

COMMON WINDOWS, LINUX AND WEB SERVER SYSTEMS HACKING TECHNIQUES



DR. HEDAIA MAHMOOD AL-ASSOULI

Common Windows, Linux and Web Server Systems Hacking Techniques

By

**Dr. Hidaia Mahmood Alassouli
Hidaia_lassouli@hotmail.com**

While every precaution has been taken in the preparation of this book, the publisher assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained herein.

Common Windows, Linux and Web Server Systems Hacking Techniques

Copyright © 2021 Dr. Hidaia Mahmood Alassouli.

Written by Dr. Hidaia Mahmood Alassouli.

1. Introduction

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system.

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code. If this replication succeeds, the affected areas are then said to be "infected" with a computer virus. Computer viruses generally require a host program.

System hacking is defined as the compromise of computer systems and software to access the target computer and steal or misuse their sensitive information. Here the malicious hacker exploits the weaknesses in a computer system or network to gain unauthorized access to its data or take illegal advantage.

Web content is generated in real time by a software application running at server-side. So hackers attack on the web server to steal credential information, passwords, and business information by using DoS (DDos) attacks, SYN flood, ping flood, port scan, sniffing attacks, and social engineering attacks.

This report covers the common techniques and tools used for System, Windows, Linux and Web Server Hacking. The report contains from the following sections:

- Part A: Setup Lab:
- Part B: Trojens and Backdoors and Viruses
- Part C: System Hacking
- Part D: Hacking Web Servers
- Part E: Windows and Linux Hacking

You can download all hacking tools and materials from the following websites

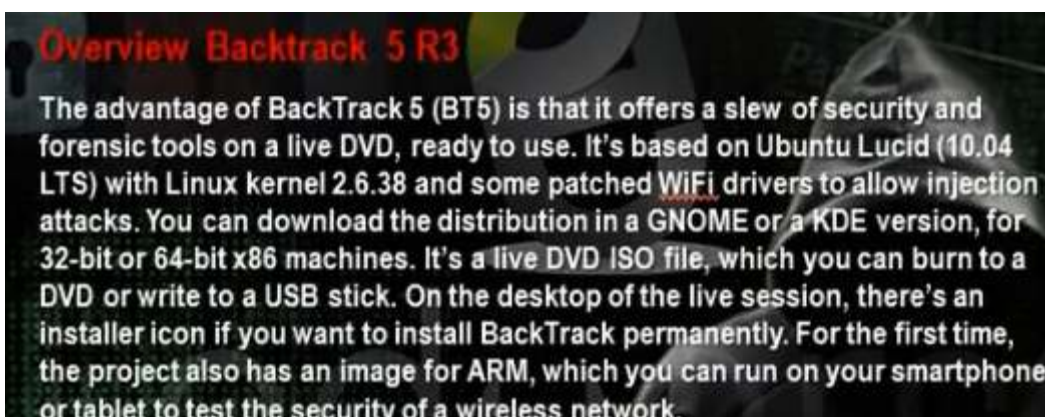
<http://www.haxf4rall.com/2016/02/13/ceh-v9-pdf-certified-ethical-hacker-v9-courseeducatonal-materials-tools/>

www.mediafire.com%2Ffolder%2Fad5szsted5end%2FEduors_Professional_Ethical_Hacker&h=gAQGad5Hf

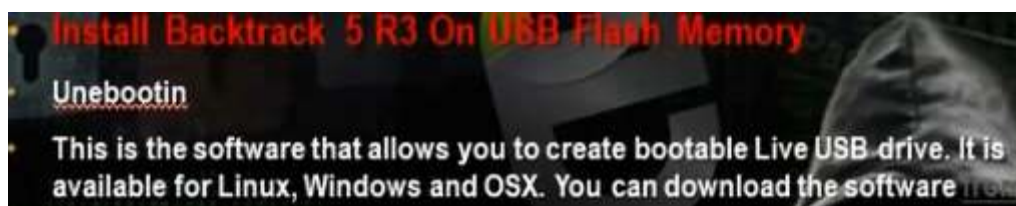
2. Part A: Setup Lab

a) Setup lab

- From the virtualization technology with software VMware or virtual box we can do more than one virtual machines, one linux and other windows 2007 or windows Xp
- Download vmware and install it
- Create folder edurs-vm in non-windows partition. Create a folder for each operating system
- Install any windows operating system.
- Download backtrack



- To install backtrack on usb, download unebootin. We need also to use the tool to support booting from flash memory in vmware.



