BackTrack 5 training guide: Part V - Pen-testing in a nutshell

Karthik R, Contributor

You can read the original story here, on SearchSecurity.in.

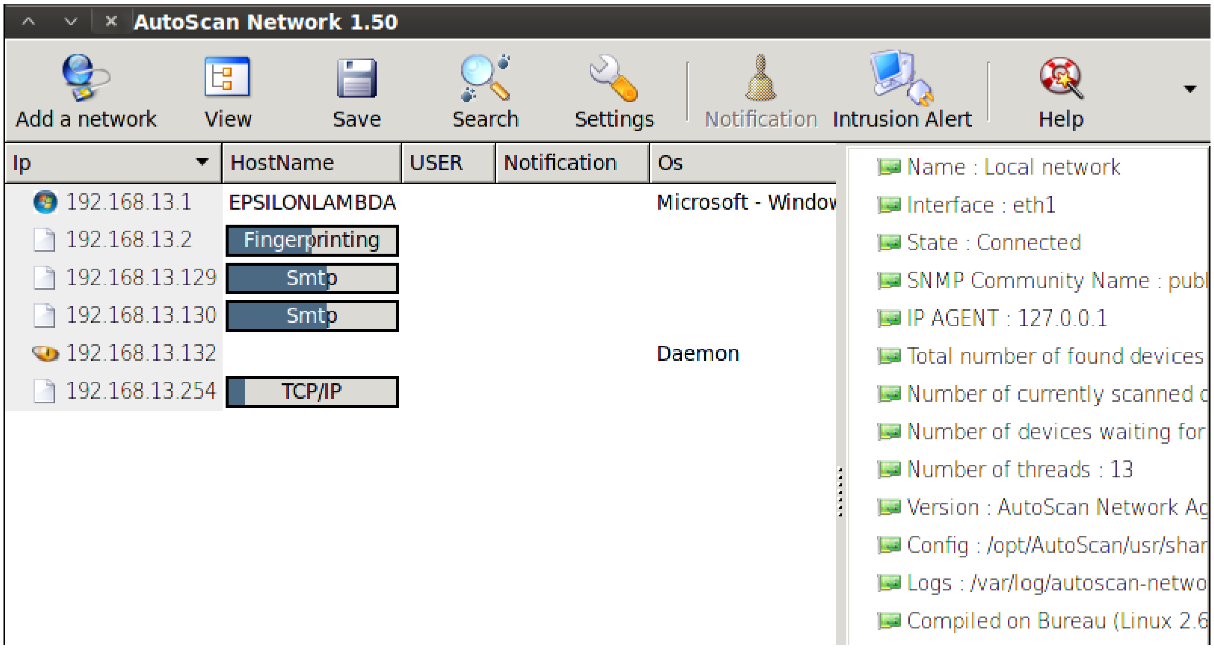
The first four installments of our BackTrack 5 training guide explained each phase of the penetration testing process in detail. Our final installment recaps all that has been covered so far, and discusses various aspects of ethical hacking and penetration testing.

For this installment of the BackTrack 5 training guide, the lab setup is as follows: A virtual machine running on Windows 7, a BackTrack 5 instance in the VM, and a few Windows systems. Let us go through each step of the attack process as we attempt to penetrate this network.

Autoscan Network on BT5

Once connected to the network, the first step in this BackTrack 5 training guide is to sweep the network and check for live systems. To accomplish this, we use the tool AutoScan Network 1.5 on BackTrack 5. The path to this tool is as follows:

Applications>Backtrack>Information gathering>Network analysis>Network scanners>Autoscan



Ip	HostName	USER	Notification	Os
192.168.13.1	EPSILONLAMBDA			Microsoft - Windov
192.168.13.2	Fingerprinting			
192.168.13.129	Smtp			
192.168.13.130	Smtp			
192.168.13.132				Daemon
192.168.13.254	TCP/IP			

Name : Local network
Interface : eth1
State : Connected
SNMP Community Name : publ
IP AGENT : 127.0.0.1
Total number of found devices
Number of currently scanned d
Number of devices waiting for
Number of threads : 13
Version : AutoScan Network Ag
Config : /opt/AutoScan/usr/shar
Logs : /var/log/autoscan-netwo
Compiled on Bureau (Linux 2.6

