Protokoll 0

Christoph Robbert 6577945, Peter Stilow 6500440

October 30, 2013

1 Aufgabe 1

Nach einem Login auf den Rechner `cultofthedeadcow.seclab.uni-paderborn.de/192.26.175.11` sah man an der Ausgabe von `ifconfig`, dass sich dieser Rechner im Subnetz `192.26.175.0/26` befand. Ein Anschließender Pingscan mittels `nmap -sP 192.26.175.0/26` zeigte, dass die Hosts aus Figure 1 in diesem Subnetz erreichbar sind. Außerdem zeigte ein anschließender Portscan(`nmap -sT -sV` die folgenden offenen Ports:

- catnetz-992.uni-paderborn.de (192.26.175.1)

  ```
  22/tcp  open  ssh      Cisco SSH 1.25 (protocol 1.99)
  80/tcp  open  http     Cisco IOS administrative httpd
  443/tcp open  ssl/http Cisco IOS administrative httpd
  Service Info: OS: IOS
  ```

  Aus den Angaben des Portscan lässt sich schließen, dass es sich um einen Cisco Router handelt bei diesem Host. Da die Automatische Dienstanalyse von `nmap` sowohl bei den Diensten Cisco Dienste identifiziert alsauch bei der Service Info das Routerbetriebssystem IOS.

- 192.26.175.10

  ```
  22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1 (protocol 2.0)
  111/tcp open  rpcbind
  Service Info: OS: Linux
  ```

  Bei diesem Host wird es sich um einen Ubuntu 12.04 Rechner handeln. Dies schließen wir aus dem Versionsstring '5ubuntu1', da diese Version des openssh Servers nur in Ubuntu 12.04 verwendet wurde. Außer dem ssh und dem rpcbind Dienst wurde kein Dienst auf diesem Server identifiziert.

- cultofthedeadcow.seclab.uni-paderborn.de (192.26.175.11)

  ```
  22/tcp   open  ssh           OpenSSH 5.9p1 Debian 5ubuntu1.1 (protocol 2.0)
  111/tcp  open  rpcbind
  3389/tcp open  microsoft-rdp xrdp
  8080/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
  Service Info: OS: Linux
  ```

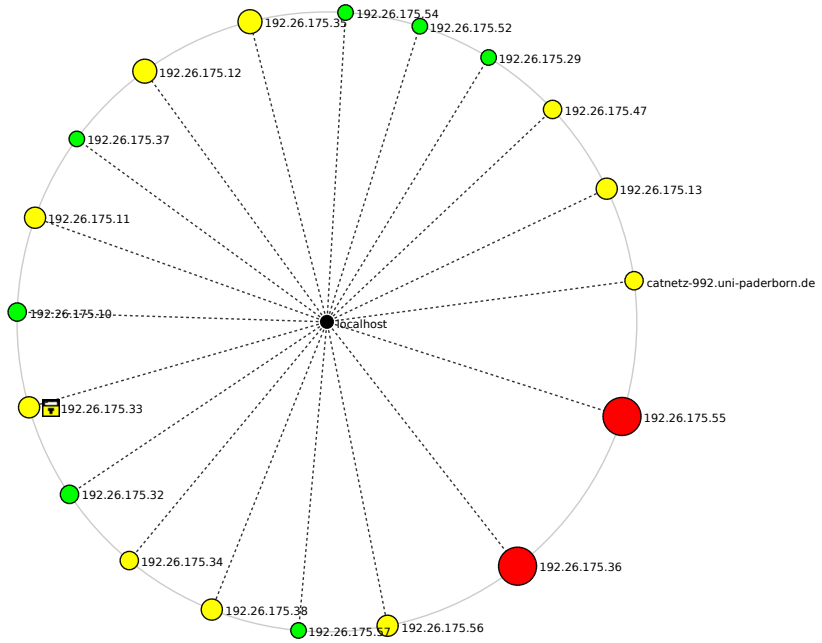

Figure 1: Struktur des Netzes im Security Lab.

Dieser Rechner ist ein Ubuntu 12.04.3 Rechner. Da Zugang zu diesem Rechner per SSH besteht kann man via `vim /etc/issue` diese Versionbezeichung eindeutig bestimmen. Neben dem schon bekannten SSH Dienst läuft auch ein rpcbind Dienst, ein Apache Tomcat Anwendungsserver und der microsoft-rdp Dienst für RemoteDesktopverbindungen.

- 192.26.175.12

```
22/tcp   open  ssh           OpenSSH 5.9p1 Debian 5ubuntu1.1 (protocol 2.0)
111/tcp  open  rpcbind
3389/tcp open  microsoft-rdp xrdp
5910/tcp open  vnc           VNC (protocol 3.3; Locked out)
Service Info: OS: Linux
```

Dieser Rechner scheint auch ein Ubuntu 12.04 Rechner zu sein. Neben dem openssh Server und dem rpcbind Dienst scheint auch ein microsoft-rdp Dienst und ein VNC Dienst für Remotelogins aktiv zu sein.

