

Best Hacking Tools 2017

#1 Metasploit

```
File View Exploits Auxiliary Payloads History Post-Exploit Console Database P
jobs console 0 Sessions

(( _ _ _ _ _ ))
  ( _ ) 0 0 ( _ )
    \_o_/
      o_o \ M S F
            \_ww_|
              |||
              |||

= [ metasploit v4.7.0-dev [core:4.7 api:1.0]
+ -- == [ 1083 exploits - 608 auxiliary - 177 post
+ -- == [ 298 payloads - 29 encoders - 8 nops

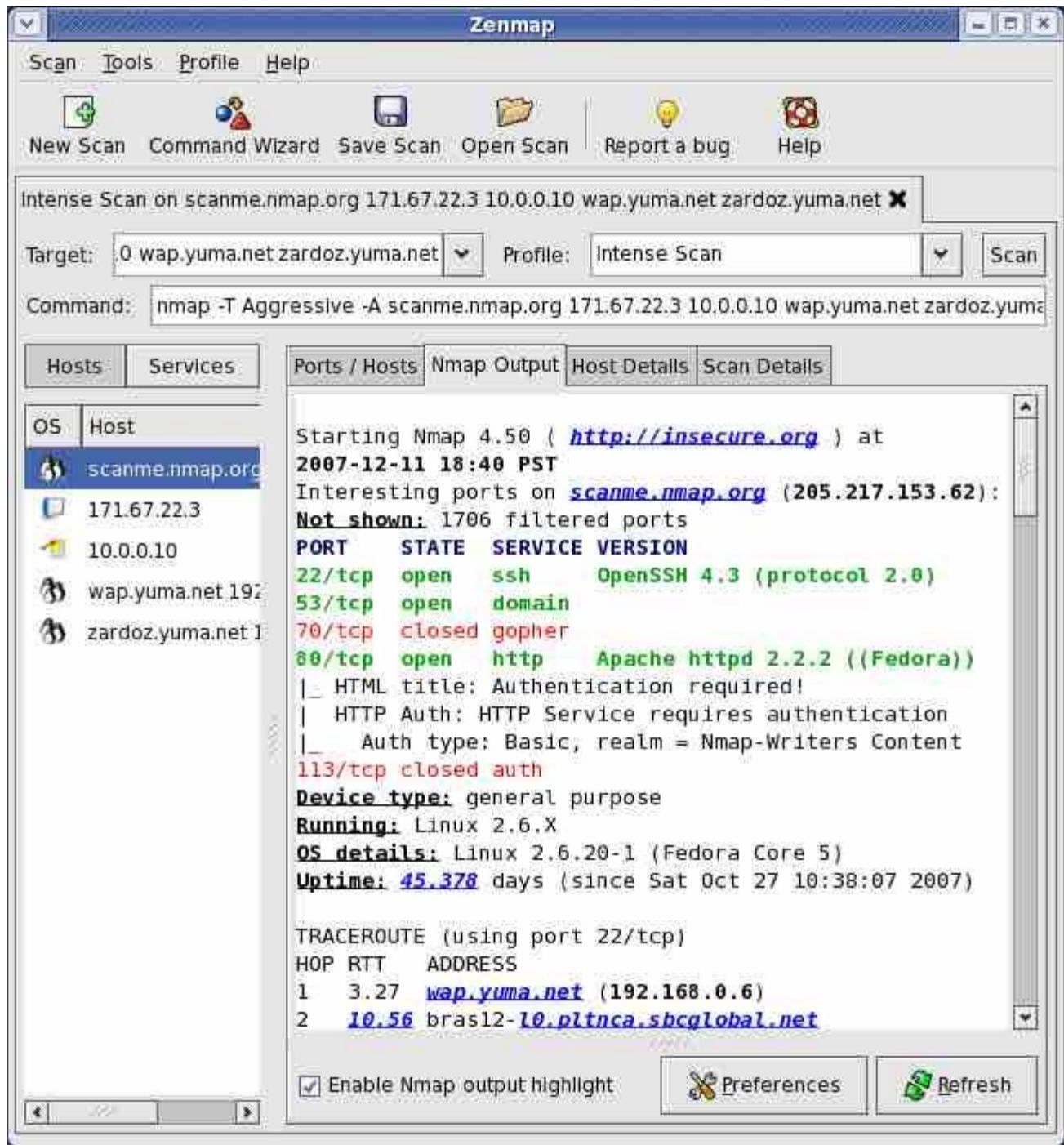
msf > use exploit/multi/browser/java_jre17_method_handle

1083 exploit 608 auxiliary 298 payload 177
```

