NMAP

Marc BEY

Využívání otevřených portů, množství služeb dostupných na strojích místní sítě, testy zranitelnosti stejně jako bezpečnostní audity: to vše je velmi důležité pro správce sítě. Je pro něj nezbytné pravidelně skenovat svou síť, dříve než se o to postarají osoby se zlými úmysly, a optimalizovat její bezpečnost. K tomu je ovšem nezbytné, aby měl k dispozici všechny nezbytné nástroje pro provedení rychlé inventarizace sítě. NMAP odpovídá všem těmto potřebám a dodává velmi přesné informace. A o tom se píše v tomto článku. Cílem textu je mimo jiné popsat skenování portů, které se jeví jako velmi výkonný diagnostický nástroj.

autorzy@lpmagazine.org

Tento článek se zaměřuje na oblast správy systému. Je záhodno používat NMAP s jistou opatrností, pokouším se zaměřit na právní aspekty skenování portů a informovat čtenáře, že jeho použití na nějaký cíl musí být dána ke schválení jeho vlastníkovi a že jakékoli skenování na síti mimo tento právní rámec je zakázáno a uživatel se v takové situaci vystavuje riziku trestu.

Nmap je *Open Source* scanner portů, který byl vytvořen FYODORem a který distribuuje Insecure.org. Je navržen tak, aby detekoval otevřené porty, služby, které na nich probíhají, stejně jako ke sběru mnoha informací o operačním systému vzdáleného počítače a službách běžících na systémech (HTTP, FTP...).

Nejnovější verzí je verze 4.11. V posledních několika letech se kolem projektu sdružuje poměrně velká komunita.

Tento nástroj, disponibilní pro Linux ale také pro Windows, je distribuován pod licencí GPL.

Naším cílem je předvést funkce tohoto nástroje instalovaného pod Open Suse Linuxem 10.0 a poukázat na význam skenování portů pro správu systému, bezpečnostní audity, ale také pro dohled nad síťovými službami.

Funkce NMAP

Pro provádění scanů vzdálených strojů používá NMAP soubor skenovacích a analytických služeb založených na různých protokolech jako TCP, IP, UDP nebo ICMP.

Jeho cílem je co nejrychlejší vytvoření mapy IP zásobníku. Právě toto mu také umožní získat popis operačního systému cílového stroje.

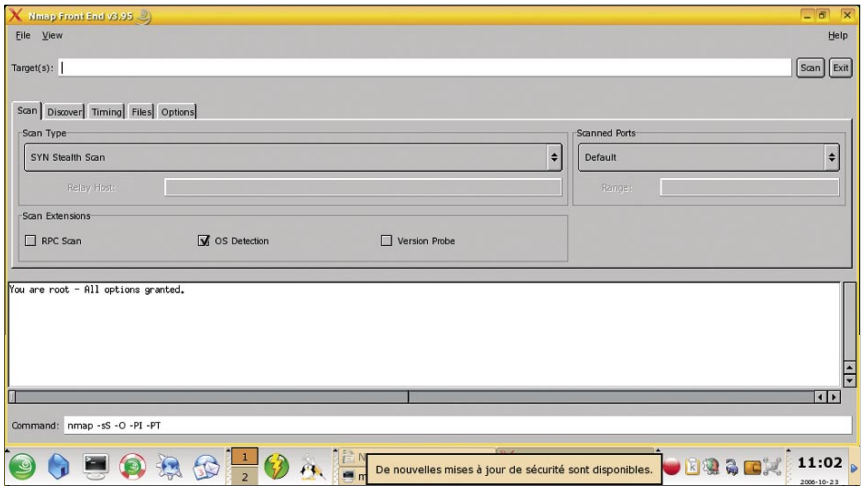
Od vydání verze 4.0 projektu NMAP je také možné provádět scany ARP rychlejší než scany IP, ale také specifikovat například MAC adresu použitou v odeslaných ethernetových paketech.

Databáze NMAP obsahuje více než 3100 reprezentativních signatur pro více než 380 různých služeb.