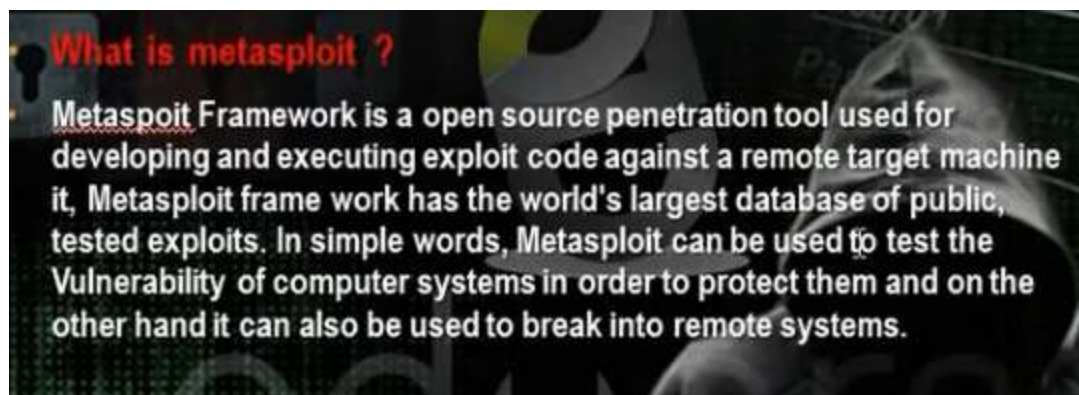
- Download and install kali linux

A presentation slide titled "Overview Kali Linux" with a background image of a person in a hoodie. The slide contains a bulleted list of information about Kali Linux.

- **Overview Kali Linux**
- Kali Linux is an advanced Penetration Testing and Security Auditing Linux distribution.
- **Kali Linux Features**
- Kali is a complete re-build of BackTrack Linux, adhering completely to Debian development standards. All-new infrastructure has been put in place, all tools were reviewed and packaged, and we use Git for our VCS.
- More than 300 penetration testing tools:
- Free and always will be
- Open source Git tree:
- **Download**
- <http://www.kali.org/downloads/>

The Kali Linux logo is visible in the bottom right corner.

- Download and install metasploit.

A presentation slide titled "What is metasploit ?" with the same background image as the first slide. It contains a paragraph describing the Metasploit Framework.

What is metasploit ?

Metasploit Framework is a open source penetration tool used for developing and executing exploit code against a remote target machine it, Metasploit frame work has the world's largest database of public, tested exploits. In simple words, Metasploit can be used to test the Vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems.


Metasploit is big project that contains a lot of modules or programs. These modules or programs can utilize the holes in windows machines or linux machines operating systems. For any hole that occur in the operating systems, we can develop the program that can utilize this hole. We can work on it through command line or graphical interface. The programs that use graphical interface are armitage and Koblet Strike . In linux we can update the metasploite using command msfupdate.

2. Part B: Trojens and Backdoors and Viruses

a) Backdoors

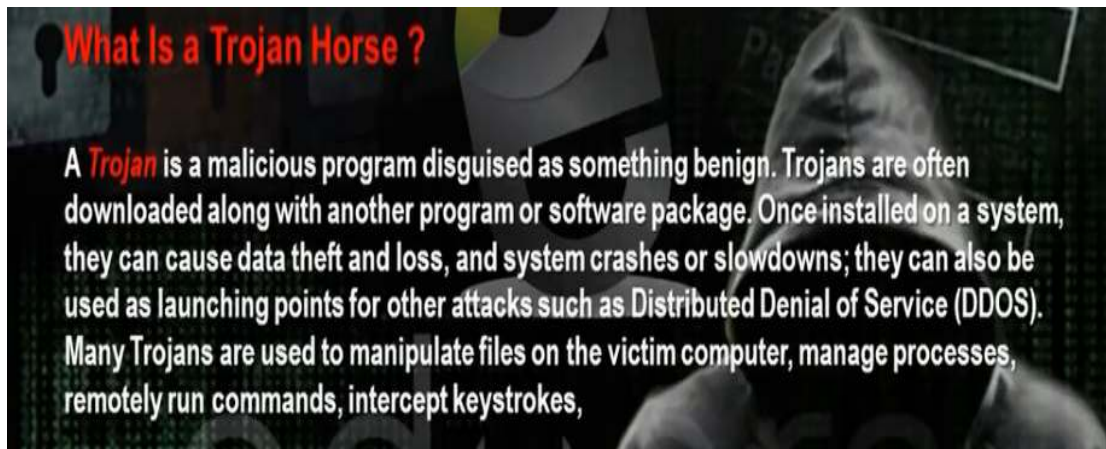
What is Backdoors ?

