Enumreation_INE_Note

SMN666

SSH Enumreation:

```
#namp -nvv -Pn- -sSV -p 22,80,139,443 --version-intensity 9 -A -oN /root/detail.txt {ip}

#search vulnerabilities in online OPENSSH version

#searchsploit 2.9 {version no.}

#searchsploit openssh

#ssh [ip]

#ssh -c aes128-cbc [ip]
```

HTTP Enumeration:

```
#use dirbuster

#locate wordlists

#nikto -h [ip][port]

#e.g nikto -h 192.168.1.1:443
```

SMB Enumeration:

```
#locate smb.conf

#nano /etc/samba/smb.conf

#enum4linux [ip]

#msfconsole
```

```
#search smb
#use auxiliary/scanner/smb/smb_version
#searchsploit samba 2.2[version no.]
#nbtscan [ip] #show NetBIOS name
#smbclient -L [ip]
#smbclient "\\\\[ip]\IPC$"
# smb:\>
```

DNS Enumeration:

```
#host -t ns xxx.com #[nameserver]
#host -t mx xxx.com #[mailserver]
#host xxx.com
#host -l xxx.com [nameserver's name]
#dnsrecon -d xxxc.om -t axfr
#dnsenum xxx.com
```

Other Enumeration:

```
#FTP,SNMP,SMTP
```