Ethical Hacking and Penetration Testing

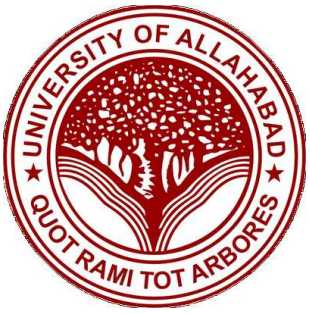
Submitted in
Partial fulfillment of the requirement for the award of
the degree
Bachelor of Computer Application

By

Rishabh Upadhyay
(12AU/135)

Under Guidance of

Professor R.R. Tewari
(Course Coordinator)



Centre of Computer Education
Institute of Professional Studies
University Of Allahabad
Allahabad
2014

ACKNOWLEDGEMENT

This Project itself is an acknowledgement to the inspiration, drive and technical assistance contributed by many individuals. This project would have never seen the light of this day without the help and guidance I have received.

I am pleased to acknowledge my indebtedness to the Head of the Department, Professor R.R. Tewari for gracious encouragement and proper guidance.

I would like to express my profound thanks to Mr.Ashutosh Verma , Mr.Rahul Mishra, Mr. Ashraf Narvi,Mr.Ashish Agarwal and other faculty members for their help and guidance throughout my project tenure.

I owe an incalculable debt to all staffs of Center of Computer Education for their direct and indirect help.

I extend my heartfelt thanks to my parents, friends and well-wishers for their support and timely help.

Above all I thank the Almighty for His blessing and providing mercies at all stages of my work.

Rishabh Upadhyay

CERTIFICATE

It is certified that Mr. RISHABH UPADHYAY of Bachelor of Computer Application, Centre of Computer Education, Institute of Professional Studies, and University of Allahabad has carried out the project work on 'ETHICAL HACKING AND PENETRATION TESTING' under my guidance. The student has tried to understand the involved concepts. To the best of my knowledge a similar work has not been submitted at any other institution for the award of any degree or diploma.

Professor R.R.Tewari
Head of Department
Centre of Computer Education
Institute of Professional Studies
University Of Allahabad

CONTENTS

Objective of the Project

- Pen Test University of Allahabad Local Area Network.
- Network Mapping: Locate Important Host and Services, Firewall and Switches and Hubs.
- Develop a Simple Network Scanner.
- Demonstrate Some Attacks.

Introduction

Hacker vs Ethical Hacker

- **Hacker:** A person who invades or interferes with another system with the intent to cause harm, without having any permission from the system owner.

- **Ethical hacker:** A professional hired by an organization to review its security posture from the eyes of the hacker. Ethical hackers test vulnerabilities of the systems.

What is Penetration Testing?

"The process of evaluating ***systems***, ***applications,*** and ***protocols*** with the intent of identifying vulnerabilities *usually* from the perspective of an unprivileged or anonymous user to **determine potential real world impacts…**"

Penetration Testing an active analysis of the system for any potential vulnerabilities that could result from poor or improper system configuration, either known and unknown hardware or software flaws, or operational weaknesses. The whole process involves a written consent and rules of engagement from the client, which clearly spell what they can or cannot do.

Types of Penetration Testing

White box testing, also known as clear box testing or glass box testing, is a **penetration testing** approach that uses the knowledge of the internals of the target system to elaborate the test cases. In application penetration tests the source code of the application is usually provided along with design information, interviews with developers/analysts, etc.
In infrastructure penetration tests network maps, infrastructure details, etc. are provided. The goal of a white box penetration test is to provide as much information as possible to the penetration tester so that he/she can gain insight understanding of the system and elaborate the test based on it.

White box penetration testing has some clear benefits:

- Deep and thorough testing
- Maximizes testing time
- Extends the testing area where black box testing cannot reach (such as quality of code, application design, etc.)

However, there are also some disadvantages:

- Nonrealistic attack, as the penetration tester is not in the same position as an non-informed potential attacker

Black box penetration test requires no previous information and usually takes the approach of an uninformed attacker. In a black box penetration test the penetration tester has no previous information about the target system.