Figure 1. *AutoScan Network 1.50 in action*

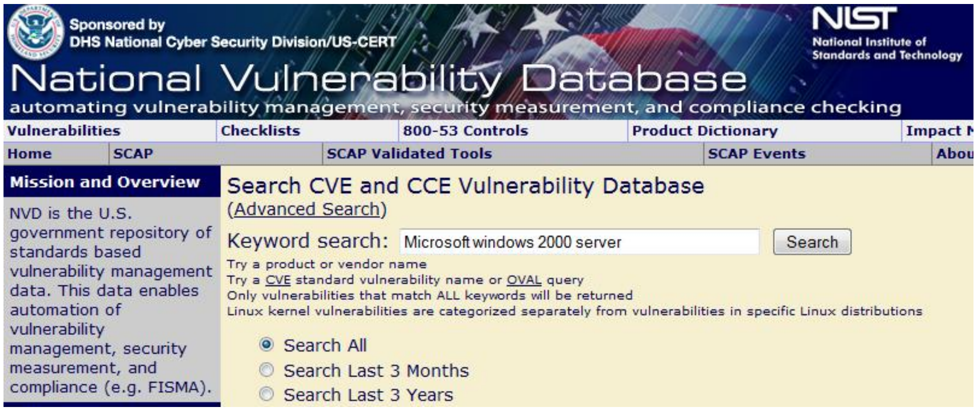
Figure 1 depicts the AutoScan Network in action. This tool provides various options for adding a range of IP addresses to scan. Once the scan is launched, it lists IP addresses and details such as hostname, users and operating systems running on the network. Figure 1 shows that SMTP, TCP/IP and fingerprinting scans happen automatically. This tool also helps in detecting intrusion alerts within the network. There is also an option to save a particular instance of the scan.

As explained in previous installments of this BackTrack 5 training guide, you can also use NMAP to check if the system is alive, for sweeping the network, banner grabbing, fingerprinting, and so on. Once the list of systems is obtained, we have a clear picture of the operating systems running, as well as the IPs that are live. Before launching an attack, we will perform vulnerability research on our target.

Suppose the target system is a Windows 2000 Server, which is running on 192.168.13.129. Vulnerability databases can be checked for information, using tools such as Nessus or OpenVAS. However, for our BackTrack 5 training guide, we will perform vulnerability scans on the target manually.

Online vulnerability database

The popular National Vulnerability Database at http://web.nvd.nist.gov/view/vuln/search provides information on various vulnerabilities of a particular system.


Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
800-53 Controls
Product Dictionary
Impact M
Home
SCAP
SCAP Validated Tools
SCAP Events
Abou
Mission and Overview
Search

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Search CVE and CCE Vulnerability Database

(Advanced Search)

Keyword search: Microsoft windows 2000 server

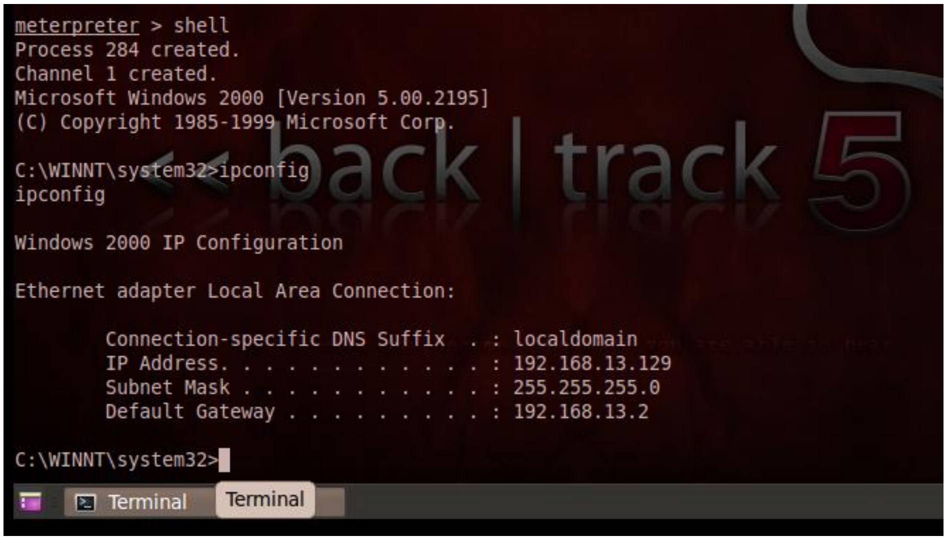
Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

● Search All
○ Search Last 3 Months
○ Search Last 3 Years

Figure 2. *National Vulnerability Database search engine*

Penetrating the target

For our BackTrack 5 training guide, we will use the vulnerability in Windows 2000 Server's RPC DCOM port that allows remote code execution, and leads to buffer overflow. In the Metasploit tutorial we have seen how to exploit the vulnerability of a target. We have spawned a meterpreter shell on the Windows 2000 Server i.e. 192.168.13.129, as shown in **Figure 3**. BackTrack 5 offers other privileges such as SET, which can be used to penetrate the system.



```
meterpreter > shell
Process 284 created.
Channel 1 created.
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>ipconfig
ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 192.168.13.129
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.13.2

C:\WINNT\system32>
```