- A **backdoor** is a means of access to a computer program that bypasses security mechanisms. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. However, attackers often use back doors that they detect or install themselves
- A **backdoor** is a program or a set of related programs that a hacker installs on a target system to allow access to the system at a later time. A backdoor's goal is to remove the evidence of initial entry from the system's log files. But a backdoor may also let a hacker retain access to a machine it has penetrated even if the intrusion has already been detected and remedied by the system administrator.



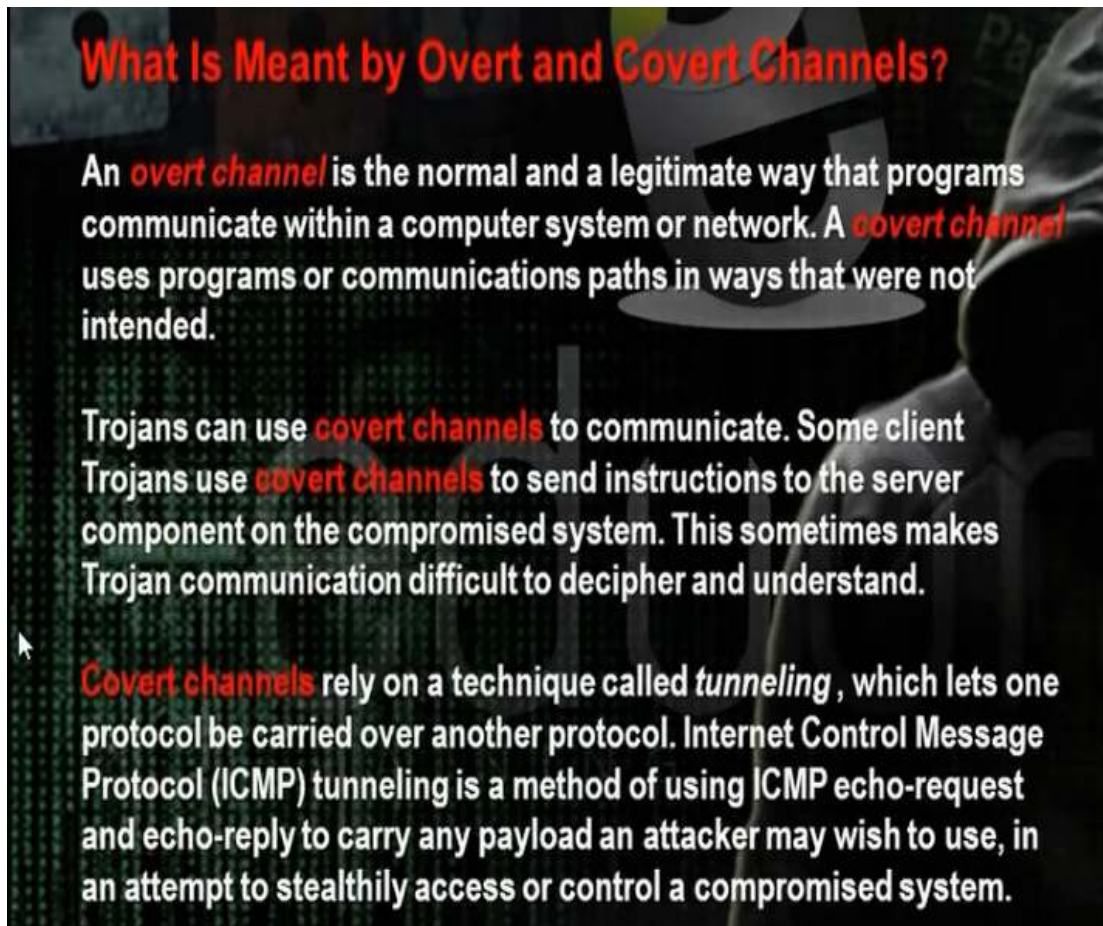
The backdoor is the backdoor that through it we can make access on the machine and we can make bypass to the existing security policies. Microsoft has a backdoors that enables it to make remote access on the machine.

b) Torjen Horse:



Trojen horse is a good program that carries bad program. When the client download the good program, it will download with it the trojen program also so the hacker can access the machine.

c) Overt channel and Covert Channel:



What Is Meant by Overt and Covert Channels?

An **overt channel** is the normal and a legitimate way that programs communicate within a computer system or network. A **covert channel** uses programs or communications paths in ways that were not intended.

