```
msf auxiliary(vmware_server_dir_trav) > run
<snip>
[*] 10.8.28.127:8333 appears vulnerable to VMWare Directory Traversal
Vulnerability
<snip>
[*] Auxiliary-Module execution completed
```

Listing 7–59 *Anwendung des VMWare-Server-Directory-Traversal-Moduls*

Wenn, wie in unserem Testlabor, ein System mit dieser Schwachstelle erkannt wurde, ist es möglich, die darauf gehosteten Systeme herunterzuladen, und im Anschluss lassen sich diese offline einer detaillierten Analyse unterziehen. Dieser nächste Schritt könnte mit dem *Gueststealer* [193] erfolgen, einem Tool, um die virtualisierten Gastsysteme herunterzuladen.

Um Systeme mit dieser Schwachstelle in zukünftigen Sicherheitsanalysen immer zu erkennen, bietet sich dieses Modul für eine Integration in das Pre-Exploitation-Resource-Skript aus Abschnitt 6.2.1 an.

7.4 IPv6-Grundlagen [1]

Das weit verbreitete IPv4-Protokoll war nie für das Internet in der heutigen Form und Größe entwickelt worden. Aus diesem Grund bietet es nur knapp 4,3 Milliarden offizielle IP-Adressen, die aufgrund unterschiedlicher struktureller Gegebenheiten wie dem Subnetting und reservierter Adressbereiche nochmals verringert werden. Die vorhandenen Adressen sind mittlerweile so gut wie erschöpft und bieten dementsprechend nur mehr wenige bis gar keine Reserven. Diese Problematik wurde von der IETF bereits frühzeitig erkannt, wodurch diese im Jahr 1995 an dem Nachfolger von IPv4, an IPv6, zu arbeiten begann.

IPv6 ist eine komplette Neuentwicklung, läuft wie IPv4 auf OSI Layer 3 und lässt sich parallel zu IPv4 einsetzen.

OSI-Schicht	TCP/IP-Schicht	Beispiel
Anwendungen (7)	Anwendungen	HTTP, FTP, SMTP, POP, Telnet, OPC UA
Darstellung (6)		
Sitzung (5)		
		SOCKS
Transport (4)	Transport	TCP, UDP, SCTP
Vermittlung (3)	Internet	IP (IPv4, IPv6)
Sicherung (2)	Netzzugang	Ethernet, Token Bus, Token Ring, FDDI, IPoAC
Bitübertragung (1)		

Abb. 7–8 *TCP/IP-Referenzmodell [194]*

1. Dieser Abschnitt basiert auf einem Artikel in der Zeitschrift »Linux Magazin« der in Ausgabe 10/2012 veröffentlicht wurde: »Durch die Hintertür: Pentests spüren Sicherheitslücken in IPv6-Netzen auf«.

Es bietet Adressierungsmöglichkeiten für 340 Sextillionen Systeme und unterstützt neben Quality of Service auch Features wie Mobile-IP und zudem auch erweiterte automatische Konfigurationen der Netzwerkschnittstellen.

IPv6-Adressierung

IPv6-Adressen sind 128 Bit lang und werden hexadezimal dargestellt. Diese 128 Bit werden in 8 Blöcke zu je 16 Bit und mit Doppelpunkt unterteilt. Um IPv6-Adressen darzustellen, gibt es verschiedene Grundregeln und Vereinfachungen:

- Die Nullen, die einen Block starten, können ausgelassen werden. Das bedeutet, dass die Adresse `2001:0db8:0000:08d3:0000:8a2e:0070:7344` dieselbe Adresse darstellt wie die kurze Form `2001:db8:0:8d3:0:8a2e:70:7344`.
- Besteht ein ganzer Block aus Nullen oder sind mehrere Blocks mit Nullen aneinandergereiht, so müssen diese Blöcke nicht dargestellt werden. Diese Regel darf allerdings pro Adresse nur einmal angewendet werden. Ausgelassene Blöcke werden mit zwei aufeinander folgenden Doppelpunkten gekennzeichnet. Die Adresse `2001:0db8:0:0:0:0:1428:57ab` stellt dieselbe dar wie die Adresse `2001:db8::1428: 57ab`.
- Speziell bei der Einbettung von IPv4 in IPv6-Adressen ist folgende Regel durchaus hilfreich. Die letzten vier Bytes einer Adresse dürfen in dezimaler Schreibweise dargestellt werden. Dementsprechend bedeutet die Adresse `::ffff:127.0.0.1` dasselbe wie `::ffff:7f00:1`.

  Wurde einem Netzwerkgerät folgende IPv6-Adresse vergeben [194]:

  `2001:0db8:85a3:08d3:1319:8a2e:0370:7347/64`,

  lässt sich diese mit der /64-Netzwerkmaske in den Netzwerkbereich und Hostbereich unterteilen.

