



DoD

Cybersecurity

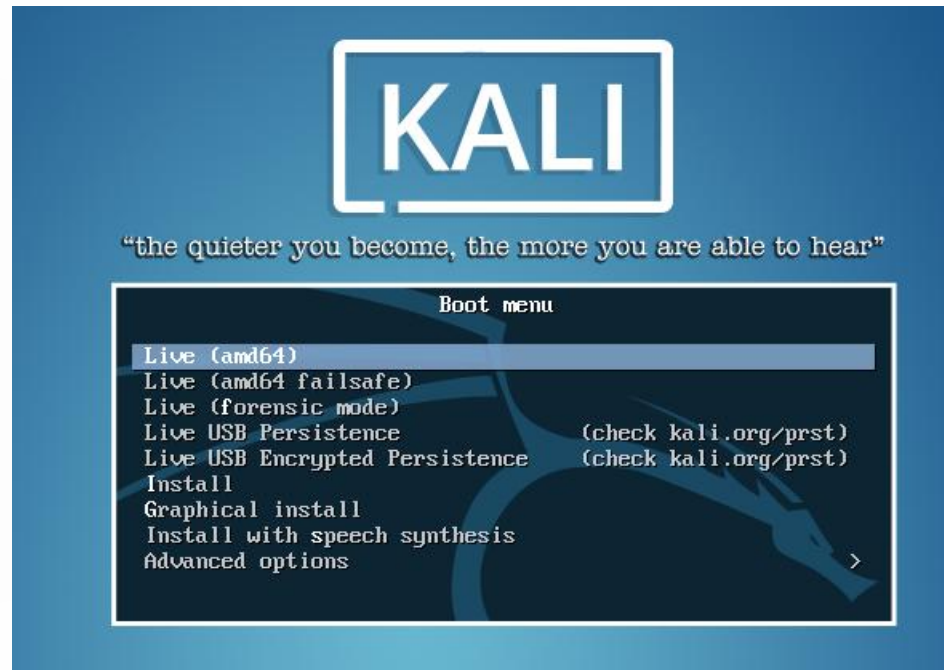
LESSON 6 KALI LINUX



KALI

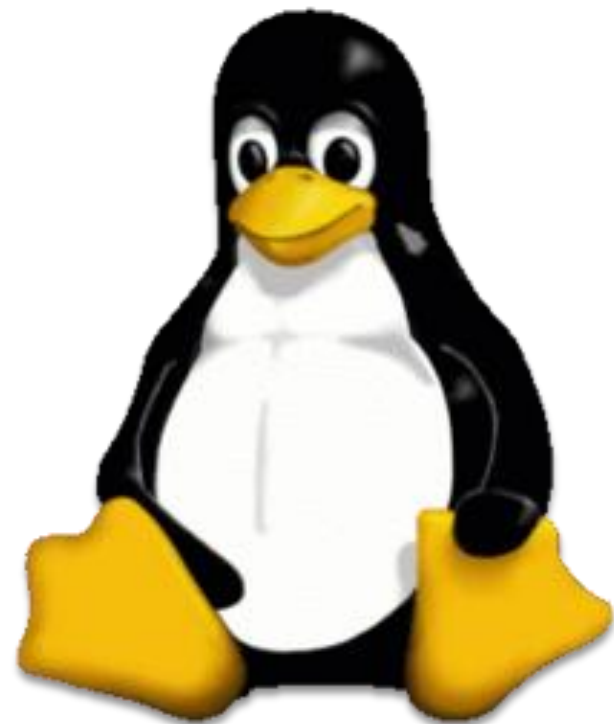
Linux

- ▶ Many hacking tools like BackTrack/Kali depend on a knowledge of Linux
- ▶ So we have a basic introduction to Linux
- ▶ You need to be at least basically comfortable with Linux in order to utilize many hacking tools.



History of Linux

- ▶ In 1987 a man named Andrew S. Tanenbaum created Minix, an operating system quite similar to Unix. Minix was a fairly stable and functional and reasonably good Unix clone.
- ▶ The story of the Linux operating system, starts with young computer science graduate student named Linus Torvalds. Linus was introduced to Minix and, while still in graduate school, decided to create his own open-source Unix clone. Linus found many things he liked about the Minix operating system, but he believed that he could make a better Unix variant. He chose the name Linux, as a combination of his first name, Linus, and the end of Unix, nix.
- ▶ Finally, Linus Torvalds released Linux 0.01 on the Internet under a GNU public license. Torvalds not only released the operating system for free, he released the source code, and even invited other programmers to lend a hand in making the system more workable



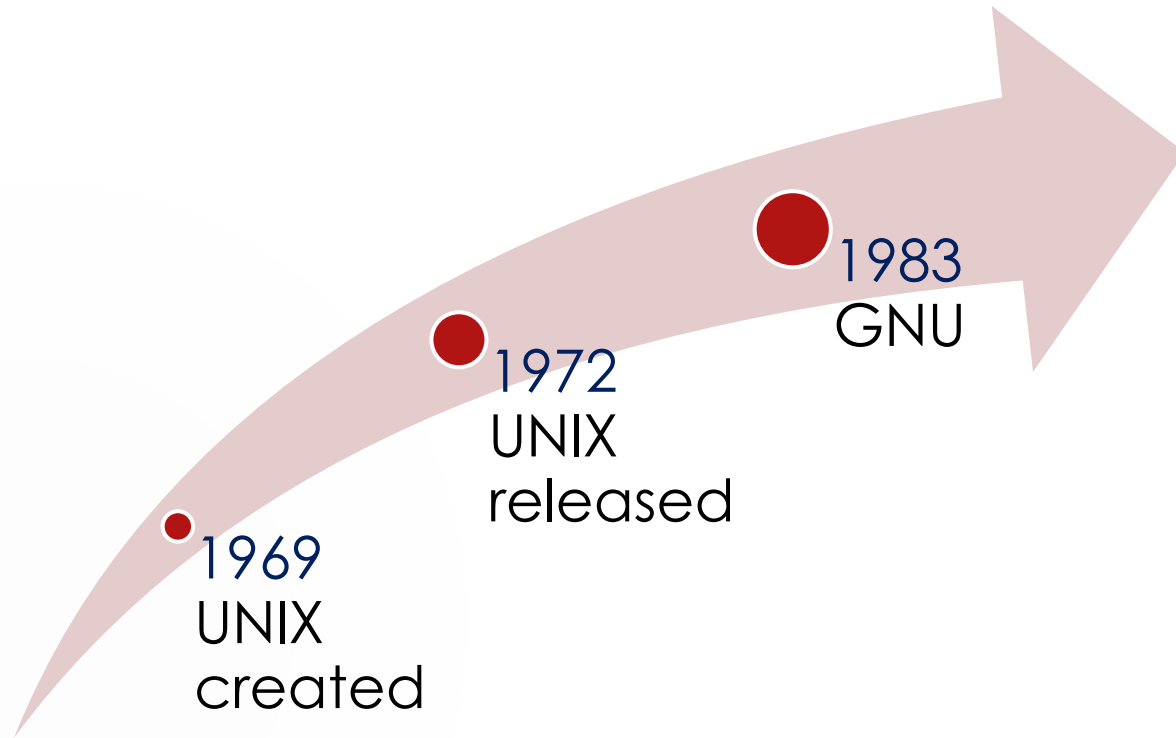
File System

EXT -The extended file system or ext was implemented in April 1992 as the first file system created specifically for the Linux operating system. It has metadata structure inspired by the traditional Unix File System (UFS) and was designed by Rémy Card to overcome certain limitations of the Minix file system

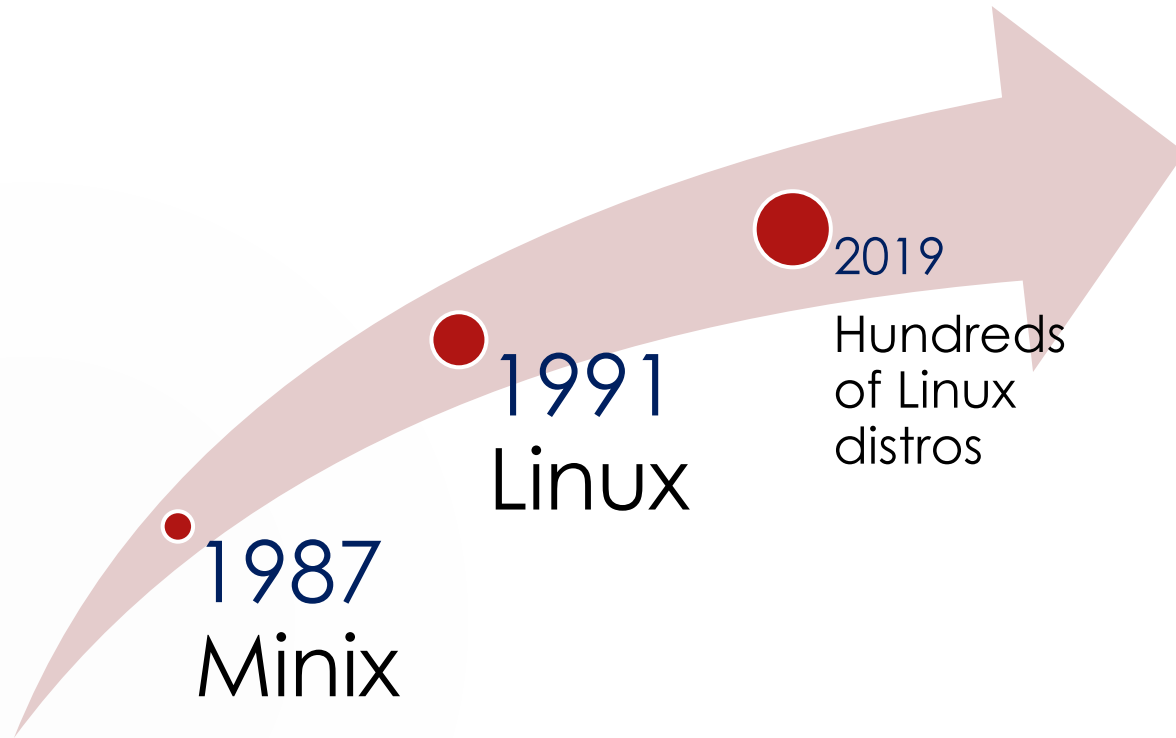
EXT 4 is current

Linux can also work with FAT

History of Linux



History of Linux (Cont.)



