



EVALUATION OF INTERNSHIP REPORT

B.Tech: III Year

Department of Computer Science & Information Technology

Name of the Student	-	Mokshi Diwde
Branch & section	-	CSIT-2
Roll No	-	0827CI201111
Year	-	2022-23

Department of Computer Science & Information Technology
AITR, Indore,

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

Department of Computer Science & Information Technology

Certificate

Certified that training work entitled “*Cyber Security*” is a bonafied work carried out after fourth semester by “*Mokshi Diwde*” in partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from “*Mr. Yash Arya*” Acropolis Institute of Technology and Research during the academic year 2022-23.

Name and Sign of Training Coordinator

Name & Sign of Internship Coordinator

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

Department of Computer Science & Information Technology

ACKNOWLEDGEMENT

I would like to acknowledge the contributions of the following people without whose help and guidance this report would not have been completed. I acknowledge the counsel and support of our training coordinator, *Prof. Nidhi Nigam (Assistant Prof., CSIT Department)*, with respect and gratitude, whose expertise, guidance, support, encouragement, and enthusiasm has made this report possible. Their feedback vastly improved the quality of this report and provided an enthralling experience. I am indeed proud and fortunate to be supported by him/her. I am also thankful to Dr. Shilpa Bhalerao, H.O.D of Computer Science Information Technology Department, for her constant encouragement, valuable suggestions and moral support and blessings. Although it is not possible to name individually, I shall ever remain indebted to the faculty members of CSIT Department, for their persistent support and cooperation extended during this work.

Mokshi Diwde

0827CI201111

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

INDEX

S.no	CONTENTS	Page no
1.	Introduction to technology Undertaken.....	5
2.	Objectives	6
3.	Project detail	7
4.	Screenshots of Project and Certificates.....	8
5.	Github Links (Project/certificate/video/copy of report.... ..	10
7.	Conclusion.....	11
8.	References/ Bibilography.....	12

INTRODUCTION

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks.

Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology (IT) security, cybersecurity measures are designed to combat threats against networked system and applications, whether those threats originate from inside or outside of an organization.

Security system complexity, created by disparate technologies and a lack of in-house expertise, can amplify these costs. But organizations with a comprehensive cyber security strategy, governed by best practices and automated using advanced analytics, artificial intelligence (AI) and machine learning, can fight cyberthreats more effectively and reduce the lifecycle and impact of breaches when they occur.

Cyber security is not only essential to business organizations and governmental institutions. It should be for everyone who is using digital devices like computers, mobile phones, tablets, etc. These devices contain many personal pieces of information that digital thieves would love to have. What is also important about it is that if your information is exposed to hackers, they can use you as a bait to lure your friends or family into a digital scam.

Every little thing that is connected to the internet, used for communication and other purposes, can be affected by a breach of security.

OBJECTIVES

- ❖ Exhibit knowledge about how system get corrupted, protect personal data, and secure computer networks.
- ❖ Security of computer networks and systems is almost always discussed within information security that has three fundamental objectives, namely confidentiality, integrity, and availability.
- ❖ To prepare students with the technical knowledge and skills needed to protect and defend computer systems and networks.

PROJECT UNDERTAKEN

NMAP INTRODUCTION :

Nmap relies on seven data files for port scanning and other operations, all of which have names beginning with nmap-. One example is nmap-services, a registry of port names to their corresponding port number and protocol. The others, which this chapter describes one by one, are nmap-service-probes (version detection probe database), nmap-rpc (SunRPC program name to number database for direct RPC scanning), nmap-os-db (OS detection database), nmap-payloads (protocol-specific payloads), nmap-mac-prefixes (ethernet MAC address prefix (OUI) to vendor lookup table), and nmap-protocols (list of IP protocols for protocol scan). Additionally this chapter covers certain files related to scripting with the Nmap Scripting Engine.

The source distribution installs these files in /usr/local/share/nmap/ and the official Linux RPMs put them in /usr/share/nmap/. Other distributions may install them elsewhere.

