TECHNOLOGY REDEFINE

Wednesday, September 27, 2017

IDS, IPS AND FIREWALL EVASION USING NMAP

NIDS – Network Intrusion Detection System

- It Uses a network tap, span port, or hub to collect packets on the network
- Attempts to identify unauthorized, illicit, and anomalous

behavior based on network traffic
 • Methods: signature file comparisons, anomaly detection, stateful protocol analysis
 • Using the captured data, the IDS system processes and flags any suspicious traffic

HIDS – Host Intrusion Detection System

 • Generally involves an agent installed on each system, monitoring and alerting on local OS and application activity
 • Attempts to identify unauthorized, illicit, and anomalous behavior on a specific device/OS
 • The installed agent uses a combination of signatures, rules, and heuristics to identify unauthorized activity

IDS : Only reports that there was an intrusion.
IPS : Also takes actions against the issue to fix it or at least lessen its impact.

Evasion Techniques

- Decoys
- Proxies
- MAC Address Spoofing
- Ping Suppression
- Half Open Scan
- Fragmentation
- Timing

LABEL

- Changing Data length
- Transmission Unit
- Random Scan
- Sending Bad Checksums
- Using Multiple Techniques

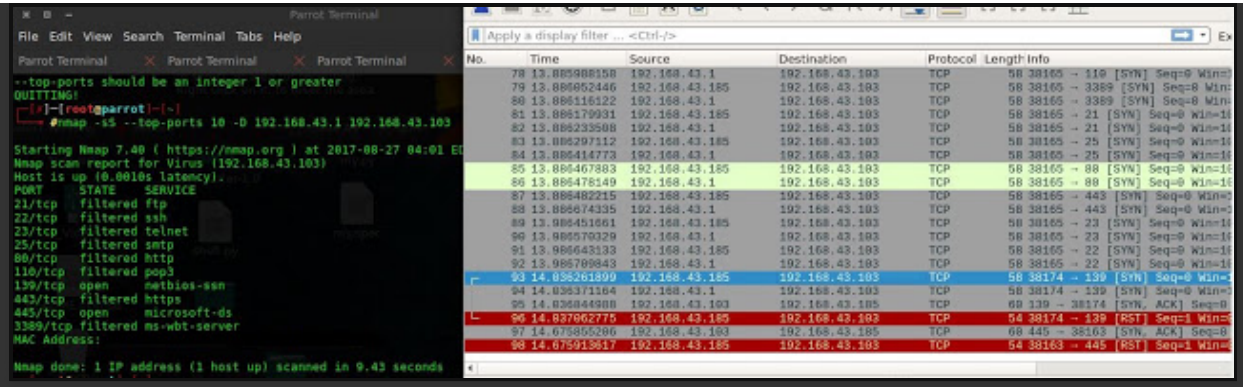
Decoys

Not strictly an evasion technique, It is used to obscure the source of the scan. we still need to send packets from our IP address but we can spoof other IP addresses while scanning so that it appears that the scan is coming from other hosts.

This might make it more difficult for the security device to automatically block our IP and more difficult for a forensic investigation to figure our IP.