Linux Distributions



- ▶ **Mint:** Ubuntu based, multi-media support, also has a Debian editor
- ▶ **Debian:** Comes with a very large amount of software
- ▶ **Ubuntu:** Ubuntu Manifesto: that software should be available free of charge, that software tools should be usable by people in their local language and despite any disabilities, and that people should have the freedom to customize and alter their software in whatever way they see fit. "Ubuntu" is an ancient African word, meaning "humanity to others".
- ▶ **Fedora:** Red Hat desktop, comes with GHNOME. There are variations called 'Fedora Spins'
- ▶ **OpenSuse:** Widely used, has been around for quite some time.
- ▶ **Qubes OS:** Security focused
- ▶ <https://distrowatch.com/>

Linux Shells

Bourne shell (sh)

Bourne-again shell (Bash)

C shell (csh)

Korn shell (ksh)

Common Linux Shell Commands

LINUX COMMAND	EXPLANATION AND EXAMPLE
<code>ls</code>	The <code>ls</code> command lists the contents of the current directory. Example: <code>ls</code>
<code>cp</code>	The <code>cp</code> command copies one file to another directory. Example: <code>cp filename.txt directoryname</code>
<code>mkdir</code>	The <code>mkdir</code> command creates a new directory. Example: <code>mkdir directoryname</code>
<code>cd</code>	The <code>cd</code> command is used to change directories. Example: <code>cd directoryname</code>
<code>rm</code>	The <code>rm</code> command is used to delete or remove a file. Example: <code>rm filename</code>

Common Linux Shell Commands (Cont.)

`rmdir` The `rmdir` command is used to remove or delete entire directories.
Example: `rmdir directoryname`

`mv` The `mv` command is used to move a file.
Example: `mv myfile.txt myfolder`

`diff` The `diff` command performs a byte-by-byte comparison of two files and tells you what is different about them.
Example: `diff myfile.txt myfile2.txt`

`cmp` The `cmp` command performs a textual comparison of two files and tells you the difference between the two.
Example: `cmp myfile.txt myfile2.txt`

`>` This is the redirect command. Instead of displaying the output of a command like `ls` to the screen, it redirects it to a file.
Example: `ls > file1.txt`

Common Linux Shell Commands (Cont.)

<code>ps</code>	The <code>ps</code> command lists all currently running processes that the user has started. Any program or daemon is a process. Example: <code>ps</code>
<code>top</code>	The <code>top</code> command lists all currently running processes, whether the user started them or not. It also lists more detail on the processes. Example: <code>top</code>
<code>fsck</code>	This is a file system check. The <code>fsck</code> command can check to see whether a given partition is in good working condition. Example: <code>fsck /dev/hda1</code>
<code>fdisk</code>	The <code>fdisk</code> command lists the various partitions. Example: <code>fdisk-1</code>
<code>mount</code>	The <code>mount</code> command mounts a partition, allowing you to work with it. Example: <code>mount /dev/fd0/mnt/floppy</code>

Run Levels

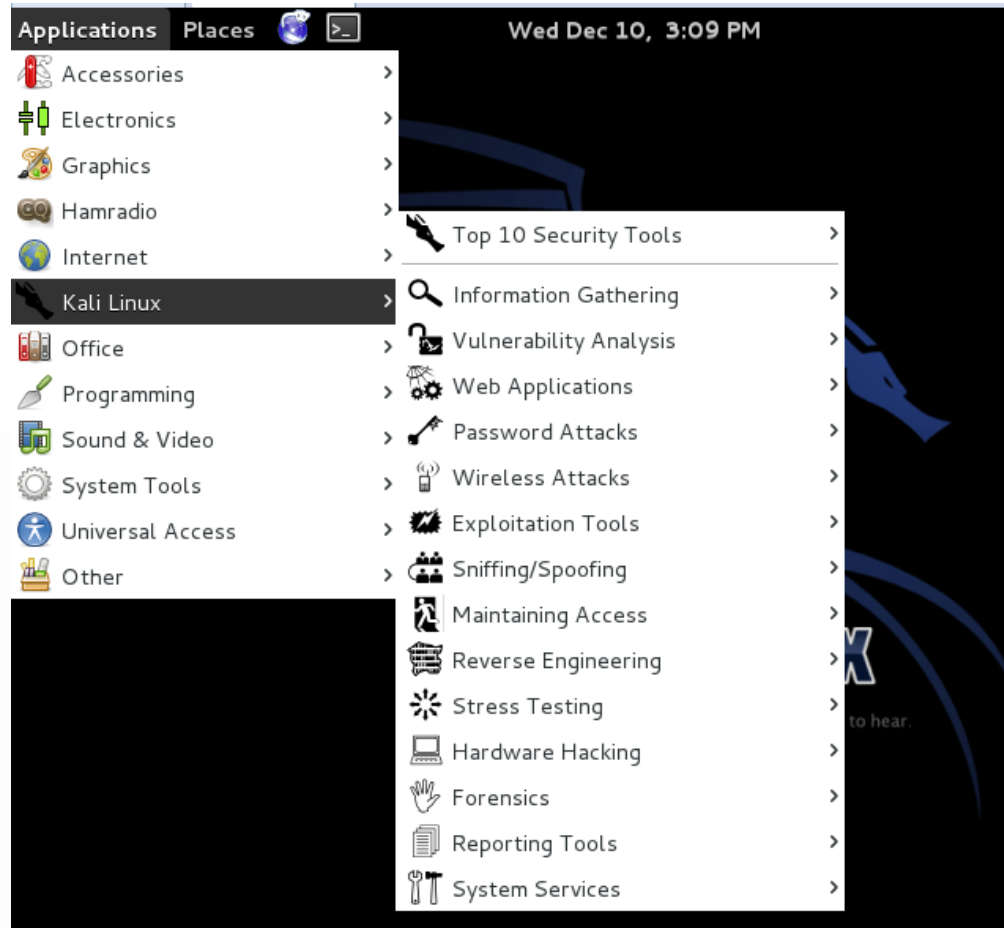


MODE	DIRECTORY	RUN LEVEL DESCRIPTION
0	/etc/rc.d/rc0.d	Halt
1	/etc/rc.d/rc1.d	Single-user mode
2	/etc/rc.d/rc2.d	Not used (user-definable)
3	/etc/rc.d/rc3.d	Full multiuser mode without GUI
4	/etc/rc.d/rc4.d	Not used (user-definable)
5	/etc/rc.d/rc5.d	Full multiuser mode with GUI
6	/etc/rc.d/rc6.d	Reboot

Kali

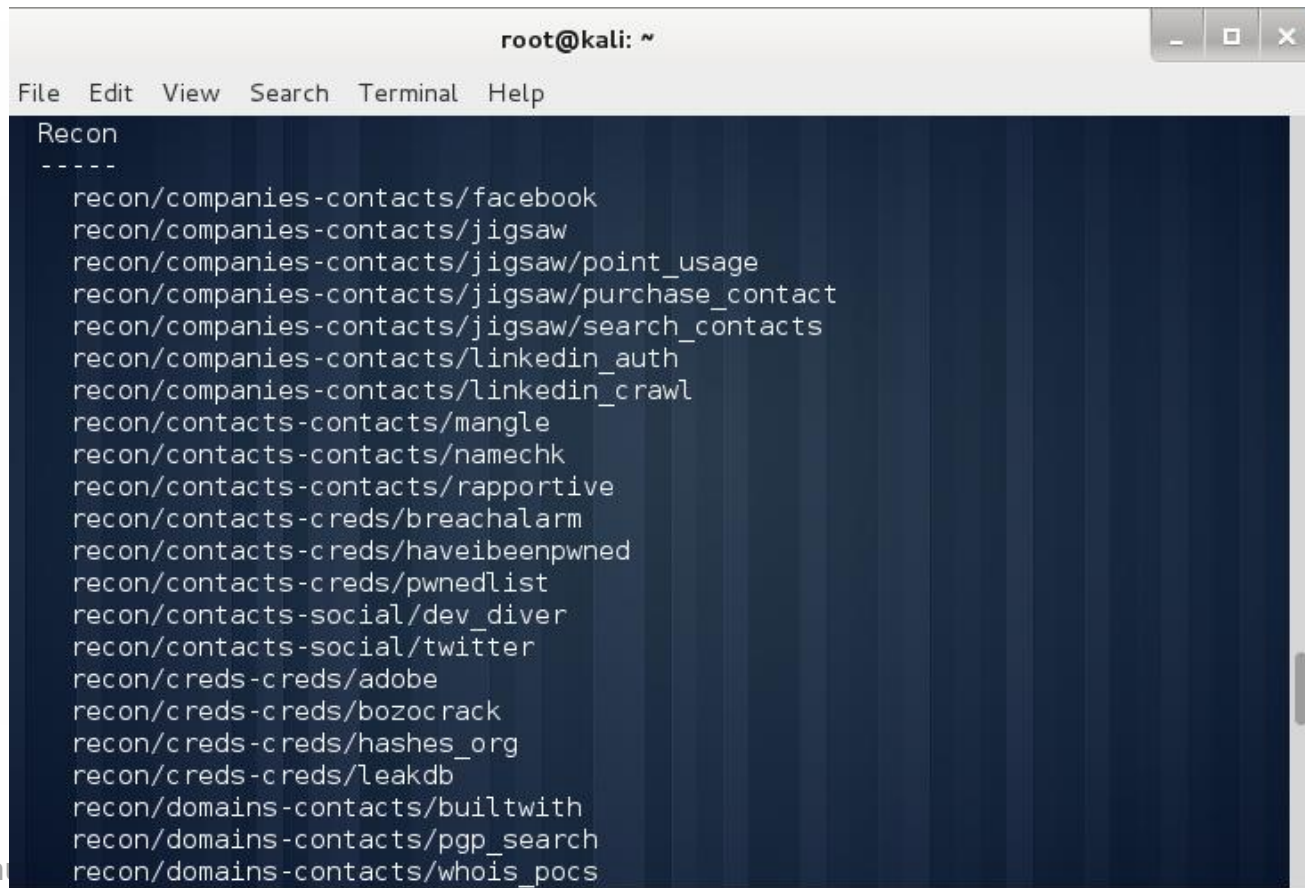
- ▶ The successor to Backtrack
- ▶ <https://www.kali.org/>
- ▶ It has a HUGE number of tools. A few are listed here
 - ▶ BBQSQL
 - ▶ Jsql
 - ▶ Reaver
 - ▶ Nmap
 - ▶ dnsenum
 - ▶ dnsrecon
 - ▶ sigguesser
 - ▶ cisco-orc