The benefits of this type of attack are:

- It simulates a very realistic scenario

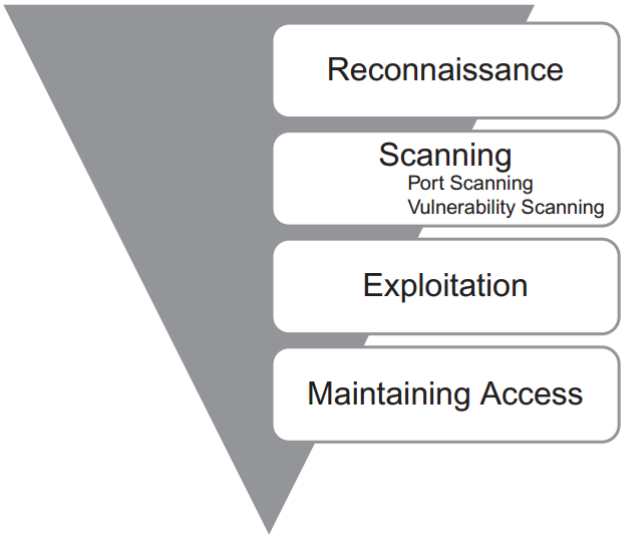
The disadvantages of a black box penetration test are:

- Testing time cannot be maximized in certain scenarios
- Some areas of the infrastructure might remain untested

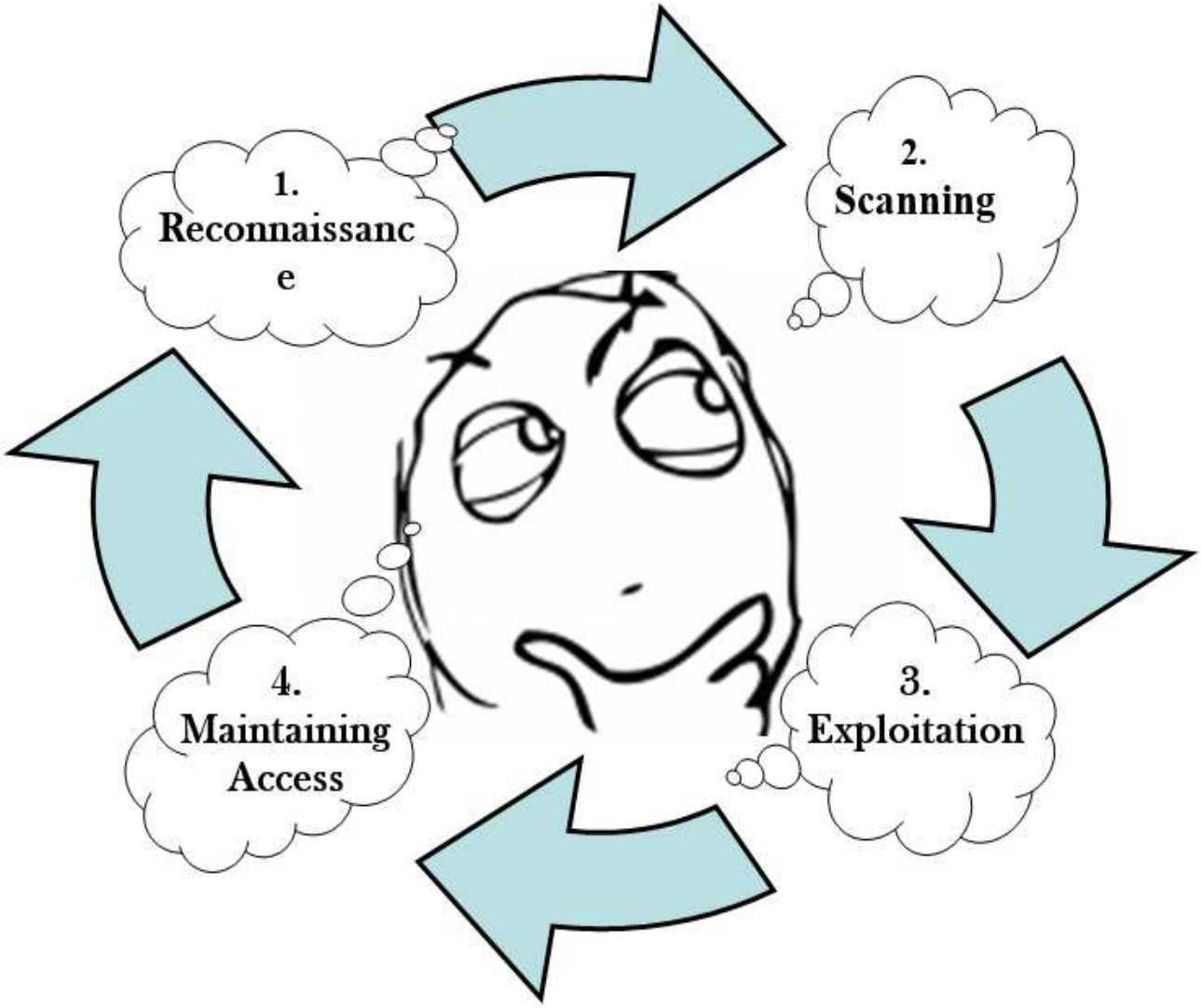
This Project follows Black box Penetration Testing Approach