Well Known Port List: nmap-services

The nmap-services file is a registry of port names to their corresponding number and protocol. Each entry has a number representing how likely that port is to be found open. Most lines have a comment as well. Nmap ignores the comments, but users sometimes grep for them in the file when Nmap reports an open service of a type that the user does not recognize.

```
gotd      17/tcp    0.002346 # Quote of the Day
gotd      17/udp    0.009209 # Quote of the Day
msp       18/udp    0.000610 # Message Send Protocol
chargen   19/tcp    0.002559 # ttytst source Character Generator
chargen   19/udp    0.015865 # ttytst source Character Generator
ftp-data  20/tcp    0.001079 # File Transfer [Default Data]
ftp-data  20/udp    0.001878 # File Transfer [Default Data]
ftp       21/tcp    0.197667 # File Transfer [Control]
ftp       21/udp    0.004844 # File Transfer [Control]
ssh       22/tcp    0.182286 # Secure Shell Login
ssh       22/udp    0.003905 # Secure Shell Login
telnet    23/tcp    0.221265
telnet    23/udp    0.006211
priv-mail 24/tcp    0.001154 # any private mail system
priv-mail 24/udp    0.000329 # any private mail system
smtp      25/tcp    0.131314 # Simple Mail Transfer
smtp      25/udp    0.001285 # Simple Mail Transfer
```


Version Scanning DB: nmap-service-probes

This file contains the probes that the Nmap service/version detection system (-sV or -A options) uses during port interrogation to determine what program is listening on a port.

```
#####NEXT PROBE#####
# DNS Server status request: http://www.rfc-editor.org/rfc/rfc1035.txt
Probe UDP DNSStatusRequest q|\0\0\x10\0\0\0\0\0\0\0\0|
ports 53,135
match domain m|^0\0\x90\x04\0\0\0\0\0\0\0\0|
# This one below came from 2 tested Windows XP boxes
match msrpc m|^x04\x06\0\0\x10\0\0\0\0\0\0\0\0|
[...]
#####NEXT PROBE#####
Probe UDP Help q|help\r\n\r\n|
ports 7,13,37
match chargen m|@ABCDEFGHIJKLMNOPQRSTUVWXYZ|
match echo m|^help\r\n\r\n$|
match time m|^[\xc0-\xc5]...$|
```

SunRPC Numbers: nmap-rpc

As with `nmap-services`, `nmap-rpc` simply maps numbers to names. In this case, SunRPC program numbers are mapped to the program name which uses them.

```

rpcbind      100000  portmap sunrpc rpcbind
rstatd       100001  rstat rup perfmeter rstat_svc
rusersd      100002  rusers
nfs          100003  nfsprog nfsd
ypserv       100004  ypprog
mountd       100005  mount showmount
rpc.operd    100080  opermsg          # Sun Online-Backup
# DMFE/DAWS (Defense Automated Warning System)
#
Gqsrv        200034  gqsrv
Ppt          200035  ppt
Pmt          200036  pmt

```

Nmap OS Detection DB: nmap-os-db

The nmap-os-db data file contains hundreds of examples of how different operating systems respond to Nmap's specialized OS detection probes. It is divided into blocks known as *fingerprints*, with each fingerprint containing an operating system's name, its general classification, and response data.

```
Fingerprint FreeBSD 7.0
Class FreeBSD | FreeBSD | 7.X | general purpose
SEQ (SP=100-10A%GCD=1-6%ISR=108-112%TI=I%II=I%SS=S%TS=21|22)
OPS (O1=M5B4NW8NNT11%O2=M578NW8NNT11%O3=M280NW8NNT11%O4=M5B4NW8NNT11%O5=M218NW8NNT11%O6=M109NNT11)
WIN (W1=FFFF%W2=FFFF%W3=FFFF%W4=FFFF%W5=FFFF%W6=FFFF)
ECN (R=Y%DF=Y%T=3B-45%TG=40%W=FFFF%O=M5B4NW8%CC=N%Q=)
T1 (R=Y%DF=Y%T=3B-45%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2 (R=N)
T3 (R=Y%DF=Y%T=3B-45%TG=40%W=FFFF%S=O%A=S+%F=AS%O=M109NW8NNT11%RD=0%Q=)
T4 (R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5 (R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6 (R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7 (R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1 (DF=N%T=3B-45%TG=40%IPL=38%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE (DFI=S%T=3B-45%TG=40%CD=S)

Fingerprint Linux 2.6.17 - 2.6.24
Class Linux | Linux | 2.6.X | general purpose
SEQ (SP=A5-D5%GCD=1-6%ISR=A7-D7%TI=Z%II=I%TS=U)
OPS (O1=M400C%O2=M400C%O3=M400C%O4=M400C%O5=M400C%O6=M400C)
WIN (W1=8018%W2=8018%W3=8018%W4=8018%W5=8018%W6=8018)
ECN (R=Y%DF=Y%T=3B-45%TG=40%W=8018%O=M400C%CC=N%Q=)
T1 (R=Y%DF=Y%T=3B-45%TG=40%S=O%A=S+%F=AS%RD=0%Q=)
T2 (R=N)
T3 (R=Y%DF=Y%T=3B-45%TG=40%W=8018%S=O%A=S+%F=AS%O=M400C%RD=0%Q=)
T4 (R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T5 (R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
T6 (R=Y%DF=Y%T=3B-45%TG=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)
T7 (R=Y%DF=Y%T=3B-45%TG=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)
U1 (DF=N%T=3B-45%TG=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE (DFI=N%T=3B-45%TG=40%CD=S)
```

