

* Identification – 确认身份 username
* Authenticity –密码 password
* Authorization –用户权限
* Access Control
* Accountability
* Non-repudiation –不阻止活动的发生

**The CIA Triad**

1. Confidentiality

方法：authentication/access controls/authorization; cryptography/encryption

Surface web

Deep web

Dark web: onion network only accessible via Tor

Lab-Tor

**apt-get -y install tor**

“Date & Time Settings”: Turn “Automatic Date & Time” and “Automatic Time Zone” to the ON position •Change the “Time Format” to AM/PM

**tor &**

Hit Enter

**curl** [**http://ipecho.net/plain**](http://ipecho.net/plain)

**torsockscurl** [**http://ipecho.net/plain**](http://ipecho.net/plain)

Option 1: Set Firefox Proxy to localhost and port 9050 under SOCKS Host with option SOCKS v5

Option 2: torsockswith Firefox

**Torsocksfirefox**

check.torproject.org

browse to the 0Day Forum: qzbkwswfv5k2oj5d.onion

****

Close Tor:

•ps–ef

•**kill 14410** or whatever your PID listed is for tor

1. Integrity

Integrity Lab:

Find tor directory:

**which tor**

chech tor’s current hash:

**md5sum /usr/sbin/tor**

copy tor to the /root directory:

**cp/usr/sbin/tor .**

**md5sum ./tor**

make another copy and check the hash again:

**cptor tor2**

**md5sum ./tor ./tor2**

change one bit of the tor2 file:

**printf“\x01” | ddof=tor2 bs=1 seek=0x100 count=1 conv=notrunc**

compare the hash of the two file again:

**md5sum ./tor ./tor2**

find where the files differ:

**cmp–b tor tor2**

find the original hash:

**cat /var/lib/dpkg/info/tor.md5sums**

check current binaries against the stored values n dpkg/info:

**apt-get –y install debsums**

**debsums tor**

1. Availability

**Inside Threats**

Phishing email: (check)

* Email headers (bottom, top)
* Verify sender IP
* Correct domain

**Outside Threats**

**Common 5 Phases of an Attack**

1.Reconnaissance

2.Scanning

3.Gaining Access

4.Maintaining Access

5.Covering Tracks

SANS Security Incident Handling Phases:

1.Preparation

2.Identification

3.Containment

4.Eradication

5.Recovery

6.Lessons Learned

Recent Popular Security Threats

•Heartbleed : OpenSSL

Check if vulnerable for SSL:

**dpkg–l | grepopenssl**

**更正或弥补：**

1.Upgrade version of OpenSSL to 1.0.1g or above

apt-get update

apt-get install openssl

2.Take server offline

3.Generate new private/public keys

Submit new public keys to certificate authority

Install new certificate on server

Ensure old key pairs are no longer being used

4.Bring server online

5.Revoke old certificates

6.Force password changes for users on server

7.Invalidate session keys

•Shellshock: GNU Bash shell

1.Update repos

apt-get update

2.Upgrade bash

apt-get install --only-upgrade bash

•POODLE

•GHOST: glibc library

•GHOST.ctool to test for vulnerability:

**Wget https://webshare.uchicago.edu/orgs/ITServices/itsec/Downloads/GHOST.c**

**cat GHOST.c**

**gcc GHOST.c –o GHOST**

**./GHOST**

1.Update repos

apt-get update

2.Upgrade bash

apt-get install --only-upgrade libc6

•Freak

•BEAST