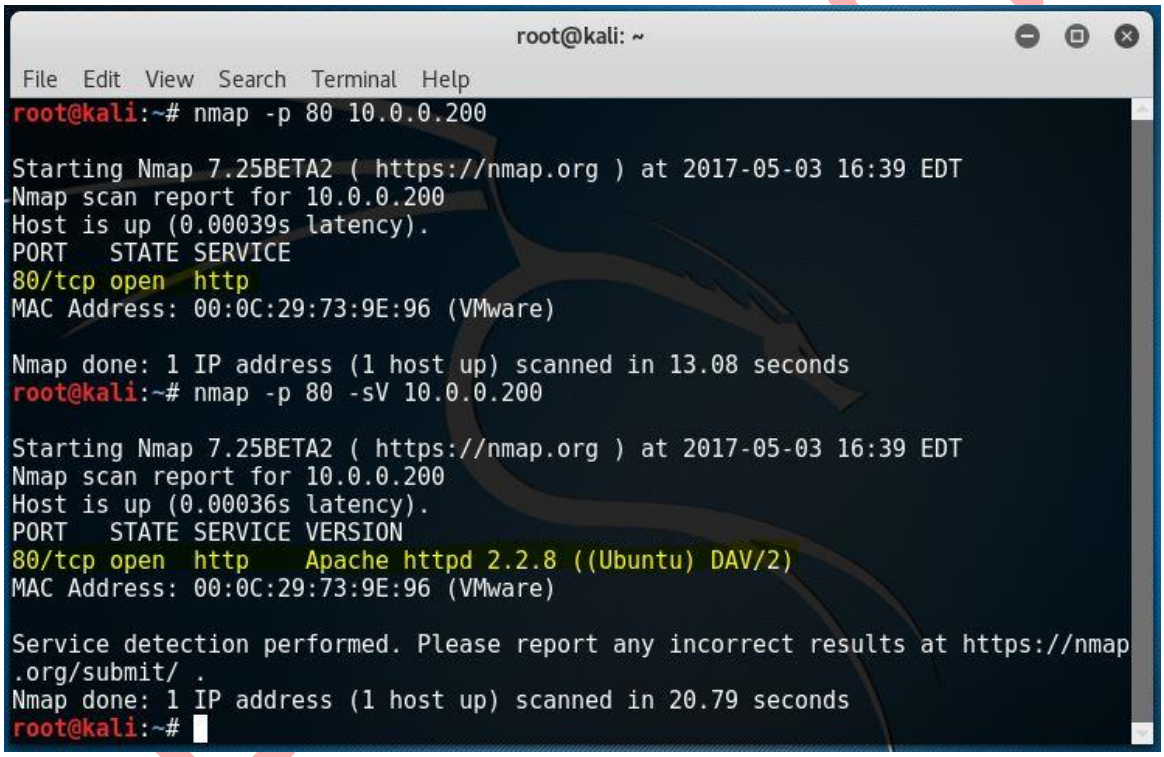
بخش پنجم

دستورات پر کاربرد در Nmap

پس از تعریف آدرس IP و پورت، برخی از سوییچ های پرکاربرد در Nmap وجود دارد که در تست نفوذ هم کاربردی می باشد.

