PEARSON IT CERTIFICATION

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CEH

Certified Ethical Hacker

MICHAEL GREGG
OMAR SANTOS

Special Offer

TIP Before you can understand how to exploit email protocol vulnerabilities (such as SMTP-based vulnerabilities), you must familiarize yourself with the standard TCP ports used in the different email protocols. The following TCP ports are used in the most common email protocols:

- **TCP port 25:** The default port used in SMTP for nonencrypted communications.
- **TCP port 465:** The port registered by the Internet Assigned Numbers Authority (IANA) for SMTP over SSL (SMTPS). SMTPS has been deprecated in favor of STARTTLS.
- **TCP port 587:** The Secure SMTP (SSMTP) protocol for encrypted communications, as defined in RFC 2487, using STARTTLS. Mail user agents (MUAs) use TCP port 587 for email submission. STARTTLS can also be used over TCP port 25 in some implementations.
- **TCP port 110:** The default port used by the POP3 protocol in nonencrypted communications.
- **TCP port 995:** The default port used by the POP3 protocol in encrypted communications.
- **TCP port 143:** The default port used by the IMAP protocol in nonencrypted communications.
- **TCP port 993:** The default port used by the IMAP protocol in encrypted (SSL/TLS) communications.

SMTP open relay is the term used for an email server that accepts and relays (that is, sends) emails from any user. It is possible to abuse these configurations to send spoofed emails, spam, phishing, and other email-related scams. Nmap has an NSE script to test for open relay configurations. The details about the script are available at https://svn.nmap.org/nmap/scripts/smtp-open-relay.nse. Example 4-13 shows how you can use the script against an email server (10.1.2.14).

Example 4-13 Testing for Open Relay Configurations on an Email Server

```
# nmap --script smtp-open-relay.nse 10.1.2.14
Starting Nmap 7.80 ( https://nmap.org )
Nmap scan report for 10.1.2.14
Host is up (0.00022s latency).
PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-open-relay: Server is an open relay (16/16 tests)
Nmap done: 1 IP address (1 host up) scanned in 6.82 seconds
```

Several SMTP commands can be useful when performing a security evaluation of an email server. The following are a few examples:

- **HELO:** Used to initiate an SMTP conversation with an email server. The command is followed by an IP address or domain name (for example, HELO 10.1.2.14).
- **EHLO:** Used to initiate a conversation with an Extended SMTP (ESMTP) server. This command is used in the same way as the HELO command.
- **STARTTLS:** Used to start a Transport Layer Security (TLS) connection to an email server.
- **RCPT:** Used to denote the email address of the recipient.
- **DATA:** Used to initiate the transfer of the contents of an email message.
- **RSET:** Used to reset (cancel) an email transaction.
- **MAIL:** Used to denote the email address of the sender.
- **QUIT:** Used to close a connection.
- **HELP:** Used to display a help menu (if available).
- **AUTH:** Used to authenticate a client to the server.
- **VRFY:** Used to verify whether a user's email mailbox exists.
- **EXPN:** Used to request, or expand, a mailing list on the remote server.

Let's look at an example of how you can use some of these commands to reveal email addresses that may exist in the email server. In this case, you connect to the email server by using telnet followed by port 25. (In this example the SMTP server is using plaintext communication over TCP port 25.) Then you use the **VRFY** (verify) command with the email username to verify whether the user account exists on the system, as demonstrated in Example 4-14.

Example 4-14 Fishing for Email Addresses

```
telnet 192.168.78.8 25
Trying 192.168.78.8...
Connected to 192.168.78.8.
Escape character is '^]'.
220 dionysus.theartofhacking.org ESMTP Postfix (Ubuntu)
VRFY sys
252 2.0.0 sys
```

```
VRFY admin
550 5.1.1 <admin>: Recipient address rejected: User unknown in local
recipient table
VRFY root
252 2.0.0 root
VRFY omar
252 2.0.0 omar
```

The **smtp-user-enum** tool (installed by default in Kali Linux) enables you to automate these information-gathering steps. Example 4-15 shows the **smtp-user-enum** options and examples of how to use the tool.

Example 4-15 smtp-user-enum Options and Usage

```
#smtp-user-enum
smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

Usage: smtp-user-enum [options] ( -u username | -U file-of-usernames )
( -t host | -T file-of-targets )

options are:
        -m n     Maximum number of processes (default: 5)
        -M mode  Method to use for username guessing EXPN, VRFY or
RCPT (default: VRFY)
        -u user  Check if user exists on remote system
        -f addr  MAIL FROM email address.  Used only in "RCPT TO"
mode (default: user@example.com)
        -D dom   Domain to append to supplied user list to make
email addresses (Default: none)
                 Use this option when you want to guess valid email
addresses instead of just usernames e.g. "-D example.com" would
guess foo@example.com, bar@example.com, etc.  Instead of simply the
usernames foo and bar.
        -U file  File of usernames to check via smtp service
        -t host  Server host running smtp service
        -T file  File of hostnames running the smtp service
        -p port  TCP port on which smtp service runs (default: 25)
        -d       Debugging output
        -t n     Wait a maximum of n seconds for reply (default: 5)
        -v       Verbose
        -h       This help message
```

```
Also see smtp-user-enum-user-docs.pdf from the smtp-user-enum tar
ball.

Examples:

$ smtp-user-enum -M VRFY -U users.txt -t 10.0.0.1
$ smtp-user-enum -M EXPN -u admin1 -t 10.0.0.1
$ smtp-user-enum -M RCPT -U users.txt -T mail-server-ips.txt
$ smtp-user-enum -M EXPN -D example.com -U users.txt -t 10.0.0.1
```

Example 4-16 shows how to use the **smtp-user-enum** command to verify whether the user **omar** exists in the server.

