# Ethics in IT

## Class 8

## Lab 6

UNITED TRUST

bdeducation
Bangladesh Digital Education Research Limited
সময়ের পাঠশালা

## Lab Objectives:

- ●Tools of hacking

In this lab, we will discuss in brief some of famous tools that are widely used to prevent hacking and getting unauthorized access to a computer or network system.

## NMAP

Nmap stands for Network Mapper. It is an open source tool that is used widely for network discovery and security auditing. Nmap was originally designed to scan large networks, but it can work equally well for single hosts.

Nmap can determine −

√ what hosts are available on the network,

√ what services those hosts are offering,

√ what operating systems they are running on,

√ what type of firewalls are in use, and other such characteristics.

Nmap runs on all major computer operating systems such as Windows, Mac OS X, and Linux.

## Metasploit

Metasploit is one of the most powerful exploit tools. It comes in two versions − commercial and free edition. Matasploit can be used with command prompt or with Web UI.

With Metasploit, you can perform the following operations −

- √ Conduct basic penetration tests on small networks
- √ Run spot checks on the exploitability of vulnerabilities
- √ Discover the network or import scan data
- √ Browse exploit modules and run individual exploits on hosts

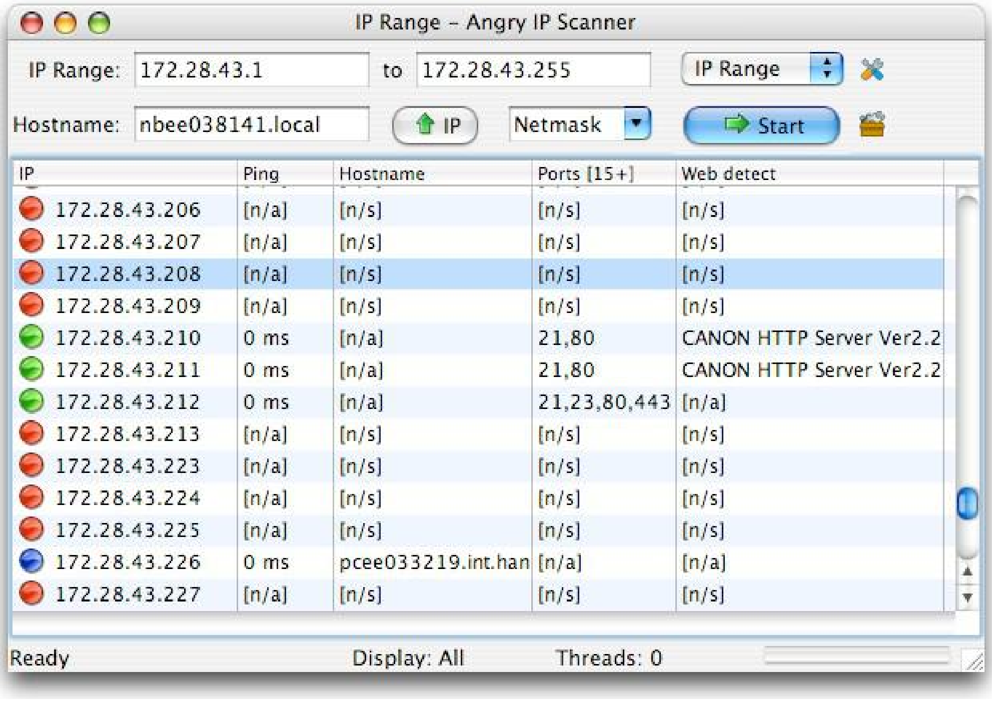
## Burp Suit

Burp Suite is a popular platform that is widely used for performing security testing of web applications.

## Angry IP Scanner

Angry IP scanner is a lightweight, cross-platform IP address and port scanner. It can scan IP addresses in any range.

Angry IP Scanner simply pings each IP address to check if it’s alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc.