Metasploit is available for all major platforms including **Windows, Linux, and OS X**. Rather than calling Metasploit a collection of exploit tools, I'll call it an infrastructure that you can utilize to build your custom tools. This free tool is one of the most popular cyber security tools around that allows you to locate vulnerabilities at different platforms. Metasploit is backed by more than 200,000 users and contributors that help you to get insights and uncover the weaknesses in your system.

This top hacking tool package of 2017 lets you simulate real-world attacks to tell you about the weak points and finds them. As a penetration tester, it pinpoints the vulnerabilities with Nexpose closed-loop integration using Top Remediation reports. Using the open source Metasploit framework, users can build their tools and take the best out of this multi-purpose hacking tool.

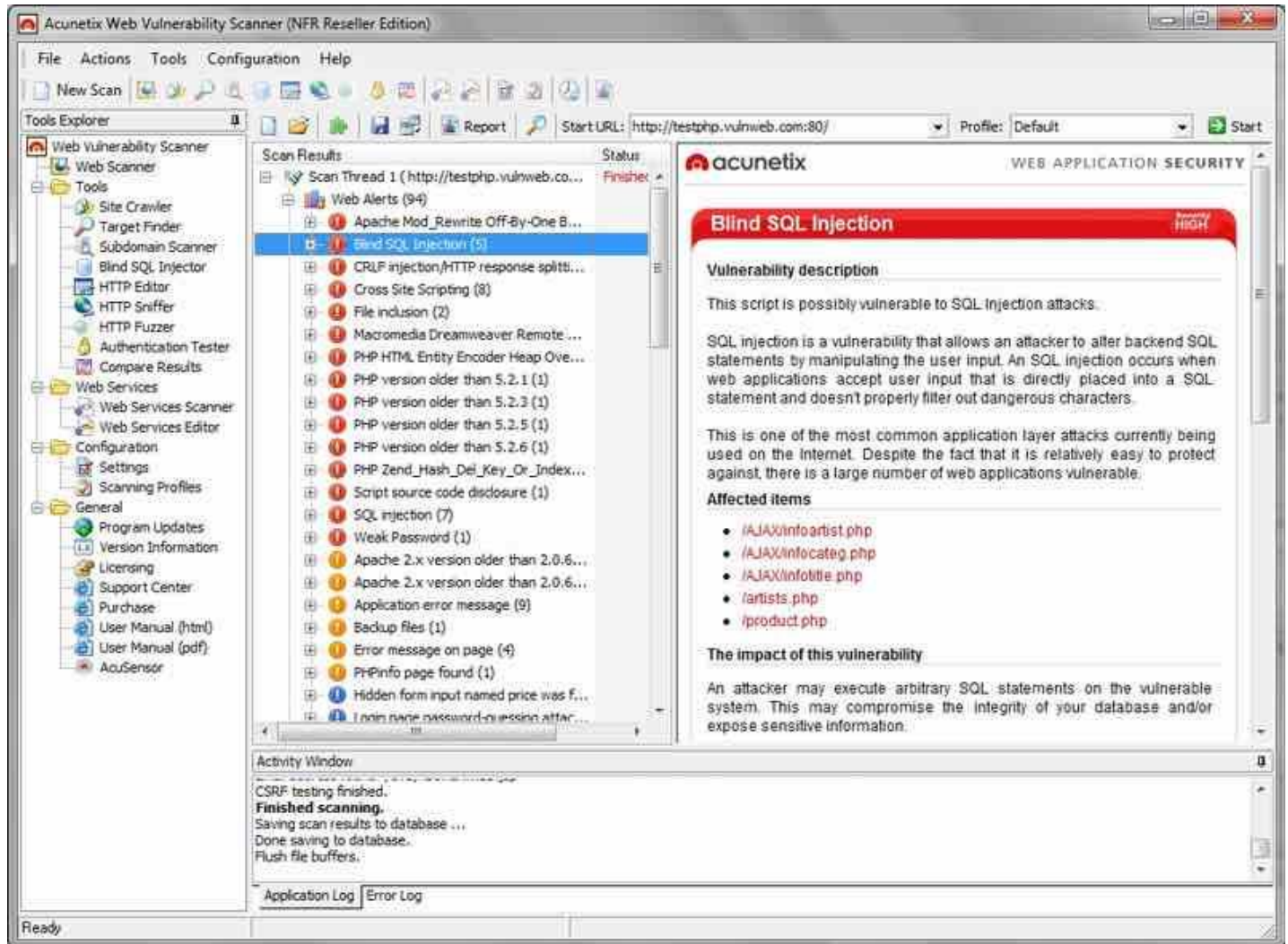
#2 [Nmap](#)