Trojans can use **covert channels** to communicate. Some client Trojans use **covert channels** to send instructions to the server component on the compromised system. This sometimes makes Trojan communication difficult to decipher and understand.

Covert channels rely on a technique called *tunneling*, which lets one protocol be carried over another protocol. Internet Control Message Protocol (ICMP) tunneling is a method of using ICMP echo-request and echo-reply to carry any payload an attacker may wish to use, in an attempt to stealthily access or control a compromised system.

The overt channel means that any program when run makes for it channel between it and the system. The covert channel means that the program will use the channel in the wrong direction to access the machine.

d) Different Types of Trojans:

List the Different Types of Trojans

Trojans can be created and used to perform different attacks. Some of the most common types of Trojans are:

Remote Access Trojans (RATs) —used to gain remote access to a system

Data-Sending Trojans—used to find data on a system and deliver data to a hacker

Destructive Trojans—used to delete or corrupt files on a system

Denial of Service Trojans—used to launch a denial or service attack

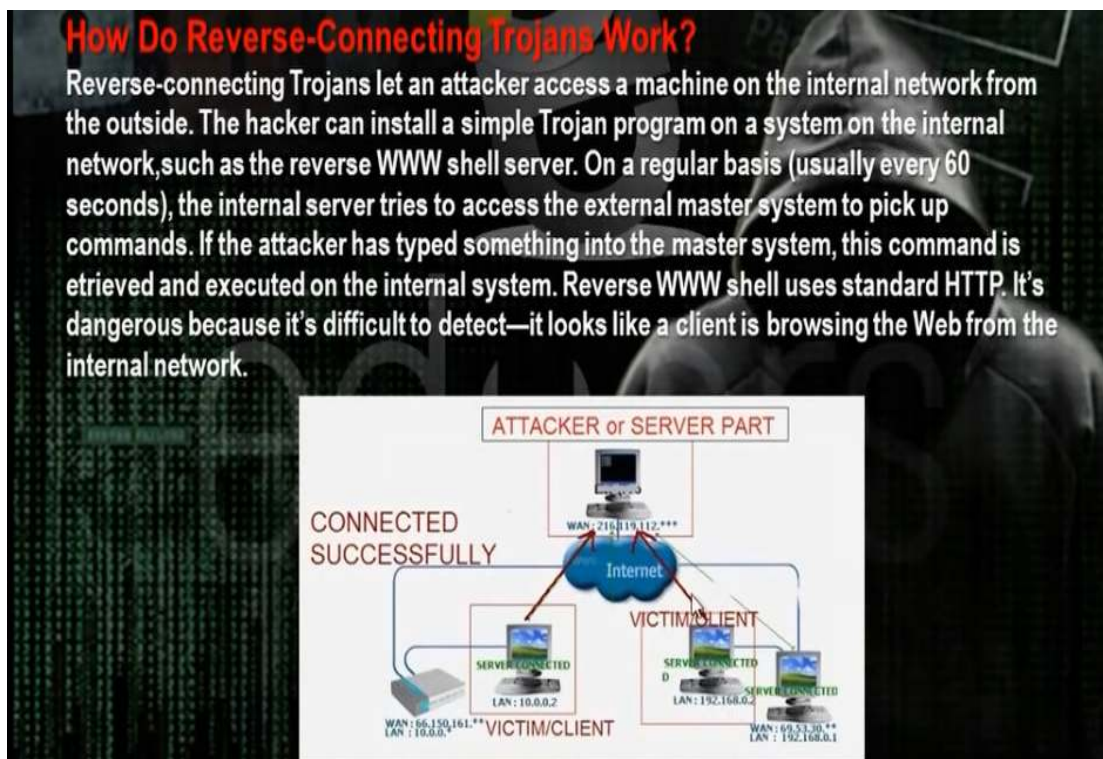
Proxy Trojans—used to tunnel traffic or launch hacking attacks via other system

FTP Trojans—used to create an FTP server in order to copy files onto a system

Security software disabler Trojans—used to stop antivirus software

e) How Do Reverse Connecting Torjans work :

Trojan program in the hacker computer which creates server that installed in the client computer. In the reverse connection technique, the server on the client computer will make connection to the Trojan program on the hacker machine. We have problem that the hacker needs constant real ip that does not change.



