

Nessus mit Nmap Output

Ivan Bütler – 12. August 2009



Vulnerability Scanning

Beim Scanning von grossen Netzen arbeitet Compass oftmals zuerst mit nmap und speichert die Ergebnisse in den NMAP XML Dokumenten ab. Dies ermöglicht es rasch einen Überblick über ein Netz zu verschaffen. Wird daraufhin das Netz noch mit Nessus gescannt, werden die NMAP Portscans oftmals wiederholt, obwohl man Nessus anweisen kann, die NMAP Output Files zu berücksichtigen. Das schont die Bandbreite und IDS System. In diesem kurzen Bericht zeige ich, wie man NMAP Outputs in Nessus verwendet.

Installation von NMAP NASL Nessus Server

Im ersten Schritt muss man dem Nessus Server die NMAP NASL bereitstellen. Leider sind diese Plugins nicht im Default Verzeichnis von Nessus, so dass dies gemäss untenstehender Anleitung manuell gemacht werden muss.

<http://www.nessus.org/documentation/index.php?doc=nmap-usage>

Die beiden NASL Files (siehe unten) müssen ins Nessus Plugin Verzeichnis kopiert werden.

<http://www.nessus.org/documentation/nmap.nasl>
<http://www.nessus.org/documentation/nmapxml.nasl>

Beispiel Nessus Plugin Verzeichnis

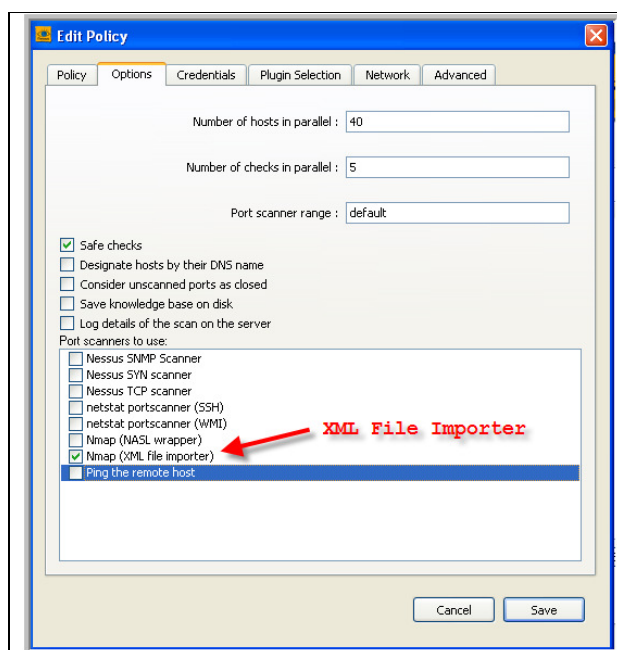
`/opt/nessus/lib/nessus/plugins/.`

Danach ist ein Restart von Nessusd notwendig. Nun kennt der Nessus Daemon die NMAP Schnittstelle. Gemäss Doku von Tenable sollten auch gewisse Switches während dem Nmap Scan gesetzt sein. Hier ein Beispiel mit den geforderten -sC , -sV und -oA (XML Output) Switches.

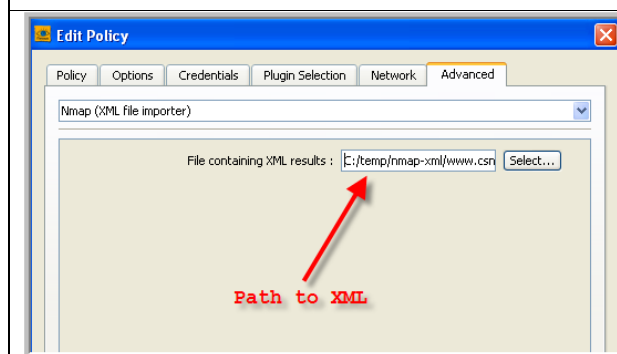
```
nmap -oA /opt/data/nmap/nmapscan --reason -P0 -sV -sC <hostname>
```

Installation von NMAP NASL Nessus Client

Um die NMAP XML Files unter Nessus zu berücksichtigen, muss man folgende Anpassungen der Scan Policy machen.



Beim Nessus Client wird ausschliesslich das NMAP (XML file importer) Plugin aktiviert. Diese Option ist unter "Options" ersichtlich.



Und unter Advanced wird der Pfad des XML dem Nessus Client bekannt gegeben.

Achtung: Fehlt diese Konfigurationsmöglichkeit, muss zuerst eine neue Scan Policy erzeugt werden. Alte Scan Policies kennen die Option nicht. Hilft auch das nicht, sollte man die Nessusd Plugins re-scannen (nessusd -R)

Mit diesem Vorgehen kann man die Nmap/Nessus Scans effizienter gestalten.

Gruss e1