Example 4-16 Verifying a User with **smtp-user-enum**

```
# smtp-user-enum -M VRFY -u omar -t 192.168.78.8
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-
user-enum )

 ----------------------------------------------------------
|                    Scan Information                      |
 ----------------------------------------------------------
Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Sat Apr 21 19:34:42 #########
192.168.78.8: omar exists
######## Scan completed at Sat Apr 21 19:34:42 #########
1 results.

1 queries in 1 seconds (1.0 queries / sec)
```

Most modern email servers disable the **VRFY** and **EXPN** commands. It is highly recommended that you disable these SMTP commands. Modern firewalls also help protect and block any attempts at SMTP connections using these commands.

Additional Enumeration Techniques

Any service can be enumerated. As an example, searching for the components of IPsec can determine whether those services are being used. IPsec uses Encapsulated Security Payload (ESP) and Authenticated Header (AH). A scan for port 500 can indicate whether a VPN gateway is present.

Voice over IP (VoIP) uses a set of specific ports. VoIP's main use of the Session Initiation Protocol (SIP) uses ports 2000, 2001, 5050, and 5061. A scan for these ports can be used to determine whether VoIP is being used. After ports are identified, an attacker might launch a distributed denial-of-service (DDoS) attack, launch a spoofing attack, or even attempt to eavesdrop.

Table 4-4 lists additional enumeration techniques and tools for other common protocols.

Key Topic

Table 4-4 Enumeration Techniques for Other Common Protocols

Protocol	Tool or Command
IPsec and the Internet Key Exchange (IKE) protocol	You can use the **ike-scan** tool to enumerate and discover devices configured for IPsec/IKE. You can download ike-scan from the following GitHub repository: https://github.com/royhills/ike-scan. The documentation can be accessed at https://royhills.co.uk/wiki/index.php/Ike-scan_Documentation.
FTP	You can enumerate a server that is running FTP by using the basic Linux and Windows **ftp** command or by using tools like Nmap with NSE scripts like ftp-anon.nse, ftp-bounce.nse, ftp-brute.nse, ftp-libopie.nse, ftp-proftpd-backdoor.nse, ftp-syst.nse, ftp-vsftpd-backdoor.nse, and ftp-vuln-cve2010-4221.nse.
TFTP	You can use the Nmap NSE script tftp-enum.nse to enumerate TFTP implementations.
BGP	BGP is the protocol that most Internet service providers use to route traffic on the Internet. BGP leverages autonomous system numbers (ASNs) for different operations. IANA assigns AS numbers to different organizations. You can enumerate ASNs by using the Whois tool or by using websites such as the BGP toolkit from Hurricane Electric at https://bgp.he.net.

DNS Enumeration

Domain Name System (DNS) enumeration is the process of locating all information about DNS. This can include identifying internal and external DNS servers; performing lookups of DNS records for information such as usernames, computer names, and IP addresses of potential target systems; and performing zone transfers. Much of this activity was demonstrated in Chapter 3, "Footprinting,

Reconnaissance, and Scanning." The most straightforward way is to use Nslookup or attempt a DNS zone transfer to copy the entire zone file for the domain from the DNS server.

One of the unique attributes of Microsoft Windows is that when a client can't resolve a hostname using DNS, it will resort to the Link-Local Multicast Name Resolution (LLMNR) protocol. LLMNR is used to resolve both IPv4 and IPv6 addresses. If LLMNR fails, NetBIOS will be used. NetBIOS functions in a similar way as LLMNR; the big difference between the two is NetBIOS works over IPv4 only.

When LLMNR or NetBIOS are used to resolve a request, any host on the network who knows the IP of the host being asked about can reply. Even if a host replies to one of these requests with incorrect information, it will still be regarded as legitimate. What this means is that the service can be spoofed. A number of attack tools have been developed that will reply to all these queries in the hope of receiving sensitive information. The primary defense against these two attacks is to disable these services.

Enumeration Countermeasures

Table 4-5 includes a few security best practices that can help you protect your systems from being easily enumerated by attackers.

Key Topic

Table 4-5 Enumeration Countermeasures

Protocol	Countermeasure
DNS	You should disable DNS zone transfers to untrusted hosts.
	Ensure that internal hosts and their IP addresses are not published into DNS zone files of public DNS servers.
	Leverage DNS registration services that hide sensitive information.
	Use generic network administrative contacts when registering a domain to avoid social engineering attacks.
SNMP	Use SNMPv3 instead of earlier versions or use NETCONF or RESTCONF in network infrastructure devices (which are a more secure alternative to SNMP).
	Implement the Group Policy security option called "Additional restrictions for anonymous connections."
	Ensure that the access to null session pipes, null session shares, and IPsec filtering is restricted.