Ubuntu Security Hardening

Pete
Herefordshire Linux User Group
August 2017

Topics

- Threats
- Intrusion Analysis – Hands on
- CLI
- Security Principles
- Ubuntu Hardening - Points
- References

Notes

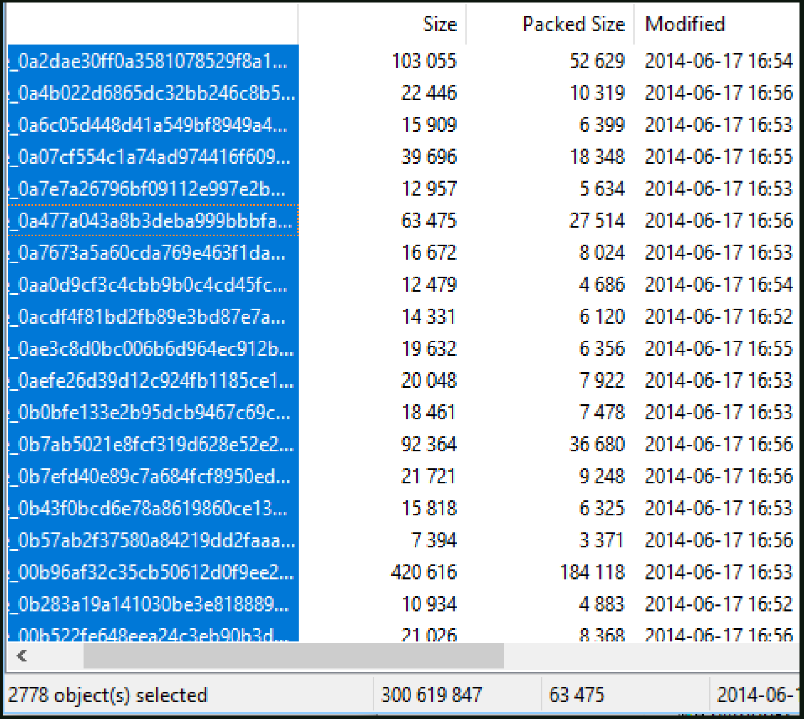
- Using Ubuntu 16.04 LTS
- Warning – Danger ahead
- Use at own risk
- VM is a standalone Linux installation
- I’m not liable for any damage!

Threats – Why Care?

- Malware – varying forms
  - General; a nuisance
  - Change settings to destructive behavior
  - Encrypt
  - Trojans/Worms
- Intrusions
  - Remote access
  - C2
  - Exfil
- Accidental

