Team: Team 3

Inject Number: 38

Inject Duration: 75 Minutes

Inject Start Date/Time: Sat, 04 Mar 2017 20:24:45 +0000

From: IT Operations

To: To Infrastructure Team

Subject: 003 DNS Cache Poisoning Investigation

Our IT Director read a recent security article about DNS Cache Poisoning that contained the following paragraph:
This attack is usually accomplished while a DNS request to other DNS. So this attack can be prevented on DNS by less trusting on information sent by other DNS servers. The most basic defense against this attack is use of latest version of DNS. Latest DNS uses port randomization with transaction ID so it's hard for attacker to guess for the port. DNS based on BIND 9.5.0 or above perform these checks. Transaction ID is also cryptographically secure which reduce the probability of attack. But BIND version must be hidden within the query packets. Remove unnecessary services running on the DNS servers. Attackers can use these unnecessary services to attack on DNS.Recursive queries should be limited and DNS should only store information about the domain it has requested. It must be configured not to add additional domains information in a query response. Most of the DNS servers are vulnerable to this attack.
He is concerned that we are vulnerable to this attack.
Evaluate our DNS and reply with a management memo as to our status: The memo must include an outline of the steps you took to determine whether we are vulnerable and if it is determined that we are vulnerable, you must also include your recommendation to remediate or mitigate these vulnerabilities.

Thank you.

IT Operation

Thank you.

IT Operations