باسمه تعالی

NetBIOS
(Network Basic Input/Output System)

معرفی NetBIOS

در اصل، NetBIOS یک رابط برنامه‌نویسی (API) است که با سرویس‌های ارائه شده امکان تبادل داده میان برنامه‌های نصب شده بر روی تجهیزات مختلف را درون شبکه LAN مهیا می‌سازد (برنامه‌های مختلف با استفاده از آن به منابع موجود بر روی LAN دسترسی می‌یابند). این برنامه ابتدا برای شبکه اختصاصی IBM نوشته شده و سپس توسط مایکروسافت توسعه داده شده است. NetBIOS به خودی خود قادر به مسیریابی در شبکه نیست و در شبکه‌های محلی مورد استفاده قرار می‌گیرد. در شبکه‌های امروزی، NetBIOS بر روی TCP/IP هم اجرا می‌گردد و سه سرویس مجزای نام (NS)، توزیع دیتاگرام (DGM) و نشست (SSN) را به ترتیب از طریق شماره پورت‌های پیش فرض ۱۳۷، ۱۳۸ و ۱۳۹ ارائه می‌نماید (هم UCP و هم UDP). امروزه از پروتکل مستقل دیگری به نام SMB نیز استفاده می‌شود که از پورت‌های TCP با شماره‌های ۱۳۹ و ۴۴۵ استفاده می‌نماید.

آسیب‌پذیری‌های NetBIOS

حملات متداول علیه رایانه‌ای که NetBIOS بر روی آن فعال است عبارتند از:

۱. امکان جمع‌آوری اطلاعات راجع به شبکه هدف: با استفاده از دستور NBSTAT به راحتی می‌توان اطلاعاتی از قبیل نام رایانه، لیستی از نام‌های NetBIOS و ... را به دست آورد. همچنین گاهی امکان خواندن از (یا نوشتن بر روی) سیستم راه دور نیز وجود دارد.

۲. امکان اجرای حمله جعل (Spoofing): در صورتی‌که فرد حمله‌کننده به پیام‌های همه پخشی سرویس نام NetBIOS در شبکه محلی گوش دهد، می‌تواند تحت شرایطی خاص و با ارسال مناسب پاسخ مجعول، خود را به عنوان تجهیز مورد نظر معرفی نماید. درنتیجه به راحتی امکان اجرای حمله فردی در میان وجود دارد.

۳. امکان اجرای حمله DoS: سرویس نام NetBIOS که وظیفه نگاشت نام NetBIOS به آدرس IP را برعهده داشته و در استانداردهای RFC1001 و RFC1002 توصیف شده است، فاقد قابلیت احراز اصالت است. درنتیجه فرد مهاجم می‌تواند با ارسال پیام‌های مجعول Name Release یا Name Conflict، تجهیز قربانی را مجبور به حذف نام قانونی خود نموده و جلوی پاسخ‌گویی وی به درخواست‌های NetBIOS را بگیرد. این امر موجب قطع ارتباط قربانی با سایر میزبان‌های NetBIOS و درنتیجه وقوع

حمله DoS می‌گردد. برای جلوگیری از وقوع این حمله از سوی کاربران خارجی، بایستی با وضع قوانین مناسب در دیواره آتش مرزی شبکه برای پورت‌های TCP و UDP با شماره‌های ۱۳۷، ۱۳۸ و ۱۳۹ ، مانع از ارسال ترافیک NetBIOS NS از میزبان‌های خارجی به سوی میزبان‌های داخلی شد.

۴. امکان اجرای حمله DrDoS (Distributed reflection denial of service): حمله انعکاسی NetBIOS یکی از حملات شایع DDoS در حال حاضر در سطح جهان است. دلیل وقوع حمله نیز همانند سایر حملات انعکاسی، عدم وجود قابلیت احراز اصالت در پروتکل UDP و همچنین بزرگتر بودن سایز پیام پاسخ نسبت به پیام پرسش است. بنابراین فرد حمله‌کننده می‌تواند با جعل آدرس IP فرستنده و قرار دادن آدرس IP فرد قربانی، حجم زیادی از پیام‌های پرسش را برای افراد مختلف ارسال نماید. نتیجه این کار، سرازیر شدن ترافیک حجیمی از پاسخ‌ها به سوی فرد قربانی است. برای اجرای موفق این حمله، بایستی حمله‌کننده لیستی از تجهیزاتی که NetBIOS بر روی آن‌ها فعال بوده و از طریق شبکه اینترنت قابل دسترسی هستند و ضمناً به کوئری‌های درخواست نام پاسخ می‌دهند را در اختیار داشته باشد. هرچه تعداد تجهیزات این لیست بیشتر باشد، حمله سهمگین‌تر خواهد شد.

از این‌رو بایستی راهبران شبکه جلوی سوءاستفاده از این آسیب‌پذیری را بگیرند. برای جلوگیری از وقوع این حمله بایستی راهبران هر شبکه با وضع قوانین مناسب در دیواره آتش مرزی شبکه (برای پورت UDP با شماره ۱۳۷)، مانع از ارسال ترافیک NetBIOS NS از میزبان‌های خارجی به سوی میزبان‌های داخلی شوند.

با استفاده از دستور nbtstat -A [ip] نیز می‌توان از وضعیت NetBIOS برای یک آدرس IP خاص مطلع شد.

حمله چهارم (حمله DrDoS) یکی از شایع‌ترین حملات DDoS در سطح جهان بوده و مقابله با آن نیازمند امن‌سازی سرویس NetBIOS توسط تمامی کاربران (به خصوص راهبران شبکه) در سطح جهان است. از این‌رو در ادامه نحوه تشخیص حمله و همچنین نحوه مقابله با حمله و نحوه جلوگیری و سوءاستفاده از تجهیزات شبکه خودی شرح داده خواهد شد.