Instalace NMAP

Navrhujeme vám instalovat poslední verzi NMAP na Open Suse Linux 10.0.

Můžete jej nainstalovat s pomocí správce balíčků přes YAST nebo také přímo:



Obrázek 1. NMAP a jeho grafické rozhraní

```
rpm -vhU http://download.insecure.org/
nmap/dist/nmap-4.11-1.i386.rpm
nebo přes archiv .tar.bz2
bzip2 -cd nmap-4.11.tar.bz2 | tar xvf
-
cd nmap-4.11
./configure
make
su root
make install
```

NMAP navíc disponuje poměrně šikovným grafickým rozhraním: `nmap-frontend-4.11-1.i386.rpm`.

Můžete jej také nainstalovat:

```
rpm -Uvh nmap-frontend-4.11-1.i386.rpm
```

Poznamenejme, že NMAP je k dispozici ve většině Linuxových distribucí. Výše popsané postupy samozřejmě platí také pro ně.

Jakmile je nástroj nainstalován, je připraven k použití.

Použití NMAP

Před začátkem používání NMAP je dobré znát některé charakteristiky tohoto nástroje.

Různé odpovědi NMAP na skenování a v závislosti na portu:

- *Open* (otevřený): znamená to, že aplikace přijímá spojení TCP nebo pakety UDP na příslušný port;
- *Closed* (zavřený): znamená to, že na daném portu není k dispozici žádná aplikace, ale že port je přístupný;
- *Filtered* (filtrovaný): znamená to, že port je filtrovaný. Nmap nesděluje k tomuto stavu příliš detailů, možná, že pravidlo Iptable zabraňuje scanu nebo se například požadavek vrací se zprávou ICMP typu host unreachable;
- *Nefiltrovaný*: znamená, že port není filtrovaný, ale že je přístupný. Tento stav odpovědi je možno zjišťovat s pomocí scanu ACK;
- *otevřený/filtrovaný*: tento stav označuje absenci odpovědi skenovaných portů a NMAP nemůže určit jejich skutečný stav;
- *zavřený/filtrovaný*: označuje, stejně jako předchozí situace, nepřítomnost odpovědi skenovaného portu. Týká se to zejména scanů Idle založených na identifikátorech paketů IP.

Co se týká syntaxe, NMAP přijímá prostřednictvím příkazového řádku rozmanité formáty, jako IP adresy, jména hostitelů, CIDR, IPv6 nebo intervaly.

Specifikace cílů

Pro účinné používání NMAP je vhodné přesně definovat stroje nebo sítě, na kterých má být skenování prováděno. A právě v této oblasti se popisovaný nástroj plně uplatňuje a na bízí mnohé možnosti.

My si nicméně přiblížíme pouze ty nejpoužívanější:

- *nmap – iL <soubor>* zaměřuje se na všechny hostitele obsažené v souboru soubor. Ideální pro použití na síti fungující se serverem DHCP, který přenáší mnoho IP;
- *nmap –exclude <cíl...>* vyznačí pro NMAP cíle, které mají být vyřazeny ze skenování nebo rozmezí IP adres;
- *nmap –excludefile <vyřadit>* volba –excludefile v argumentu specifikuje, co je třeba vynechat ze skenování, na základě seznamu v souboru.