Penetration Testing Methodology

Penetration Testing Phases follow a drill down approach and focus on more specific details of the target



Life Cycle of Penetration Testing



Reconnaissance:

Reconnaissance denotes the work of information gathering before any real attacks are planned. The idea is to collect as much interesting information as possible about the target. Reconnaissance is probably the longest phase, sometimes lasting weeks or months. The black hat uses a variety of sources to learn as much as possible about the target business and how it operates, including

- Internet searches
- Social engineering
- Dumpster diving
- Domain name management/search services
- Non-intrusive network scanning

The activities in this phase are not easy to defend against. Information about an organization finds its way to the Internet via various routes. Employees are often easily tricked into providing bits of information which, over time, act to complete a complete picture of processes, organizational structure, and potential soft-spots. However, there are some things you can do which make it much harder for an attacker, including

- Make sure your systems don't leak information to the Web, including:
  - Software versions and patch levels
  - Email addresses
  - Names and positions of key personnel
- Ensure proper disposal of printed information
- Provide generic contact information for domain name registration lookups
- Prevent perimeter LAN/WAN devices from responding to scanning attempts

HTTrack:Website Copier,Google Dorks,The Harvester, Whois,Netcraft,NSLookup,Dig,Social Engineering

Scanning:

Once the attacker has enough information to understand how the business works and what information of value might be available, he or she begins the process of scanning perimeter and internal network devices looking for weaknesses, including

- Open ports
- Open services
- Vulnerable applications, including operating systems
- Weak protection of data in transit
- Make and model of each piece of LAN/WAN equipment

Scans of perimeter and internal devices can often be detected with intrusion detection (IDS) or prevention (IPS) solutions, but not always. Veteran black hats know ways around these controls. In any case, some steps you can take to thwart scans include

- Shutting down all unneeded ports and services
- Allow critical devices, or devices housing or processing sensitive information, to respond only to approved devices
- Closely manage system design, resisting attempts to allow direct external access to servers except under special circumstances and constrained by end-to-end rules defined in access control lists
- Maintain proper patch levels on endpoint and LAN/WAN systems

Network Mapper (nmap), Traceroute, Nessus, Hping3
Nikto,WireSkark,Etherape

Exploitation:

Exploitation or Gaining access to resources is the whole point of a modern-day attack. The usual goal is to either extract information of value to the attacker or use the network as a launch site for attacks against other targets. In either situation, the attacker must gain some level of access to one or more network devices.

In addition to the defensive steps described above, security managers should make every effort to ensure end-user devices and servers are not easily accessible by unauthenticated users. This includes denying local administrator access to business users and closely monitoring domain and local admin access to servers. Further, physical security controls should detect attempts at a hands-on attack, and delay an intruder long enough to allow effective internal or external human response (i.e., security guards or law enforcement).

Finally, encrypt highly sensitive information and protect keys. Even if network security is weak, scrambling information and denying attacker access to encryption keys is a good final defence when all other controls fail. But don't rely on encryption alone. There are other risks due to weak security, such as system unavailability or use of your network in the commission of a crime.

Metasploit,Burpsuit,Cain&Able,John The Ripper,
Nessus,Armitage,Sicial Enginer ToolKit,
Ethercap,AirCrack-ng

Maintaining Access:

Having gained access, an attacker must maintain access long enough to accomplish his or her objectives. Although an attacker reaching this phase has successfully circumvented your security controls, this phase can increase the attacker's vulnerability to detection.

In addition to using IDS and IPS devices to detect intrusions, you can also use them to detect extrusions. A short list of intrusion/extrusion detection methods includes

- Detect and filter file transfer content to external sites or internal devices
- Prevent/detect direct session initiation between servers in your data center and networks/systems not under your control
- Look for connections to odd ports or nonstandard protocols
- Detect sessions of unusual duration, frequency, or amount of content
- Detect anomalous network or server behavior, including traffic mix per time interval

NetCat,CryptCat,Hacker Defender,
RootKits,Zues Bots,Trojans

Types of Attacks

Defacing

- Making Alteration to something
- Primarily a Web Site things

Buffer Overflow

- Pieces of data in memory are called **Buffers**
- When too much data is sent ,it can overflow
- Because of stack memory and storing return addresses, a buffer overflow can lead to control of program flow

Format String Attacks

- The C programming language make use of "format string" to determine how the data is going to be input/output

- Leaving off the format string from I/O function can lead to attackers providing.