Using Kali Linux



Recon-ng

- ▶ Type show modules to see what modules are available.



```
root@kali: ~  
File Edit View Search Terminal Help  
Recon  
-----  
recon/companies-contacts/facebook  
recon/companies-contacts/jigsaw  
recon/companies-contacts/jigsaw/point_usage  
recon/companies-contacts/jigsaw/purchase_contact  
recon/companies-contacts/jigsaw/search_contacts  
recon/companies-contacts/linkedin_auth  
recon/companies-contacts/linkedin_crawl  
recon/contacts-contacts/mangle  
recon/contacts-contacts/namechk  
recon/contacts-contacts/rapportive  
recon/contacts-creds/breachalarm  
recon/contacts-creds/haveibeenpwned  
recon/contacts-creds/pwnedlist  
recon/contacts-social/dev_diver  
recon/contacts-social/twitter  
recon/creds-creds/adobe  
recon/creds-creds/bozocrack  
recon/creds-creds/hashe_org  
recon/creds-creds/leakdb  
recon/domains-contacts/builtwith  
recon/domains-contacts/pgp_search  
recon/domains-contacts/whois_pocs
```


Recon-ng

- ▶ To use a module type in use then the module

```
root@kali: ~  
File Edit View Search Terminal Help  
[recon-ng][default] > use recon/contacts-creds/haveibeenpwned  
[recon-ng][default][haveibeenpwned] >
```

- ▶ To see module options type show options

```
[recon-ng][default] > use recon/contacts-creds/haveibeenpwned  
[recon-ng][default][haveibeenpwned] > show options  
  
Name      Current Value  Req  Description  
-----  -  
SOURCE    default        yes  source of input (see 'show info' for details)  
  
[recon-ng][default][haveibeenpwned] >
```

Recon-ng

- ▶ To check to see if an email is compromised

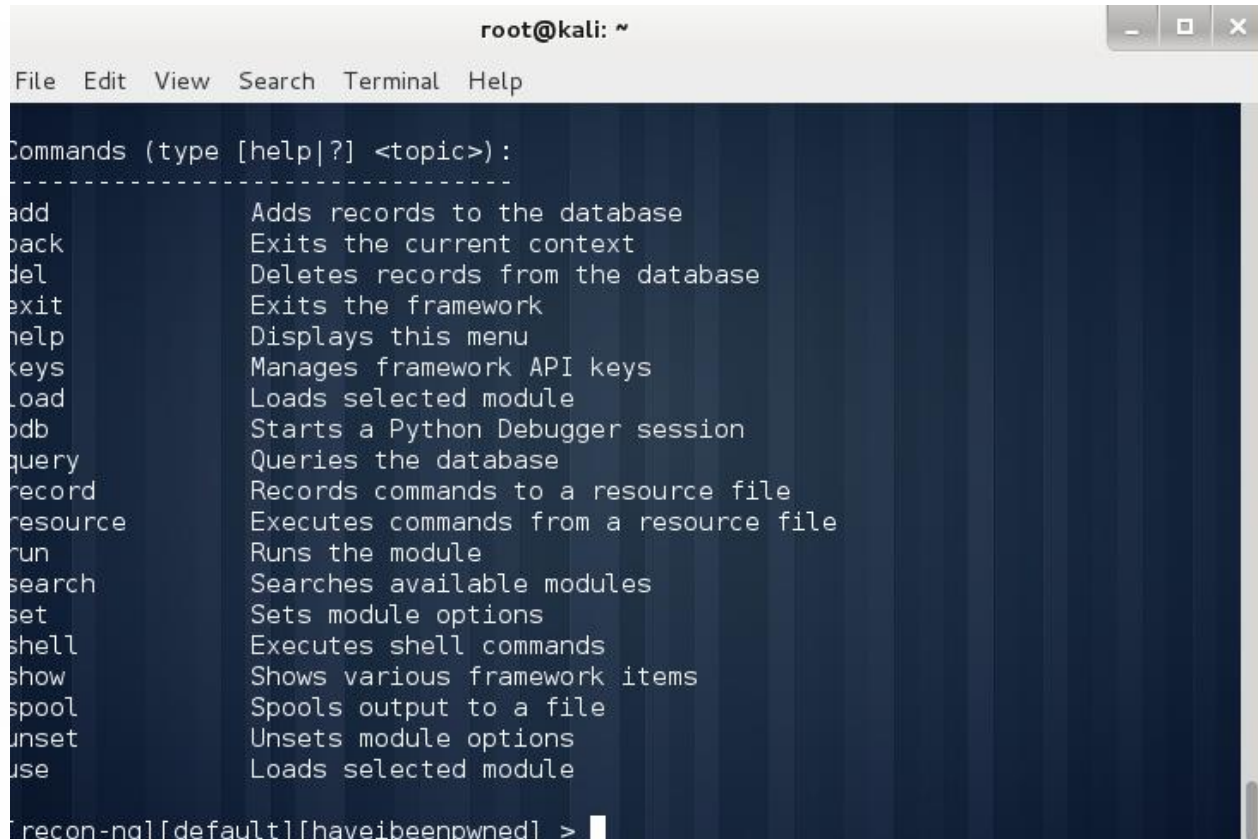
```
[recon-ng][default] > use recon/contacts-creds/haveibeenpwned
[recon-ng][default][haveibeenpwned] > show options

Name      Current Value  Req  Description
-----  -
SOURCE    default        yes  source of input (see 'show info' for details)

[recon-ng][default][haveibeenpwned] > set source chuck@chuckeasttom.com
SOURCE => chuck@chuckeasttom.com
[recon-ng][default][haveibeenpwned] > █
```

Recon-ng

- ▶ Use the help file to learn more



```
root@kali: ~  
File Edit View Search Terminal Help  
Commands (type [help|?] <topic>):  
-----  
add           Adds records to the database  
back          Exits the current context  
del           Deletes records from the database  
exit          Exits the framework  
help          Displays this menu  
keys          Manages framework API keys  
load          Loads selected module  
pdb           Starts a Python Debugger session  
query         Queries the database  
record        Records commands to a resource file  
resource      Executes commands from a resource file  
run           Runs the module  
search        Searches available modules  
set           Sets module options  
shell         Executes shell commands  
show          Shows various framework items  
spool         Spools output to a file  
unset         Unsets module options  
use           Loads selected module  
[recon-ng][default][haveibeenpwned] >
```

Recon-ng

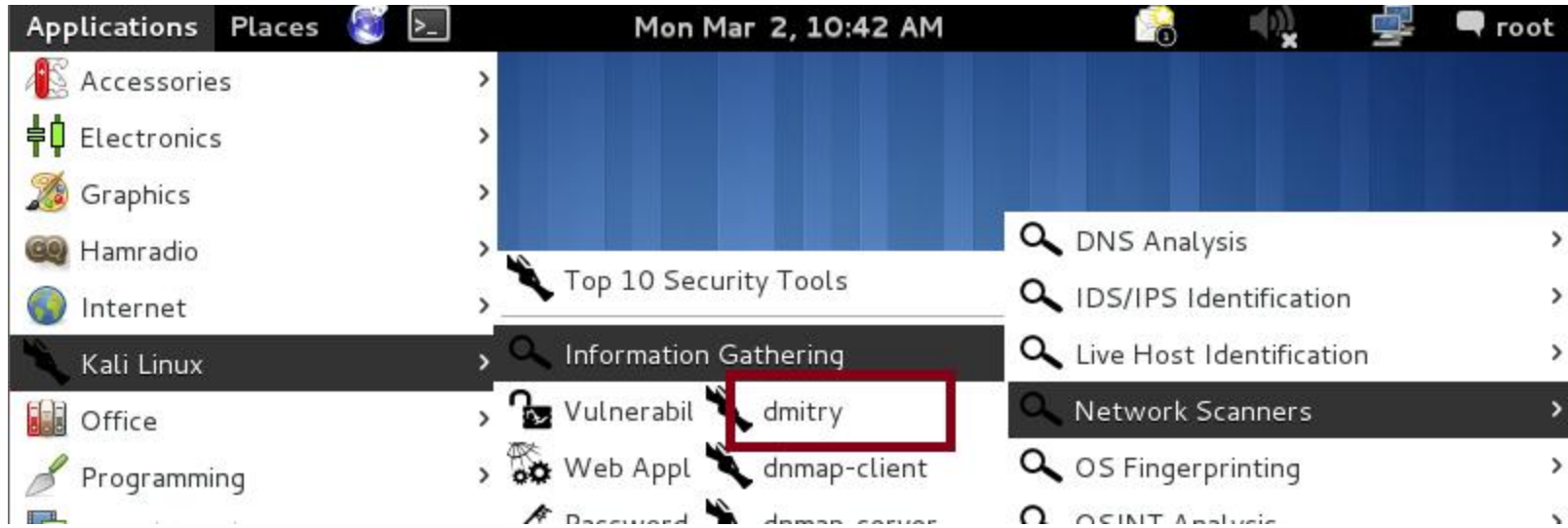
- ▶ Use the shodanhq api

```
[recon-ng][default][haveibeenpwned] > use shodan
[*] Multiple modules match 'shodan'.

Recon
-----
recon/domains-hosts/shodan_hostname
recon/locations-pushpins/shodan
recon/netblocks-hosts/shodan_net

[recon-ng][default][haveibeenpwned] > use recon/domains-hosts/shodan_hostname
[recon-ng][default][shodan_hostname] > |
```