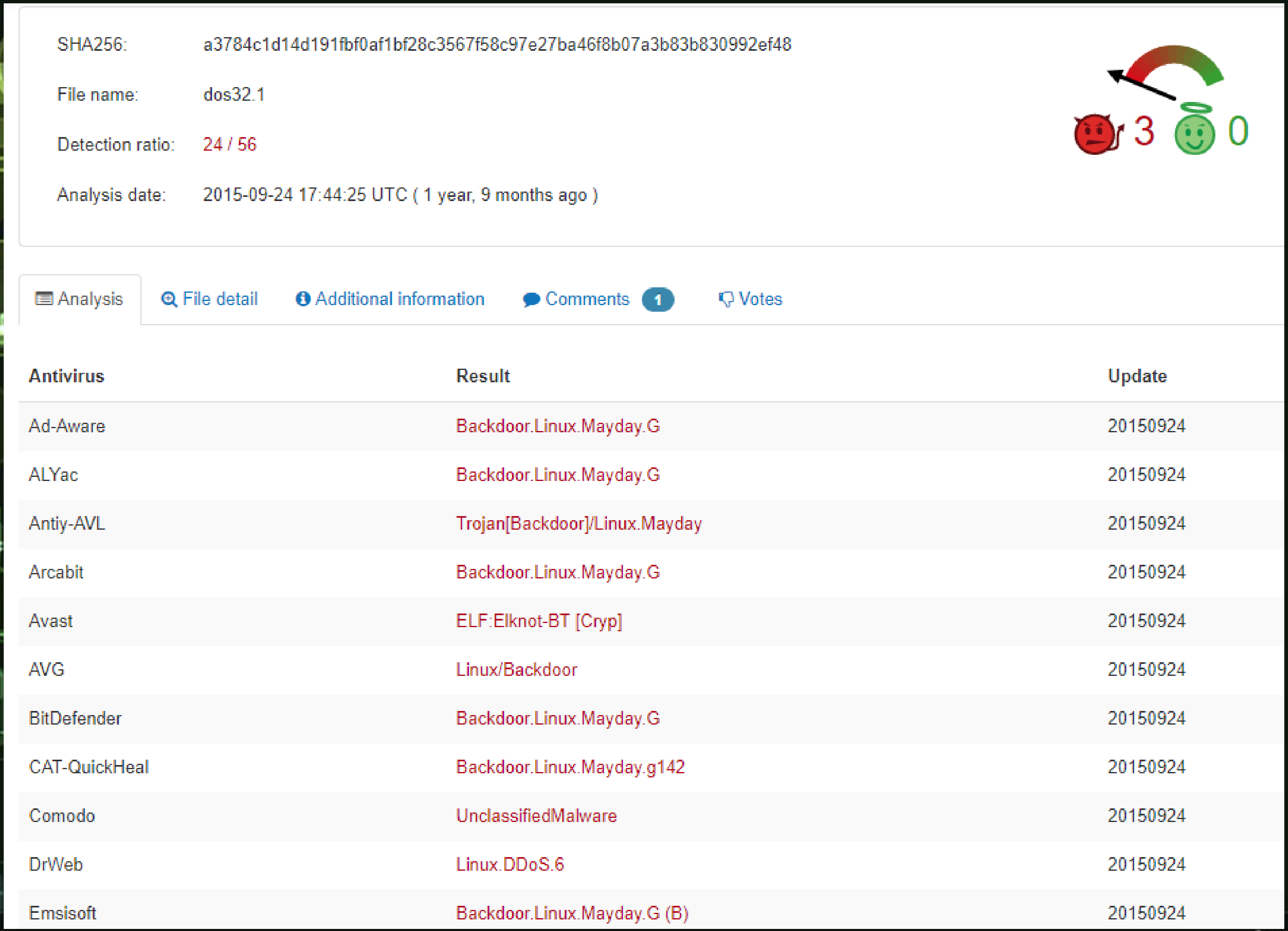
Linux Malware Samples

- Linux isn't immune to malware
- Example malware collection: 2778 samples.



	Size	Packed Size	Modified
_0a2dae30ff0a3581078529f8a1...	103 055	52 629	2014-06-17 16:54
_0a4b022d6865dc32bb246c8b5...	22 446	10 319	2014-06-17 16:56
_0a6c05d448d41a549bf8949a4...	15 909	6 399	2014-06-17 16:53
_0a07cf554c1a74ad974416f609...	39 696	18 348	2014-06-17 16:55
_0a7e7a26796bf09112e997e2b...	12 957	5 634	2014-06-17 16:53
_0a477a043a8b3deba999bbbfa...	63 475	27 514	2014-06-17 16:56
_0a7673a5a60cda769e463f1da...	16 672	8 024	2014-06-17 16:53
_0aa0d9cf3c4cbb9b0c4cd45fc...	12 479	4 686	2014-06-17 16:54
_0acdf4f81bd2fb89e3bd87e7a...	14 331	6 120	2014-06-17 16:52
_0ae3c8d0bc006b6d964ec912b...	19 632	6 356	2014-06-17 16:55
_0aefe26d39d12c924fb1185ce1...	20 048	7 922	2014-06-17 16:53
_0b0bfe133e2b95dcb9467c69c...	18 461	7 478	2014-06-17 16:53
_0b7ab5021e8fcf319d628e52e2...	92 364	36 680	2014-06-17 16:56
_0b7efd40e89c7a684fcf8950ed...	21 721	9 248	2014-06-17 16:56
_0b43f0bcd6e78a8619860ce13...	15 818	6 325	2014-06-17 16:53
_0b57ab2f37580a84219dd2faaa...	7 394	3 371	2014-06-17 16:56
_00b96af32c35cb50612d0f9ee2...	420 616	184 118	2014-06-17 16:53
_0b283a19a141030be3e818889...	10 934	4 883	2014-06-17 16:52
_00b522fe648eea24c3eb90b3d...	21 026	8 368	2014-06-17 16:56
2778 object(s) selected	300 619 847	63 475	2014-06-

