Mandiant

ASSESSMENT CAPABILITIES

The Mandiant Advantage Attack Surface Management (MA-ASM) team monitors the threat landscape and adds new capabilities into the discovery process on a near-daily basis. This document discusses some of the specifics of these capabilities.

Port Scanning

By default, MA-ASM scans the following TCP ports across IPv4 hosts:

```
20, 21, 22, 23, 35, 53, 79, 80, 81, 82, 95, 102, 106, 110, 111, 113, 115,
135, 137, 138, 139, 143, 161, 443, 445, 465, 502, 503, 587, 635, 902, 993, 995,
1090, 1098, 1270, 1433, 1521, 1583, 1723, 1812, 1813, 1883, 1900, 2049, 2181, 2222,
2375, 2376, 2379, 2888, 3050, 3299, 3306, 3351, 3389, 3479, 3888, 4190, 4369, 4443,
4444, 4445, 4505, 4506, 4786, 4848, 5000, 5432, 5555, 5556, 5672, 5900, 5901, 5902,
5903, 5984, 5985, 5986, 6379, 6443, 6556, 7001, 7002, 7003, 7004, 7070, 7071, 7443,
7547, 7777, 7990, 8000, 8001, 8002, 8003, 8009, 8111, 8032, 8040, 8080, 8081, 8278,
8291, 8443, 8649, 8686, 8883, 9000, 9001, 9002, 9003, 9012, 9090, 9091, 9092, 9094,
9100, 9200, 9201, 9300, 9301, 9398, 9401, 9419, 9443, 9503, 10250, 10255, 10999,
10443, 11099, 11111, 11211, 11443, 11994, 12443, 13389, 13443, 20000, 20443, 22222,
25002, 27017, 27018, 27019, 30443, 32400, 40443, 45000, 45001, 47001, 47002, 49152,
49154, 50001, 50500, 51001, 51080, 53413, 61001, 61616
```

By default, MA-ASM scans the following UDP ports across IPv4 hosts:

```
53, 123, 135, 139, 161, 500, 631, 1434, 1900, 2049, 17185
```

Protocol Interaction

To determine the protocol that is used by an open port, MA-ASM initiates communication by using the standard protocol that is associated with the port. If a successful protocol-specific connection cannot be established, MA-ASM performs a fallback HTTP connection test. MA-ASM interacts with the following protocols:

- AMQP
- Apache Zookeeper Atomic Broadcast (Ra
- Cisco Smart Insta
- DNS
- Elasticsearch
- FTP
- Ganglia (Raw)
- HTTP / HTTPS
- IMAP
- Memcached (Raw)
- MongoDB
- MySQL
- Oracle IIOP (Raw)
- Oracle T3 (Raw)
- POP3 RDP (Raw)
- Redis
- SAP NI (Raw)
- SMB

- SMTP
- SNMP
- SSH
- Telnet
- UPnP

Exposed Service Issues are automatically created when the following protocols are detected:

- Database Service (Detected: AMQP, Zookeeper, Elasticsearch, Memcached, MongoDB, MySQL, Oracle IIOP, Oracle T3, Redis)
- FTP Service
- SMB Service
- Telnet Service
- UPnP Service

Technologies Fingerprinted

Over 3100 Hardware, Operating System, and Application technologies are fingerprinted when a new NetworkService or Uri is identified. To see the full list of these technologies, see the **MA-ASM Library (https://asm.advantage.mandiant.com/library/technologies)**.

CVE Inference

All discovered technologies are passively checked against the NIST NVD CVE database when a new NetworkService or Uri is identified. To see the full list of these CVEs, see the **National Vulnerability Database (NVD) website (https://nvd.nist.gov/)**.

Vulnerability Checks

MA-ASM provides over 500 passive and active vulnerability checks when a known vulnerability, misconfiguration, leak, or compromise is identified. To see the full list of these checks, see the **MA-ASM Library (https://asm.advantage.mandiant.com/library)**.