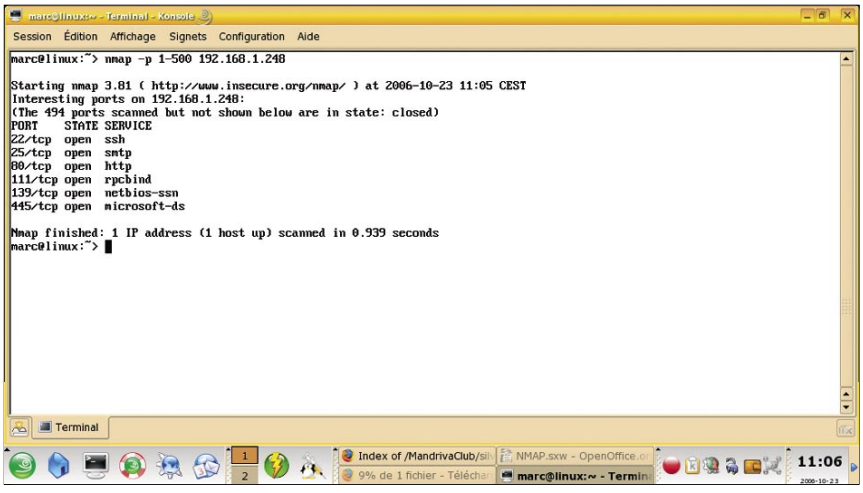
Specifikace portů

S pomocí NMAP je možné nastavit jako cíle skenování a požadavků vybrané porty.

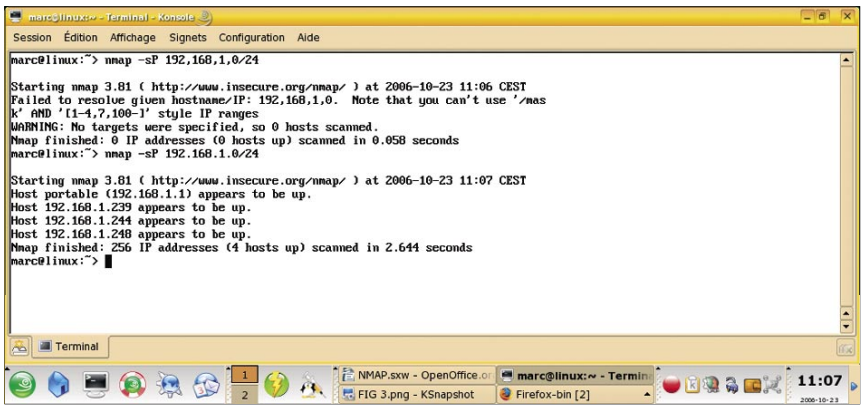
Soubor *nmap-services* umístěný v */usr/share/nmap* obsahuje přednastavený seznam portů NMAP s více než 1600 (nejznámějšími) porty, `nmap -p 1-500 192.168.1.248` bude skenovat všechny porty od 1 do 500 na uvedeném stroji.

NMAP -F<cíl> znamená, že si přejete použít nmap-services v argumentu. NMAP pak velmi rychle skenuje nejznámější porty, `nmap -sP 192,168,1,0/24` umožní provést *ping scan* a velmi rychlé rozpoznání strojů v síti v podobě seznamu zařízení, která odpověděly na požadavek. Tento příkaz umožňuje vidět nejenom stroje, které jsou v dané síti, ale také stav serverů.

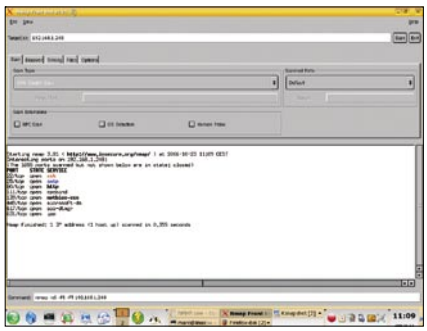
NMAP -PS 22,23,80,631 192,168,1,248 odesílá prázdný paket TCP s SYN vlajkou (*flag*) aktivovanou na portech 22, 23, 80, 631 uvedeného cíle. SYN vlajka se pokouší vytvářet na vzdáleném stroji spojení. Pokud je cílový port zavřený, je odeslán RST (*reset*) *paket*. Pokud se port vyjeví jako otevřený, přejde cíl k druhé etapě vytváření spojení TCP ve třech krocích



Obrázek 2. Skenování portů 1 až 500



Obrázek 3. Rychlé zobrazení strojů v síti



Obrázek 4. Scan TCP/SYN s pomocí NMAP

(*TCP 3-way-handshake*) a odpoví paketem TCP SYN/ACK.

Stejný příkaz, ale s volbou -PA v argumentu umožňuje provést odeslání paketu TCP, ale s ACK vlajkou.