Linux Malware



SHA256: a3784c1d14d191fbf0af1bf28c3567f58c97e27ba46f8b07a3b83b830992ef48

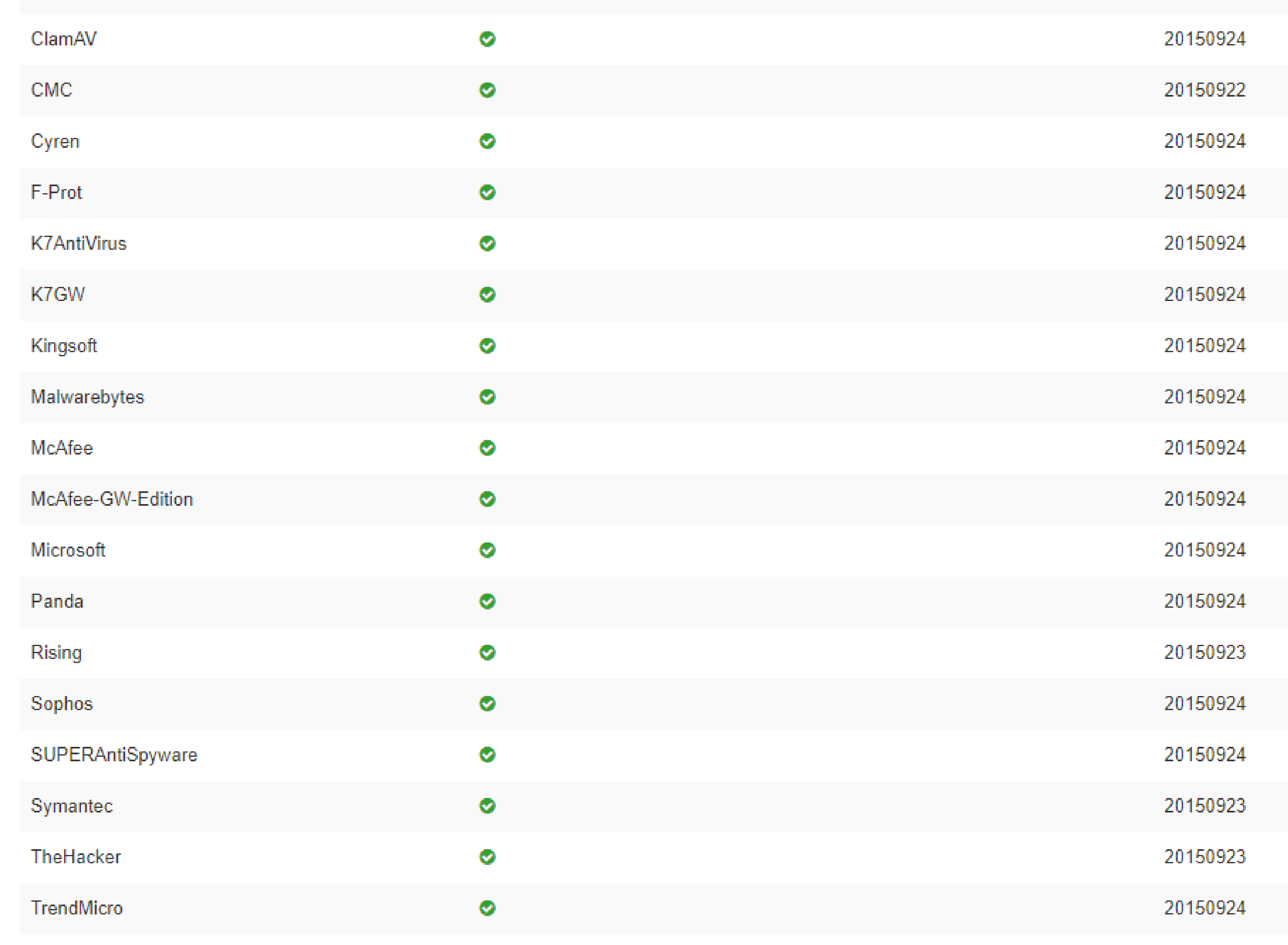
File name: dos32.1

Detection ratio: 24 / 56

Analysis date: 2015-09-24 17:44:25 UTC (1 year, 9 months ago)