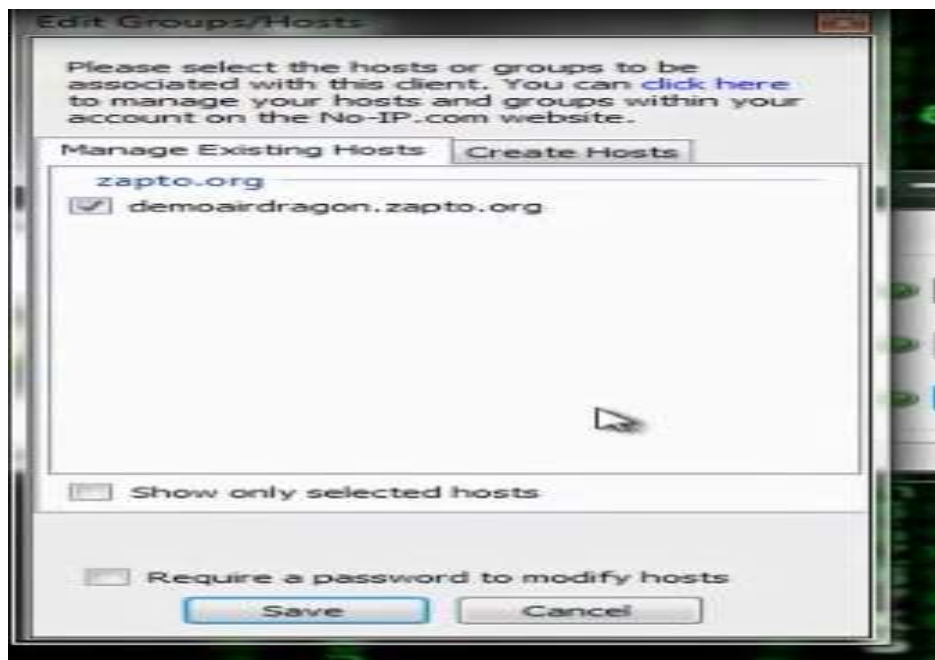
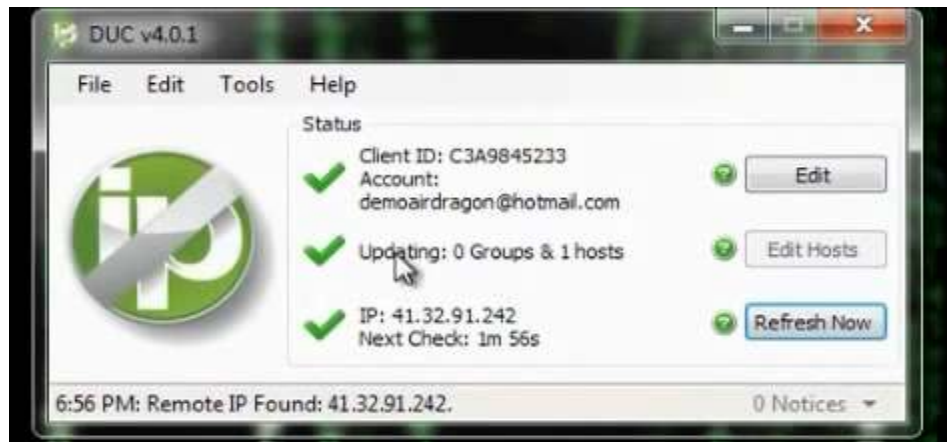
- Windows Torjans Tools are Biforst and Poison Ivy
- We must make port forward and dynamic dns. Go to basics then nat in the router configuration website. Choose the start and end port number and the internal ip of the hacker computer. We need to make the ip of the hacker computer static and same as the ip in the router configuration. It means if the router will come to the real ip of the router at port 81, it must forward the hacker computer with the internal ip 192.168.1.150 at port 81.

- The problem that the real ip of the router not constant and changing. One solution that we buy real ip. To buy real ip, we need to have phone line registered for the hacker. So better solution is to register for dynamic domain name in dynamic dns server. This domain name will point to the real ip of the router. If the real ip changes, the router will change the data in the dynamic dns server. The client Trojan will make connection with the dynamic dns server and it tell him the real ip of the router. So the Trojan makes the connection to the router at the port given in the Trojan program and the router will make port forward to the hacker computer.

NAT - Virtual Server	
Virtual Server for	PVC0 - Multiple IP Account
Rule Index	1 ▾
Application	Bifrost - ▾
Protocol	ALL ▾
Start Port Number	81
End Port Number	81
Local IP Address	192.168.1.150
Start Port(Local)	81
End Port(Local)	81

Virtual Server Listing							
Rule	Application	Protocol	Start Port	End Port	Local IP Address	Start Port(Local)	End Port(Local)
1	Bifrost	ALL	81	81	192.168.1.150	81	81
2	Poison	ALL	3460	3460	192.168.1.150	3460	3460

- The site no-ip.com can provide dynamic dns. Register, then choose add host.
- Download and setup the no-ip program at hacker computer.