Nmap is available for all major platforms including **Windows, Linux, and OS X**. I think everyone has heard of this one, Nmap (Network Mapper) is a free open source utility for network exploration or security auditing. It was designed to Nmap rapidly scan large networks, although it works fine against single hosts. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It may be used to

discover computers and services on a computer network, thus creating a “map” of the network. Nmap runs on most types of computers, and both console, and graphical versions are available. Nmap is a fee and open source tool that can be used by beginners (-sT) or by pros alike (packet_trace). A very versatile tool, once you fully understand the results.

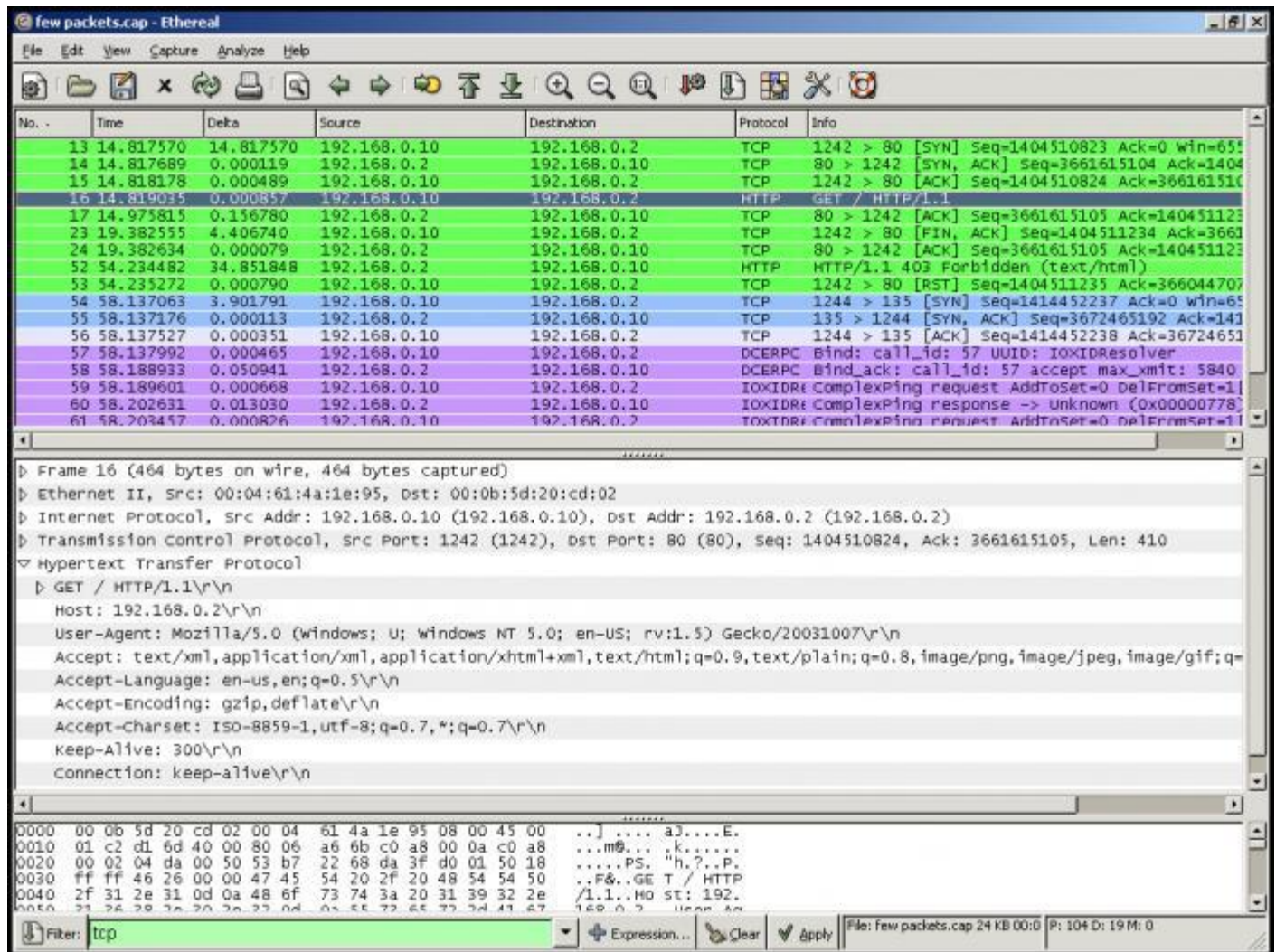
#3 [Acunetix WVS](#)



