IT Scripting and Automation

Monitoring Security on *Unix Systems

Lecturer: Art Ó Coileáin

Cybersecurity

- A general definition of cybersecurity: it is the body of
  - technologies,
  - processes and
  - Practices

  designed to protect networks, computers, programs and data from attack, damage or unauthorized access.
- Elements of cybersecurity are:
  - Application security
  - Information security
  - Network security
  - Disaster recovery/business continuity planning
  - End-user education.
- Even a system is not 100% secure, you can work to make your system somewhat more resistant to attack.

Cybersecurity (2)

- Unix is optimised for convenience and doesn´t make security easy or natural. The system’s philosophy stress easy manipulation of data in a networked, multiuser environment.

- The software that runs on Unix systems is developed by a large community of programmers. They range in experience level, attention to detail, and knowledge of the system and its interdependencies. As a result, even the most well-intended new features can introduce large security holes.

- Most administrative functions are implemented outside the kernel, where they can be inspected and tampered with.

- The more secure your system, the more constrained you and your users will be.

How security is compromised

- Social Engineering
  - The human users (including administrators) of a system are the weakest links in the chain of security.
  - Users with good intentions are easily convinced to give away sensitive information.
  - No amount of technology can protect against the user element.
  - Ensure that your community has a high awareness of security threats so that they can be part of the defence.
  - “Phishing” describes the attempts to collect information from users through deceptive email, instant messages, or even SMS messages.
  - Social engineering continues to be a powerful hacking technique and is one of the most difficult threats to neutralise.
  - Regular organisation-wide communications are an effective way to provide security information.

How security is compromised (2)

- Software vulnerabilities
  - Over the years, countless security-sapping bugs have been discovered in computer software (including commercial and free software)
  - By exploiting subtle programming errors or context dependencies hacker have been able to manipulate systems
  - Buffer overflows are common programming error and one with complex implications. Buffer overflows are a subcategory of a larger class of software security bugs known as validation vulnerabilities.
- Configuration errors
  - Unfortunately from the system administrator point of view, software is developed to be useful instead of annoying, not-so-securely is often default.
  - A typical example of a host configuration vulnerability is the standard practice of allowing Linux systems to boot without requiring a boot loader password.

Security tips and Philosophy

- Patches
  - A regular schedule for installing routine patches that is diligently followed
  - A change plan that documents the impact of each set of patches, outlines appropriate post-installation testing steps, and describe how to back out the changes in the event of problems
  - An understanding of what patches are relevant to the environment
- Unnecessary services
  - Most systems come with several services configured to run by default. Be sure to disable (or remove) any that are unnecessary, especially if they are network daemons
  - Use: **$ netstat -an | grep LISTEN** to see which services are running
  - The security risk inherent in some network protocols render them unsafe in almost all circumstances. FTP, Telnet, and the BSD “r” programs (rcp, rlogin and rsh)

Security tips and Philosophy

- Remote event logging
  - Syslog facility forward log information to files, list of users, or other hosts on your network. Consider setting up a secure host to act as a central logging machine that parses forwarded events and takes appropriate action.
- Backups
  - Regular backups are essential part of any site security plan.
- Viruses and worms
  - Unix and Linux **have been** mostly immune from viruses. Only a handful exist and none have done the costly damage that has become commonplace in the Windows world.
  - **ClamAV** by Tomasz Kojmis a popular, free antivirus product for UNIX and Linux. This widely used GPL tool is a complete antivirus toolkit with signatures for thousands of viruses.

Security tips and Philosophy

- Rootkits
  - The craftiest hackers try to cover their tracks and avoid detection.
  - Rootkits are programs and patches that hide important system information such as process, disk or network activity
  - Intrusion detection software - **OSSEC** is an effective way to monitor systems for the presence of rootkits
  - There are also rootkit finder scripts such as **chkrootkit**, chkrootkit.org
- Packet filtering
  - If you are connecting a system to a network that has Internet access, you must install a packet-filtering router or firewall between the system and the outside world
- Passwords
  - Every account must have a password and it needs to be something that can’t easily guessed.