- You can utilize a property in routers called dynamic dns

HG520b

- Status
- Basic
- Advanced
 - RIP
 - Security
 - Firewall
 - Filter
 - QoS
 - Port Mapping
 - TimeZone
 - ACL
 - TR069
 - UPnP
 - DDNS
 - Option60
- Tools

Dynamic DNS

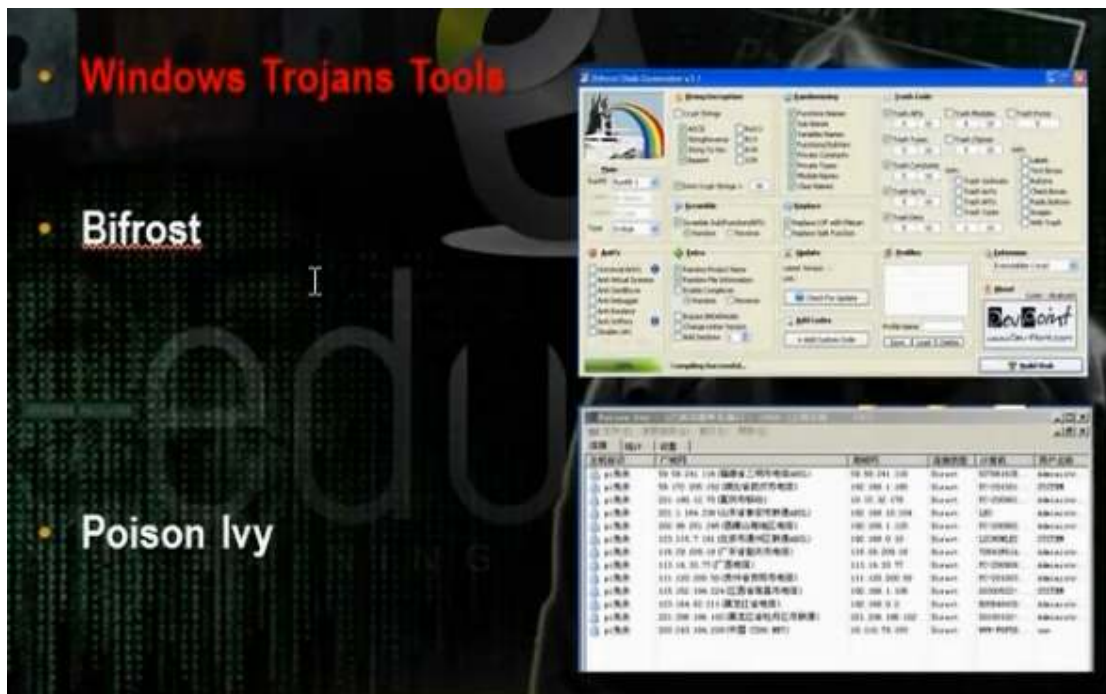
Active	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Service Provider	www.dyndns.org	
Host Name		
E-mail Address		
User		
Password		
Enable Wildcard	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable

Submit

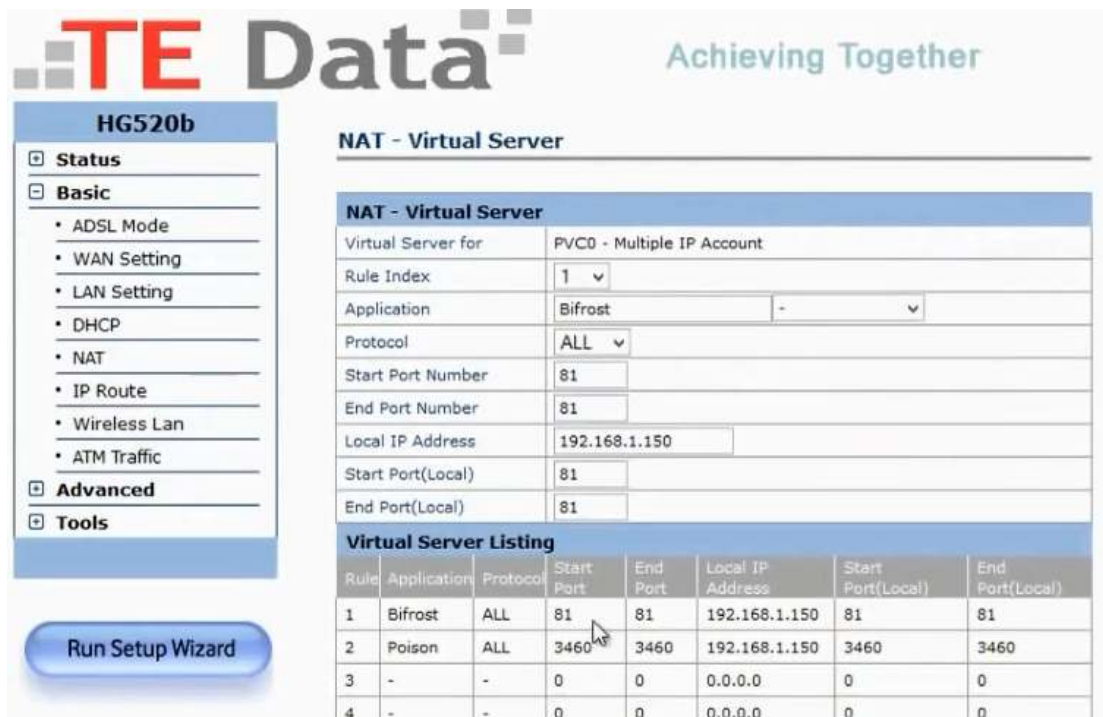
Copyright © 2009 All Rights Reserved.

- Register for account in dyndns.com and put the registration information in the router configuration. When the router restarts, it will register its ip in dynamic dns.
- We can use VPS machine. VPS will have real IP and it is a device connected directly to internet and we put through it Trojan program. The Trojan server in the client will make reverse connection to this real IP so the real IP will not change and VPS up in 24hrs.

f) Windows Torjan Tools :



- Download bifrost. The bifrost has small size and accept encryption in many ways. Make registration.
- Make the port forward at the router.

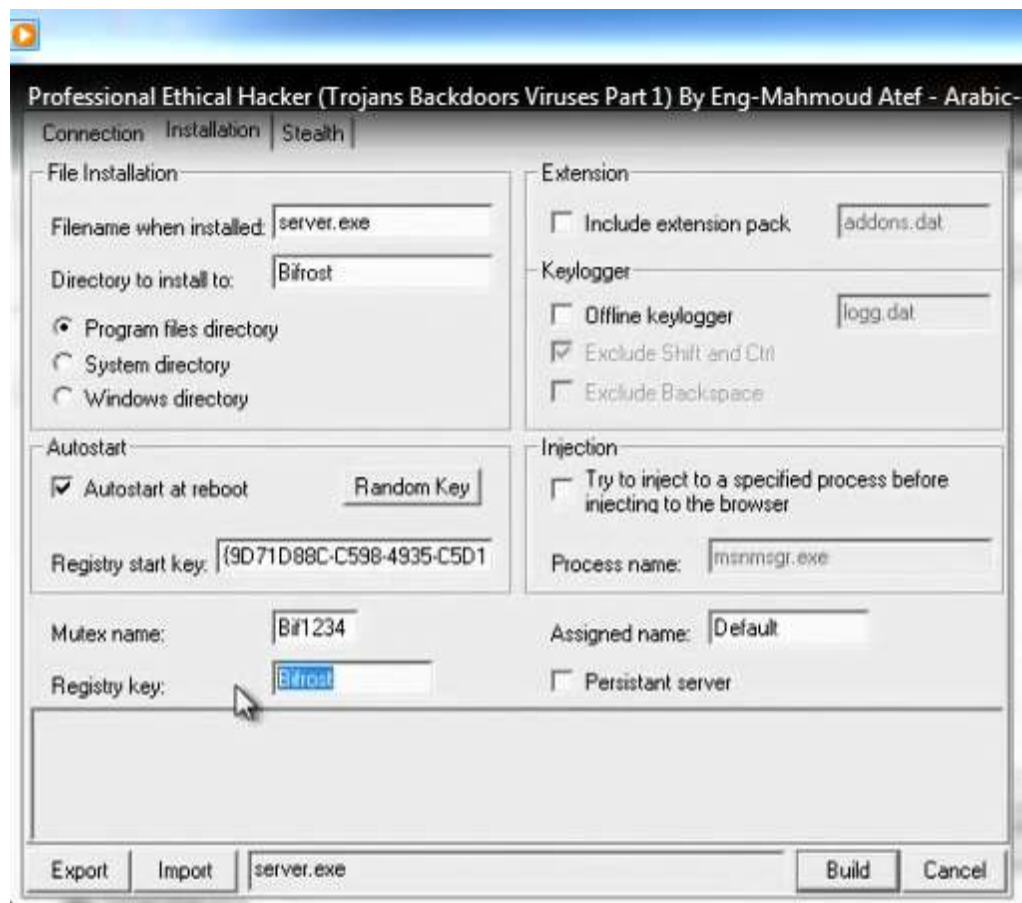
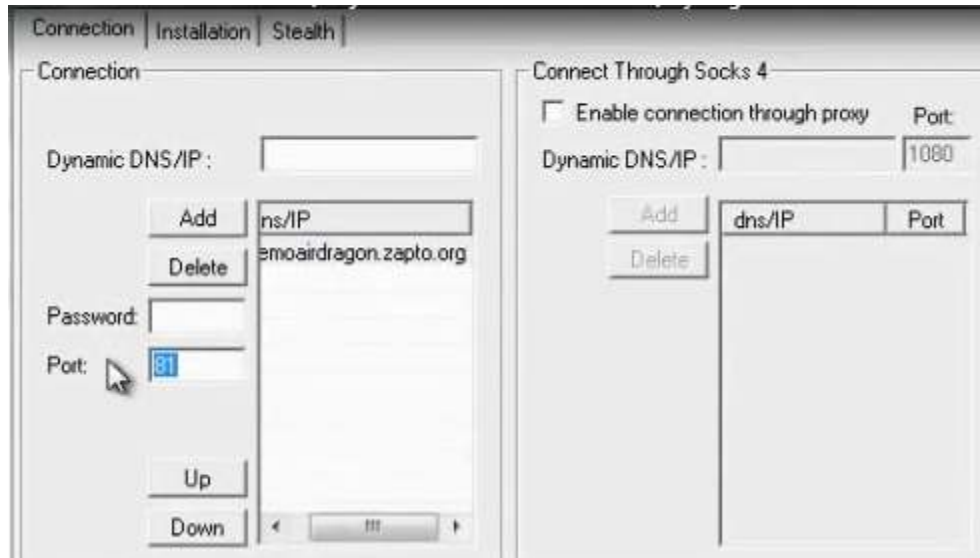


