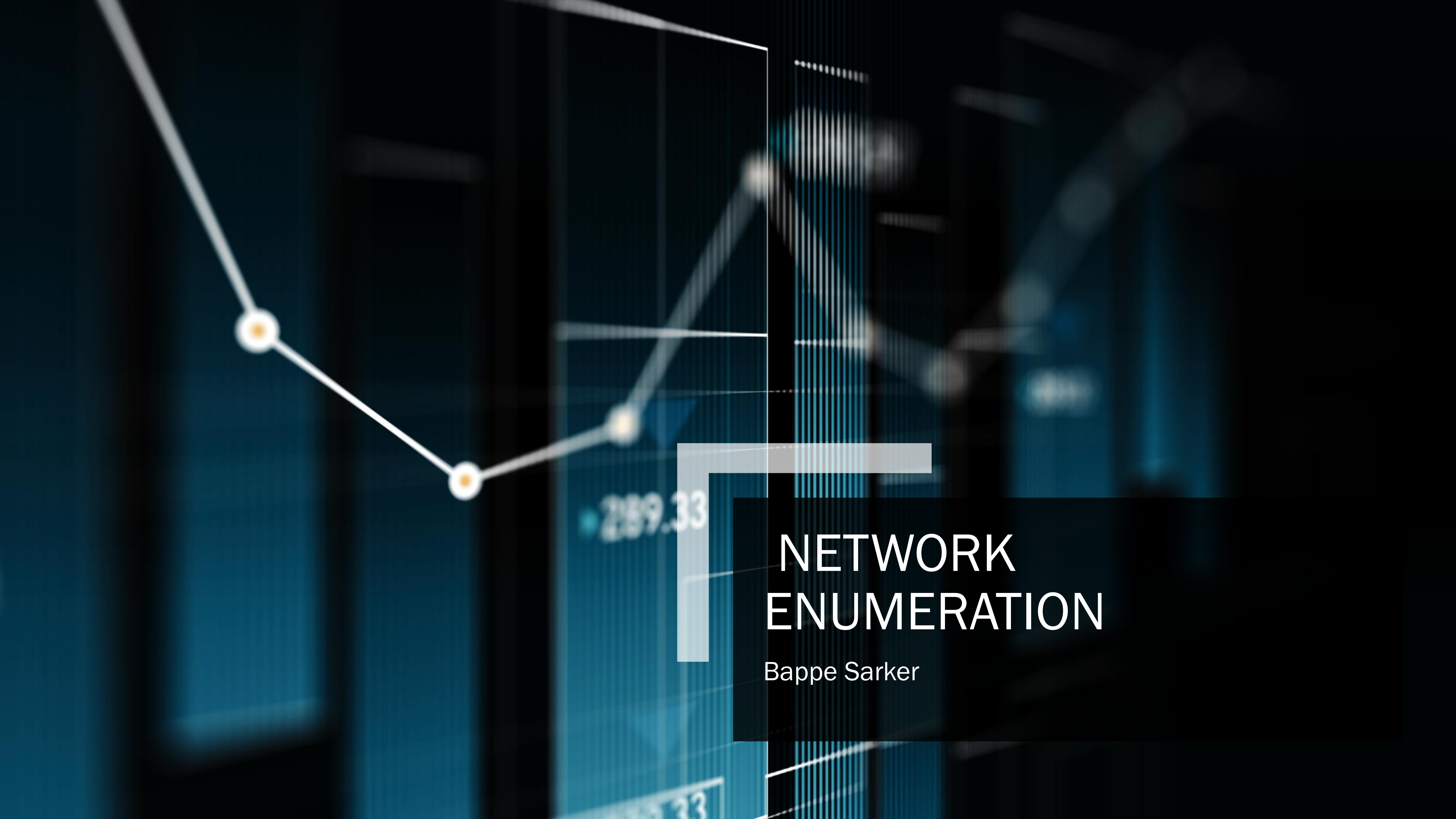

NETWORK ENUMERATION

Bappe Sarker

What is Network Enumeration?

Network enumeration is a process which creates an active connection with the target hosts for discovering potential attack vectors, or for further exploiting the system.

- *It is used to gather the following:*
- *Hostnames*
- *Usernames, group names*
- *IP tables and routing tables*
- *Application and banners*
- *Network shares and services*
- *Audit configurations and service settings*
- *DNS and SNMP details*

Services Enumeration

- FTP
- SSH
- SMTP
- DNS
- HTTP
- SMB
- SNMP
- NFS

FTP Enumeration

- **Anonymous user check**

```
# nmap –sV –sC <target_ip>        or     you can run ftp anon scripts
```

- **FTP login**

```
# ftp <target_ip>
```

- **FTP bruteforce**

```
# hydra –L users.txt –P password.txt –t 3 –s 21 <target_ip> ftp
```

SSH Enumeration

- **Banner Grabbing**

```
# nc <target_ip> 22
```

- **Bruteforce**

```
#hydra –L users.txt –P password.txt –t 3 –s 22 <target_ip> ssh
```

SMTP Enumeration

- Banner Grabbing

```
# nc <target_ip>  25
```

- Verfiy user

```
VRFY <user>
```

- Automated verification

```
#smtp-user-enum -M VRFY -U /root/Desktop/users.txt -t 192.168.31.25
```

SMTP Enumeration

- Send email via cmd without authentication

```
EHLO <IP>
VRFY root
EXPN root
Mail from: me@test.com
To: root@test.com
Data:
Subject: Message
Hi,

Just a test message.
```

(Double carriage return)

DNS Enumeration

- DNS record query

```
#host -t a vulnweb.com  (a record)
#host -t mx  test.com (mx record)
```

- DNS Zone Transfer

```
# Port scan and trying zone transfer
nmap --script=dns-transfer-zone -p 53 domain
# DNS Zone Transfer using dig
dig axfr @IP guess_domain_name
```

- Automated - #dnsenum domain.com

HTTP Enumeration

- Banner Grabbing

#whatweb testphp.vulnweb.com

- Nikto –h <target_host>

- Vulnerability Scan

# nmap –script = http-vuln*

SMB Enumeration

- **List shares**

```
# smbclient -L //IP

# smbclient -L <ip>
```

- **Connect**

```
#smbclient \\\\x.x.x.x\\share

#smbclient -U “DOMAINNAME\Username” \\\\IP\\IPC$ password
```

SMB Enumeration

- **Password spray with crackmapexec**

```
#crackmapexec smb 192.168.100.0/24 -u "admin" -p "password1“
#crackmapexec smb 192.168.100.0/24 -u user_file.txt -p pass_file.txt
#crackmapexec smb 192.168.100.0/24 -u user_file.txt -H ntlm_hashFile.txt
```

SNMP Enumeration

- SNMP community string enumeration

```
#onesixtyone -c comm.txt  -p 161 192.168.31.120
```

- SNMP Enumeration

```
#nmap -sU -sV  -p 161 192.168.31.120

#snmpwalk -v 1 -c public 192.168.31.120

#snmp-check 192.168.31.120
```

NFS Enumeration

- Check mountable drive

```
# showmount -e 192.168.31.25
```

- Mount the drive

```
#mount -t nfs 192.168.31.25:/ /root/Desktop/Imount
```

Thank You