Tyto dvě techniky umožňují správcům sítí obejít firewally nebo routery. Ovšem některé z nich, zejména *Iptables/Netfilter*, způsobí často neúspěch těchto testů, jmenovitě testů ACK, díky jejich stavu stateful anebo ještě použitím volby –syn v pravidlech *Iptables*. Jde o techniky, které používá rootový uživatel, *nmap -PR <cíl>* umožňuje provádět ARP pingy. Záměrem je skenování na celé místní síti, zejména na takové, která používá rozsah adres bez RFC 1918. Význam uvedeného spočívá v tom, že pokud Nmap dostává odpovědi na požadavky, nemusí potom pokračovat s pingy založenými na IP, protože již ví, zda je ten který cíl aktivní. Takový typ skenování je mnohem rychlejší než scany založené na IP, nmap -PU <cíl> umožní provedení pingu UDP odesláním prázdného UDP paketu na cíl. Smyslem takových požadavků je, že pokud požadavek pošleme na zavřený port na příslušném stroji, očekává UDP test obdržení ICMP paketu (*port unreachable*) a další. To ukazuje, že stroj je aktivní a disponibilní.

Techniky skenování

Nmap nabízí mnoho skenovacích technik. Několik z nich si zde přiblížíme i s jejich specifiky, jako je detekce protokolu nebo verzí. Tyto techniky nemohou být použity simultánně bez scanů UDP, které mohou být kombinovány se scany TCP.

Scan TCP/SYN (-sS v argumentu)

Jde o přednastavený scan, nejčastěji používaný, který také nabízí výbornou schopnost rozlišení mezi jednotlivými stavy portů (otevřený/zavřený). Takový scan nazýváme „polootevřený". Spojení TCP není navázáno, SYN paket je odeslán. Odpověď SYN/ACK nám říká, že port je otevřený, kdežto RST paket znamená zavřený stav portu (Obrázek 4).

Scan TCP CONNECT (-sT v argumentu)

Ideální například pro skenování IPV6 sítí nebo v případě, kdy uživatel nemá nezbytná práva pro odeslání raw paketů. Tento typ scanů je méně účinný a delší (Obrázek 5).

Scan UDP (-sU v argumentu)

Správci tuto techniku skenování příliš nepoužívají, protože jim často připadá zdlouhavá. Dělají však chybu, protože jakkoli jsou mnohé síťové služby založené na TCP, služby založené na UDP jako třeba DHCP, SNMP nebo DNS jsou také široce používány. Je nicméně nezbytné použít tuto techniku rychle, protože otevřené porty obvykle pouze výjimečně odesílají odpověď umožňující NMAP dostatečnou dobu spojení. Tyto scany jsou relativně obtížné na zavřených portech, které odesílají odpověď typu *host unreachable*. Jde o techniku, které chybí dostatečná citlivost a musí být doplňována simultánním SYN scanem (Obrázek 6).

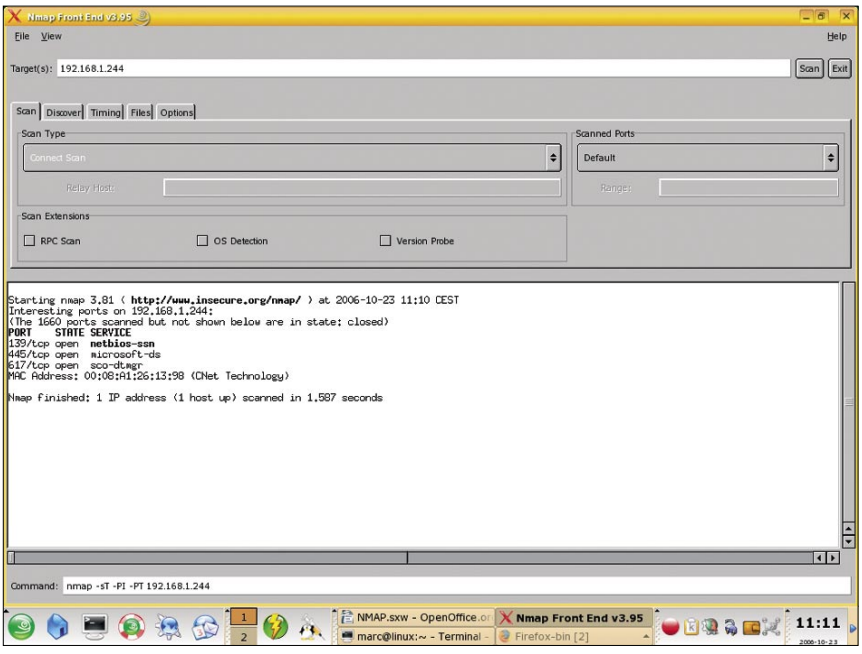
Scan TCP ACK (-sA v argumentu)