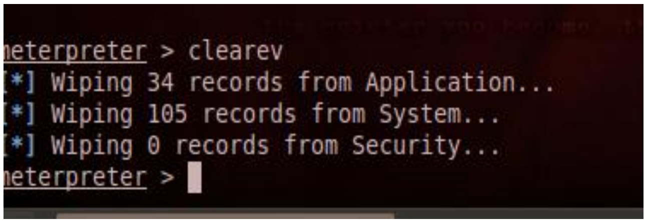
Figure 3. *Inside Windows 2000 Server*

Once inside the system, several details about the system can be obtained. Following are a few of the important commands that can be executed:

1. **Hashdump**
   This command dumps the hashes (NT/LM) of the target system, which can later be cracked using privilege escalation software, such as John the Ripper.
2. **Sysinfo**
   A sysinfo command on the target would give us the basic system details such as the OS, vendor, admin name, and so on.
3. **Execute**
   This command is very powerful. Here, we can run any file of our choice on the target system. Even the promiscuous mode of operation is facilitated by the meterpreter shell.
4. **Portfwd**
   This powerful command allows the execution of remote service on a port of the target. This can be used to create a backdoor to the target, enabling hassle-free access in the future.

Clearing the traces

The next part of this BackTrack 5 training guide covers clearing any traces of the attack in the target system. A simple **clearev** command clears the event logs in the system, leaving no trace of any unauthorized presence (**Figure 4).**



```
neterpreter > clearev
[*] Wiping 34 records from Application...
[*] Wiping 105 records from System...
[*] Wiping 0 records from Security...
neterpreter >
```

Figure 4. Clearev in action

Windows maintains application logs, system logs and security logs. The screenshot in **Figure 5** shows them in the target system.

The **clearev** command clears the logs in these categories and leaves no traces of any penetration. Of course, an astute system administrator would immediately suspect something amiss on seeing the entire log entries cleared. It is thus advisable to set up backdoors and rootkits to maintain access for extended periods of time.

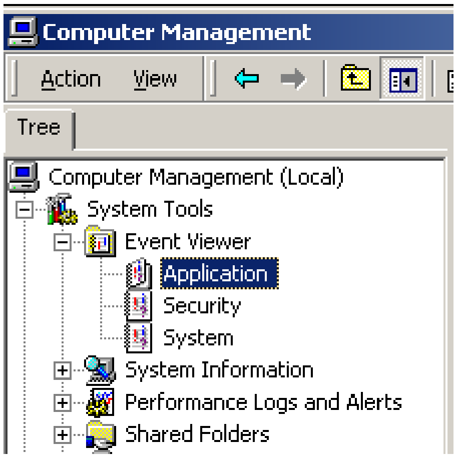


***Figure 5**. Event logs in Windows 2000 Server*

Overview of Windows security model

The Windows security model is pretty simple. Every user has a unique SID (security identifier). The SID is of the following form:

S-1-5-21-9867453210-2389765341-23768956-1023

Red - Revision level
Green – Identified Authority Value
Orange – Domain or local ID
Peach – Relative ID

Subsequent to login, several processes are created on behalf of each user. Each process is assigned a token, defining the privileges accorded to the associated user. The SID forms part of the token.

In our Metasploit tutorial earlier, we used the **steal_token** command on meterpreter to change tokens for elevating and exchanging privileges with other user groups. The users we came across included ‘system’ and ‘administrator’.

To sum up

Our BackTrack 5 training guide has discussed penetration into a system on the network from scratch. We started with network sweeping and gathering of information in the initial phase, and followed with vulnerability research using an online vulnerability database.

We also performed an attack on the system, checked a few important commands in the post-exploitation section, and finally cleared any traces of our attack. We also briefly covered the Windows security model.

This concludes our BackTrack 5 training guide series that focused on important aspects of information security, especially ethical hacking. Here's wishing you safe and happy ethical hacking with BackTrack 5!

About the author: ***Karthik R*** *is a member of the NULL community. Karthik completed his training for EC-council CEH in December 2010, and is at present pursuing his final year of B.Tech. in Information Technology, from National Institute of Technology, Surathkal. Karthik can be contacted on rkarthik.poojary@gmail.com. He blogs at http://www.epsilonlambda.wordpress.com*

You can subscribe to our twitter feed at @SearchSecIN. You can read the original story here, on SearchSecurity.in.