Acunetix is available for Windows XP and higher. Acunetix is a web vulnerability scanner (WVS) that scans and finds out the flaws in a website that could prove fatal. This multi-threaded tool crawls a website and finds out malicious Cross-site Scripting, SQL injection, and other vulnerabilities. This fast and easy to use tool scans WordPress websites from more than 1200 vulnerabilities in WordPress.

Acunetix comes with a Login Sequence Recorder that allows one to access the password protected areas of web sites. The new AcuSensor technology used in this tool allows you to reduce the false positive rate. Such features have made Acunetix WVS a preferred hacking tools that you need to check out in 2017.

#4 [Wireshark](#)



This free and open source tool was originally named Ethereal. Wireshark also comes in a command-line version called TShark. This GTK+-based network protocol analyzer runs with ease on **Linux, Windows, and OS X**. Wireshark is a GTK+-based Wireshark network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames. The goal of the project is to create a commercial-quality analyzer for Unix and to give Wireshark features that are missing from closed-source sniffers. Works great on both Linux and Windows (with a GUI), easy to use and can reconstruct TCP/IP Streams.

#5 [oclHashcat](#)

```
root@sf:~/oclHashcat-lite-0.10# ./oclHashcat-lite64.bin 9b957cc6ab97cbf88c4f6f0f146adafe
oclHashcat-lite v0.10 by atom starting...

Password lengths range: 8 - 55
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 80c
Device #1: Cayman, 1024MB, 830Mhz, 24MCU
Device #2: Cayman, 1024MB, 830Mhz, 24MCU

9b957cc6ab97cbf88c4f6f0f146adafe:hashcat!

Status.....: Cracked
Hash.Target..: 9b957cc6ab97cbf88c4f6f0f146adafe
Hash.Type....: MD5
Time.Running.: 7 mins, 43 secs
Time.Left....: 1 min, 12 secs
Plain.Mask...: ?1?2?2?2?2?2?2?3
Plain.Text...: **w4ceq
Plain.Length.: 8
Progress.....: 4793460326400/5533380698112 (86.63%)
Speed.GPU.#1.: 5243.4M/s
Speed.GPU.#2.: 5242.7M/s
Speed.GPU.#..: 10486.1M/s
HwMon.GPU.#1.: 99% Util, 66c Temp, 41% Fan
HwMon.GPU.#2.: 99% Util, 71c Temp, N/A Fan

Started: Fri Jun 29 10:15:11 2012
Stopped: Fri Jun 29 10:22:56 2012
```

This useful hacking tool can be downloaded in different versions for **Linux, OSX, and Windows**. If password cracking is something you do on a daily basis, you might be aware of the free password cracking tool Hashcat. While Hashcat is a CPU-based password cracking tool, oclHashcat is its advanced version that uses the power of your GPU.

oclHashcat calls itself world's fastest password cracking tool with world's first and only GPGPU based engine. For using the tool, NVIDIA users require ForceWare 346.59 or later, and AMD users require Catalyst 15.7 or later.