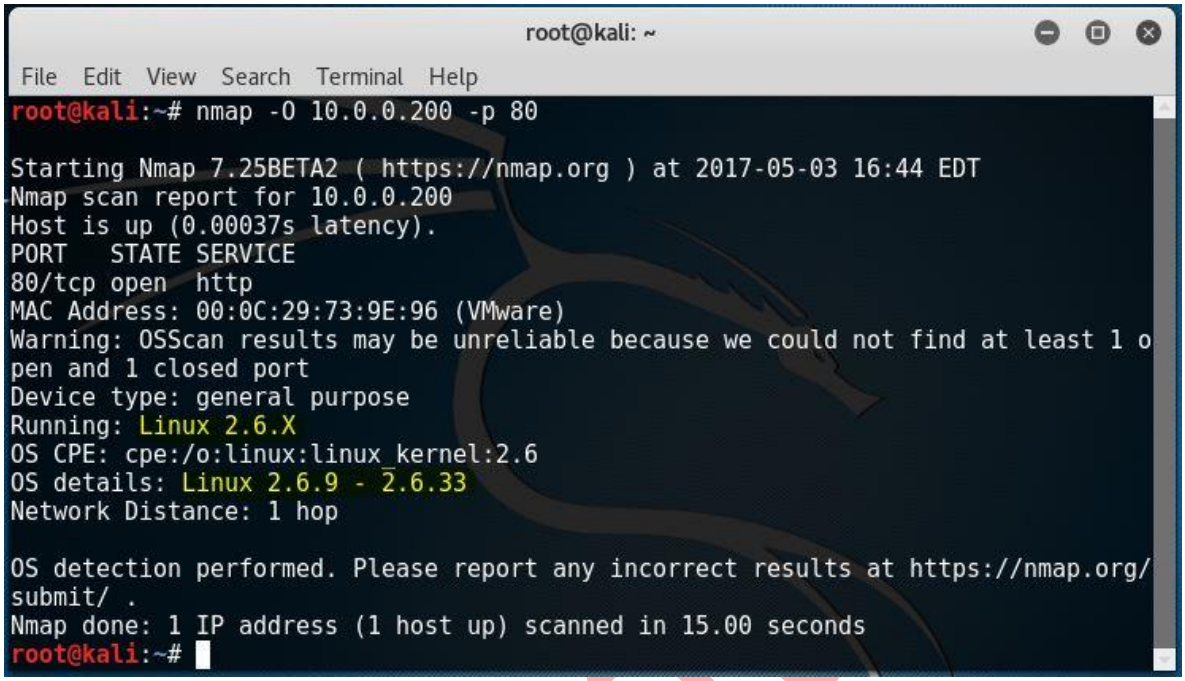
Nmap -sV ➔ Verbose

این دستور باعث می شود که اطلاعات بیشتری در مورد سرویس ارائه شود. به عنوان مثال اگر پورتی باز باشد و از این سوییچ استفاده شود، اطلاعات بیشتری در مورد پورت و سرویسی که بر روی آن قرار دارد، داده می شود. در تصویر زیر تفاوت بین خروجی Nmap بدون sV- و با این سوییچ را مشاهده می نمایید.



Nmap -O ➔ OS Detection

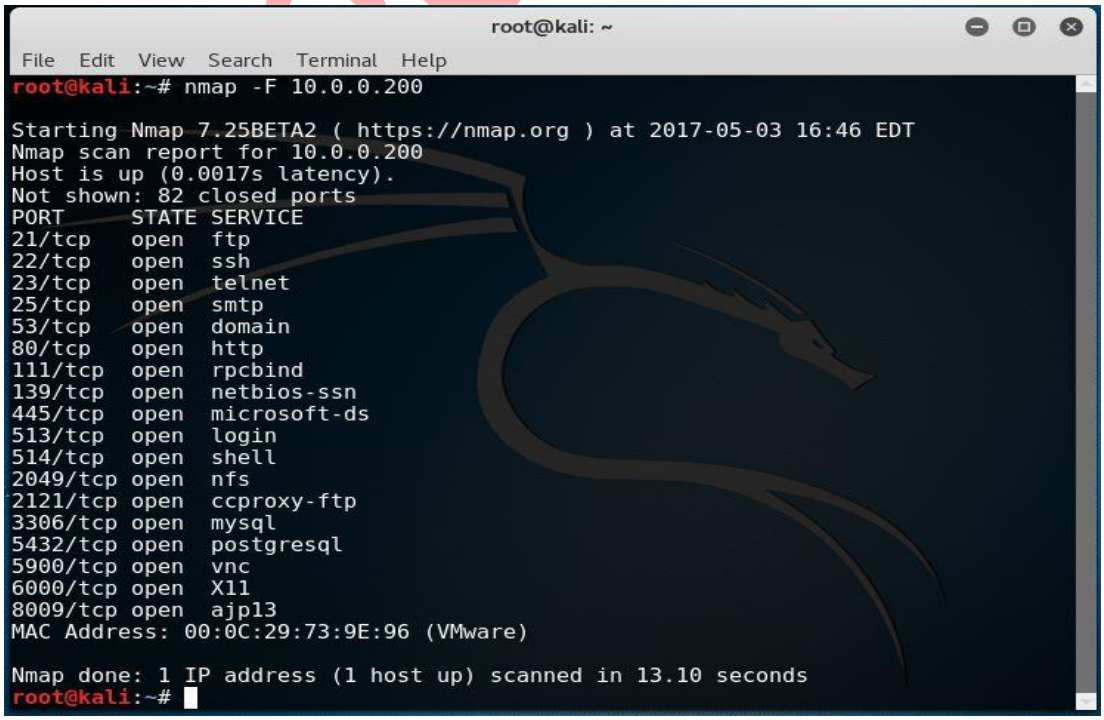
برای شناسایی سیستم عامل هدف می توان از سوییچ O- استفاده کرد.