- This can yield information off the stack being presented to the user

Denial of Service and DDoS

- Any attack or action that prevents a service from being available to its legitimate/authorized user.

- SYN flood,PING flood,SMUR attack , malformed packets

Distributed Denial of Service :

- Overwhelming use of resources
- Often botnets

Sniffing:

- Packet sniffing allows individuals to capture data as it is transmitted over a network.
- Packet sniffer programs are commonly used by network professionals to help diagnose network issues and are also used by malicious users to capture unencrypted data like passwords and usernames in network traffic
- Tools used: WireShark,Cain

Man in the Middle Attack:

- Such type of attack are very easy to launch.
- In this type of attack the ,the attacker poisons the ARP Table(Address Resolution Protocol)
- Hence, can divert all the traffic through its System and can also alter the packets, if he wishes..
- Tools: Etherape,Driftnet

Vulnerability Assessment
&
Penetration Test Report
for
University Of Allahabad

Performed by

Rishabh Upadhyay

Executive Summary

This report presents the results of the vulnerability assessment and penetration test of University of Allahabad and underlying Internet and network infrastructure. The purpose of this assessment is to identify application and network-level security issues that could affect University of Allahabad network infrastructure.

The scope of this exercise includes evaluating the security of the network and application, a attempted to perform unauthorized transactions, obtain confidential information, and determine the overall security of the application by performing a wide variety of vulnerability checks. The testing also included the servers, operating systems and network devices associated with the University.

This result is intended to be an overall assessment of the UoA network, including that of applications that fall within the scope of this project.

Furthermore, the findings in this report reflect the conditions found during the testing, and do not necessarily reflect current conditions.

Introduction

Due to the recent hacking incident I performed the security assessment of the web application and underlying network infrastructure. The purpose of this assessment is to identify network and application-level security issues as well as vulnerabilities affecting the servers and network devices providing access to the organization.

The objective of the analysis is to simulate an attack to assess UoA's immunity level, discover weak links and provide recommendations and guidelines to vulnerable entities discovered. This report is a report which contains sub-sections. Each Sub-section discusses in detail all relevant issues and avenues that can be used by attackers to compromise and gain unauthorized access to sensitive information. Every issue includes an overview, issues found and security guidelines, which, if followed correctly, will ensure the confidentiality and integrity of the systems and applications.

Phase One **(Foot printing and Enumeration)** of the test was executed within UoA premises while phase two (**Scanning, and Exploitation**) was conducted via the Internet from outside the country using Tor (the onion router).

This testing did not explicitly attempt **Denial of Service (DoS)** attacks against any of University of Allahabad (UoA) systems.

However, we performed the security assessment of the external network and web application as an authorized and an unauthorized user.
Login credentials were obtained as part of the testing process. This was a complete **black box test simulating** a typical external hacker's view of the organization.

Target System

IP Addresses Discovered			
172.16.8.3	172.31.1.13	172.31.1.15	172.16.1.210
172.16.8.1	172.16.8.2	172.16.8.4	172.16.35.1
172.16.47.1	172.16.32.1	172.16.38.12	172.16.102.105

Tools used

Activity	Tools
Port Scanning& Foot printing	Nmap,dig,nslookup, netcat,Google Dorks
Web Application Enumeration	Nikto
Vulnerability Assessment	Nessus
Network Penetration Test	Metasploit,Armitage, Ethercap,driftnet
Web Application Penetration Test	Burp Suite
Vulnerability Research & Varification	www.exploit-db.com,www.1337day.com

Overall Vulnerability Risk Classification

Throughout the document, each vulnerability or risk identified has been labeled as a Finding and
categorized as a **High-Risk**, **Medium-Risk**, or **Low-Risk**. In addition, each supplemental testing note
is labeled as an Issue. These terms are defined below:

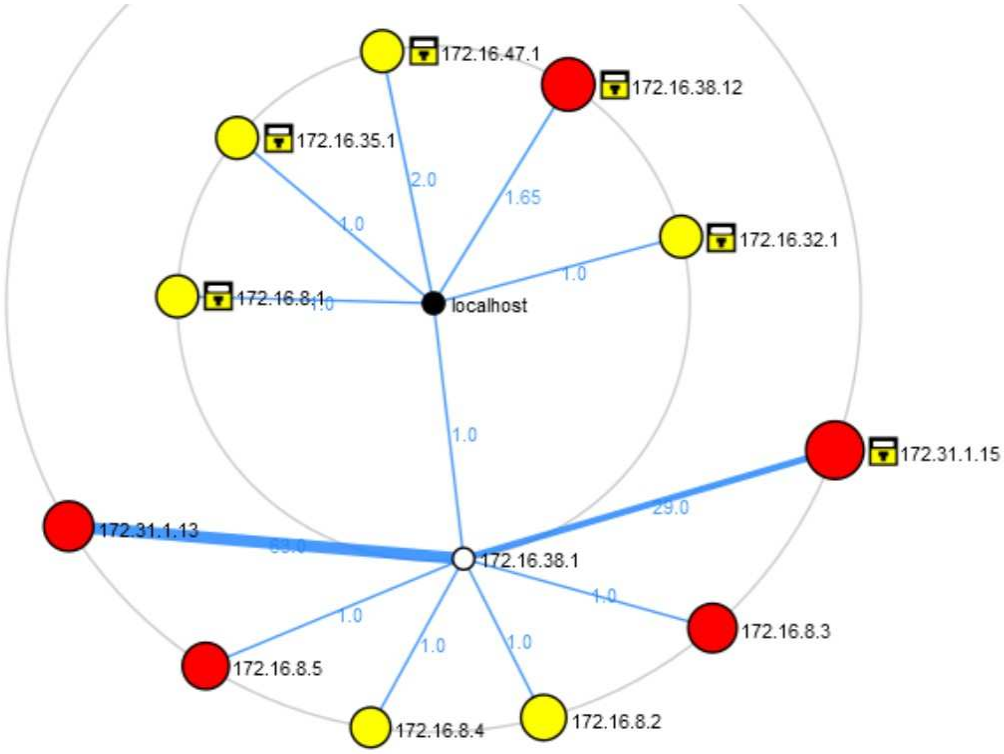
High Risk: These finding identify conditions that could that compromise or unauthorized access of a network, system, application or information. Example – No Password, No encryption, Denial of Service, buffer overflows.

Medium Risk: These findings identify condition that do not immediately or directly result in the compromise or unauthorized access of a network, system, application or information but do provide a capability or information that could, in combination with other capabilities or information, result in the compromise or unauthorized access of a network, system, application or information. Examples – Unprotected system .files and services that could result in DoS on non-critical services that could be further exploited.

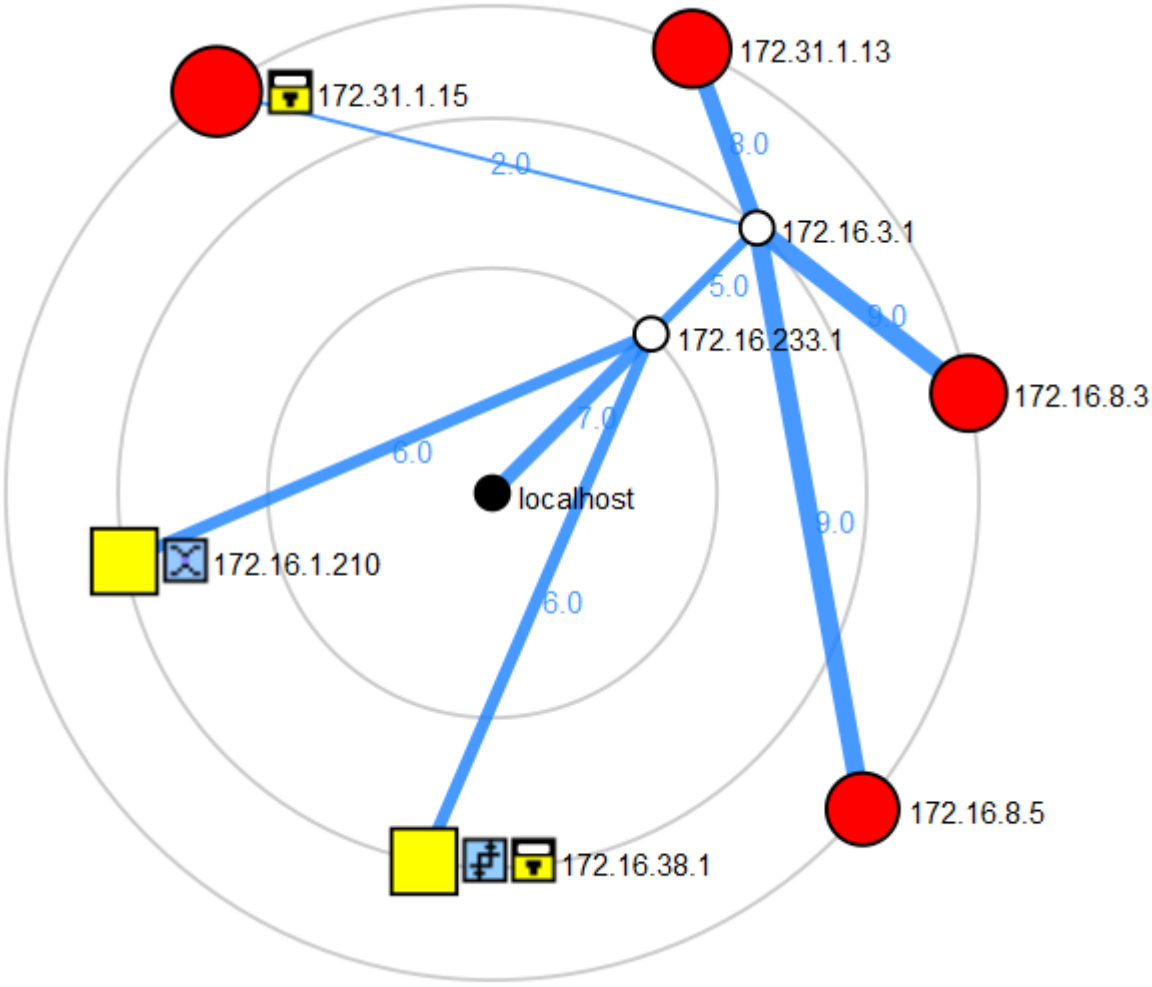
Low Risk: These finding identify condition that do not immediately or directly result in the compromise of a network.system,application,or information ,but do provide information that could be used in combination with other information to gain insight into how to compromise or gain unauthorized access to a network ,system, application or information .Low risk findings may also demonstrate an incomplete approach to or application of security measure within the environment .Examples of Low risk include cookies not marked secure ;concurrent session and revealing system banners