dmitry



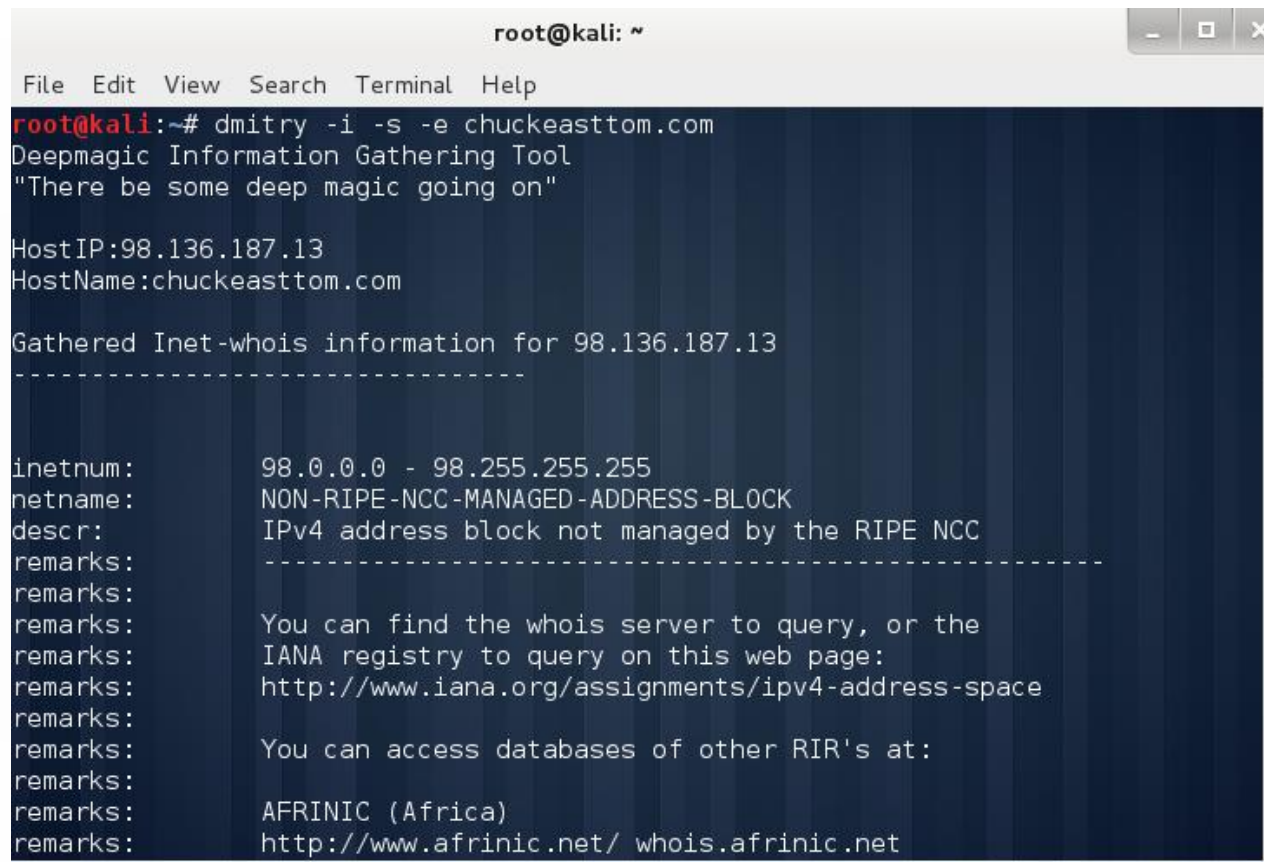
dmitry

```
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o      Save output to %host.txt or to file specified by -o file
  -i      Perform a whois lookup on the IP address of a host
  -w      Perform a whois lookup on the domain name of a host
  -n      Retrieve Netcraft.com information on a host
  -s      Perform a search for possible subdomains
  -e      Perform a search for possible email addresses
  -p      Perform a TCP port scan on a host
* -f      Perform a TCP port scan on a host showing output reporting filtered ports
* -b      Read in the banner received from the scanned port
* -t 0-9  Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@kali:~#
```


dmitry

- ▶ Dmitry -i -s -e www.chuckeasttom.com



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# dmitry -i -s -e chuckeasttom.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

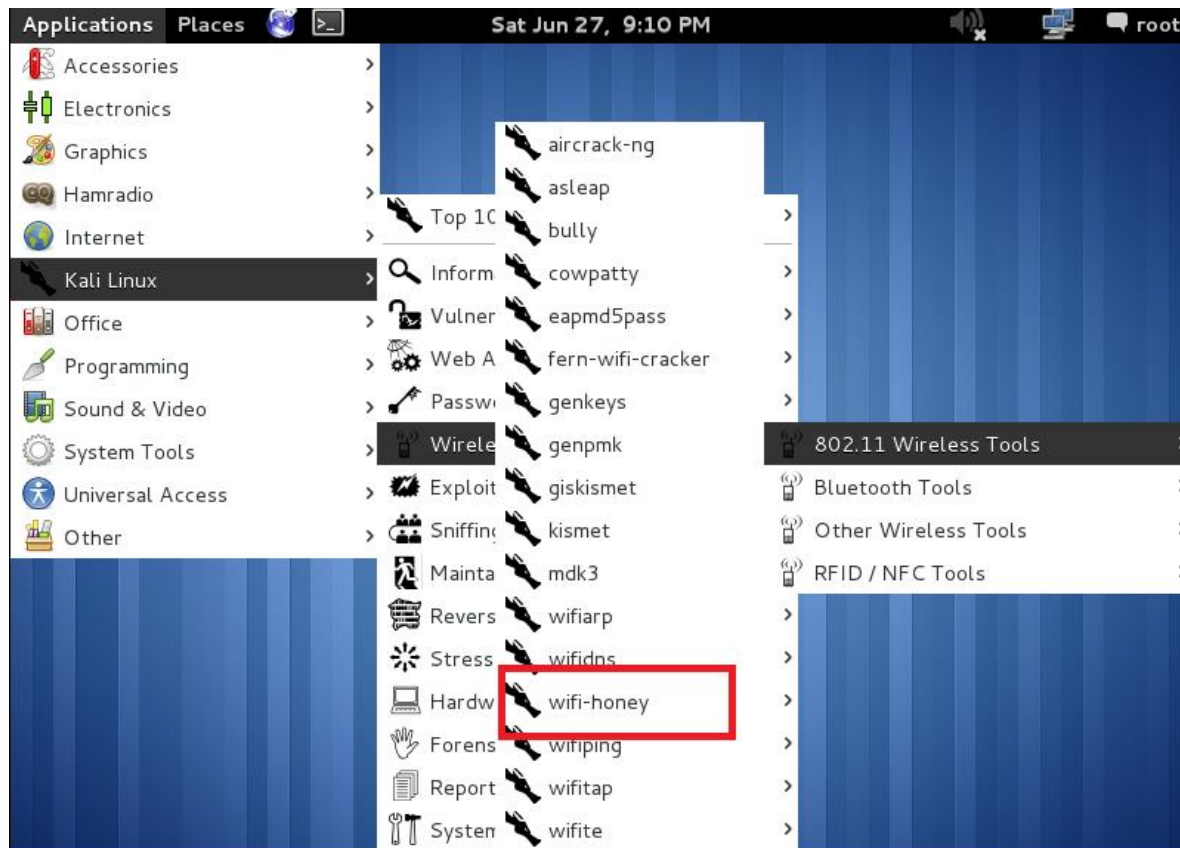
HostIP:98.136.187.13
HostName:chuckeasttom.com