Jde o techniku, která je ideální pro správce, zejména pro zavedení pravidel firewallu. Jejím cílem není určit, zda je port otevřený či filtrovaný, nýbrž určení stavu stateful nebo stateless firewallů a testování pravidel.

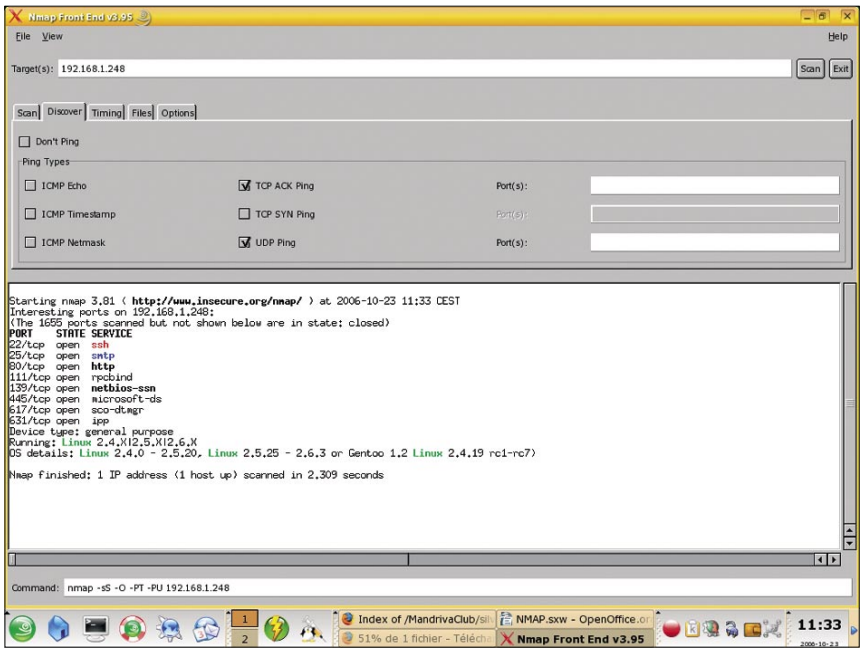
Scan ACK aktivuje pouze ACK vlajku paketů. Nefiltrované systémy reagují odesláním RST paketu. Nmap tedy považuje port za nefiltrovaný, to znamená přístupný s pomocí ACK paketu, ale bez znalosti, zda je port otevřený. Porty, které neodpovídají nebo odesílají některá chybová hlášení jako ICMP, jsou považovány za filtrované.

Nastavitelný Scan TCP (-scanflags v argumentu)

NMAP je nastavitelný. Je totiž možné vytvořit individuálně nastavený scan používající několik vlajek (ACK, RST, SYN), což umož-



Obrázek 5. Scan TCP connect



Obrázek 6. Scan XMAS s pomocí NMAP

ňuje správci testovat nově instalovaný IDS (systém detekce napadení).

Scan okna TCP (-sW v argumentu)

Tato technika se velmi podobá scanu ACK, s tím rozdílem, že je mnohem citlivější k zavřeným portům, jejichž otevřený či zavřený stav charakterizuje na základě délky odeslaného RST paketu.