Network Flow Diagram

Network diagram drawn from 172.16.38.11



Network diagram drawn from 172.16.233.7

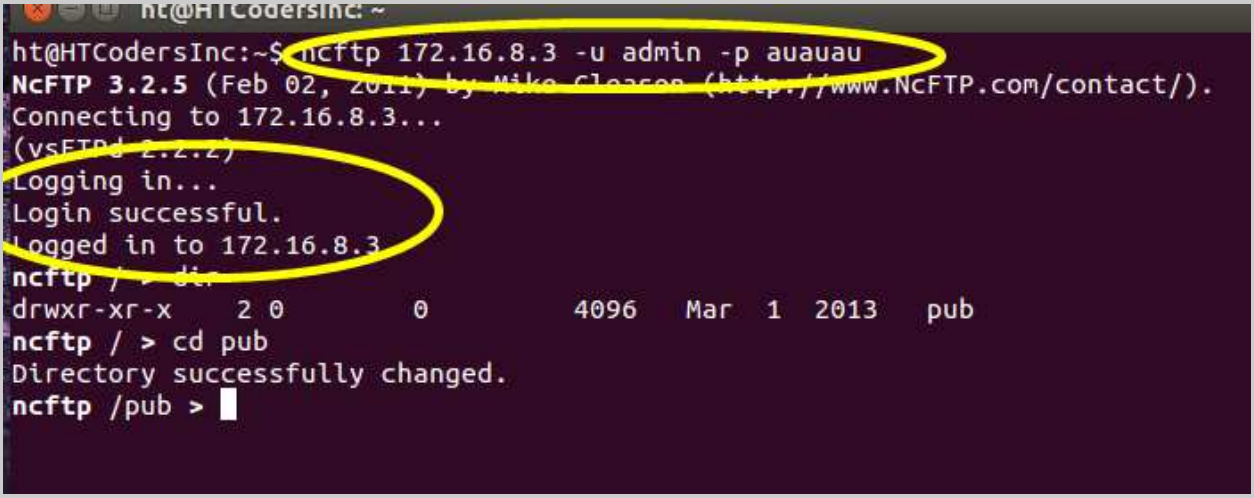


Findings

- 172.16.8.3/www.allduniv.ac.in

Issue	Risk Factor	Recommendation
According to its banner, the version of PHP installed on the remote host is older than 5.4.29. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.	High	Upgrade to 5.4.36
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections. In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials	High	Disable the Trace Request by changing the configuration in Apache Server
It is possible to enumerate directories on the web server. The following directories were: /backup/ /includes/ /logs/ /new/ /test/ /temp/	Low	While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards
The Web Server has the backup files hosted in the Directory browsing such as www.allduniv.ac.in/backup-english.zip	High	Remove the files as soon as possible

Hackers can use it to make a phishing site.		
An FTP server is listening on this port.	Modrate	Disable FTP if not needed
The FTP Server allows anonymous login and also uses weak password	Modrate	Change the password



- 172.16.3.4/www.ns2.allduniv.ac.in

Issue	Risk Factor	Recommendation
The remote DNS resolver does not use random ports when making queries to third party DNS servers. This problem might be exploited by an attacker to poison the remote DNS server more easily, and therefore divert legitimate traffic to arbitrary sites	High	Contact your DNS server vendor for a patch The ports used by 172.16.8.4 are not random. An attacker may spoof DNS responses. List of used ports : - 59574 - 59574 - 59574 - 59574

This web server leaks a private IP address through its HTML Body. This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server. This web server leaks the following private IP address: 172.31.1.15	Medium	Not Applicable

- 172.16.8.1/172.16.38.1/172.16.32.1/172.16.233.1 (Nortel Network Switches)

Issue	Risk Factor	Recommendation
Almost all the switches has telnet (23) enabled with weak password or no password Root logging enabled leading to privilege escalation Some logging credential are : **login : rwa** **password: rwa** **login :l2** **password : l2**	High	Password protect as soon a possible Risk of man in the middle attack
No immunity to deal with Denial of Service	High	Implementing Static ARP Table is suggested.

- 172.16.1.210/172.16.1.211/172.16.1.213
  (Cisco Small Business SG 300 28 28 port Gigabit Managed Switch)

Issue	Risk Factor	Recommendation
Almost all the switches has telnet (23) enabled with weak password or no password Root logging enabled leading to privilege escalation Some logging credential are : **login : cisco** **password: cisco**	High	Password protect as soon a possible Risk of man in the middle attack
No immunity to deal with Denial of Service	High	Implement the Denial of Service Prevention Mechanism provided in the Security Section of the Switch.

- 172.31.1.13
  (JK Institute Webserver)

Issue	Risk Factor	Recommendation
According to its banner, the version of PHP and Apache installed on the remote host is older. Such versions may be affected by several issues, including buffer overflows, format string vulnerabilities, arbitrary code execution, 'safe_mode' and 'open_basedir' bypasses, and clobbering of super-globals.	High	Upgrade Required
The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP	High	Disable the Trace Request by changing the configuration in Apache Server

methods which are used to debug web server connections. In addition, it has been shown that servers supporting the TRACE method are subject to cross-site scripting attacks, dubbed XST for "Cross-Site Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate web users to give him their credentials		
It is possible to enumerate directories on the web server. The following directories were: /includes/ /logs/ /new/ /tmp/ /hirani/	Low	While this is not, in and of itself, a bug, you should manually inspect these directories to ensure that they are in compliance with company security standards

Miscellaneous

- In Central Library, The CCTV Camera Sends unencrypted video streaming over the network, with can be easily viewed and altered.

Login: admin
Password:1234

Below are the Screen Shot from the CCTV camera

- At IP Address 172.16.102.105, an unprotected RICOH Aficio MP 2000L2 Printer is present.

Conclusion

This analysis is based on the technologies and known threats as of the date of this report. It is recommends that all modifications suggested in this document be performed in order to ensure the overall security of the web application and Internet segment. Specifically, the following action should be taken:

- *Password protect the FTP Administrator account on the Internet application server*
- *We also recommend that the issue of the reflected cross site scripting on the Internet banking web application be looked into*
- *The updates and Security patches is must for better security controls on the webserver.*

All in all we found that the current security posture of the systems and applications within the scope in decent shape from an external point of view although as with most networks there is room for improvement.

- -- - - - - - - - - - END OF REPORT -- - - - - - - - - - - - -

Simple Network Scanner in C

This simple network scanner scans the given work group/domain for computers in Directory Services

The Developed Network Scanner take the limit of I P addresses as Input
and scans the entire domain and outputs the Computer Name.

It uses the following
Namespaces:

```
using System.Net;
using System.Net.Dns;
```