Gathered Inet-whois information for 98.136.187.13
-----
inetnum:          98.0.0.0 - 98.255.255.255
netname:          NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:           IPv4 address block not managed by the RIPE NCC
remarks:          -----
remarks:
remarks:          You can find the whois server to query, or the
remarks:          IANA registry to query on this web page:
remarks:          http://www.iana.org/assignments/ipv4-address-space
remarks:
remarks:          You can access databases of other RIR's at:
remarks:
remarks:          AFRINIC (Africa)
remarks:          http://www.afrinic.net/ whois.afrinic.net
```

Wifi Honey

- ▶ Create your own fake AP with wifi-honey
- ▶ Generic Example
 - ▶ `wifi-honey <ssid> <channel> <interface>`
- ▶ Specific Example
 - ▶ `wifi-honey FreeWiFi 6 eth0`

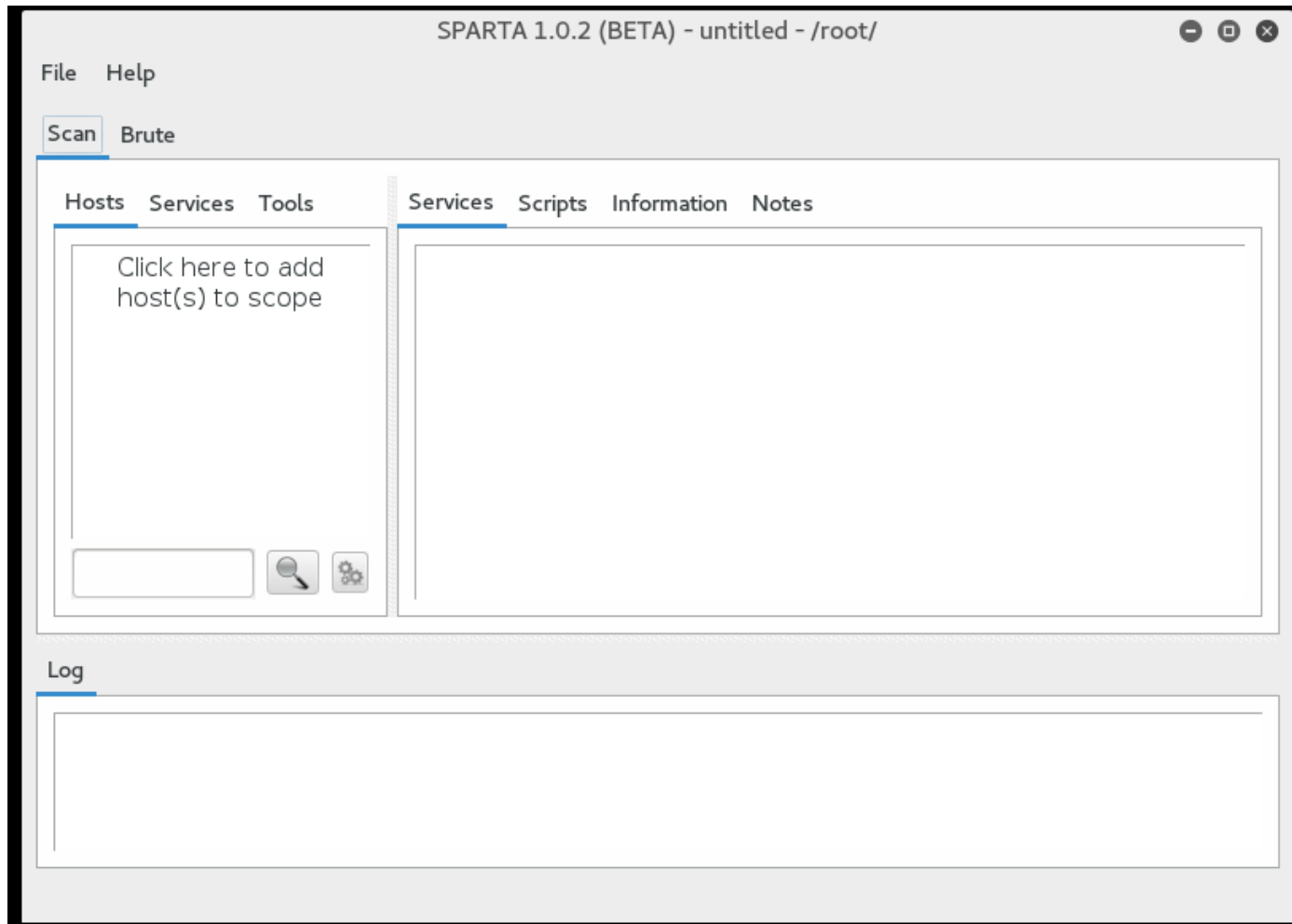
WiFi Honey



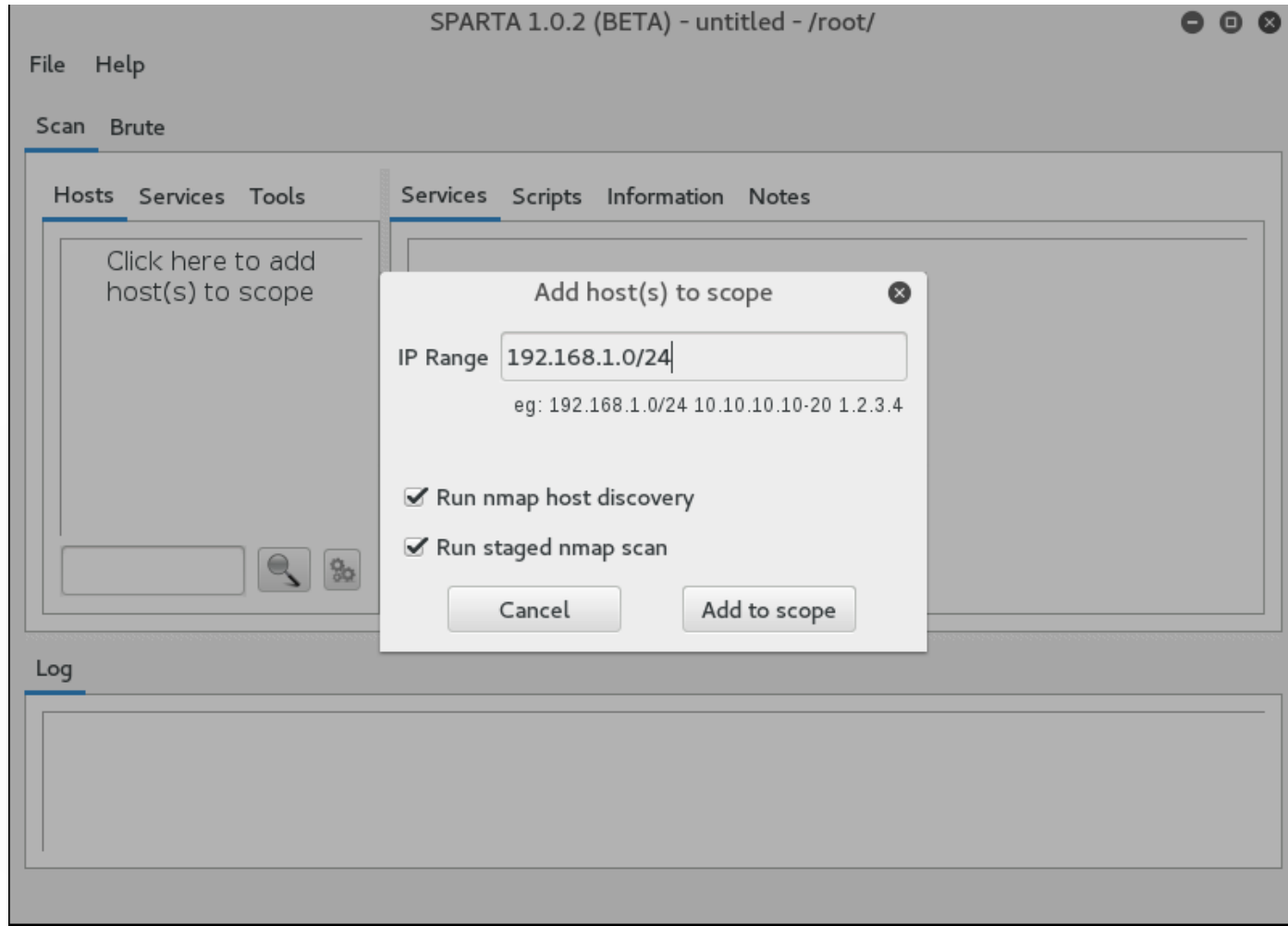
Legion

- ▶ A vulnerability scanner in Kali Linux that incorporates many tools including
 - ▶ •Mysql-default
 - ▶ •Nikto
 - ▶ •Snmp-enum
 - ▶ •Sntp-enum-vrfy
 - ▶ •Snmp-default
 - ▶ •Snmp-check

Legion



Legion



Legion

SPARTA 1.0.2 (BETA) - untitled - /root/

File Help

Scan Brute

Hosts Services Tools

OS	Host
?	192.168.1.156
🐧	192.168.1.158
?	192.168.1.160
🇺🇸	192.168.1.177
?	192.168.1.206

Services Scripts Information Notes smbenum (445/tcp) [x]

Port	Protocol	State	Name	Version
135	tcp	open	msrpc	Microsoft Wind...
137	udp	open	netbios-ns	Microsoft Wind...
139	tcp	open	netbios-ssn	Microsoft Wind...
445	tcp	open	microsoft-ds	Microsoft Wind...

Log

Progress	Tool	Host	Start time	End time
██████████	screenshot (8080/tcp)	192.168.1.1	02 Sep 2016 09:09:36	02 Sep 2016 09:09:36
██████████	screenshot (8080/tcp)	192.168.1.105	02 Sep 2016 09:09:36	02 Sep 2016 09:09:36

Legion

SPARTA 1.0.2 (BETA) - untitled - /root/

File Help

Scan Brute

1

IP Port Service

Try blank password Try login as password Exit on first valid Verbose Add

Username Username

Password Password

Found usernames

Found passwords

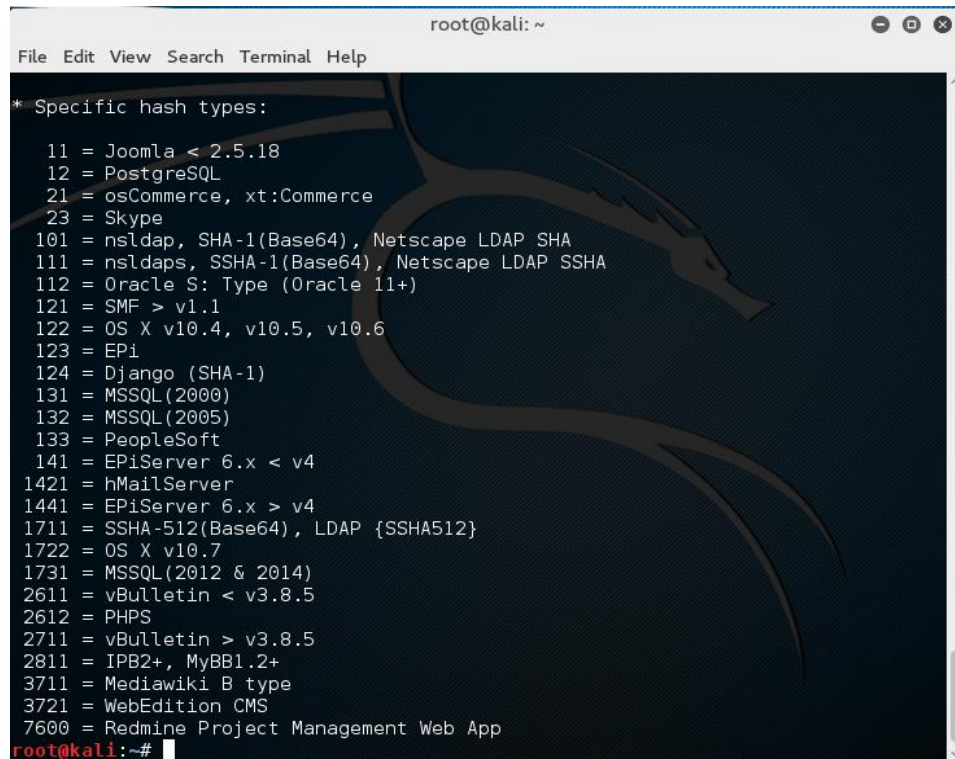
ssh
rsh
s7-300
sip
smb
smtp
smtps
smtp-enum
snmp
socks5
ssh

Log

Progress	Tool	Host	Start time	End time
	screenshot (8080/tcp)	192.168.1.1	02 Sep 2016 09:09:36	02 Sep 2016 09:09:36
	screenshot (8080/tcp)	192.168.1.105	02 Sep 2016 09:09:36	02 Sep 2016 09:09:36

hashcat

Hashcat is a rainbow table tool that tries to find passwords. It is completely shell, no GUI interface. Its main strength is that it can work with a variety of hash formats. Different applications can store their hashed passwords in a variety of ways. Hashcat can handle several widely used formats, including Mac OS