- Then go bifrost stub customizer and generate the trojan with the following settings. The file generated will be Customized.

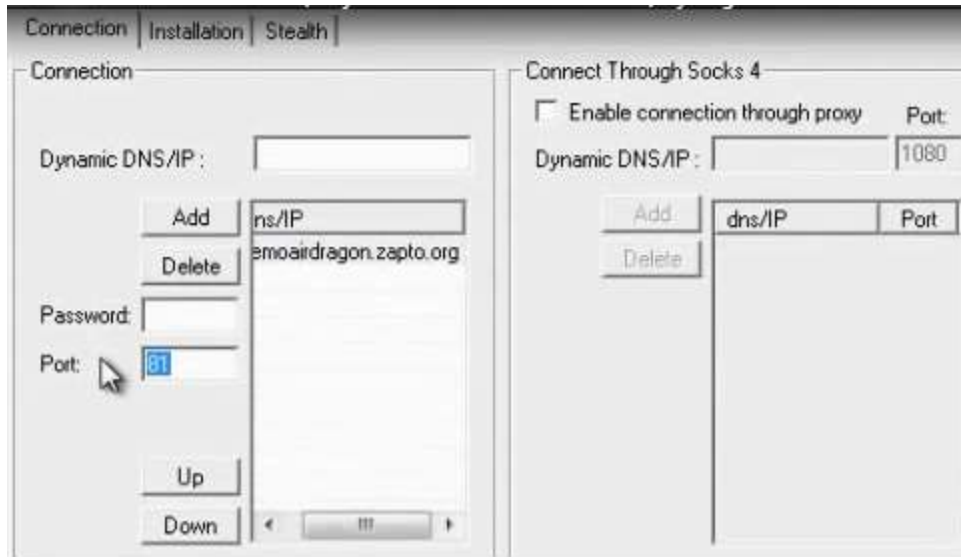


- Open the program bifrost. Put the dynamic dns name and the port number the Trojan program will

work.



- We put the customize file in the machine we want to attack and we can browse the machine



- Build the program. Give him the file output of the customizer Customized.
- Send the file to the client you want to hack.
- When the client access the Trojan file, we will get notice of reverse connection



- Choose file manager on the machine you received