نحوه تشخیص حمله

تشخیص حمله DrDoS به سادگی امکان‌پذیر نیست. اما مشاهده ترافیک حجیم و نامتعارف NetBIOS برای یکی از آدرس‌های IP شبکه می‌تواند نشانه‌ای از وقوع این امر باشد. سایر نشانه‌های این حمله عبارتند از:

۱. وجود بسته‌های UDP حجیم به مقصد شماره پورت‌های بالا
۲. دریافت بسته‌های پاسخ UPD بدون ارسال پرسش (از نوع non-stateful)

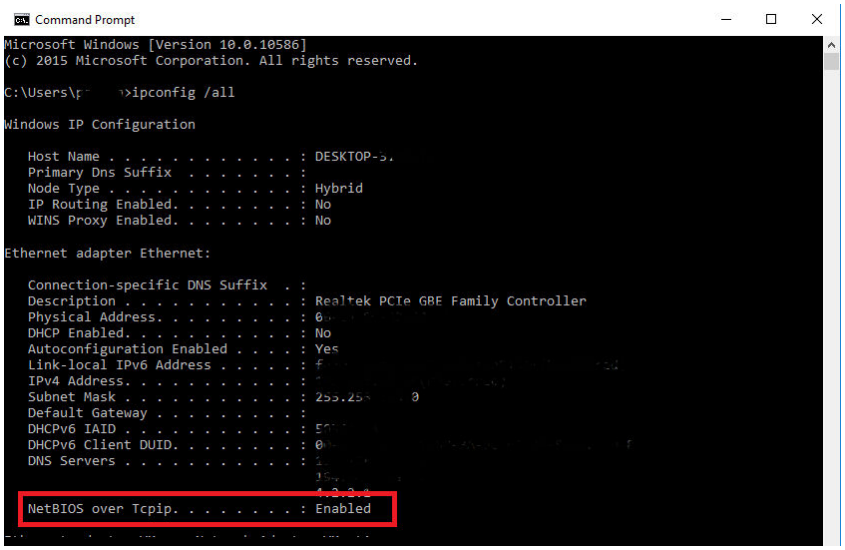
راه‌حل مقابله با حمله

در صورتی‌که سازمانی تحت حمله DrDoS قرار گیرد، بایستی اقدامات زیر انجام گیرند:

۱. استفاده از تجهیزاتی مرزی که قابلیت نظارت بر Stateful بودن ترافیک UDP دارند.
۲. استفاده از پروتکل مسیریابی BGP و ایجاد RTBH (Remotely Triggered Blackhole)
۳. هماهنگی با ارائه‌کننده بالادستی سرویس اینترنت سازمان برای محدودسازی حمله

نحوه بررسی وضعیت NetBIOS

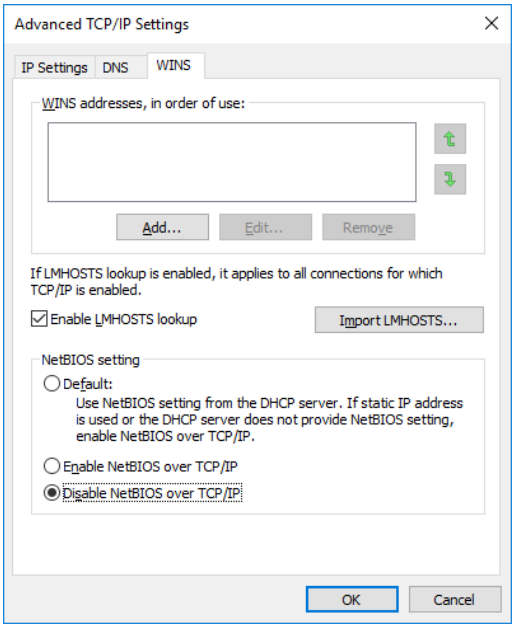
برای بررسی فعال بودن یا غیرفعال بودن NetBIOS بر روی سیستم عامل ویندوز می‌توان از دستور ipconfig /all استفاده نمود. با اجرای این دستور، وضعیت NetBIOS برای تک‌تک اینترفیس‌ها نمایش داده خواهد شد.



نحوه غیرفعال‌سازی NetBIOS

NetBIOS در سیستم عامل ویندوز به‌صورت پیش‌فرض فعال است و برای غیرفعال‌سازی آن بایستی به ترتیب مراحل زیر را اجرا نمود:

- بایستی در بخش Control Panel وارد قسمت Network Connections شده و با کلیک راست بر روی کارت شبکه مورد نظر، گزینه Properties را انتخاب نمود.
- بایستی با انتخاب Internet Protocol Version 4 در زبانه Networking ، گزینه Properties را انتخاب نمود.
- بایستی در زبانه General بر روی دکمه Advanced کلیک نمود.
- می‌توان در زبانه WINS تنظیمات NetBIOS را تغییر داد. با انتخاب Disable NetBIOS over TCP این سرویس غیرفعال می‌گردد.



البته بدیهی است که انجام این کار، بر روی تمامی برنامه‌ها و سرویس‌هایی که از NetBIOS استفاده می‌کنند، تاثیر می‌گذارد.

توجه: برای غیرفعال‌سازی NetBIOS over TCP/IP می‌توان مستقیماً از دستورات زیر استفاده نمود:

```
wmic /interactive:off nicconfig where TcpipNetbiosOptions=0 call SetTcpipNetbios 2
wmic /interactive:off nicconfig where TcpipNetbiosOptions=1 call SetTcpipNetbios 2
```