Antivirus	Result	Update
Ad-Aware	Backdoor.Linux.Mayday.G	20150924
ALYac	Backdoor.Linux.Mayday.G	20150924
Antiy-AVL	Trojan[Backdoor]/Linux.Mayday	20150924
Arcabit	Backdoor.Linux.Mayday.G	20150924
Avast	ELF:Elknot-BT [Cryp]	20150924
AVG	Linux/Backdoor	20150924
BitDefender	Backdoor.Linux.Mayday.G	20150924
CAT-QuickHeal	Backdoor.Linux.Mayday.g142	20150924
Comodo	UnclassifiedMalware	20150924
DrWeb	Linux.DDoS.6	20150924
Emsisoft	Backdoor.Linux.Mayday.G (B)	20150924

Linux Malware



ClamAV	✓	20150924
CMC	✓	20150922
Cyren	✓	20150924
F-Prot	✓	20150924
K7AntiVirus	✓	20150924
K7GW	✓	20150924
Kingsoft	✓	20150924
Malwarebytes	✓	20150924
McAfee	✓	20150924
McAfee-GW-Edition	✓	20150924
Microsoft	✓	20150924
Panda	✓	20150924
Rising	✓	20150923
Sophos	✓	20150924
SUPERAntiSpyware	✓	20150924
Symantec	✓	20150923
TheHacker	✓	20150923
TrendMicro	✓	20150924

VM Image

- Compromised – covert attack
- What has the attacker done?
- Hints
  - Accounts?
  - Programs running?
  - Configuration changes?
- Password is: password123

Ideal World

- Forensics would snapshot HDD
- Use a write-blocker – Chain of custody

- In this case, a VM. Use the snapshot
  - Preserves integrity of the image – rollback
- Lets get started

Scenario

- Scenario:
  - – Suspect VM has been compromised
- Attackers interested in:
  - – Files – sensitive i.e. banking, blackmail, ransom
  - – Compute resources – use your computer to attack other victims – no attribution to attacker. Part of mining, botnet etc
  - – Fun - destructive

Scenario Pt 2

- No AV installed
- No backup to recover
- Need to discover what has been compromised
- Focus on accounts, system changes, networking

Challenges

- History is a good starting point
- Provides a transcript of user actions
- history
- the pitfalls of intrusion analysis
- ---
- booby traps
- alias check for self destruct
- --
- check logs
- cat /var/log/syslog
- can do this via the GUI - type in log
- ---------------------------------------

Challenges

- any network ports open?

- listening (netcat)
- crontab -e

- netstat -tulpn
- lsof -i | grep LISTEN
- ps aux | grep 2384

- https://www.cyberciti.biz/faq/what-process-has-open-linux-port/

Challenges

- --
- what services/apps running
- ---
- who is logged in?
- who or w
- whoami
- --
- user accounts
- less /etc/passwd | more
- less /etc/group | more

Challenges

- --
- what has 'baduser' been up to?

- sudo more /home/baduser/.bash_history

- not always good to login, maybe booby trapped
- inspect files - act with caution.. check with file command
- What is the name of the zip in the Documents folder belonging to user? What happens when you extract the files? (password is 42)