Nmap -O --osscan-guess

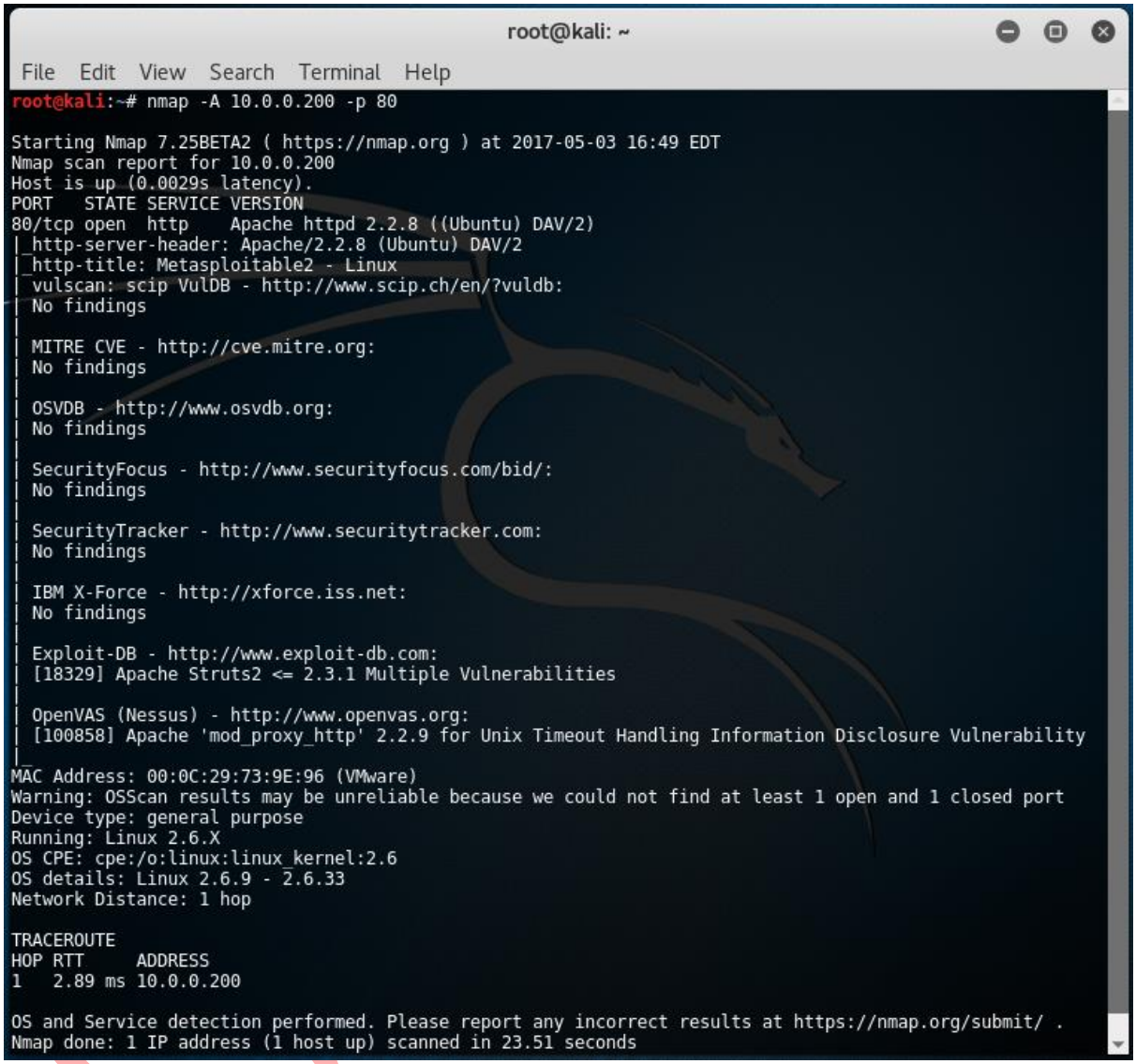
اگر روش قبلی برای شناسایی سیستم عامل پاسخ گو نبود، از روش حدس سیستم عامل استفاده می شود که مطابق مثال عمل می شود.

Nmap -F ➔ Fast Scan (top 100 ports)



سوییچ دیگر F- می باشد که اصطلاحاً اسکن سریع می باشد و ۱۰۰ پورت پرکاربرد را اسکن می کند.

Nmap -A ➔ Aggressive Scan = -sV , -sC , -O



سوییچ بعد A- یا Aggressive می باشد که تلفیقی از سوییچ های sV-، O- و sC- می باشد که sC- شامل اعمال اسکریپت های پیش فرض می باشد. این مورد و همچنین چگونگی شناسایی top ports در سمینار آموزشی Nmap که در سایت Esecurity.ir وجود دارد، توضیح داده شده است.

برای مشاهده جزئیات فیلم سمینار Nmap به لینک زیر مراجعه نمایید. لازم به ذکر است این سمینار به صورت رایگان برای اعضای مدرسه امنیت برگزار گردید.

همچنین شما که این کتاب را مطالعه می نمایید می توانید این بسته آموزشی را باتخفیف بسیار ویژه تهیه نمایید. برای اطلاعات بیشتر و خرید فیلم کامل آموزشی سمینار Nmap به لینک زیر مراجعه نمایید.

