

DNS SOCKET POOLING

The socket pool enables a DNS server to use source port randomization when issuing DNS queries. This provides enhanced security against cache poisoning attacks. The socket pool is enabled with default settings on computers that have installed [Security Update MS08-037](#). You can also customize socket pool settings.

When a query is made to a DNS server that query is sent to a recursive DNS server. The recursive server then sends a query to the authoritative DNS server using a port. The reply comes back through the a source port which in turn makes you data susceptible to an attacker because the same source port is being used all the time. This makes it easy for the attacker to learn your route and attack the data.

With source port randomization, the DNS server will randomly pick a source port from a pool of available sockets that it opens when the service starts.

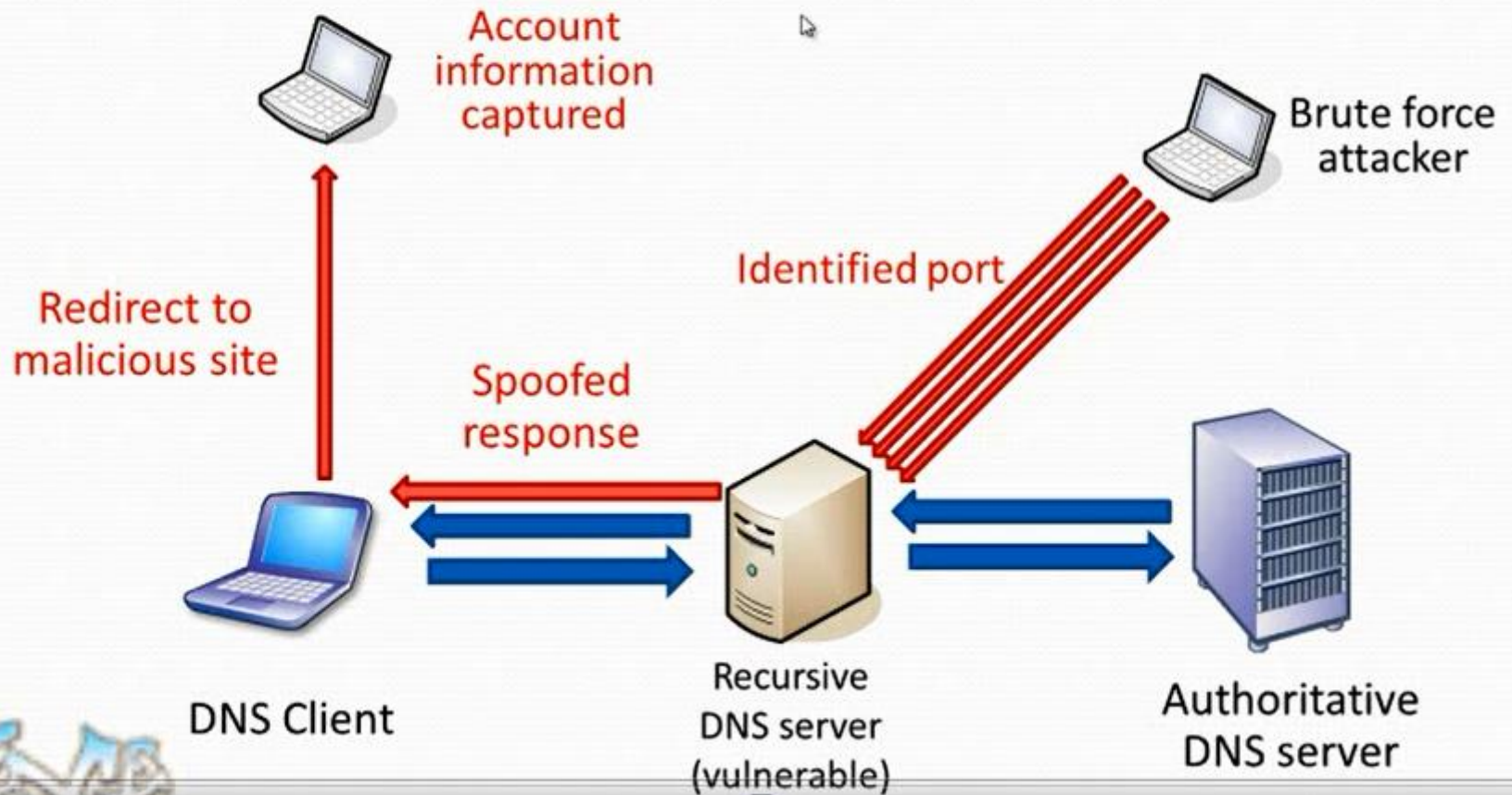
With source port randomization, the DNS server will randomly pick a source port from a pool of available sockets that it opens when the service starts.

What does Socket Pool do?