Challenges

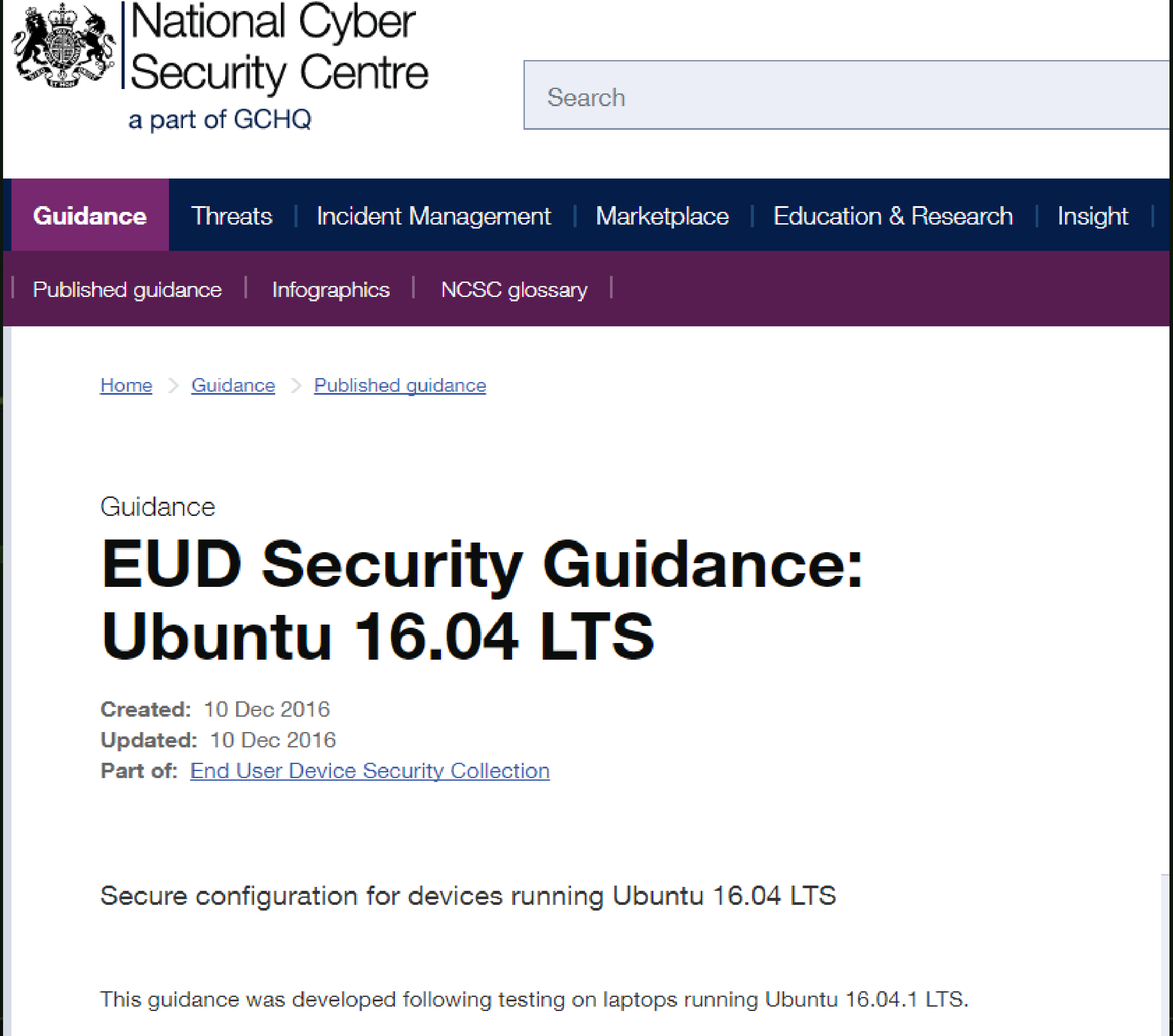
- ---
- modifid hosts
- /etc/hosts
- What does this file do? What would have happened? could be man in the middle perhaps?
- --

Linux Commands

- Hostname
- Whoami
- Logname
- Id
- Ifconfig
- Uptime
- Uname –a
- Printenv
- Sa
- Sar
- Who
- Netstat –anp
- Ss
- Netstat –nr
- Arp –a
- Ps aux
- Ps –ef
- top

- Hostname
- Whoami
- Logname
- Id
- Ifconfig
- Uptime
- Uname –a
- Printenv
- Sa
- Sar
- Who
- Netstat –anp
- Ss
- Netstat –nr
- Arp –a
- Ps aux
- Ps –ef
- top

Ubuntu Hardening



National Cyber Security Centre
a part of GCHQ
Search
Guidance | Threats | Incident Management | Marketplace | Education & Research | Insight
Published guidance | Infographics | NCSC glossary

Home > Guidance > Published guidance

Guidance

EUD Security Guidance: Ubuntu 16.04 LTS

Created: 10 Dec 2016
Updated: 10 Dec 2016
Part of: End User Device Security Collection

Secure configuration for devices running Ubuntu 16.04 LTS

This guidance was developed following testing on laptops running Ubuntu 16.04.1 LTS.

Security Principles

- Patch OS
  - – Sudo apt….
- Update signatures
- Limit applications, services
- Least privilege
- Backup

References

- CIS Benchmark - https://www.cisecurity.org/cis-benchmarks/
- NCSC - https://www.ncsc.gov.uk/guidance
- 42.zip - http://www.unforgettable.dk/
- AIDE - https://help.ubuntu.com/community/FileIntegrityAIDE
- Linux Bastille - http://bastille-linux.sourceforge.net/

Now For Something Completely Different

- Warning !
- Fork Bomb
- :(){ :|: & };: