Using LDAP Ping to Enumerate Active Directory Users

blog.netwrix.com/2022/12/13/using-ldap-ping-to-enumerate-active-directory-users

Joe Dibley

LDAP Nom Nom is a recently discovered brute-force technique for enumerating valid usernames in Active Directory — anonymously and without leaving any log entries behind. It abuses LDAP Ping, a little-known mechanism in Active Directory normally used by computers to check whether a domain controller is alive.

Handpicked related content:

[On-demand Webinar] Cyber Battle. Active Directory Security: Hacker vs Netwrix

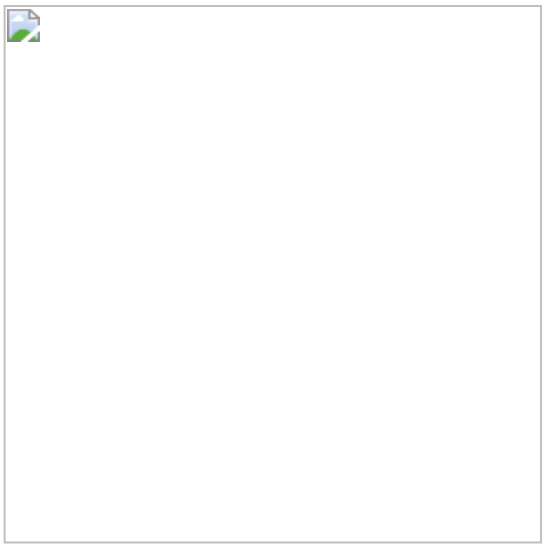
This blog post explains how LDAP Ping works and how adversaries can abuse it with LDAP Nom Nom.

How do I send an LDAP ping?

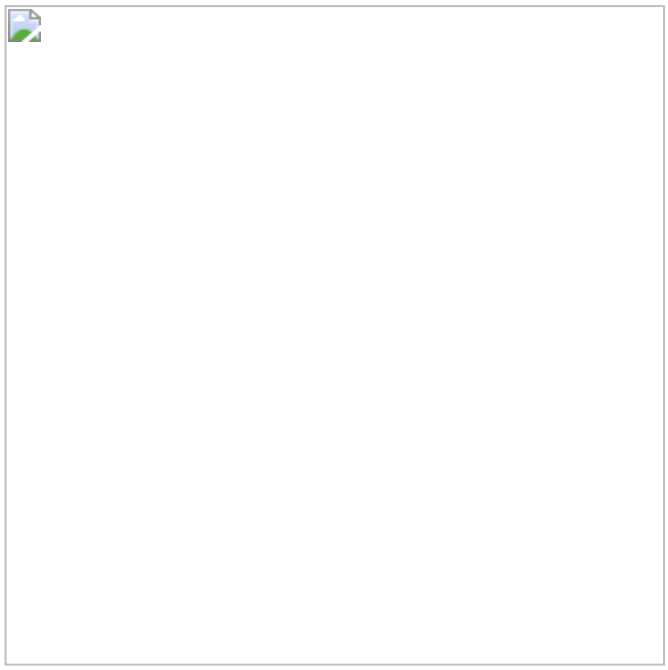
To send an LDAP ping, we can use LDP.exe, a built-in tool for executing LDAP requests on Windows operating systems.

1. First, we need to connect to a domain controller but not authenticate: Go to **Connection -> Connect…**, enter your DC name or IP address in the Server box, and click **OK**.

2. Because an LDAP ping returns a byte structure, we need to parse the returned values as binary rather than the standard string output. Go to **Options -> General** and set **Value Parsing** to **Binary**, as shown in the screenshot below:



3. Now we need to create the filter to search for a user account. In this example, we'll search for a user with a sAMAccountName of BETHANY_WHITLEY. Here are the details we need to craft our search filter:



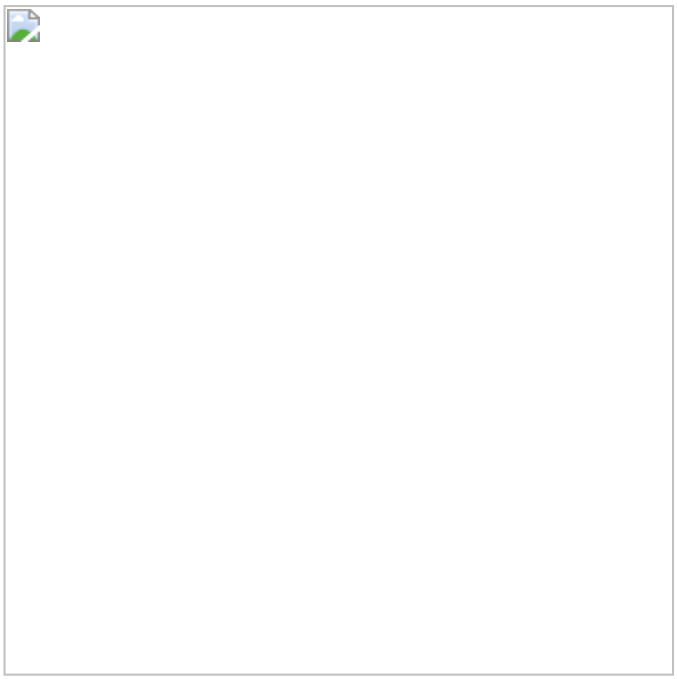
Attribute	LDAP Filter	Note
NtVer	(NtVer=\06\00\00\00)	Taken from Microsoft's LDAP Ping example
AAC	(AAC=\10\00\00\00)	The AAC filter to search for user accounts, determined by converting from the USER_ACCOUNT code of 0x00000010 using CyberChef
User	(User=BETHANY_WHITLEY)	The sAMAccountName to search for

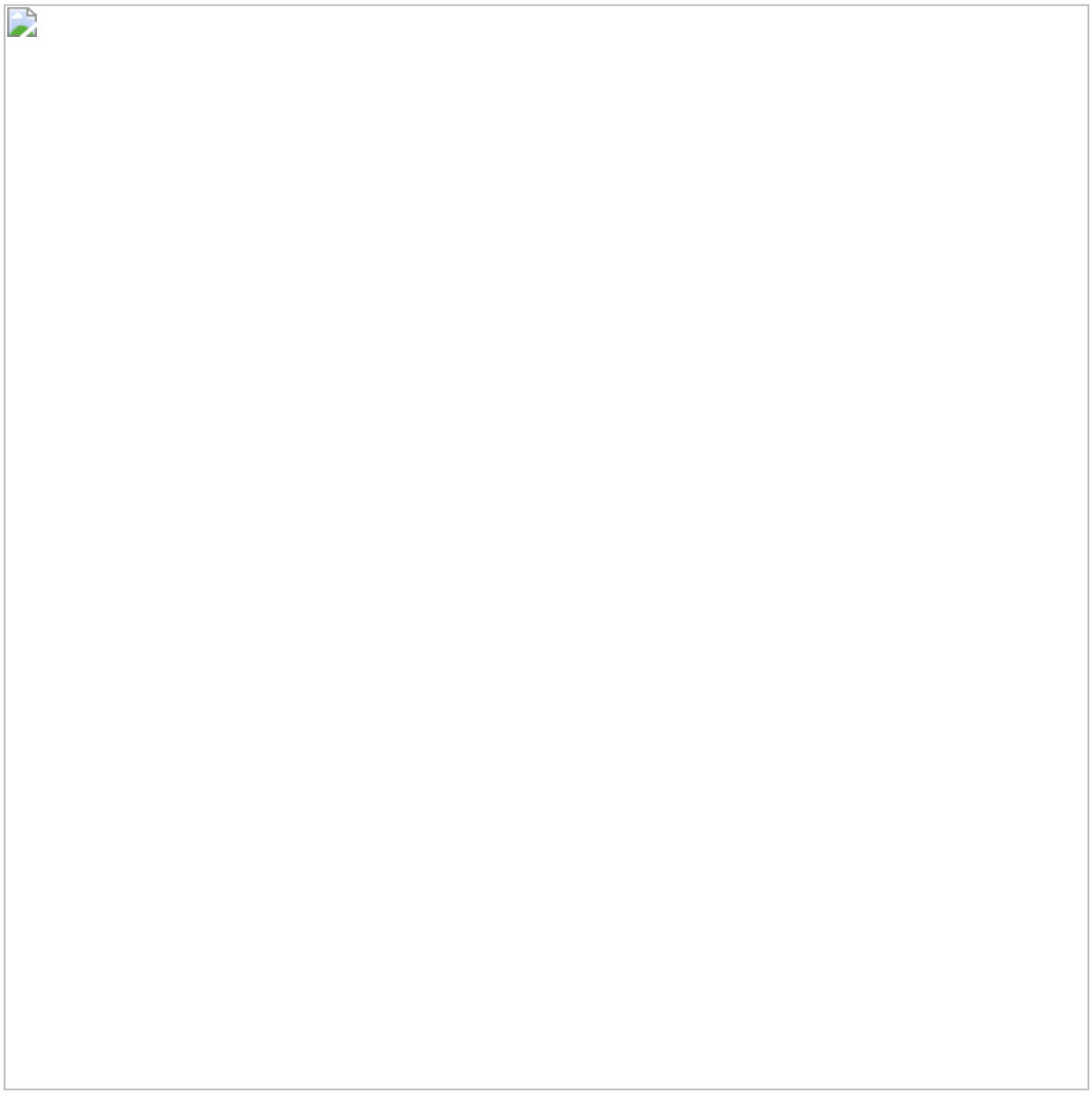
This means our LDAP Ping search filter will be:

```
(&(NtVer=\06\00\00\00)(AAC=\10\00\00\00)(User=BETHANY_WHITLEY))
```