UDP payloads: nmap-payloads

The nmap-payloads file contains the protocol-specific payloads sent with some UDP probes. UDP scanning is difficult because most services don't send a reply to an empty probe, making it impossible to distinguish open and filtered ports. For some ports, Nmap knows a payload that is safe to send and tends to elicit a positive response. The payloads are stored in this file.

```
# Routing Information Protocol version 1. Special-case request
for the entire
# routing table (address family 0, address 0.0.0.0, metric 16).
RFC 1058,
# section 3.4.1.
udp 520
"\x01\x01\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
0"
"\x00\x00\x00\x00\x00\x00\x00\x00\x10"
```

MAC Address Vendor Prefixes: nmap-mac-prefixes

Users rarely modify this file, which maps MAC address prefixes to vendor names. Read on for the complete treatment.

Ethernet devices, which have become the dominant network interface type, are each programmed with a unique 48-bit identifier known as a MAC address. This address is placed in ethernet headers to identify which machine on a local network sent a packet, and which machine the packet is destined for. Humans usually represent it as a hex string, such as 00:60:1D:38:32:90.

```

006017 Tokimec
006018 Stellar ONE
006019 Roche Diagnostics
00601A Keithley Instruments
00601B Mesa Electronics
00601C Telxon
00601D Lucent Technologies
00601E Softlab
00601F Stallion Technologies
006020 Pivotal Networking
006021 DSC
006022 Vicom Systems
006023 Pericom Semiconductor
006024 Gradient Technologies
006025 Active Imaging PLC
006026 Viking Modular Solutions

```

IP Protocol Number List: nmap-protocols.

This file maps the one-byte IP protocol number in the IP header into the corresponding protocol name.

```

hopopt      0      HOPOPT      # IPv6 Hop-by-Hop
Option
icmp        1      ICMP        # Internet Control
Message
igmp        2      IGMP        # Internet Group
Management
gcp         3      GCP         # Gateway-to-
Gateway
ip          4      IP          # IP in IP
(encapsulation)
st          5      ST          # Stream
tcp         6      TCP         # Transmission
Control
cbt         7      CBT         # CBT
egp         8      EGP         # Exterior Gateway
Protocol
[ ... ]
chaos       16     CHAOS       # Chaos
udp         17     UDP         # User Datagram

```

CERTIFICATE



GITHUB LINK

<https://github.com/Mokshidiwde1111/EOI-submission.git>

CONCLUSION

Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap is clearly the “Swiss Army Knife” of networking, thanks to its inventory of versatile commands.

It lets you quickly scan and discover essential information about your network, hosts, ports, firewalls, and operating systems.

Nmap has numerous settings, flags, and preferences that help system administrators analyze a network in detail.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the “interesting ports table”. That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port.

REFERENCES

https://www.youtube.com/watch?v=b4-ZZb_4Zr4&t=179s

<https://nmap.org/download.html>

<https://www.itgovernance.co.uk/cybersecurity>

