



Falko Dressler Tobias Limmer

Netzwerksicherheit WS 2007/08

9. Übungsblatt

22.1.2008

Netzwerkmonitoring

Es werden in dieser Übung verschiedene Methoden betrachtet, Netzwerke zu überwachen. In einem ersten Schritt werden die Programme Tcpcmdump in Kombination mit Nmap und Xprobe2 betrachtet. Der Flowaggregator Vermont wird anschließend getestet.

1. Loggen Sie sich in das Übungsnetz mittels `ssh user@fai7t1.informatik.uni-erlangen.de` und `ssh root@routerX-1` auf Ihrem Monitoring-Rechner ein. Alle Pakete, welche an und von pcX-2 übertragen werden, können auf routerX-1 an Schnittstelle eth2 überwacht werden (durch Port-Mirroring auf dem Switch). Sie können pcX-1 als "Angriffsrechner" verwenden.
2. Starten Sie Tcpcmdump mit dem Kommando `tcpcmdump -i eth2 -n` auf dem Monitoring-Rechner.
3. Überprüfen Sie auf dem Angriffsrechner, welche Rechner im aktuellen Subnetz vorhanden sind mit dem Befehl `nmap -sP 192.168.10X.0/24`.
4. Führen Sie Nmap auf dem Angriffsrechner mit dem Befehl `nmap 192.168.10X.2` aus.
5. Was findet Nmap heraus? Welche Pakete werden übertragen?
6. Nmap benutzt mit UID root normalerweise den TCP SYN-Scan. Führen Sie Nmap erneut mit der Option `-sT` (TCP-Connect Scan) aus und beobachten Sie mit Tcpcmdump speziell einen offenen Port am Zielrechner. Dazu ergänzen Sie das Aufrufkommando von Tcpcmdump mit `port <Portnummer>`.
7. Welchen Unterschied beachten Sie? Welchen "Vorteil" besitzt der TCP SYN-Scan gegenüber dem TCP Connect-Scan?
8. Testen Sie nun das Programm Xprobe2 auf pcX-1 mit `xprobe2 192.168.10X.2` und beobachten Sie es mit Tcpcmdump. Damit Tcpcmdump weitere Informationen über überwachte Pakete anzeigt, kann der Parameter `-v` übergeben werden.
9. Das Tool Vermont kann Flowdaten generieren. Dazu starten Sie auf dem Monitoring-Rechner Vermont mit dem Befehl `~/vermont.sh`. Dies startet eine Instanz von Vermont, welche auf eth2 einkommende Pakete aggregiert und die entsprechenden Flows auf der Kommandozeile ausgibt.
10. Starten Sie auf dem Angriffsrechner eine TCP-Verbindung und beobachten Sie die Ausgaben von Vermont. Warum werden Flows erst verzögert ausgegeben?
11. Starten Sie nun auf dem Angriffsrechner einen Portscan und beobachten Sie die Ausgaben von Vermont.

12. Editieren Sie die Datei `~/vermont/printer.xml` und entfernen Sie die Einträge

```
<flowKey>
  <ieName>sourceTransportPort</ieName>
</flowKey>
<flowKey>
  <ieName>destinationTransportPort</ieName>
</flowKey>
```

Führen Sie den Portscan erneut durch. Wie verändert sich die Ausgabe von Vermont? Warum?

13. Überlegen Sie sich Antworten auf folgende Fragen, sie werden am Ende der Übung behandelt:

- Wie kann ein Webserver mit Hilfe von Flowdaten erkannt werden?
- Nehmen wir an, der Webserver benutzt beliebige Ports und ist nicht anhand der Ports 80 und 443 identifizierbar. Kann der Webserver dennoch erkannt werden?

Hausaufgabe:

Sie erhalten eine Textdatei im Format CSV mit aggregierten bidirektionalen Flows. Ihre Aufgabe ist, darin einen vertikalen Portscan zu erkennen. Beschreiben Sie Ihre Vorgehensweise mit Begründung und die Ergebnisse.

Die Textdatei erhalten Sie unter der URL

<http://fau17as.informatik.uni-erlangen.de/~limmer/netsec/flows.csv.bz2>

Benutzername und Passwort wird Ihnen in der Übung mitgeteilt.

Technische Hinweise:

- Die Aufgaben sind in C/C++, Java, Perl, Python oder einer anderen gängigen (und lesbaren!) Programmiersprache zu erstellen.
- Bei Bedarf kann eine leichtgewichtige Datenbank wie SQLite verwendet werden. Ein Skript für die Erstellung der benötigten Datenbankstrukturen und -inhalte aus der CSV-Datei ist mitzuliefern.
- Der Code muss auf dem Betriebssystem Debian/Linux im CIP-Pool der Informatik mit der dort installierten Software kompilieren und lauffähig sein.
- Es ist ein Makefile oder ein ausführbares Skript zu bereitzustellen, welches temporäre Daten löschen (Target „clean“) und eine Binärdatei (Target „all“) erstellen kann.
- Es ist eine Dokumentation im ASCII-Format zu erstellen, welche einen typischen Programmstart dokumentiert und über Besonderheiten des Programms berichtet.

Abgabe der Lösungen per Mail an tobias.limmer@informatik.uni-erlangen.de bis Montag, den 4.2.2008 als *Archiv* im Format `.tar.(gz|bz2)` oder `.zip`. Als Betreff der Mail `Netsec Aufgabe 9, Gruppe X` angeben.