Instead of using a predictable source port when issuing queries, the DNS server uses a random port number selected from this pool, known as the socket pool. The socket pool makes cache poisoning attacks more difficult because an attacker must correctly guess the source port of a DNS query in addition to a random transaction ID to successfully execute the attack.

Let's take a look at what can occur without port randomization.

DNS spoofing attack



DNS socket pool (Socket Pool randomization)

- The DNS socket pool enables randomization of queries to prevent cache poisoning attacks.
- This feature is enabled by default in Windows Server 2012. The DNS socket pool uses several source ports for issuing queries.
- Both the number of source ports to be used and any exclusions or ports not to be used for issuing queries can be configured.
- This feature can't be controlled using the DNS management tool and must instead be configured by using either the dnscmd tool or the registry.

CA

Administrator: Command Prompt

Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

E:\Users\Administrator>dnscmd /info /socketpoolsize

Query result:

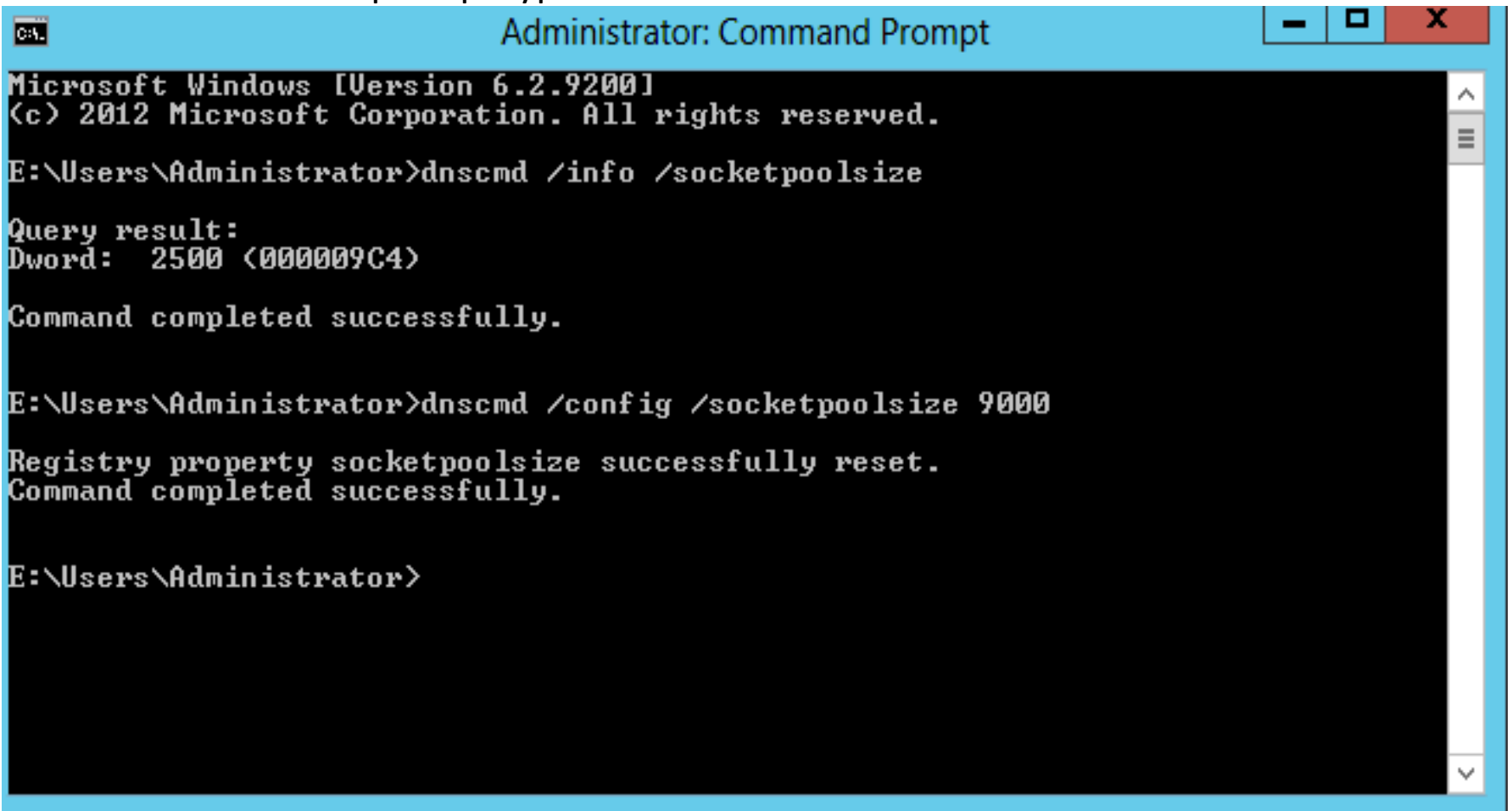
Dword: 2500 (000009C4)

Command completed successfully.

E:\Users\Administrator>_

We now want to change that to 9000

At the command prompt type:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.
E:\Users\Administrator>dnscmd /info /socketpoolsize

Query result:
Dword: 2500 (000009C4)

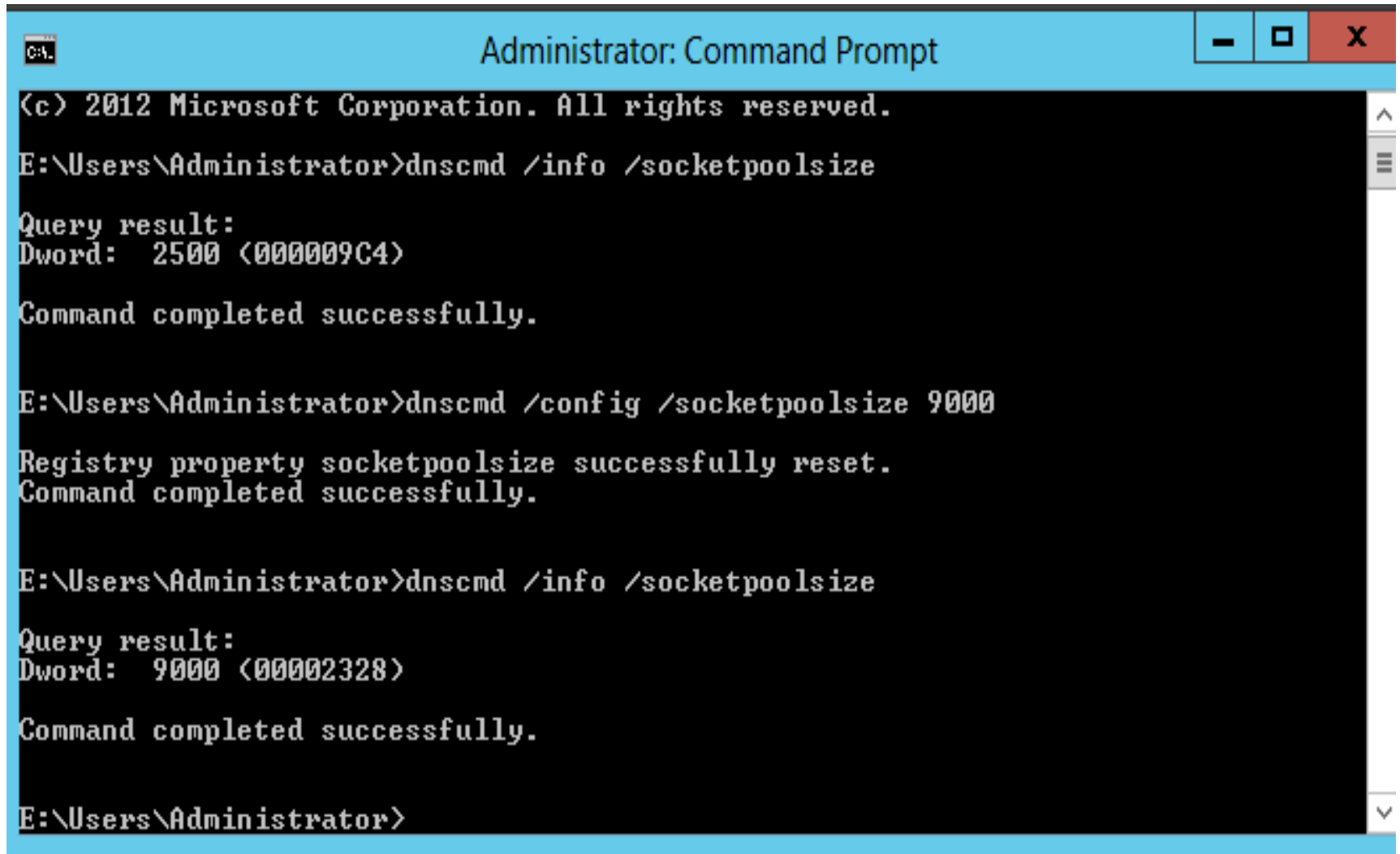
Command completed successfully.

E:\Users\Administrator>dnscmd /config /socketpoolsize 9000

Registry property socketpoolsize successfully reset.
Command completed successfully.

E:\Users\Administrator>
```

Enter the info command at the command prompt again to see that we are now running at 9000



```
Administrator: Command Prompt
(c) 2012 Microsoft Corporation. All rights reserved.
E:\Users\Administrator>dnscmd /info /socketpoolsize

Query result:
Dword: 2500 (000009C4)

Command completed successfully.

E:\Users\Administrator>dnscmd /config /socketpoolsize 9000

Registry property socketpoolsize successfully reset.
Command completed successfully.

E:\Users\Administrator>dnscmd /info /socketpoolsize

Query result:
Dword: 9000 (00002328)

Command completed successfully.

E:\Users\Administrator>
```