```
root@kali: ~
File Edit View Search Terminal Help
* Specific hash types:
  11 = Joomla < 2.5.18
  12 = PostgreSQL
  21 = osCommerce, xt:Commerce
  23 = Skype
 101 = nsldap, SHA-1(Base64), Netscape LDAP SHA
 111 = nsldaps, SSHA-1(Base64), Netscape LDAP SSHA
 112 = Oracle S: Type (Oracle 11+)
 121 = SMF > v1.1
 122 = OS X v10.4, v10.5, v10.6
 123 = Epi
 124 = Django (SHA-1)
 131 = MSSQL(2000)
 132 = MSSQL(2005)
 133 = PeopleSoft
 141 = EPiServer 6.x < v4
 1421 = hMailServer
 1441 = EPiServer 6.x > v4
 1711 = SSHA-512(Base64), LDAP {SSHA512}
 1722 = OS X v10.7
 1731 = MSSQL(2012 & 2014)
 2611 = vBulletin < v3.8.5
 2612 = PHPS
 2711 = vBulletin > v3.8.5
 2811 = IPB2+, MyBB1.2+
 3711 = Mediawiki B type
 3721 = WebEdition CMS
 7600 = Redmine Project Management Web App
root@kali:~#
```

hashcat

This particular tool is meant to change the MAC address your Kali machine sends out. That makes it more difficult to trace the attack back to the Kali machine. Also MAC spoofing can be a way to circumvent some forms of authentication. First turn your network card off

ifconfig eth0 down

Then run the macchanger

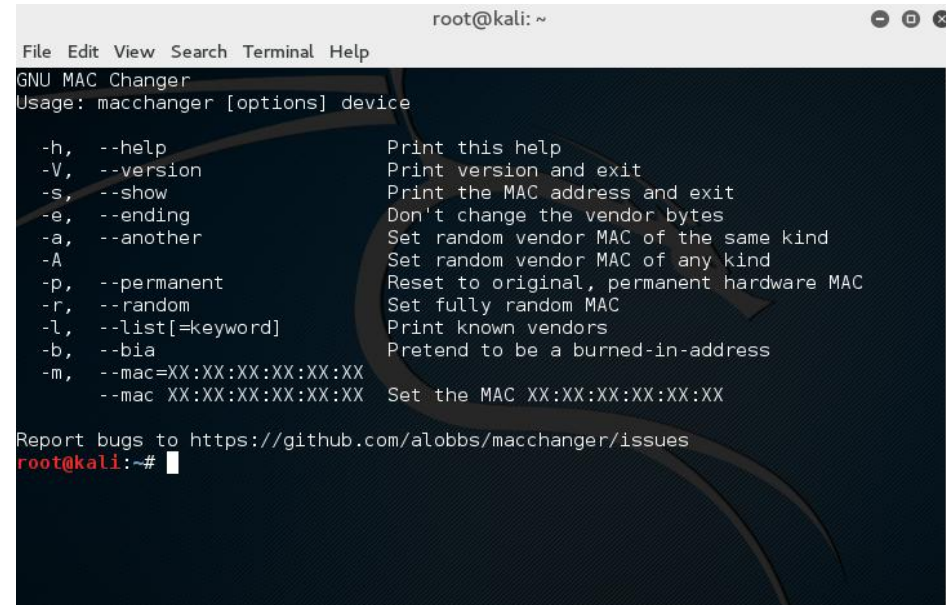
macchanger -m a1:b2:c3:11:22:33 eth0

or set it to some random number

macchanger -r eth0

Now bring your network card backup

ifconfig eth0 up

A screenshot of a terminal window titled 'root@kali: ~'. The terminal displays the help text for the 'GNU MAC Changer' tool. The text includes the usage 'Usage: macchanger [options] device' and a list of options: -h, --help; -V, --version; -s, --show; -e, --ending; -a, --another; -A; -p, --permanent; -r, --random; -l, --list[=keyword]; -b, --bia; -m, --mac=XX:XX:XX:XX:XX:XX; and --mac XX:XX:XX:XX:XX:XX. At the bottom, it says 'Report bugs to https://github.com/alobbs/macchanger/issues' and shows the prompt 'root@kali:~#'.

```
root@kali: ~
File Edit View Search Terminal Help
GNU MAC Changer
Usage: macchanger [options] device

-h, --help          Print this help
-V, --version       Print version and exit
-s, --show          Print the MAC address and exit
-e, --ending        Don't change the vendor bytes
-a, --another       Set random vendor MAC of the same kind
-A                  Set random vendor MAC of any kind
-p, --permanent     Reset to original, permanent hardware MAC
-r, --random        Set fully random MAC
-l, --list[=keyword] Print known vendors
-b, --bia           Pretend to be a burned-in-address
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX

Report bugs to https://github.com/alobbs/macchanger/issues
root@kali:~#
```

If you get errors, the most common issue is not having root level privileges.

Ghost Phisher

This is a very versatile tool, with several interesting functions.

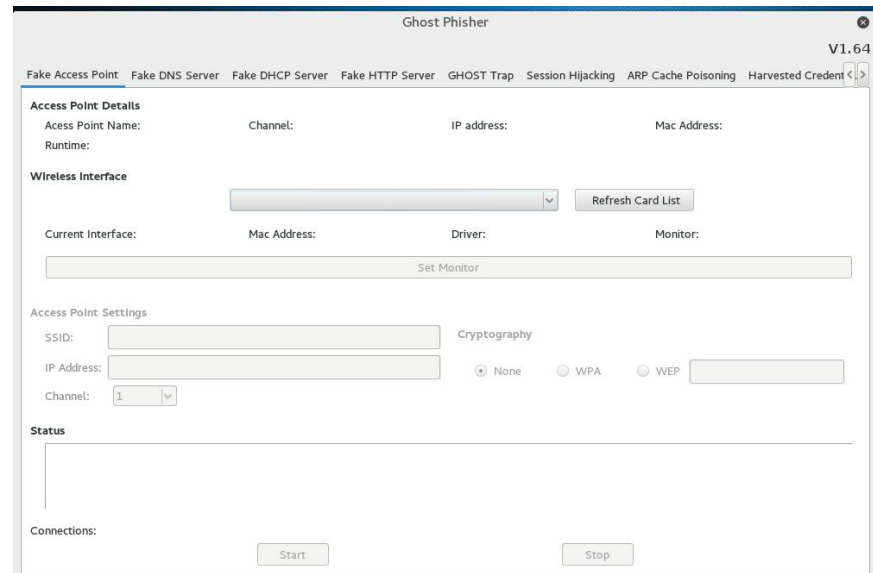
Each tab has settings to turn your Kali Linux machine into:

A fake wireless access point

A fake DNS server

A fake DHCP server

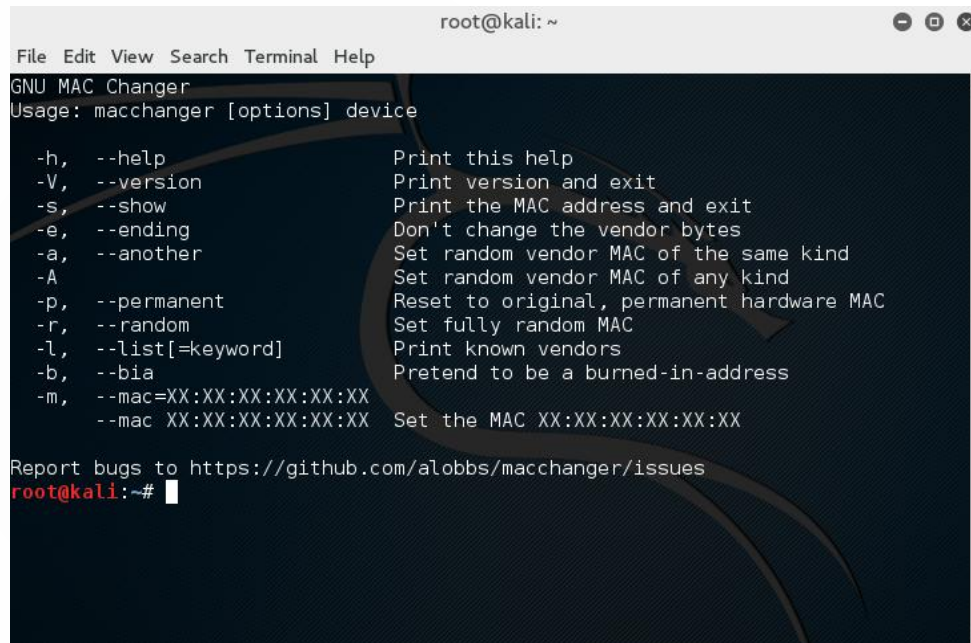
A fake HTTP server



And more. There are tabs for session hijacking and harvesting credentials.

Macchanger

- ▶ This particular tool is meant to change the MAC address your Kali machine sends out. That makes it more difficult to trace the attack back to the Kali machine. Also MAC spoofing can be a way to circumvent some forms of authentication