Security Tips and Philosophy

- Vigilance
  - You must monitor your system’s health, network connections, process table, and overall status regularly

Passwords and Users Accounts

- Password aging
  - Most systems that have shadow passwords also allow you to compel users to change their passwords periodically, a facility known as password aging
- On Linux, the **chage** command controls password aging. Using chage, administrators can enforce minimum and maximum times between password changes, password expiration dates, the number of days to warn users before their passwords expire, the number of days of inactivity that are permissible before accounts are automatically locked, and more.
- The following command sets the minimum number of days between password changes to 2, the maximum number to 90, the expiration date to July 31, 2018, and warns the user for 14 days that the expiration date is approaching:
- **$ sudo chage -m 2 -M 90 -E 2018-07-31 -W 14 ben**

Passwords and Users Accounts

- Group logins and shared logins
  - Any login that is used by more than one person is bad news.
  - Group logins (*guest, demo*) are sure terrain for hackers
- User shells
  - The use of shells other than standards such as **bash** and **tcsh** is a dangerous practice
- Root Logins
  - Do not allow root to log in remotely, even through the standard root account. OpenSSH, you can set the *PermitRootLogin* configuration option to '**No**' in the **/etc/ssh/sshd_config** file to enforce this restriction
- PAM "Pluggable Authentication Modules"
  - It sets the right level of security for authentication. PAM can authenticate all sorts of activities: user logins, other forms of system access, user protected web sites, applications, etc.

Setuid Programs

- Programs that run **setuid**, especially ones that run **setuid** to root, are prone to security problems.

  The setuid commands distributed with the system are theoretically secure; however, security holes have been discovered in the past and will be discovered in the future.

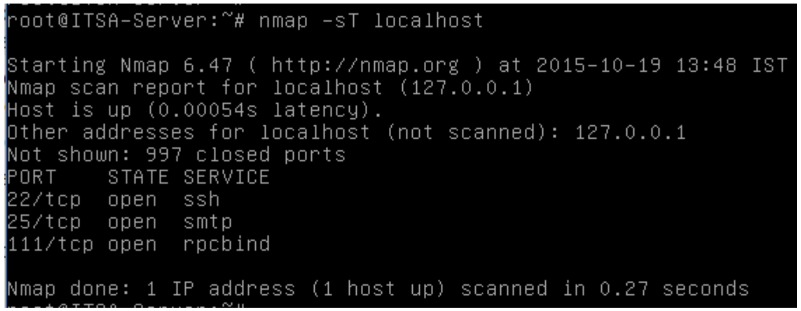
- It is possible disable **setuid** and **setgid** execution on individual filesystems by specifying the **nosuid** option to **mount**.

- It is useful to scan your disks periodically to look for new setuid programs. A hacker who has breached the security of your system sometimes creates a private setuid shell or utility to facilitate repeat visits. One-liner script can be used:

- **$ find / -user root -perm -4000 -print**

Security Power Tools

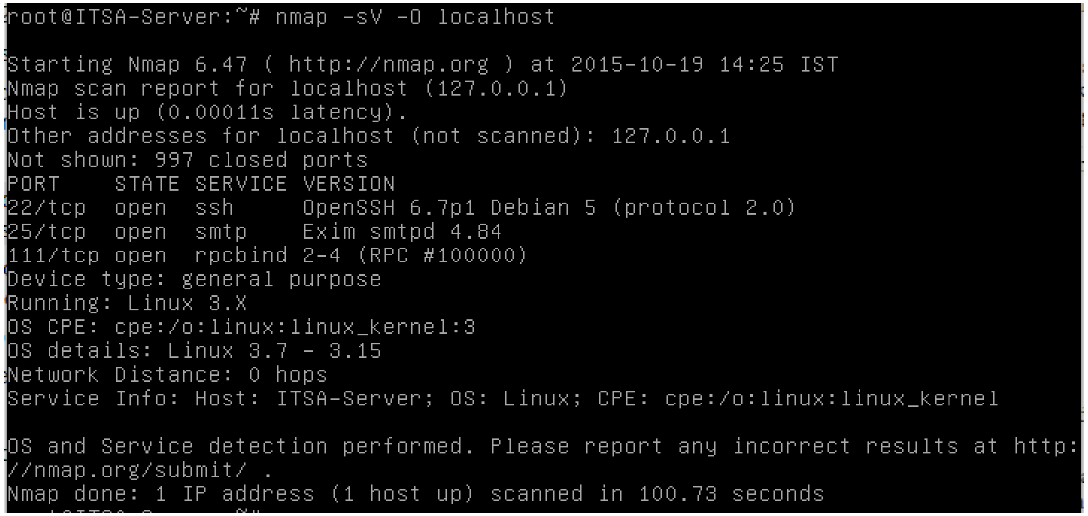
- **nmap**: network port scanner
  - Its main function is to check a set of target hosts to see which TCP and UDP ports have servers listening on them.
  - Nmap is a great way to find out what a system looks like to someone on the outside who is trying to break in.
- **$ nmap -sT *hostname/ip_address***
- **$ nmap -sV -O *hostname/ip_address***



```
root@ITSA-Server:~# nmap -sT localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2015-10-19 13:48 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00054s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
111/tcp open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```



```
root@ITSA-Server:~# nmap -sV -O localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2015-10-19 14:25 IST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 997 closed ports
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
25/tcp  open  smtp    Exim smtpd 4.84
111/tcp open  rpcbind 2-4 (RPC #100000)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.15
Network Distance: 0 hops
Service Info: Host: ITSA-Server; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 100.73 seconds
```

Security Power Tools

- Nessus: next-generation network scanner. It is a powerful and useful software vulnerability scanner.
  - http://www.tenable.com/blog/auditing-open-ports-with-nessus?gclid=CNvrmtzTzsgCFeSD2wodBl4IeQ
- John the ripper -Finder of insecure passwords: a way of prevent poor passwords choices is to ty to break the passwords yourself and to force users to change passwords that you have broken.
  - http://www.openwall.com/john/
- Hosts_access: host access control
  - Network firewalls are a first line of defence against access by unauthorised hosts, but they shouldn't be the only barrier in place. Two files, **/etc/host.allow** and **/etc/hosts.deny**, also referred to as TCP wrappers, can restrict access to services according to the origin of network requests.

Security Power Tools

- Zeek (formerly Bro): the programmable network intrusion detection system
  - It is an open source network intrusion detection system (NIDS) that monitors network traffic and looks for suspicious activity.
  - It inspects all traffic flowing into and out of a network
  - https://www.zeek.org/
- Snort: a popular NIDS
  - It is an open source network intrusion prevention and detection system.
  - Snort is distributed for free as an open source package; however, Sourcefire (a commercial entity) charges a subscription fee for access to the most recent set of detection rules.
  - https://www.snort.org/
- OSSEC: host-based intrusion detection
  - http://www.ossec.net/

Cryptographic Security Tools

- Kerberos system attempts to address some of the issues of network security in a consistent and extensible way. Kerberos is an authentication system, a facility that “guarantees” that users and services are in fact who they claim to be.
  - http://web.mit.edu/kerberos/
- PGP:Pretty Good Privacy –It focuses on email security, it encrypts data, to generate signatures, and to verify the origin of files and messages.
- SSH: the secure shell -it is a secure replacement for rlogin, rcp and telnet. It uses cryptographic authentication to confirm a user’s identity and encrypts all communication between the two hosts.
  - http://www.openssh.com/

Cryptographic Security Tools

- Stunnel is an open source package that encrypts arbitrary TCP connections, much in the manner of SSH. It uses SSL to create end-to-end tunnels through which it passes data to and from an unencrypted service (telnet, IMAP, POP).
  - https://www.stunnel.org/index.html

Firewalls/VPNs

- The firewall is one of the basic tools of network security.

  It is a device or piece of software that prevents unwanted packets from accessing networks and systems.

- A packet-filtering firewalls limits the types of traffic that can pass through your Internet gateway.

- Packet-filtering software is included in Linux systems in the form of **iptables**, in some Unix as **genfilt**.

- Virtual Private Network (VPNs) is a connection that makes a remote network appear as if it is directly connected, even if it is physically thousands of miles and many router hops away.

Sources of Security Information

- CERT: a registered service mark of Carnegie Mellon University
- **C**omputer **E**mergency **R**esponse **T**eam acts as clearing house for computer security information. Good contact point for security information.
  - forms.us-cert.gov/maillists
- The National Cyber Security Centre (NCSC)
  - https://www.ncsc.gov.ie/
- SecurityFocus.com and BugTraqmail list
  - http://www.securityfocus.com/ -It specialises in security-related news and information.
  - The BugTraqlist is a moderated forum for the discussion of security vulnerabilities and their fixes.

Sources of Security Information

- Schneieron Security
  - Source of information about computer security and cryptography
  - https://www.schneier.com/
- SANS: the System Administration, Networking, and Security Institute
  - SANS is a professional organisation that sponsors security-related conferences and training programs, as well as publishing a variety of security information.
  - https://www.sans.org/
- Vendor-specific security resources

What to do when your site has been attacked?

- Do not panic !
  - It is very likely that by the time you discover the intrusion, most of the damage has already been done.
- Decide on an appropriate level of response
  - No one benefits from an over-hyped security incident. Proceed calmly
- Collect all available tracking information
  - Check accounting files and logs. Try to determine where the original breach occurred.
- Asses you degree of exposure
  - Determine what crucial information has 'left' the company, and devise an appropriate, mitigation strategy.
- Pull the plug
  - If necessary and appropriate, disconnect compromised machines from the network

What to do when your site has been attacked?

- Device a recovery plan
  - Draw up a recovery plan on nearby whiteboard
- Communicate the recovery plan
  - Educate users and management about the effects of the break-in, the potential for future problems, and your preliminary recovery strategy.
- Implement the recovery plan
  - Follow your plan and instincts. Speak with colleagues at a similar institution.
- Report the incident to authorities
  - If the incident involved outside parties, report the matter to CERT.