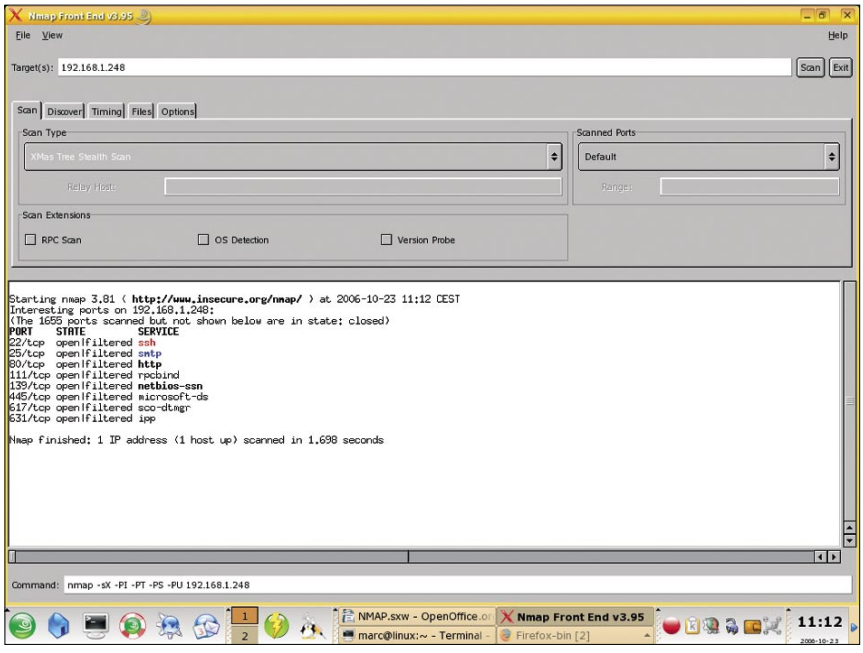
Této technice nicméně schází spolehlivost a není určena pro všechny systémy, protože je založena na malém detailu v rozpoznávání otevřeného či uzavřeného stavu portu.

Scany TCP Null, FIN , Xmas (-sN; -sF; -sX v argumentu).

Tyto tři typy scanů zlepšují citlivost detekce otevřených/zavřených portů s využitím chyby RCF.

Pro všechny systémy, které respektují tento dokument, bude s každým paketem, který neobsahuje SYN nebo RST nebo ACK, odeslán RST pokud je port zavřený a žádná odpověď pokud je port otevřený. Jestliže není použitá žádná z uvedených vlajek, je platná jakákoli kombinace tří ostatních (FIN, PSH a URG). NMAP toho využívá ve třech typech scanů:

- Při scanu Null (-sN) není aktivován žádný bit (vlajka záhlaví TCP = 0);



Obrázek 7. Kontrola verze s pomocí NMAP

Co je třeba znát...

Síťová bezpečnost je důležitým aspektem dnešní doby, která je nezadržitelně stále více digitální. Správci sítí čelí stále větším obtížím při ochraně jim svěřených sítí. Musí proto vědět, že existují velmi dobré nástroje, jejichž příkladem je právě NMAP, které jim umožní optimalizovat bezpečnostní politiku s pomocí rychle získaných informací o stavu různých hostitelů a služeb jejich sítě, aby tak mohli účinně reagovat různým útokům a exploitům masově přicházejícím z internetové sítě.

Je také třeba vědět, že tento nástroj je třeba používat s rozvahou a že uživatel nebo správce se musí vyvarovat použití nástroje ke škodě ostatních.

Tento článek neuvádí podrobně všechny skenovací techniky, nýbrž představuje přehled nejpoužívanějších požadavků. Schopnosti tohoto nástroje a jeho grafického rozhraní jsou demonstrovány s pomocí snímků obrazovky.

- Co se týká scanu FIN (-sF), bit FIN je aktivován;
- při scanu Xmas (-sX) jsou aktivovány vlajky FIN, PSH,URG.

Velkou nevýhodou těchto tří typů scanů je fakt, že ne všechny systémy respektují RFC 793 a výsledek tak může být zavádějící.