This tool employs following attack modes for cracking:

- Straight
- Combination
- Brute-force
- Hybrid dictionary + mask
- Hybrid mask + dictionary

Mentioning another major feature, oclHashcat is an open source tool under MIT license that allows an easy integration or packaging of the common Linux distros.

#6 [Nessus Vulnerability Scanner](#)

The screenshot shows the Nessus 'Edit Policy' window. The left sidebar has a 'General' tab selected. The main content area is divided into several sections:

- Basic:** Name: test, Visibility: Private, Description: (empty text area).
- Scan:** A list of checkboxes: Save Knowledge Base (checked), Safe Checks (checked), Silent Dependencies (unchecked), Log Scan Details to Server (checked), Stop Host Scan on Disconnect (unchecked), Avoid Sequential Scans (unchecked), Consider Unscanned Ports as Closed (unchecked), Designate Hosts by their DNS Name (checked).
- Network Congestion:** Reduce Parallel Connections on Congestion (unchecked), Use Kernel Congestion Detection (Linux Only) (unchecked).
- Port Scanners:** TCP Scan (checked), UDP Scan (unchecked), SYN Scan (checked), SNMP Scan (checked), Netstat SSH Scan (checked), Netstat WMI Scan (checked), Ping Host (checked).
- Port Scan Options:** Port Scan Range: default.
- Performance:** Max Checks Per Host: 5, Max Hosts Per Scan: 80, Network Receive Timeout (seconds): 5, Max Simultaneous TCP Sessions Per Host: unlimited, Max Simultaneous TCP Sessions Per Scan: unlimited.

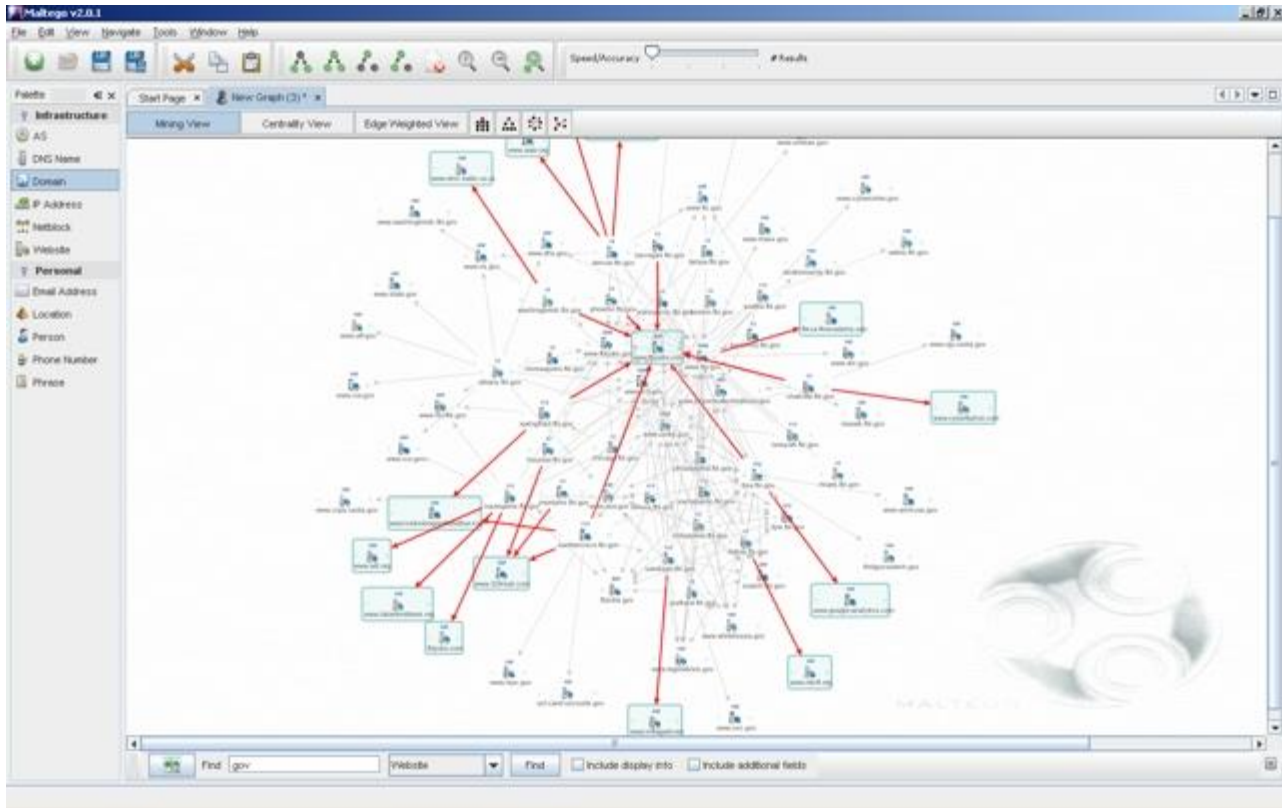
At the bottom right, there are 'Cancel' and 'Submit' buttons.