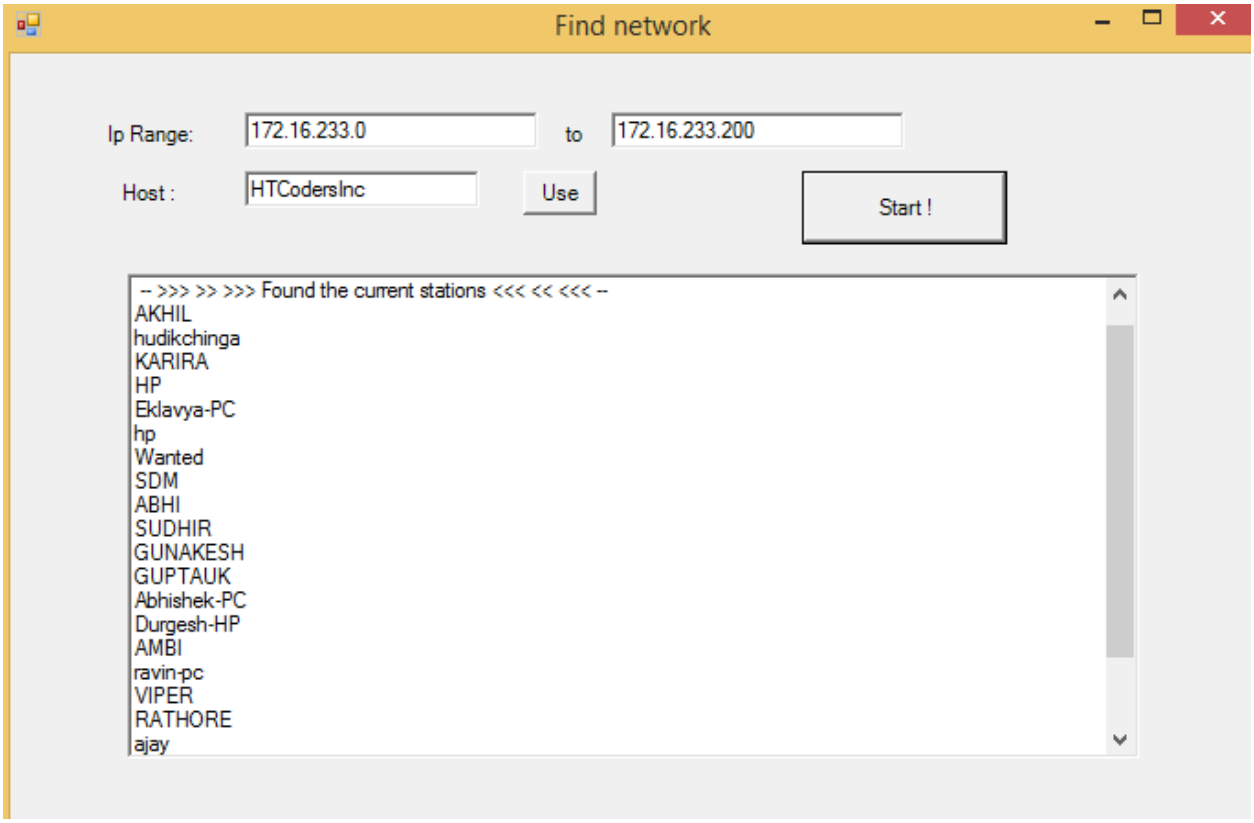
Methods:

```
Dns.GetHostByAddress();
```

Code :

```
void Search( )
        {
            Add( "-- >>> >> >>> Found station <<< << <<< -- " );
            int lastF       =   ipFrom.Text.LastIndexOf(".");
            int lastT       =   ipTo.Text.LastIndexOf(".");
            string frm      =   ipFrom.Text.Substring(lastF+1);
            string tto      =   ipTo.Text.Substring(lastT+1);
            int result = 0;
            System.Diagnostics.Debug.WriteLine( frm + " " + tto);
            for( int i = int.Parse( frm);
                    i <= int.Parse(tto );i++)
            {
                    try
                    {
                       string address = ipTo.Text.Substring(0,lastT+1);
        System.Diagnostics.Debug.WriteLine(ipTo.Text.Substring(0,lastT+1)+i);
                    IPHostEntry he   =Dns.GetHostByAddress( address+i);
                            Add( he.HostName );
                            result += 1;
                    }
                    catch( SocketException )
                    {
                    }
                    catch( Exception )
                    {
                    }
            }
        Add( "All done search retrieved " + result + " working stations.");
    }
```

ScreenShot:


Find network
Ip Range:
172.16.233.0
to
172.16.233.200
Host :
HTCodersInc
Use
Start !
-- >>> >> >>> Found the current stations <<< << <<< --
AKHIL
hudikchinga
KARIRA
HP
Eklavya-PC
hp
Wanted
SDM
ABHI
SUDHIR
GUNAKESH
GUPTAUK
Abhishek-PC
Durgesh-HP
AMBI
ravin-pc
VIPER
RATHORE
ajay

Bibliography

- The Basic of Hacking and Penetration Testing
  by Patrick Engerbretson

- Gray Hat Hacking: The Ethical Hacker's Handbook
  Third Edition