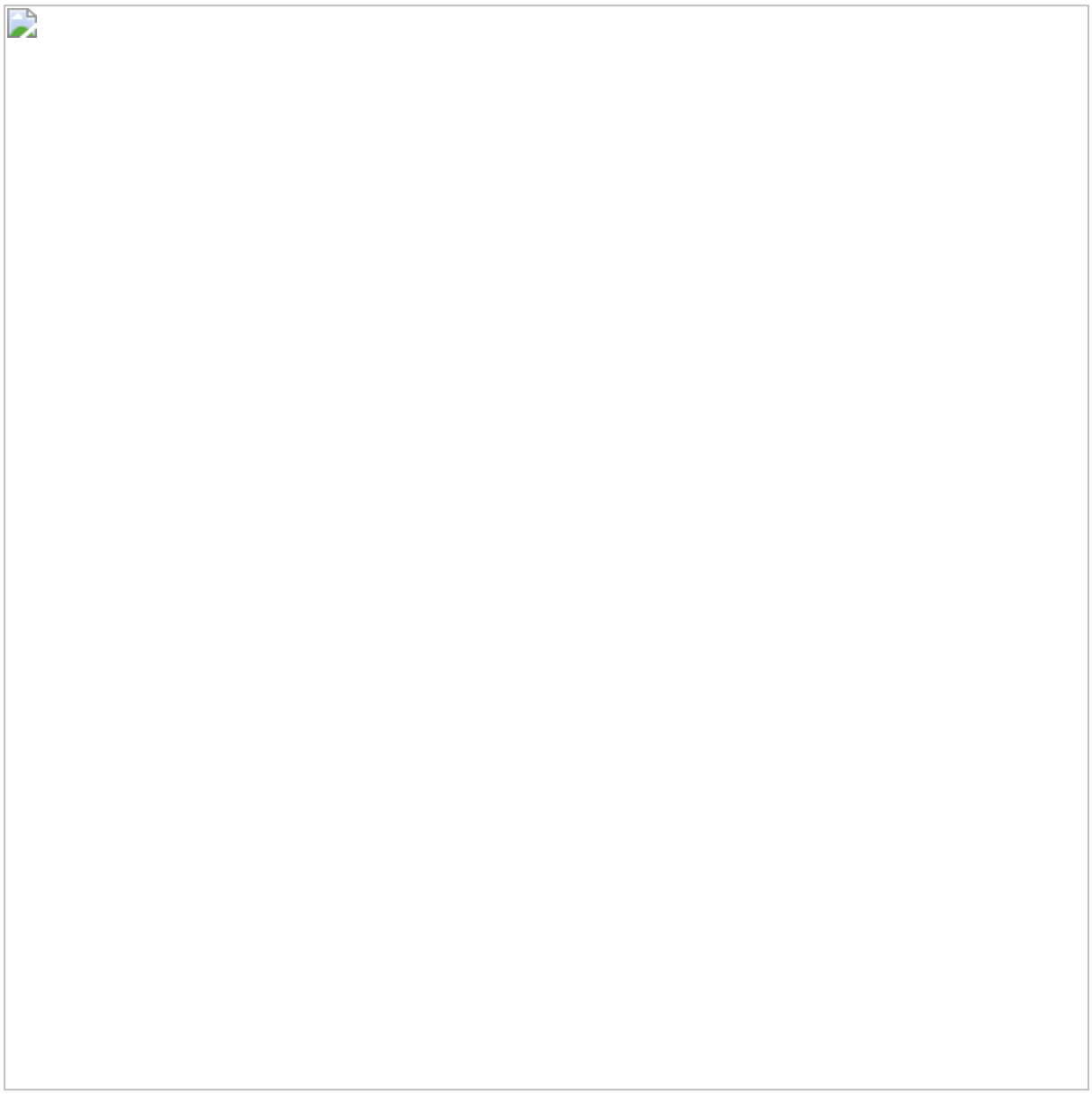
4. Now we execute the search: Open the Search dialog (**Browse -> Search**), fill it in as shown below and click **Run**.