Scan protokolu (-sO)

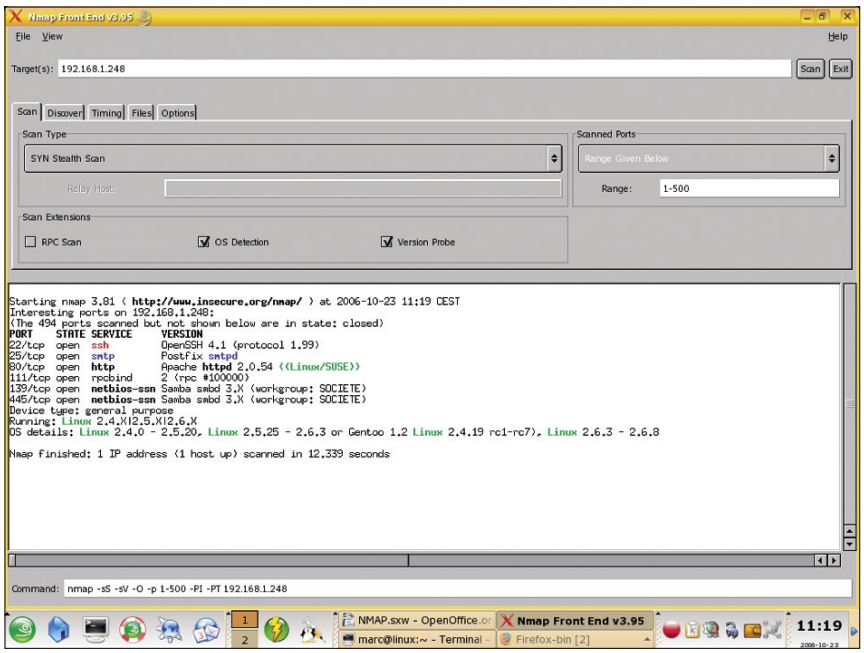
Tento scan je velmi zajímavý, protože umožňuje zjistit, které protokoly jsou podporovány cílovým strojem (TCP, ICMP...). Na první pohled nejde o skenování portů. Tento scan se chová jako scan UDP. Když tedy Nmap dostane odpověď protokolu pocházející z cílového stroje, považuje tento protokol za otevřený. Chyba ICMP (protocol unreachable) způsobí, že port je považován za zavřený.

Detekce služeb a verzí s pomocí NMAP

NMAP nabízí mnohé pokročilé funkce jako je například detekce služeb a verzí.

Záměrem není sestavovat seznam serverů SMTP, HTTP nebo jiných pro naši podnikovou síť nebo klienta. Tuto informaci lze jednoduše získat provedením jednoduchého bezpečnostního auditu.

Nikoli, záměrem je přesně určit verze aplikací a takto vědět, ke kterým *exploitům* jsou náchylné servery našeho klienta nebo společnosti.



Obrázek 8. Aktivní operační systémy a detekované služby

Pro tento účel je zde databáze *nmap-service-probes*, která obsahuje testy k provedení pro jednotlivé služby stejně jako řetězce znaků, se kterými bude třeba porovnat různé odpovědi. NMAP se pokusí určit protokol (telnet, http...), jméno aplikace (ISC Bind...), číslo verze, jméno hostitele, typ zařízení (router, ...), rodinu operačního systému (BSD, Linux). NMAP disponuje přibližně 3 000 charakteristickými znaky, které odpovídají 350 různým protokolům.

Pokud jsme tedy kompilovali NMAP s podporou OpenSSL, NMAP se připojí k serverům SSL, aby zjistil služby poslouchající za kryptovací vrstvou. Pokud máme co dočinění s RPC službami, bude automaticky použit RPC modul NMAP (-sR) pro zjištění RPC programu a jeho verze.