```
root@kali: ~  
File Edit View Search Terminal Help  
GNU MAC Changer  
Usage: macchanger [options] device  
  
-h, --help          Print this help  
-V, --version       Print version and exit  
-s, --show          Print the MAC address and exit  
-e, --ending        Don't change the vendor bytes  
-a, --another       Set random vendor MAC of the same kind  
-A                  Set random vendor MAC of any kind  
-p, --permanent    Reset to original, permanent hardware MAC  
-r, --random        Set fully random MAC  
-l, --list[=keyword] Print known vendors  
-b, --bia           Pretend to be a burned-in-address  
-m, --mac=XX:XX:XX:XX:XX:XX Set the MAC XX:XX:XX:XX:XX:XX  
--mac XX:XX:XX:XX:XX:XX  
  
Report bugs to https://github.com/alobbs/macchanger/issues  
root@kali:~#
```

Macchanger

- ▶ The basic syntax is two steps:
- ▶ First turn your network card off
- ▶ `ifconfig eth0 down`
- ▶ Then run the macchanger
- ▶ `macchanger -m a1:b2:c3:11:22:33 eth0`
- ▶ or set it to some random number
- ▶ `macchanger -r eth0`
- ▶ Now bring your network card back up
- ▶ `ifconfig eth0 up`
- ▶
- ▶ If you get errors, the most common issue is not having root level privileges.

nikto

▶ Basic website scan

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nikto -h www.chuckeasttom.com  
- Nikto v2.1.6  
-----  
+ Target IP: 98.137.244.36  
+ Target Hostname: www.chuckeasttom.com  
+ Target Port: 80  
+ Start Time: 2020-05-07 10:21:22 (GMT-5)  
-----  
+ Server: ATS/7.1.2  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ Uncommon header 'x-inkt-site' found, with contents: http://www.chuckeasttom.com  
+ Uncommon header 'x-inkt-uri' found, with contents: http://www.chuckeasttom.com//index.htm  
+ Uncommon header 'x-host' found, with contents: p10w62.geo.gq1.yahoo.com  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Cookie BX created without the httponly flag  
█
```

Nikto

- ▶ Takes a while to finish, but when done you will see this

```
root@kali: ~  
File Edit View Search Terminal Help  
+ Target Hostname: www.chuckeasttom.com  
+ Target Port: 80  
+ Start Time: 2020-05-07 10:21:22 (GMT-5)  
-----  
+ Server: ATS/7.1.2  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS  
+ Uncommon header 'x-inkt-site' found, with contents: http://www.chuckeasttom.com  
+ Uncommon header 'x-inkt-uri' found, with contents: http://www.chuckeasttom.com//index.htm  
+ Uncommon header 'x-host' found, with contents: p10w62.geo.gq1.yahoo.com  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type  
+ Cookie BX created without the httponly flag  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ Allowed HTTP Methods: GET, HEAD, OPTIONS  
+ OSVDB-3268: /style/: Directory indexing found.  
+ 7517 requests: 0 error(s) and 9 item(s) reported on remote host  
+ End Time: 2020-05-07 10:33:02 (GMT-5) (700 seconds)  
-----  
+ 1 host(s) tested  
root@kali:~#
```

nikto

- ▶ You may also scan a group of IP addresses. Just put them all in a text file
- ▶ `nikto -h targetIP.txt`
- ▶ You can export scan results into a format Metasploit can read:
- ▶ `nikto -h <IP or hostname> -Format msf+`

Nikto tuning

- ▶ You can specify attacks to try
- ▶ Tuning options will control the test that Nikto will use against
- ▶ a target. By default, if any options are specified, only those tests will be performed.

Nikto tuning

- ▶ 0 – File Upload
- ▶ 1 – Interesting File / Seen in logs
- ▶ 2 – Misconfiguration / Default File
- ▶ 3 – Information Disclosure
- ▶ 4 – Injection (XSS/Script/HTML)
- ▶ 5 – Remote File Retrieval – Inside Web Root
- ▶ 6 – Denial of Service
- ▶ 7 – Remote File Retrieval – Server Wide
- ▶ 8 – Command Execution / Remote Shell
- ▶ 9 – SQL Injection
- ▶ a – Authentication Bypass
- ▶ b – Software Identification
- ▶ c – Remote Source Inclusion
- ▶ x – Reverse Tuning Options (i.e., include all except specified)

Nikto tuning

- ▶ You can specify attacks to try
- ▶ Tuning options will control the test that Nikto will use against a target. By default, if any options are specified, only those tests will be performed.
- ▶ Check SQL Injection
 - ▶ `nikto -Tuning 9 -h www.chuckeasttom.com`
 - ▶ Or check everything except SQL injection
 - ▶ `nikto -Tuning x 9 -h www.chuckeasttom.com`
- ▶ You can also save your results
 - ▶ `nikto -Display V -o results.html -Format htm -Tuning 9 -h www.chuckeasttom.com`
- ▶ You can choose from several formats for output
 - ▶ `csv` Comma-separated-value
 - ▶ `htm` HTML Format
 - ▶ `nbe` Nessus NBE format
 - ▶ `sql` Generic SQL (see docs for schema)
 - ▶ `txt` Plain text
 - ▶ `xml` XML Format
 - ▶ if not specified the format will be taken from the file extension passed to `-output`

Nikto tuning

```
root@kali: ~
File Edit View Search Terminal Help
+ 1 host(s) tested
root@kali:~# clear

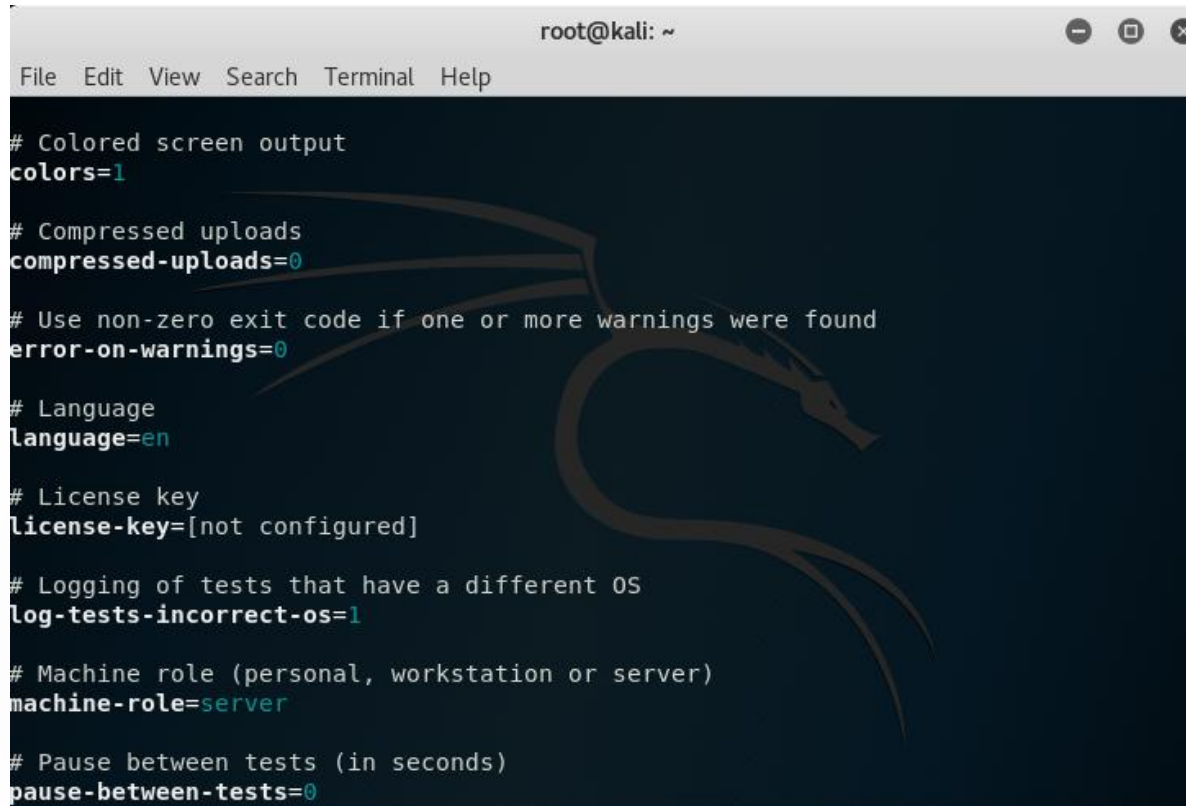
root@kali:~# nikto -Tuning -9 -h www.chuckeasttom.com
- Nikto v2.1.6
-----
+ Target IP:          98.137.244.36
+ Target Hostname:    www.chuckeasttom.com
+ Target Port:        80
+ Start Time:         2020-05-07 10:36:55 (GMT-5)
-----
+ Server: ATS/7.1.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-inkt-uri' found, with contents: http://www.chuckeasttom.com//index.htm
+ Uncommon header 'x-host' found, with contents: p10w77.geo.gq1.yahoo.com
+ Uncommon header 'x-inkt-site' found, with contents: http://www.chuckeasttom.com
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie BX created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Lynis

- ▶ Lynis is a host-based, open-source security auditing application that can evaluate the security profile and posture of Linux and other UNIX-like operating systems.

Lynis

► lynis show settings

A terminal window titled 'root@kali: ~' with a menu bar (File, Edit, View, Search, Terminal, Help) and window control buttons. The terminal displays the output of the 'lynis show settings' command, showing various configuration options and their values. A faint dragon logo is visible in the background of the terminal.