- 192.26.175.13 Der Portscan brachte dieselben Ergebnisse wie beim Rechner mit der IP 192.26.175.11
- 192.26.175.14 Der Portscan brachte dieselben Ergebnisse wie beim Rechner mit der IP 192.26.175.12
- 192.26.175.29

```
139/tcp open  netbios-ssn
137/udp open|filtered netbios-ns
138/udp open|filtered netbios-dgm
```

Da hier der netbios Dienst läuft, schließen wir, dass es sich um einen Windows Rechner handelt. Die genaue Version ist Aufgrund der Portscans nicht zu ermitteln.

- 192.26.175.32

```
22/tcp open  ssh     OpenSSH 5.8p2_hpn13v11 (FreeBSD 20110503; protocol 2.0)
25/tcp open  smtp
```

Bei diesem Rechner wird es sich laut der verwendeten OpenSSH Serverversion um einen FreeBSD Rechner handeln. Neben dem OpenSSH Server läuft auch ein smtp Server(E-Mailannehmender Server).

- 192.26.175.33
- 192.26.175.34
- 192.26.175.35
- 192.26.175.36
- 192.26.175.37
- 192.26.175.38
- 192.26.175.47
- 192.26.175.49
- 192.26.175.54
- 192.26.175.55
- 192.26.175.56

2 Aufgabe 2

flgbab8e275f92ee6cf9fd48333dfeb0b85 Beim Aufstellen der Stützen unter der Tastatur fiel dieser Hardwareflag auf.

flgbb315509cf9c5caac09624d258c3d95d Beim einloggen via `ssh` auf den Rechner `192.26.175.11` und anschließendem "orientieren" via `ls` fiel auf, dass ein Windowsbatch mit dem Namen `runme.bat` auf einem Linuxsystem erstellt wurde. Um zu schauen was es damit aufsich hat, begutachteten wir den Inhalt des Skriptes mittels `vim`. Das Skript gibt via `echo` den String dieses Flags aus. Außerdem fanden wir dieses Flag auf dem FTP Server auf dem Rechner `192.26.175.38` in der Datei `/follow/the/white/rabbit/runme.bat`

flg58594831dfbe63560f940365d517fa68 Zum finden dieses Flags haben wir mit Wireshark im Capture Mode einfach alle Packete im Netzwerk abgefangen. Dabei fiel dieses Flag in einen UDP Packet vom Rechner 192.26.175.36 zum Rechner 192.26.175.63 auf.

flg8e7fa2f4b3e3390175badcc38141bd1f Auf dem Rechner `192.26.175.35` läuft ein FTP-Server. Beim Durchsuchen der Inhalte fiel eine Datei auf, in der der Benutzer Bernd dazu aufgefordert wurde ein Passwort für sein MySQL Account zu setzen. Da auf demselben Rechner ein MySQL Server lief, loggten wir uns als Benutzer `bernd` auf diesem MySQL Server ein. In der Datenbank `bernd` fanden wir die Tabelle `hier_gibts_aktuelle_flags`. Ein `select * from hier_gibts_aktuelle_flags;` brachte das obengenannte Flag zu Tage.

flg0607547c0d12497a21ab8a0b53dd5bed Auf dem Rechner `192.26.175.35` läuft auch ein HTTP-Server. Beim Aufrufen der URL `http://192.26.175.35` fanden wir im HTML-Quelltext der angezeigten Website dieses Flag. Es war im Webbrowser nicht zu sehen, da es auskommentiert wurde im HTML Quellcode.

flgd0d1741e939d8fc51e0dae50ff39bed4 Beim Scannen des Rechners `192.26.175.35` mit dem nmap Kommando `nmap -T4 -A -v 192.26.175.35` viel als UFT8 Servername im Dienst Netatalk dieses Flag auf.

flg9fa80db0f34a75d1f474f29e8ed8f1ac In der SMB Freigabe `smb://arch/dontlookhere/` fanden wir das Bild `SMBFLAG.png`. Der Inhalt des Bildes enthielt die oben genannte Flag.

flgc905381d9e34b1efd02594423806e1d7 Beim Beobachten des Netzwerkverkehrs in Wireshark viel uns ein Packet von `192.26.175.38` nach `192.26.175.63` auf in dem stand `bernd@192.26.175.37` gefolgt von zwei Packeten die einen RSA Private Key enthielten. Nachdem wir uns mit dem Private Key per `ssh bernd@192.26.175.37` einloggten, erschien der Key auf der Kommandozeile.