5. Last, we need to check the search results. If the user exists, the results will look like this:





However, if we had searched for an account that did not exist (BETHS_NOT_HERE), the results will look like this:



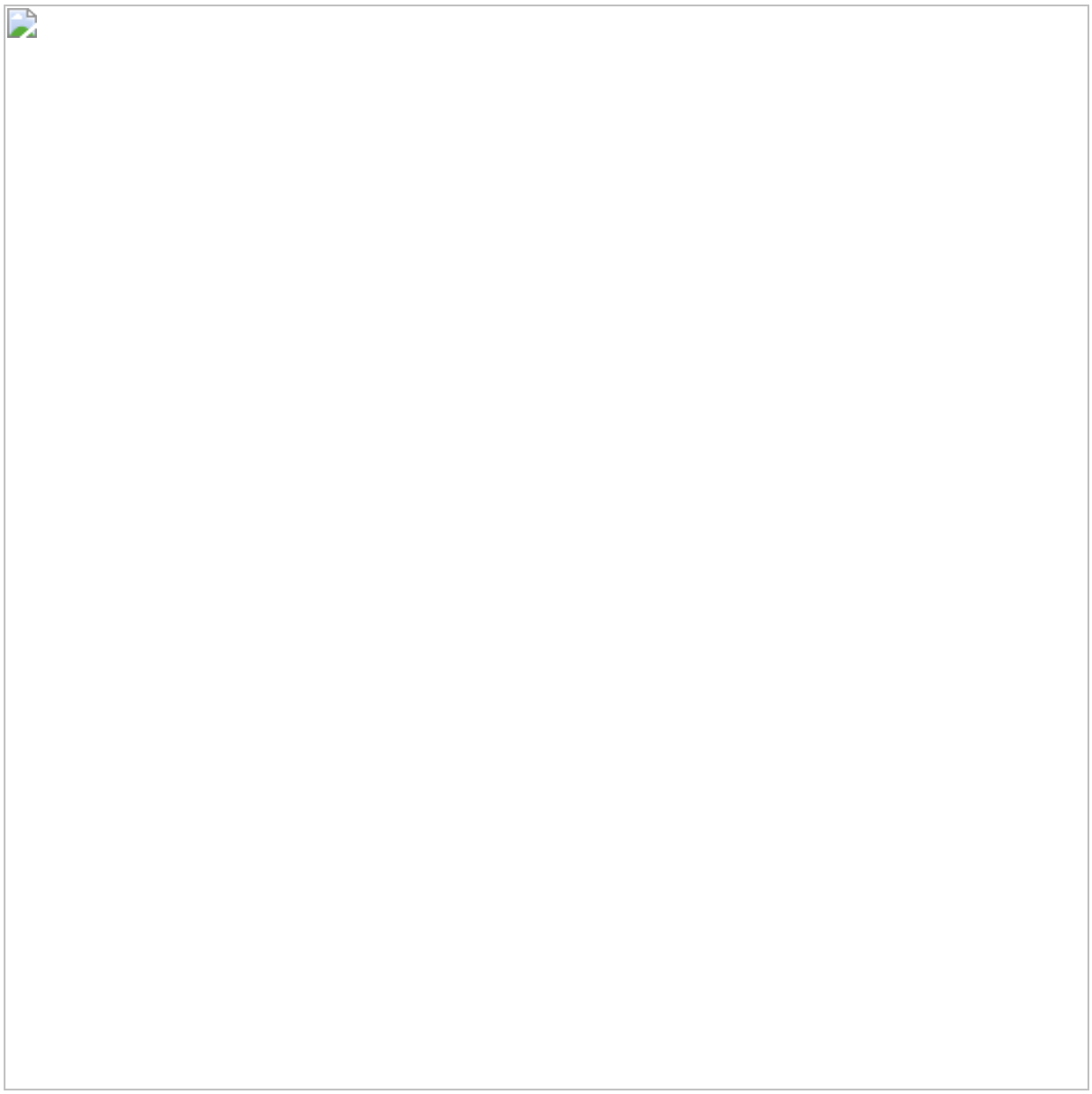
The numbers shown are different from the operation codes listed by Microsoft because they are hexadecimal. A hex value of 19 is equivalent to 25 in decimal, which indicates an unknown user.