Nessus is supported by a variety of platforms including **Windows 7 and 8, Mac OS X, and popular Linux distros like Debian, Ubuntu, Kali Linux** etc. This top free hacking tool of 2017 works with the help of a client-server framework. Developed by Tenable Network Security, the tool is one of the most popular vulnerability scanners we have. Nessus serves different purposes to different types of users – Nessus Home, Nessus Professional, Nessus Manager and Nessus Cloud.

Using Nessus, one can scan multiple types of vulnerabilities that include remote access flaw detection, misconfiguration alert, denial of services against TCP/IP stack, preparation of PCI DSS audits, malware detection, sensitive data searches etc. To launch a dictionary attack, Nessus can also call a popular tool Hydra externally.

Apart from the above mentioned basic functionalities, Nessus could be used to scan multiple networks on IPv4, IPv6, and hybrid networks. You can set scheduled scan to run at your chosen time and re-scan all or a subsection of previously scanned hosts using selective host re-scanning.

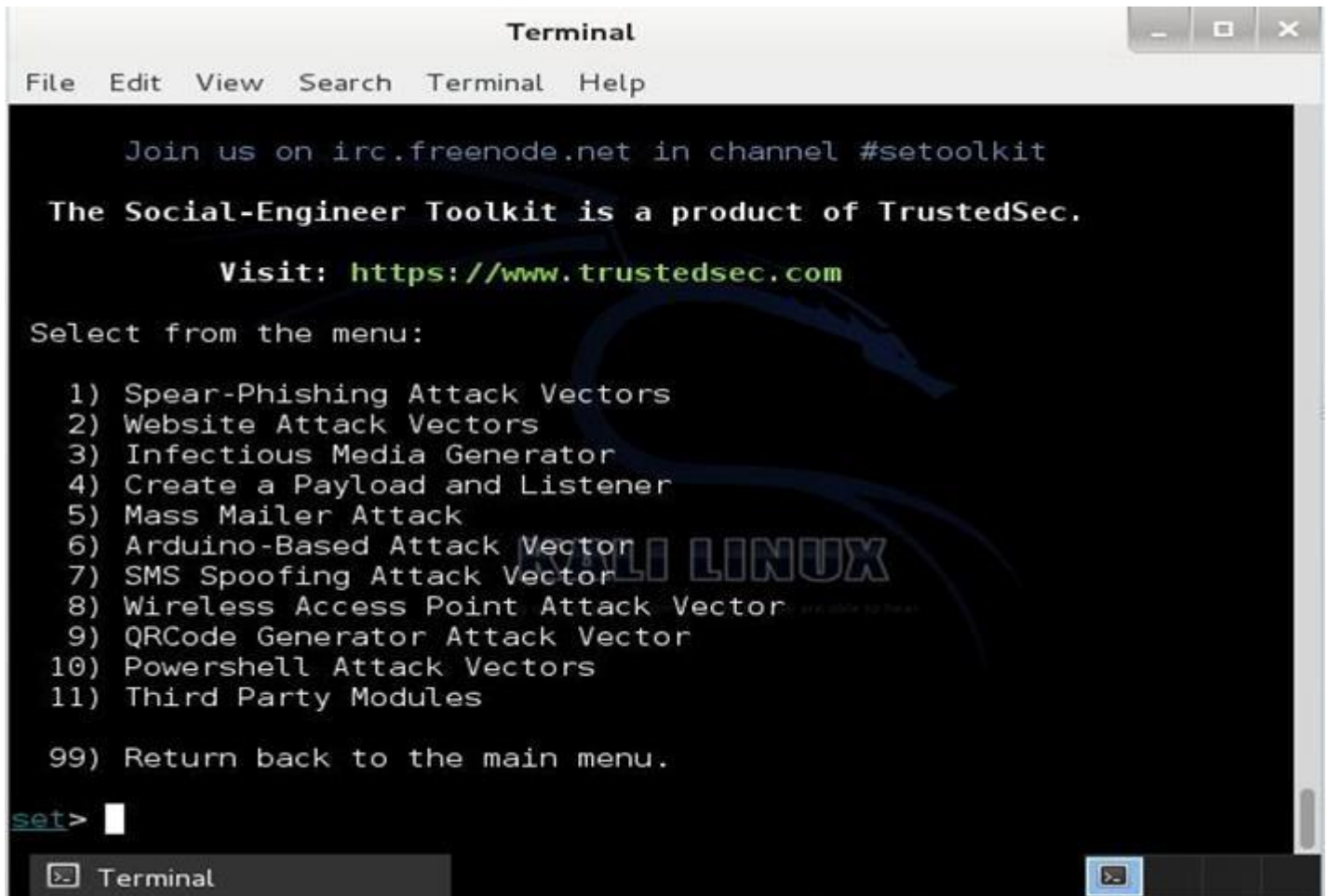
#7 [Maltego](#)



