Mandiant

Figure 1: Enterprise firewall bypass using RDP and network tunneling with SSH as an example

```
Example Plink Executable Command:

plink.exe <users>@<IP or domain> -pw <password>
```

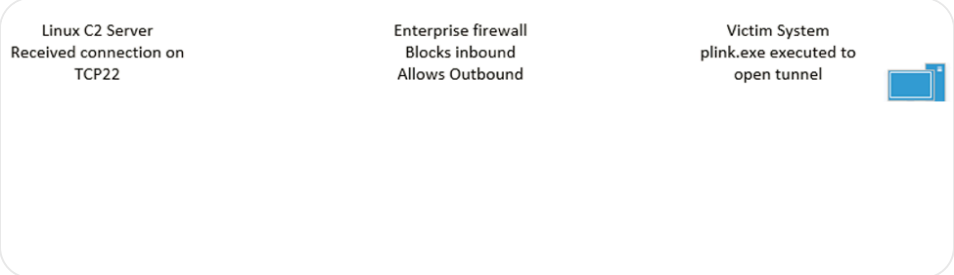

Figure 2: Example of successful RDP tunnel created using Plink

Figure 3: Example of successful port forwarding from the attacker C2 server to the victim

```
netsh interface portproxy add v4tov4 listenport
Example Shortened netsh Port Forwarding Command
netsh I p a v l=8001 listena=<JUMP BOX IP> conn
```

Figure 4: Lateral Movement via RDP using a jump box to a segmented network

---

-

-

-

Registry Keys:

-
  -
  -
-

-

Event Logs:

-
  -
  -
-

-
-
-
-
-
-
-

-

-

-

```
alert tcp any [21,22,23,25,53,80,443,8080] -> a
```

```
alert tcp any [21,22,23,25,53,80,443,8080] -> a
```

Figure 5: Sample Snort Rules to identify RDP tunneling