Automating username checking with LDAP Nom Nom

An adversary can use LDAP Nom Nom to automate the process of sending LDAP ping requests for each username in a list (such as a list from SecLists) and checking whether it is valid. LDAP Nom Nom boasts performance of as many as 10,000 usernames per second against a single server.

To run this for yourself, you can install the tool and either download a username list or make your own. Then execute the tool using the following syntax

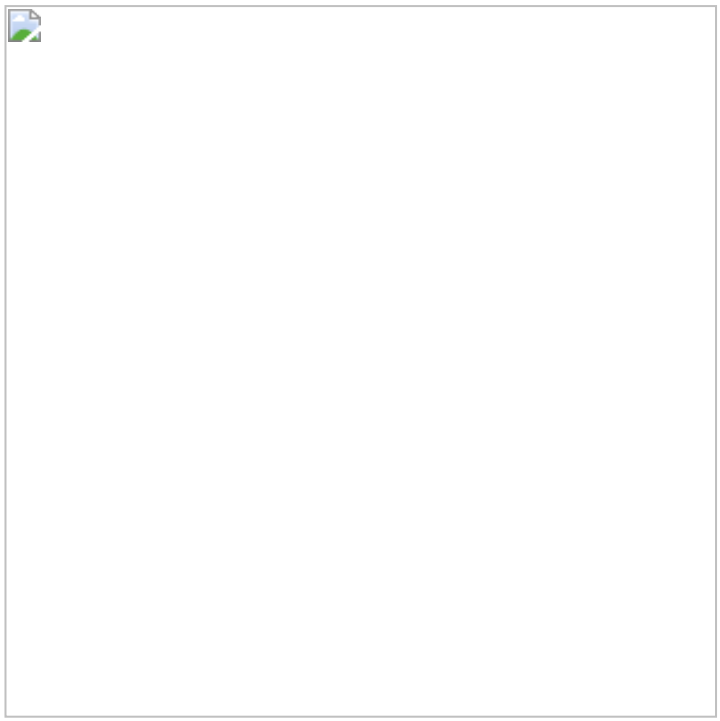
```
nomnom.exe –input <Path to username file>
```



What can I do to detect this?

LDAP Nom Nom cannot be detected using native logging. Instead, you need a solution that monitors LDAP traffic from the network layer, or a solutions such as Netwrix StealthINTERCEPT or Netwrix StealthDEFEND, which can detect LDAP Ping queries and analyse them for brute-forcing behaviour.

For example, the Netwrix StealthINTERCEPT screenshot below shows a query for a user (dowens); Since Objects Returned=0, the user does not exist.



Conclusion

Attackers who want to enumerate AD users have many techniques at their disposal. However many of these attacks are readily spotted by threat detection solutions. Although we're not aware of LDAP Nom Nom being used in the wild yet, its ability to evade most detection solutions may make it attractive for cyber criminals, so organizations would be wise to be prepared for it.

Joe Dibley
Security Researcher at Netwrix and member of the Netwrix Security Research Team. Joe is an expert in Active Directory, Windows, and a wide variety of enterprise software platforms and technologies, Joe researches new security risks, complex attack techniques, and associated mitigations and detections.