Maltego hacking tool is available for **Windows, Mac, and Linux**. Maltego is an open source forensics platform that offers rigorous mining and information gathering to paint a picture of cyber threats around you. Maltego excels in showing the complexity and severity of points of failure in your infrastructure and the surrounding environment.

Maltego is a great hacker tool that analyzes the real world links between people, companies, websites, domains, DNS names, IP addresses, documents and whatnot. Based on Java, this tool runs in an easy-to-use graphical interface with lots of customization options while scanning.

#8 Social-Engineer Toolkit



```
Terminal
File Edit View Search Terminal Help

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.

set> 
```

Apart from Linux, Social-Engineer Toolkit is partially supported on **Mac OS X and Windows**. Also featured on Mr. Robot, TrustedSec's Social-Engineer Toolkit is an advanced framework for simulating multiple types of social engineering attacks like credential harvestings, phishing attacks, and more. On the show, Elliot is seen using the SMS spoofing tool from the Social-Engineer Toolkit.

This Python-driven tool is the standard tool for social engineering penetration tests with more than two million downloads. It automates the attacks and generates disguising emails, malicious web pages and more.

#9 [Nessus Remote Security Scanner](#)

Multiple Assessment Types		Nessus Professional	Nessus Cloud	Nessus Manager
Vulnerability scanning	Assess systems, networks and applications for weaknesses	✓	✓	✓
Configuration auditing	Ensure that IT assets are compliant with policy and standards	✓	✓	✓
Compliance checks	Audit system configurations and content against standards	✓	✓	✓
Malware detection	Detect malware as well as potentially unwanted and unmanaged software	✓	✓	✓
Web application scanning	Discover web server and services weaknesses and OWASP vulnerabilities	✓	✓	✓
Sensitive data searches	Identify private information on systems or in documents	✓	✓	✓
Control system auditing	Scan SCADA systems, embedded devices and ICS applications	✓	✓	✓
Cloud Support	Assess configuration weaknesses in Amazon Web Services, Microsoft Azure and Rackspace public clouds	✓	✓	✓
Rich Assessment Capabilities		Nessus Professional	Nessus Cloud	Nessus Manager

Recently went closed source, but is still essentially free. Works with a client-server framework. Nessus is the Remote Security Scanner most popular vulnerability scanner used in over 75,000 organizations worldwide. Many of the world's largest organizations are realizing significant cost savings by using Nessus to audit business-critical enterprise devices and applications.