IP Range – Angry IP Scanner

IP Range: 172.28.43.1 to 172.28.43.255 IP Range

Hostname: nbee038141.local

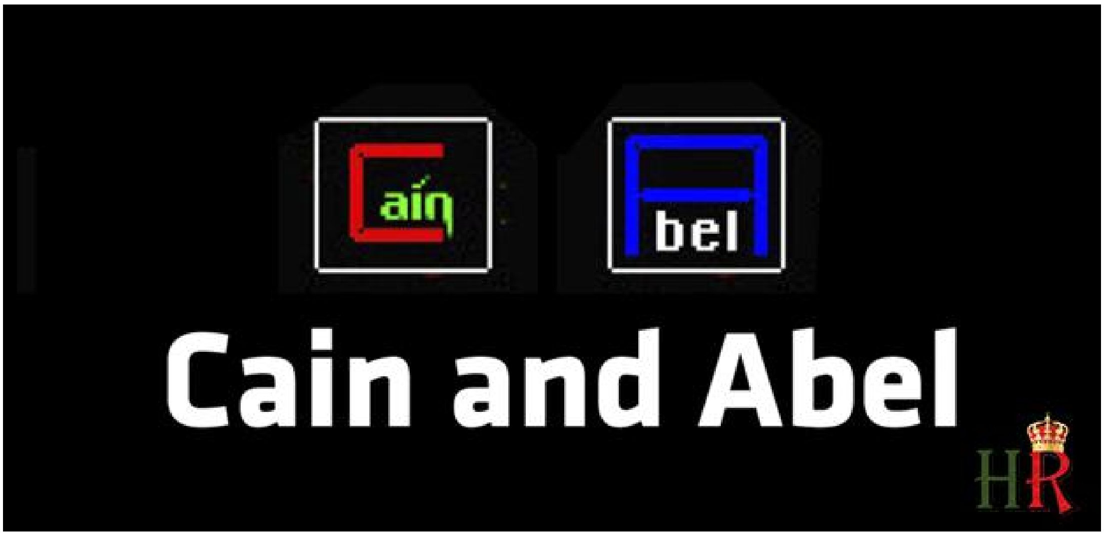
Netmask

| IP | Ping | Hostname | Ports [15+] | Web detect |
|---|---|---|---|---|
| 🔴 172.28.43.206 | [n/a] | [n/s] | [n/s] | [n/s] |
| 🔴 172.28.43.207 | [n/a] | [n/s] | [n/s] | [n/s] |
| 🔴 172.28.43.208 | [n/a] | [n/s] | [n/s] | [n/s] |
| 🔴 172.28.43.209 | [n/a] | [n/s] | [n/s] | [n/s] |
| 🟢 172.28.43.210 | 0 ms | [n/a] | 21,80 | CANON HTTP Server Ver2.2 |
| 🟢 172.28.43.211 | 0 ms | [n/a] | 21,80 | CANON HTTP Server Ver2.2 |
| 🟢 172.28.43.212 | 0 ms | [n/a] | 21,23,80,443 | [n/a] |
| 🔴 172.28.43.213 | [n/a] | [n/s] | [n/s] | [n/s] |
| 🔴 172.28.43.223 | [n/a] | [n/s] | [n/s] | [n/s] |
| 🔴 172.28.43.224 | [n/a] | [n/s] | [n/s] | [n/s] |
| 🔴 172.28.43.225 | [n/a] | [n/s] | [n/s] | [n/s] |
| 🔵 172.28.43.226 | 0 ms | pcee033219.int.han | [n/a] | [n/a] |
| 🔴 172.28.43.227 | [n/a] | [n/s] | [n/s] | [n/s] |

Ready Display: All Threads: 0

## Cain & Abel

Cain & Abel is a password recovery tool for Microsoft Operating Systems. It helps in easy recovery of various kinds of passwords by employing any of the following methods −



Cain & Abel is a useful tool for security consultants, professional penetration testers and everyone else who plans to use it for ethical reasons.

## Ettercap

Ettercap stands for Ethernet Capture. It is a network security tool for Man-in-the-Middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks. Ettercap has inbuilt features for network and host analysis. It supports active and passive dissection of many protocols.

## EtherPeek

EtherPeek is a wonderful tool that simplifies network analysis in a multi protocol network environment. EtherPeek is a small tool (less than 2 MB) that can be easily installed in a matter of few minutes.

## SuperScan

SuperScan is a powerful tool for network administrators to scan TCP ports and resolve hostnames.

## QualysGuard

QualysGuard is an integrated suite of tools that can be utilized to simplify security operations and lower the cost of compliance. It delivers critical security intelligence on demand and automates the full spectrum of auditing, compliance and protection for IT systems and web applications.

QualysGuard includes a set of tools that can monitor, detect, and protect your global network.

## WebInspect

WebInspect is a web application security assessment tool that helps identify known and unknown vulnerabilities within the Web application layer.

It can also help check that a Web server is configured properly, and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and more.

## LC4

LC4 was formerly known as L0phtCrack. It is a password auditing and recovery application. It is used to test password strength and sometimes to recover lost Microsoft Windows passwords, by using dictionary, brute-force, and hybrid attacks.