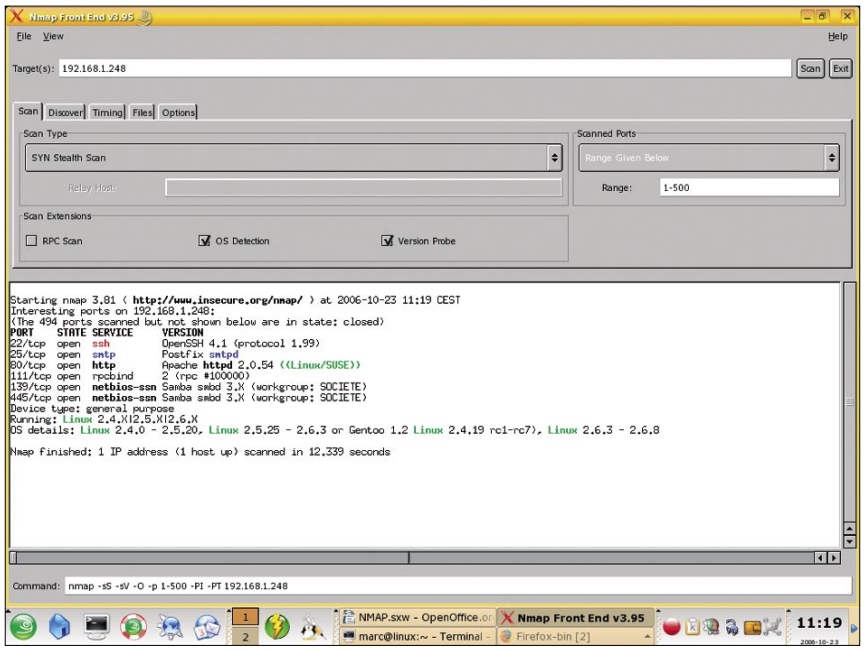
Tento typ scanů je umožněn volbami *-sV* (detekce verze),*-allports* (všechny porty),*-version-all nebo -version-light.*

Detekce operačního systému s pomocí NMAP

Mezi pokročilé funkce tohoto báječného nástroje patří schopnost detekce OS (operačního systému). K tomu účelu použije NMAP „otisk" TCP/IP zásobníku cílového stroje. Tento otisk je posléze porovnán s databází *map-os-fingerprints*, která obsahuje více než 1500 otisků OS. Funkce je použitelná pokud je na cílovém stroji nalezen alespoň jeden port otevřený a jeden zavřený.

Tato technika se provádí vložením následujících voleb do argumentu NMAP:

- *-O pro* aktivaci detekce OS. Je možno přidat -A pro současné zjištění verze,
- *-osscan-limit* pro omezení skenování na stroje odpovídající zadaným podmínkám (Obrázek 9).



Obrázek 9. -osscan-limit: volba umožňující omezit detekci na některé síťové stroje

Závěr

NMAP zůstává nejkompletnějším nástrojem pro skenování portů, který disponuje jednou z nejaktivnějších komunit. Jeho použití, jak jsme již předeslali v úvodu, musí podléhat etickým pravidlům, zejména v síti internet. Představuje výborný nástroj pro správce sítí umožňující rychle vytvořit mapu sítě, zobrazit stav serverů, upravovat bezpečnostní politiku s pomocí testů a nastavování firewallů. Umožňuje také správu verzí používaných protokolů a služeb a takto čelit možným *exploitům*, tedy konsolidovat bezpečnost na síti, za níž je zodpovědný.

Mohli bychom o NMAP napsat více a upřesnit více aspektů jeho použití, nicméně zdroje na síti jsou vyčerpávající.

Připomínám ještě, že NMAP musí být používán v zákonných mezích. Takových připomenutí nebude nikdy dost.

O autorovi

Marc BEY je ředitelem společnosti *BASHPROFILE*. *BASHPROFILE* je vývojovou společností volného software se sídlem v Marseille (Francie). Nabízí svým zákazníkům softwarová řešení založená na prostředí Open Source. Jednou z jejích priorit je síťová a systémová bezpečnost.

BASHPROFILE je členem ASS2L (*Asociace společností vyvíjejících volný software*) *http://www.bashprofile.net, marcbey@bashprofile.net*

Na síti

- NMAP je ke stažení na: *http://insecure.org/nmap/download.html;*
- Grafické rozhraní NMAP je ke stažení na: *http://download.insecure.org/nmap/dist/nmap-frontend-4.20ALPHA9-1.i386.rpm.*