|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Decorative | | | | |
|  |  |  | |  |
| Incident Disclosure Report  Incident report # 01001 | | |
| Curtis Crawford | | 2024-05-21 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Decorative | | | | |
|  |  |  | |  | |
|  | Executive summary  On 2023-06-06, an attacker performed multiple scans of Network 172.16.14.0 and was able to retrieve various forms of information such as what hosts are online, what ports are open, and what operating systems they are running. | |  | |

|  |  |
| --- | --- |
|  |  |
| The incident On 2023-06-06 at 13:37:35 & at 17:36:40, separate scans were made of Network 172.16.14.0. During these scans, they begun by utilizing ARP to figure out which hosts were active. Then through a series of HTTP & TCP conversations, were able to discover which ports were open. Furthermore it seems like they've discovered (through HTTP Protocol) what operating systems are on specific machines. What was discovered? Active hosts Open ports Operating Systems | |
| A picture of many lightbulbs with only one lit | |  |
| Figure 1 | |  |
| Attacker IP(s)  172.16.14.3  Attacker MAC(s)  00:50:56:9f:66:38 | |  |

|  |
| --- |
|  |
|  | |

More Information

Time of attack (first packet of attack)

13:36:44  
  
Packet number of first packet in attack

10  
  
Protocol(s) used in attack

HTTP  
TCP  
ARP  
  
  
Suspected Nmap/scan configuration

Intense Scan, All Ports.

Screen captures and explanations below.  
  
A screenshot of a computer

Description automatically generatedHere we can see where a network scan using ARP is being used to figure out what hosts are currently active on the network.

Following that, the attacker starts checking to see what ports are open.

A screen shot of a computer

Description automatically generated

The user then continues with a variety of scans to confirm open ports and check for what OS the machines are running.

A screenshot of a computer screen

Description automatically generatedA screenshot of a computer

Description automatically generated