  `2001:0db8:85a3:08d3::/64`

  Folgender Bereich der Adresse stellt den Identifier des Netzwerkinterface dar:

  `1319:8a2e:0370:7347`

Bei IPv6 gibt es folgende unterschiedliche Adressen:

- Link Local Unicast (fe80::/10, Nicht routbar)
- Unique Local Unicast (für interne Netze)
  - fc00::/8 (evtl. Vergabe durch »ULA-Central«)
  - fd00::/8 (Präfix zufällig generieren!)
- Global Unicast (2000::/3, Offizielle Internet-Adressen)
- Multicast
- Deprecated (Site Local Unicast)

Es ist zu beachten, dass Services ausschließlich auf IPv6 oder auf IPv4 aktiviert sein können. Bei vielen Firewallsystemen muss IPv6 dabei dediziert konfiguriert werden. Wird dies nicht berücksichtigt, bedeutet das im schlimmsten Fall, dass ohne Berücksichtigung von IPv6 mögliches Angriffspotenzial und entsprechende Schwachstellen nicht erkannt und damit ein falsches Bedrohungspotenzial ermittelt würde.

7.4.1 Konfigurationsgrundlagen

Aktuelle Betriebssysteme kommen meist mit aktiviertem IPv6-Protokoll. Ein einfacher Test lässt sich mit dem `ifconfig-` oder dem `ip`-Kommando durchführen. Die Ausgabe der Interface-Konfiguration sollte mindestens einen `inet6`-Eintrag aufweisen.

Hinweis: Gibt es im internen Netzwerk einen IPv6-fähigen Router, ist es möglich, dass neben der Link-Local-Adresse auch bereits eine Link-Global-Adresse verfügbar ist (siehe Listing 7–61).

```
root@bt:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0c:29:7c:e7:6a
          inet addr:192.168.11.138  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe7c:e76a/64 Scope:Link
<snip>

root@bt:~# ip -6 addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qlen 1000
    inet6 fe80::20c:29ff:fecf:6aba/64 scope link
       valid_lft forever preferred_lft forever
```

Listing 7–60 *Interface-Konfiguration mit IPv6 aktiviert*

Der Scope ist bezüglich des Routings wichtig. *Scope Link* bedeutet, dass die Adresse nur im lokalen Subnetz Bedeutung hat und nicht über Router bzw. Netzwerkgrenzen hinweg weitergeleitet wird und dementsprechend auch keine Kommunikation über Router ermöglicht.

Gibt es im lokalen Netzwerk einen IPv6-fähigen Router, könnte sich eine Ausgabe von `ifconfig` folgendermaßen darstellen:

```
inet6 addr: 2001:4dd0:fd42:3:20c:29ff:fe7c:e76a/64 Scope:Global**
inet6 addr: fd44:2011:1021:0:20c:29ff:fe7c:e76a/64 Scope:Global**
inet6 addr: fe80::20c:29ff:fe7c:e76a/64 Scope:Link**
```

Listing 7–61 *Interface-Konfiguration mit globaler Adresse – Scope:Global*

Weist das lokale Interface eine IPv6-Adresse auf, lässt sich bereits ein erster Ping-Test auf das *locale Loopback Interface* durchführen.

```
root@bt:~# ping6 ::1 -c1
PING ::1(::1) 56 data bytes
64 bytes from ::1: icmp_seq=1 ttl=255 time=0.052 ms

--- ::1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.052/0.052/0.052/0.000 ms
```

Listing 7–62 *Ping-Kommando auf lokales IPv6 Loopback Interface*

Um alle Systeme im lokalen Subnetz (link local) zu ermitteln, lässt sich ein Ping an die Broadcast-Adresse `ff02::1` senden. Alle Systeme im lokalen Netzwerk antworten auf dieses Paket, wodurch es möglich ist, eine erste Systemübersicht zu erstellen.

```
root@bt:~# ping6 ff02::1%2 | cut -d\  -f4
fe80::20c:29ff:fecf:6aba:
fe80::20c:29ff:fe5c:e4b6:
<snip>
fe80::20c:29ff:fe85:c24b:
fe80::20c:29ff:fe5c:e4b6:
```

Listing 7–63 *Ping auf IPv6 Broadcast-Adresse*

7.5 IPv6-Netzwerke analysieren

Mittlerweile sind viele bekannte Analysetools IPv6-fähig. Neben Metasploit lässt sich beispielsweise auch Nessus und Nmap zur Analyse von IPv6-Netzwerken einsetzen. Folgender Abschnitt stellt eine beispielhafte Analyse von IPv6-Netzwerken dar. Es werden dabei keine speziellen Angriffe gegen diese Netzwerkumgebungen umgesetzt. Vielmehr wird versucht, bereits bekannte Techniken und Schwachstellen in IPv6-Umgebungen einzusetzen. Im ersten Schritt wird versucht, die Systeme im lokalen Netzwerk zu ermitteln, um sie in weiterer Folge auf Schwachstellen zu analysieren.

Folgendes Listing stellt den Einsatz von `alive6` des THC-IPv6-Toolkits dar.

```
root@kalilinux:~# alive6 eth0
Warning: unprefered IPv6 address had to be selected
Alive: fe80::20c:29ff:feec:1a8d
Alive: fe80::20c:29ff:fed9:71ca
<snip>
Found 19 systems alive
```

Listing 7–64 *THC-IPv6-Attack-Toolkit im Einsatz*