#10 [Kismet](#)

```
Kismet Sort View Windows
Name BSSID T C Ch Freq Pkts Size Bcn% Sig Cnt Manuf Cty Seen By
TRENDnet 00:14:D1:5F:97:12 A 0 1 2417 1 0B --- --- 1 TrendwareI --- wlan0 DRD1812
QQF93 00:1F:90:F2:CD:C2 A W 1 2412 1 0B --- --- 1 ActiontecE US wlan0 Networks
landscapers 00:14:BF:07:2F:84 A N 6 2437 2 0B 10% -B6 1 Cisco-Link --- wlan0 17
linksys_SES_45997 00:16:B6:1B:E4:FF A 0 6 2447 2 0B --- --- 1 Cisco-Link --- wlan0
linksys 00:1A:70:D9:BC:13 A N 6 2437 2 0B --- --- 1 Cisco-Link --- wlan0 Packets
MPA41 00:1F:90:E6:E0:84 A W 11 2462 3 0B --- --- 1 ActiontecE --- wlan0 787
TFS 00:09:5B:D7:9D:B2 A N --- 2462 4 0B --- --- 1 Netgear --- wlan0
Autogroup Probe 00:13:E8:92:3F:CB P N --- ---- 5 0B --- 0 1 IntelCorpo --- wlan0 Pkt/Sec
meskas 00:18:01:F5:65:E1 A 0 11 2462 7 0B 10% -87 1 ActiontecE US wlan0 10
6SI03 00:1F:90:FA:F4:CB A W --- 2412 8 0B --- --- 1 ActiontecE --- wlan0
Xu Chen 00:18:01:F9:70:F0 A N 6 2442 9 0B 0% -75 1 ActiontecE US wlan0 Elapsed
7J4R0 00:1F:90:E6:04:F1 A W 11 2462 14 0B --- -70 1 ActiontecE --- wlan0 00:01.05
TK421 00:18:01:FE:68:77 A 0 6 2437 14 0B --- -82 1 ActiontecE --- wlan0
Elina-PC-Wireless 00:24:B2:0E:E6:E2 A 0 11 2462 14 0B 0% -31 1 Netgear --- wlan0
Pickles 00:1F:33:F3:C5:4A A 0 2 2422 17 0B --- --- 1 Netgear --- wlan0
38c8 00:16:CE:07:60:77 A W 6 2447 38 0B --- -76 1 HonHaiPrec --- wlan0

MAC Crypt Freq Pkts Size Manuf DHCP Host DHCP OS
00:13:10:35:59:CB 0 2462 624 0B Cisco-Link --- --- ---
00:11:24:A4:6F:B3 6 2452 6 708B AppleCompu --- --- ---
00:13:10:35:59:C9 5 2452 5 1K Cisco-Link --- --- ---
00:17:AB:3D:25:98 4 2452 4 626B Nintendo --- --- ---
00:13:E8:92:3F:CB 8 ---- 8 1K IntelCorpo --- --- ---

No GPS info (GPS not connected)

INFO: Detected new managed network "landscapers", BSSID 00:14:BF:07:2F:84, encryption no, channel 6, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: Could not connect to the spectools server localhost:30569 wlan0
INFO: Detected new managed network "QQF93", BSSID 00:1F:90:F2:CD:C2, encryption yes, channel 1, 54.00 mbit 9
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
```

Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any kismet wireless card which supports raw monitoring (rfmon) mode and can sniff 802.11b, 802.11a, and 802.11g traffic. A good wireless tool as long as your card supports rfmon.

#11 [John The Ripper](#)



John the Ripper is free and Open Source software, distributed primarily in source code form. It is the password cracking software tool. It is one of the most popular password testings and breaking programs

as it combines a number of password crackers into one package, autodetects password hash types, and includes a customizable cracker.

#12 Unicornscan



Unicornscan is an attempt at a User-land Distributed TCP/IP stack for information gathering and correlation. It is intended to provide a researcher a superior interface for introducing a stimulus into and measuring a response from a TCP/IP enabled device or network. Some of its features include asynchronous stateless TCP scanning with all variations of TCP flags, asynchronous stateless TCP banner grabbing, and active/passive remote OS, application, and component identification by analyzing responses.

#13 [Netsparker](#)



Netsparker

Netsparker is an easy-to-use web application security scanner that uses the advanced Proof-Based vulnerability scanning technology and has built-in penetration testing and reporting tools. Netsparker automatically exploits the identified vulnerabilities in a read-only and safe way, and also produces a proof of exploitation.

#14 [Burp Suite](#)



Burp Suite

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.