```
root@kali: ~  
File Edit View Search Terminal Help  
# Colored screen output  
colors=1  
# Compressed uploads  
compressed-uploads=0  
# Use non-zero exit code if one or more warnings were found  
error-on-warnings=0  
# Language  
language=en  
# License key  
license-key=[not configured]  
# Logging of tests that have a different OS  
log-tests-incorrect-os=1  
# Machine role (personal, workstation or server)  
machine-role=server  
# Pause between tests (in seconds)  
pause-between-tests=0
```

Lynis

- ▶ lynis update info
- ▶ or
- ▶ lynis update check

- ▶ will see if you need an update
- ▶ Or you might try
- ▶ lynis show version

Lynis

- ▶ The scan process starts with
- ▶ lynis audit system

```
root@kali: ~  
File Edit View Search Terminal Help  
  
Files:  
- Test and debug information      : /var/log/lynis.log  
- Report data                    : /var/log/lynis-report.dat  
  
=====
```

Notice: Lynis update available
Current version : 250 Latest version : 275

```
=====
```

Lynis 2.5.0

Auditing, system hardening, and compliance for UNIX-based systems
(Linux, macOS, BSD, and others)

2007-2017, CIS0fy - <https://cisofy.com/lynis/>
Enterprise support available (compliance, plugins, interface and tools)

```
=====
```

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

```
root@kali:~#
```

Lynis

Command	Description
audit system	Perform a system audit
show commands	Show available Lynis commands
show help	Provide a help screen
show profiles	Display discovered profiles
show settings	List all active settings from profiles
show version	Display current Lynis version

Powersploit

- ▶ This is after you have access to a target machine.
- ▶ It involves running a web server and listener on the Kali machine and navigating to that web server from the victim.

Powersploit

- ▶ Quite a few interesting tools here

```
File  Actions  Edit  View  Help
|
|---AntivirusBypass
|---CodeExecution
|---Exfiltration
|---Mayhem
|---Persistence
|---PowerSploit.psd1
|---PowerSploit.psm1
|---Privesc
|---README.md
|---Recon
|---ScriptModification
|---Tests
chuck@kali:~/usr/share/windows-resources/powersploit$ ls -l
total 60
drwxr-xr-x 2 root root 4096 May 12 07:24 AntivirusBypass
drwxr-xr-x 3 root root 4096 May 12 07:24 CodeExecution
drwxr-xr-x 4 root root 4096 May 12 07:24 Exfiltration
drwxr-xr-x 2 root root 4096 May 12 07:24 Mayhem
drwxr-xr-x 2 root root 4096 May 12 07:24 Persistence
-rw-r--r-- 1 root root 5000 Dec 18 2015 PowerSploit.psd1
-rw-r--r-- 1 root root 135 Dec 18 2015 PowerSploit.psm1
drwxr-xr-x 2 root root 4096 May 12 07:24 Privesc
-rw-r--r-- 1 root root 9972 Dec 18 2015 README.md
drwxr-xr-x 3 root root 4096 May 12 07:24 Recon
drwxr-xr-x 2 root root 4096 May 12 07:24 ScriptModification
drwxr-xr-x 2 root root 4096 May 12 07:24 Tests
chuck@kali:~/usr/share/windows-resources/powersploit$
```

Powersploit

- ▶ You can navigate to any directory and see what options are available.

```
chuck@kali:~/usr/share/windows-resources/powersploit$ cd CodeExecution
chuck@kali:~/usr/share/windows-resources/powersploit/CodeExecution$ ls -l
total 208
-rw-r--r-- 1 root root  952 Dec 18  2015 CodeExecution.psd1
-rw-r--r-- 1 root root   67 Dec 18  2015 CodeExecution.psm1
-rw-r--r-- 1 root root 12721 Dec 18  2015 Invoke-DllInjection.ps1
-rw-r--r-- 1 root root 135782 Dec 18  2015 Invoke-ReflectivePEInjection.ps1
drwxr-xr-x 7 root root  4096 May 12  07:24 Invoke-ReflectivePEInjection_Resources
-rw-r--r-- 1 root root 23817 Dec 18  2015 Invoke-Shellcode.ps1
-rw-r--r-- 1 root root 14479 Dec 18  2015 Invoke-WmiCommand.ps1
-rw-r--r-- 1 root root   770 Dec 18  2015 Usage.md
chuck@kali:~/usr/share/windows-resources/powersploit/CodeExecution$
```

GoLismero

- ▶ This is a python script.
- ▶ Simple scan
- ▶ `golismero scan www.chuckeasttom.com`

- ▶ You can export to output
- ▶ `golismero scan www.chuckeasttom.com -o - -o report.html`

GoLismero

```
root@kali: ~  
File Edit View Search Terminal Help  
[*] theHarvester: Found 3 emails and 2 hostnames on google for domain chuckedom.com  
[*] theHarvester: Searching keyword 'chuckedom.com' in bing  
[*] theHarvester: 20.00% percent done...  
[!] theHarvester: Invalid header name 'Cookie: SRCHHPGUSR=ADLT=DEMOTE&NRSLT=50'  
[*] theHarvester: Searching keyword 'chuckedom.com' in linkedin  
[*] theHarvester: 40.00% percent done...  
[*] DNS Resolver (2): 66.66% percent done...  
[*] DNS Resolver: 100.00% percent done...  
[*] DNS Resolver (2): 77.77% percent done...  
[*] DNS Resolver (2): 88.88% percent done...  
[*] theHarvester: Found 0 emails and 0 hostnames on linkedin for domain chuckedom.com  
[*] theHarvester: Searching keyword 'chuckedom.com' in dogpile  
[*] theHarvester: 60.00% percent done...  
[!] theHarvester: 'content-type'  
[*] theHarvester: 80.00% percent done...  
[*] DNS Resolver (2): 100.00% percent done...  
[*] theHarvester: 86.66% percent done...  
[*] theHarvester: 93.33% percent done...  
[*] theHarvester: 100.00% percent done...  
[*] theHarvester: Found 3 emails, 0 hostnames and 0 IP addresses for keyword 'chuckedom.com'
```

theharvester

- ▶ It allows you to harvest data using any search engine. The syntax is
- ▶ **theHarvester -d [url] -l 300 -b [search engine name]**
- ▶ **note -l 300 means you only want 300 results.**
- ▶ Or better yet search all search engines
- ▶ **theHarvester -d chuckeasttom.com -l 300 -b all**

```
*  \_/| |\_| \ \ / \_/| |  \ \_| ||__^ \_/| |  *
*                               *
*  theHarvester 3.1.0                *
*  Coded by Christian Martorella      *
*  Edge-Security Research            *
*  cmartorella@edge-security.com     *
*                               *
*****

[*] Target: chuckeasttom.com

[*] Searching Netcraft.

[*] Searching AlienVault OTX.
    Searching results.
[*] Searching Bing.
[*] Searching DuckDuckGo.
[*] Searching Hunter.
[*] Searching Yahoo.
[*] Searching CertSpotter.
    Searching results.
[*] Searching Intelx.
An exception has occurred in Intelx search: [Errno 2] No such file or directory: 'api-keys.yaml'
[*] Searching VirusTotal.
    Searching results.
[*] Searching SecurityTrails.
[*] Searching LinkedIn.
```

theharvester

- ▶ **-d:** Domain to search or company name.
- ▶ **-b:** Data source: baidu, bing, bingapi, dogpile, google, googleCSE, googleplus, google-profiles, linkedin, pgp, twitter, vhost, yahoo, all.
- ▶ **-s:** Start in result number X (default: 0).
- ▶ **-v:** Verify host name via DNS resolution and search for virtual hosts.
- ▶ **-f:** Save the results into an HTML and XML file (both).
- ▶ **-n:** Perform a DNS reverse query on all ranges discovered.
- ▶ **-c:** Perform a DNS brute force for the domain name.
- ▶ **-t:** Perform a DNS TLD expansion discovery.
- ▶ **-e:** Use this DNS server.
- ▶ **-l:** Limit the number of results to work with (bing goes from 50 to 50 results, google 100 to 100, and pgp doesn't use this option).
- ▶ **-h:** Use SHODAN database to query discovered hosts.