سمینار آموزشی Nmap

بخش ششم

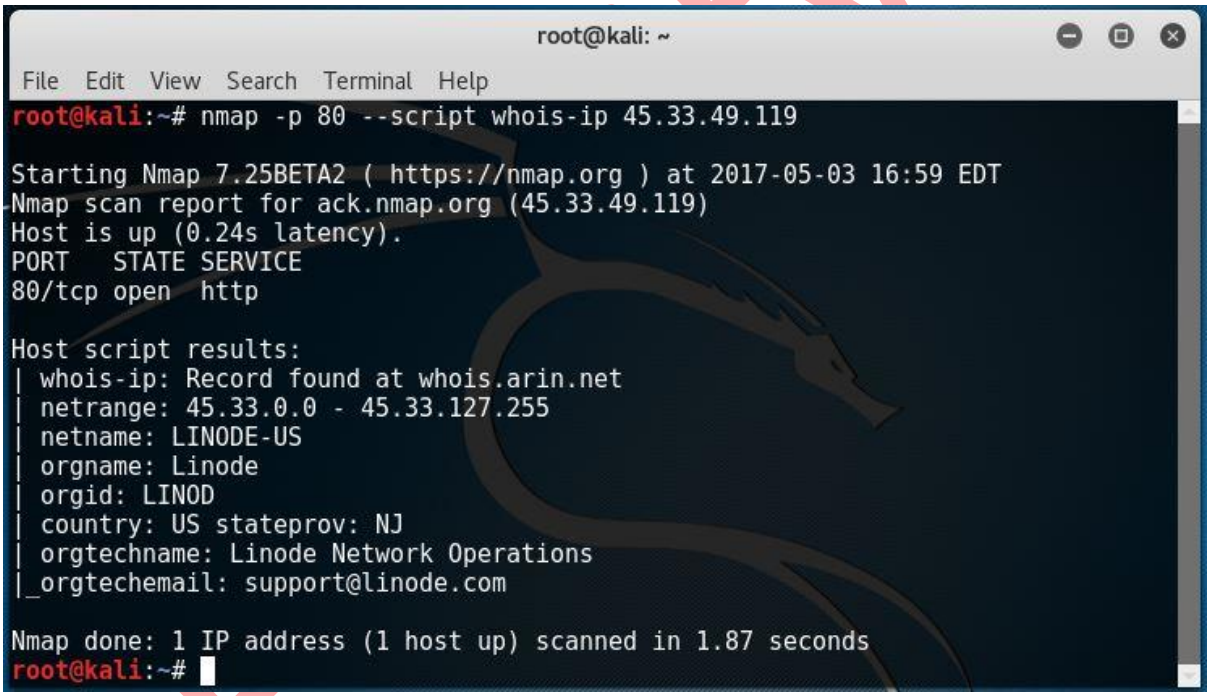
اسکریپت های Nmap

علاوه بر مواردی که به آن اشاره نمودیم، Nmap دارای یک موتور اسکریپتی هم می باشد. در واقع Nmap دارای اسکریپت هایی می باشد که کارهای خاصی را انجام می دهند. تعداد زیادی اسکریپت در Nmap وجود دارد که در کالی لینوکس در مسیر /usr/share/nmap/scripts قرار دارند.

برای مشاهده اسکریپت های موجود باید وارد مسیر ذکر شده، شوید. همچنین برای استفاده از یک اسکریپت در Nmap از سوییچ script-- استفاده شده و پس از آن نام اسکریپت مورد نظر قرار داده می شود.

مثال زیر نمونه ای از استفاده یک اسکریپت در Nmap می باشد.

nmap -p 80 --script whois-ip 20.0.0.1



در این مثال از اسکریپت whois-ip برای استخراج اطلاعات Whois مربوط به IP ۲۰،۰،۰،۱ استفاده می شود.

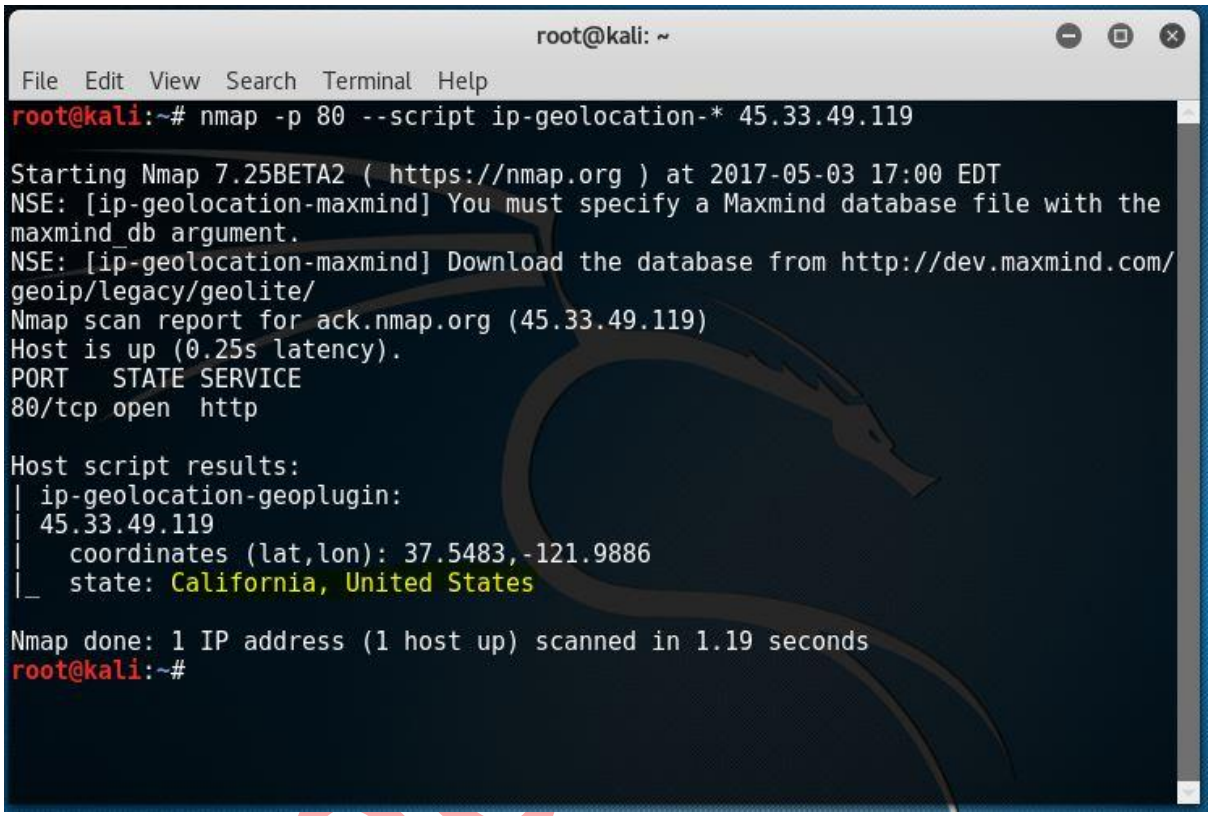
در این نوع از اسکریپت ها برای جلوگیری از اسکن پورت های پیش فرض از سوییچ p- و شماره پورت ۸۰ استفاده می شود.

نمونه های دیگری از اسکریپت های Nmap

nmap -p 80 --script whois-domain esecurity.ir

اسکریپت بالا اطلاعات Whois مربوط به دامین مورد نظر را به شما می دهد.

nmap -p 80 --script ip-geolocation-* IP

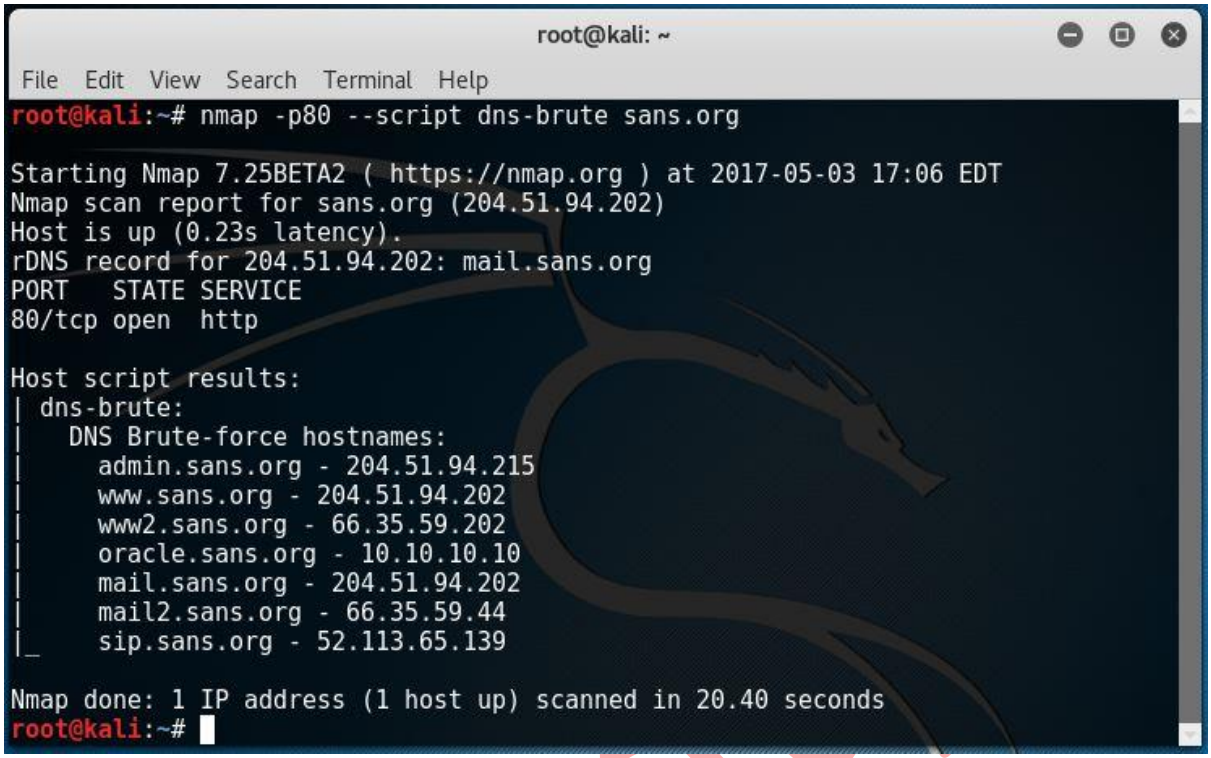


با استفاده از اسکریپت بالا، موقعیت جغرافیایی یک آدرس IP شناسایی می گردد.

nmap -p 80 --script whois-ip 193.70.88.144

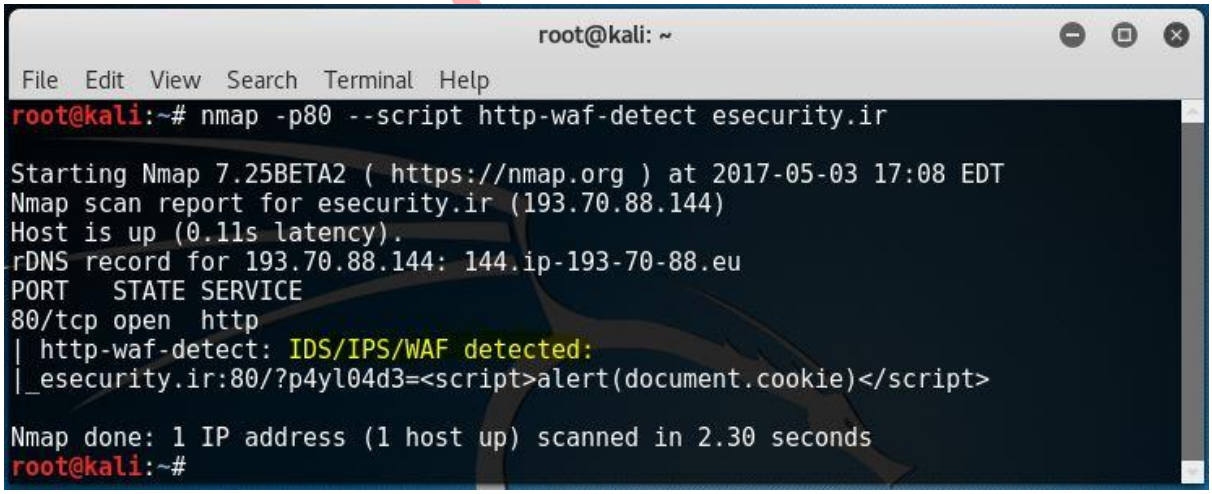
اسکریپت بالا همانطور که اشاره شد برای Whois آدرس IP استفاده می شود.

nmap -p80 --script dns-brute nmap.org



اسکریپت بالا برای پیدا کردن دامین های زیر مجموعه سایت nmap.org استفاده می شود که شما می توانید به جای این سایت، سایت مورد نظر خود را قرار دهید.

nmap -p80 --script http-waf-detect esecurity.ir



از اسکریپت بالا برای شناسایی فایروال تحت وب یا Web Application Firewall یک وب سایت استفاده می شود.

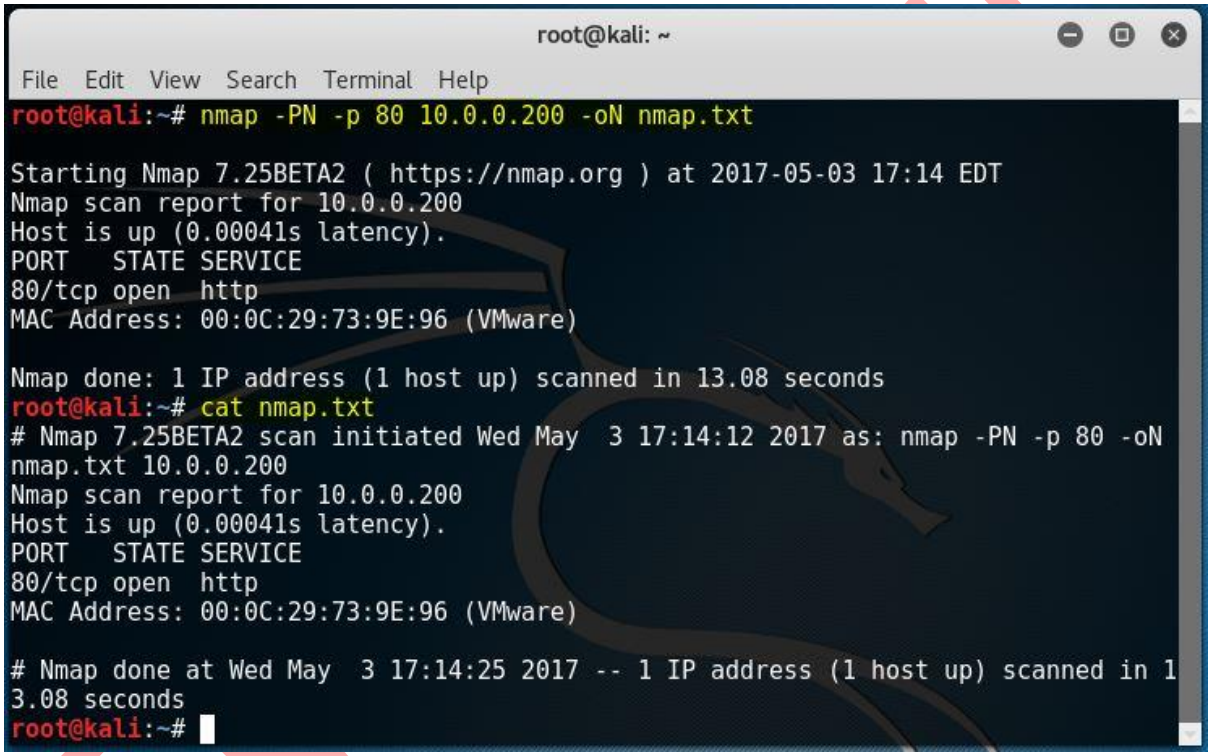
بخش هفتم

انواع خروجی ها در Nmap

پس از اینکه با سوییچ های مختلف و نحوه معرفی آدرس و پورت در Nmap آشنا شدید، هم اکنون باید اطلاعات به دست آمده را در قالب یک خروجی ذخیره نمود تا در آینده به توان از آن استفاده نمود.

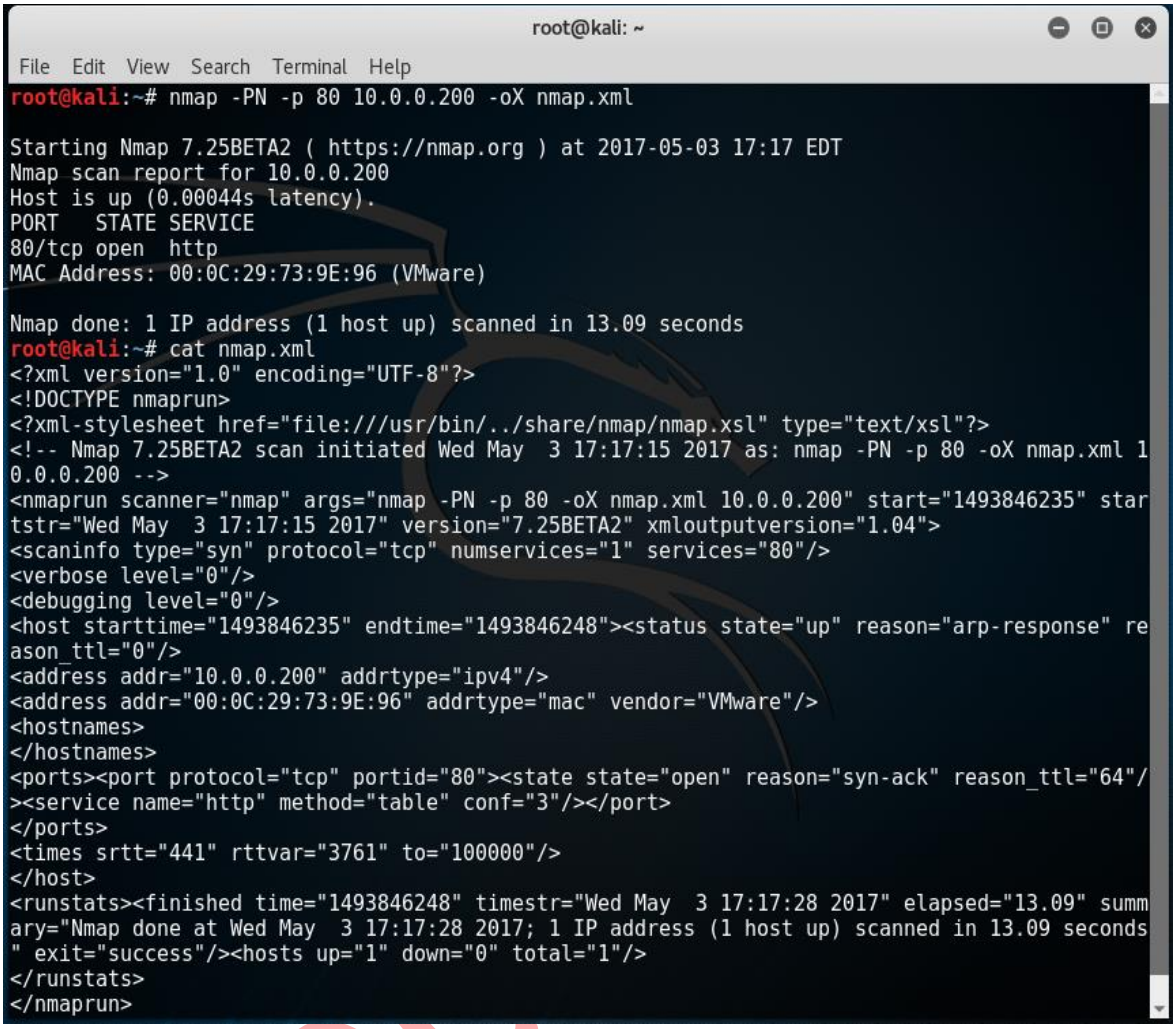
در این بخش با انواع خروجی ها و کاربرد آن آشنا خواهیم شد.

-oN ➔ Nmap File(Text file)



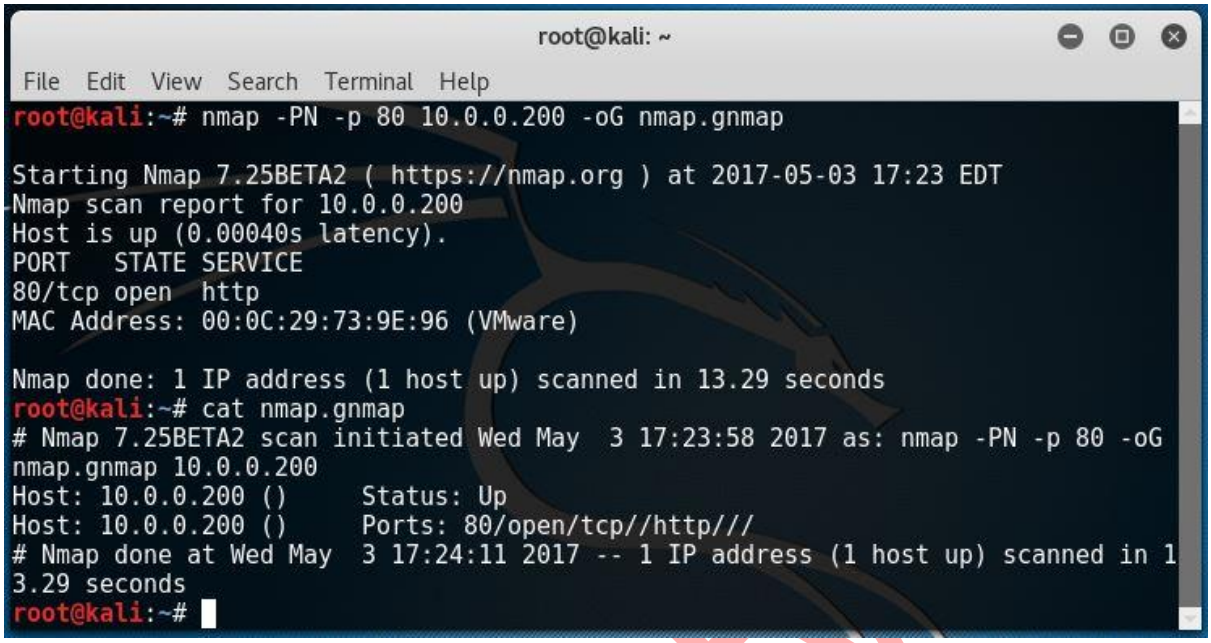
با استفاده از دستور بالا، خروجی Nmap در قالب یک فایل متنی قرار می گیرد. در برخی از کتاب های آموزشی Nmap به این نوع خروجی Nmap File هم گفته می شود.

-oX ➔ XML File



نوع دیگری از خروجی که توسط Nmap پشتیبانی می گردد، XML است. که برای این نوع خروجی از سوییچ بالا استفاده می شود.

-oG ➔ Grep support file

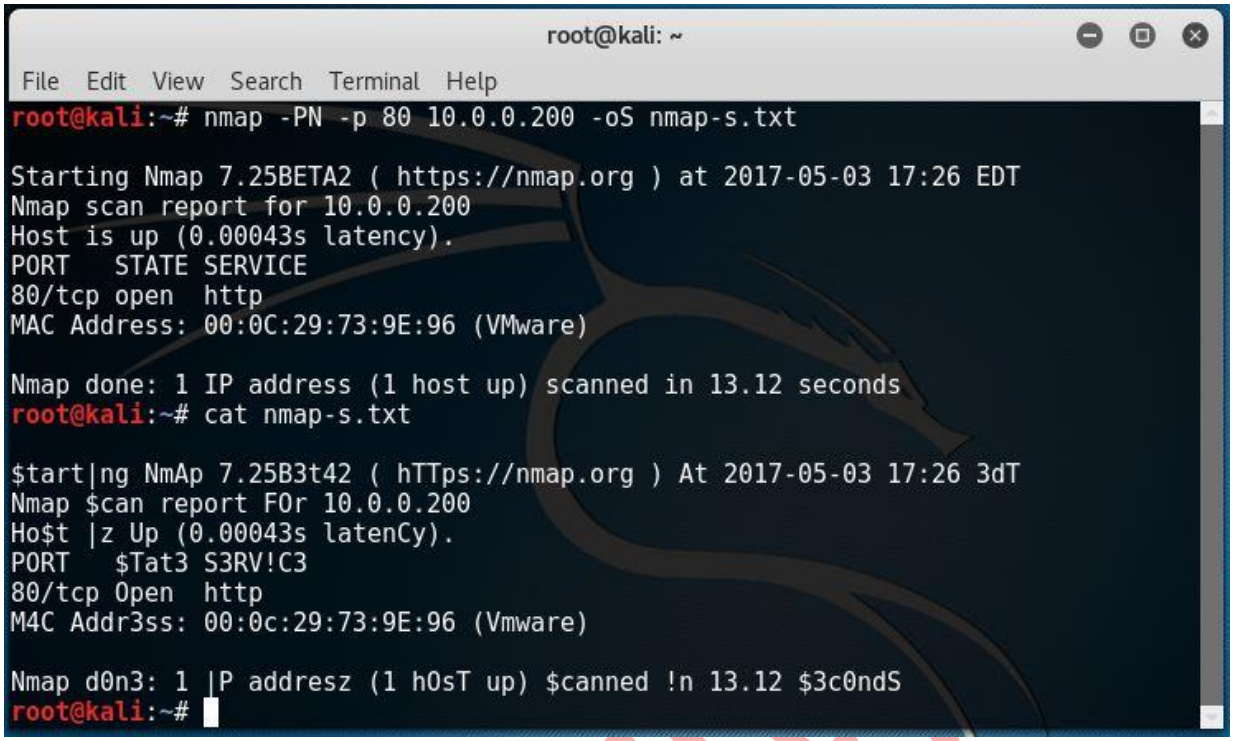


خروجی دیگری که در Nmap از آن پشتیبانی می شود، Grepable است. این نوع خروجی برای زمانی مورد استفاده قرار می گیرد که قصد داشته باشید تا از خروجی Nmap برای دستور Grep استفاده نمایید. این دستور، خروجی Nmap را برای دستور Grep آماده می کند.

-oA ➔ All (NXG)

این سوییچ هر سه خروجی بالا را به صورت یک جا ایجاد می نماید.

-oS ➔ Script Kids file ☺



این نوع خروجی بیشتر جنبه تفریحی دارد و خروجی را به صورت زبان هکرها ایجاد می نماید.

در پایان امیدوارم از کتاب الکترونیکی کوتاه و کاربردی از Nmap برای تست نفوذ استفاده لازم را برده باشید و اگر این کتاب را مفید دانستید، آن را با دوستان خود و علاقمندان به تست نفوذ به اشتراک بگذارید.

همچنین لازم به ذکر است در این کتاب به صورت کوتاه و کاربردی به برخی از توانمندی های نرم افزار قدرتمند Nmap پرداخته شد و این ابزار قابلیت های زیادتری از آنچه در این کتاب به آن اشاره شد، را داراست.

همواره موفق و سربلند باشید