

Whether you are using the Mitre ATT&CK Framework, the Cyber Kill Chain model, or some other method of mapping attacks you invariably start with reconnaissance. The following ports are commonly associated with either vulnerable services or popular targets.

The following description and possible remediations are based upon the default, registered port usage and may not be applicable if some other service is listening on that port. Commonly the remediation will be to either close a port that should never be exposed publicly or to switch to a secure alternative.

### **20 - FTP (Data) & 21 - FTP (Control)**

FTP is a cleartext file transfer protocol that uses two ports, 20 and 21. Port 20 is used for data transmission while port 21 is used for control traffic. Because it is cleartext anyone snooping traffic on that network may be able to collect and recreate the data transferred, up to and including the credentials needed to log on and access this device.

#### **Remediation**

Any form of clear text file transfer should be replaced with a secure alternative such as SCP or SFTP. FTP-Secure can work, but is a bit trickier to set up through firewalls. Depending on the need a cloud storage solution may be viable as well.

### **22 - SSH**

SSH is an encrypted service that permits the control of devices over insecure networks. While SSH is secure, having it exposed to the internet means that attackers can attempt brute force attacks on these devices, attempting to gain access. MFA commonly isn't used with SSH which means leaked and shared credentials may permit an attacker access.

#### **Remediation**

Unless required, device management channels shouldn't be exposed to the internet. They should require a VPN and have their own management VLAN to ensure outside attackers aren't able to probe these devices.

### **23 - Telnet**

Telnet is a cleartext service that permits the control of devices. Telnet traffic can be snooped and credentials can be leaked. This can expose the device to attack or permit attackers to collect credentials.

#### **Remediation**

Telnet should not be used outside of lab environments. Secure alternatives such as SSH should be used on shared networks and device access/management should be behind a dedicated management VLAN that requires a VPN for external access.

### **25 - SMTP**

SMTP is an insecure mail transfer protocol. As with all cleartext communication it can be snooped by outside attackers, exposing anything transferred. Port 25 is frequently blocked by ISPs, due to its usage in MX spamming, as an anti-spam measure.

## Remediation

Insecure mail transfer services should be replaced with their secure alternatives. Ports 587(with STARTTLS)/465/2525 are the registered ports for secure alternatives.

### **53 - DNS**

DNS servers are common targets for attacks and as such device administrators need to be aware of their exposure and any related vulnerabilities. Common attacks to be aware of are DNS Amplification attacks, where your DNS server is tricked into flooding a victim device; DNS DDoS attacks, where your DNS server is flooded with bogus requests which can inhibit its ability to function properly.

## Remediation

Notification of Port 53 is informative in nature. Ensure you are subscribed to vendor security alerts and your devices are properly configured and running supported software.

### **110 - POP3**

POP3 is a mail protocol that, on port 110, is commonly unencrypted. Much like SMTP attackers can view the contents of email.

## Remediation

Insecure mail transfer services should be replaced with their secure alternatives. Port 995 is the registered port for secure POP3.

### **135**

RPC/DCOM is a risky port to have open that is increasingly being blocked by ISPs due to being a common attack target. While this port may be needed for certain remote management functions, it is still incredibly sensitive and shouldn't be exposed over the internet or other insecure networks

### **137, 138, 139 - NetBIOS Trio**

NetBIOS was once used for communication and sharing of resources; however in modern times it is a severe security concern and common attack target. Malware such as WannaCry specifically targets NetBIOS on ports 137-139 and port 445.

## Remediation

NetBIOS should never be exposed over the internet or other untrusted networks.

### **389 - LDAP**

LDAP contains sensitive information such as usernames, login attempts, and more. LDAP commonly isn't encrypted and could permit attackers to snoop traffic, gaining credentials useful in other attacks.

## Remediation

LDAP does have a secure version that should be used. LDAP over SSL runs on port 636 and should be used.

### **445 - SMB**

SMB is a modern update to the old NetBIOS ports, however it is still a popular target and vulnerable to malware such as WannaCry and EternalBlue.

#### **Remediation**

SMB should never be exposed over the internet or other untrusted networks.

### **636**

LDAP over SSL is a secure protocol; however, since it is a popular target and could be vulnerable if patch levels aren't maintained, alternatives are recommended.

#### **Remediation**

Ensure the business need for LDAPs is valid. Implement strong firewall rules to permit only the traffic needed. Explore using a VPN to move the LDAP service inside your network

### **1433 & 1434 (Microsoft SQL Server)**

Ports 1433 and 1434 are commonly opened when Microsoft SQL Server or other services are installed.

#### **Remediation**

There is no reason to have these ports exposed over the internet. They are common attack targets.

### **3306 - MySQL**

MySQL's default port of 3306 permits remote access and is a common attack target.

#### **Remediation**

Port 3306 should never be open. Secure alternatives such as a VPN or SSH should be used instead.

### **3389 - RDP**

RDP, much like telnet, is a cleartext, easily snooped protocol that should never be used. Attackers will commonly target this port and login attempts by valid users may result in their credentials being compromised.

#### **Remediation**

Remote Desktop Gateway is a feature in Windows Server that uses port 443 and encrypts traffic with SSL. Adding MFA greatly increases the security of this solution. Requiring users to only access these RDP boxes over VPN can also be a secure alternative.