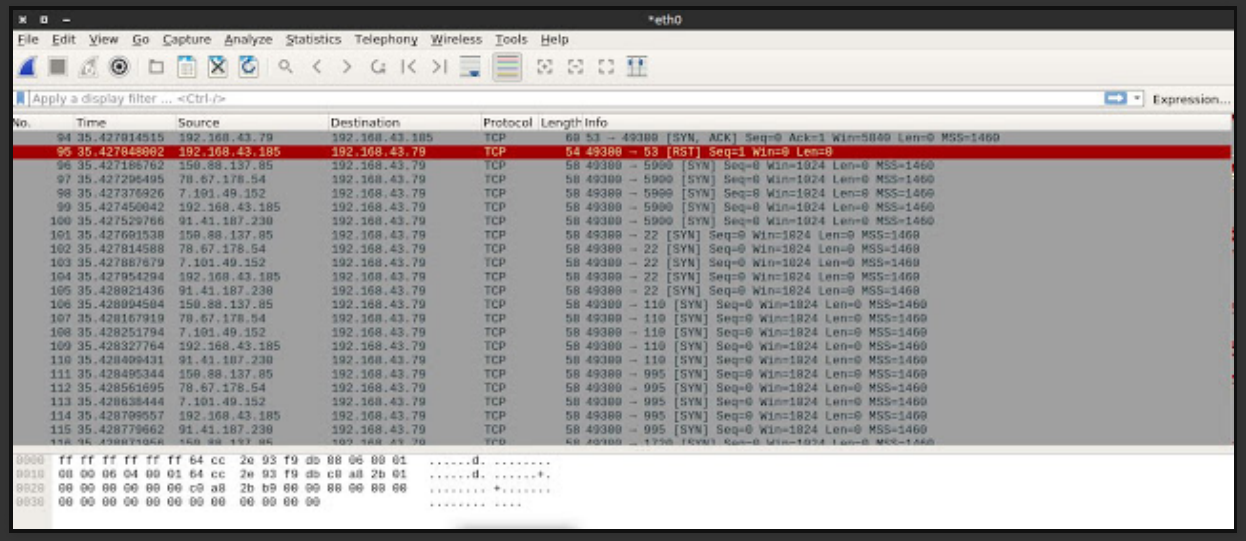
```
nmap -sS --top-ports 10 -D 192.168.43.1 192.168.43.103
```


- Network Access Control
- Nmap Cheatsheet
- Nmap Scanning
- NTLM Hashes
- Password Hacking
- Password Hacking Countermeasures
- Password Sniffing
- payload generator
- post exploitation
- Reconnaissance
- Remote Access
- Reverse Proxy Server
- Risk Assessment
- Router Attacks
- Scanning
- Scanning Types
- Social Engineering
- Surveillance
- Virtual Ports
- Zone Transfer




```
nmap -sS -D Rnd:5 192.168.43.103
```

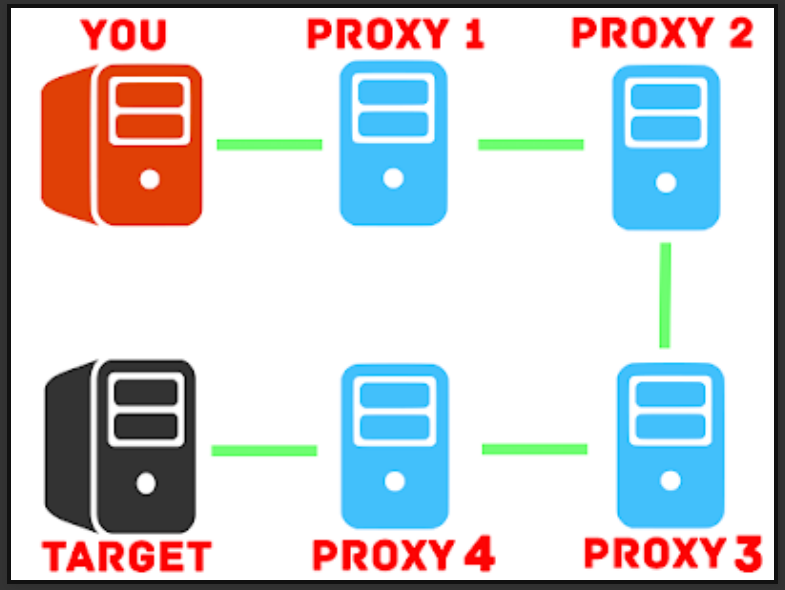
Rnd:5 will generate 5 random decoys



Using Proxies

We can use proxies between ourselves and the target system. By using proxies, the IP address of the proxies is recorded at the target, rather than our own. Makes it VERY difficult to trace the source of the scan.

```
nmap -sS --proxies socks4://115.29.161.103:1080,
http://213.85.92.10:80 Target
```



You can also scan using Tor network or Proxychain

MAC Address Spoofing

This technique can be very effective especially if there is a

MAC filtering rule to allow only traffic from certain MAC addresses so you will need to discover which MAC address you need to set in order to obtain results.

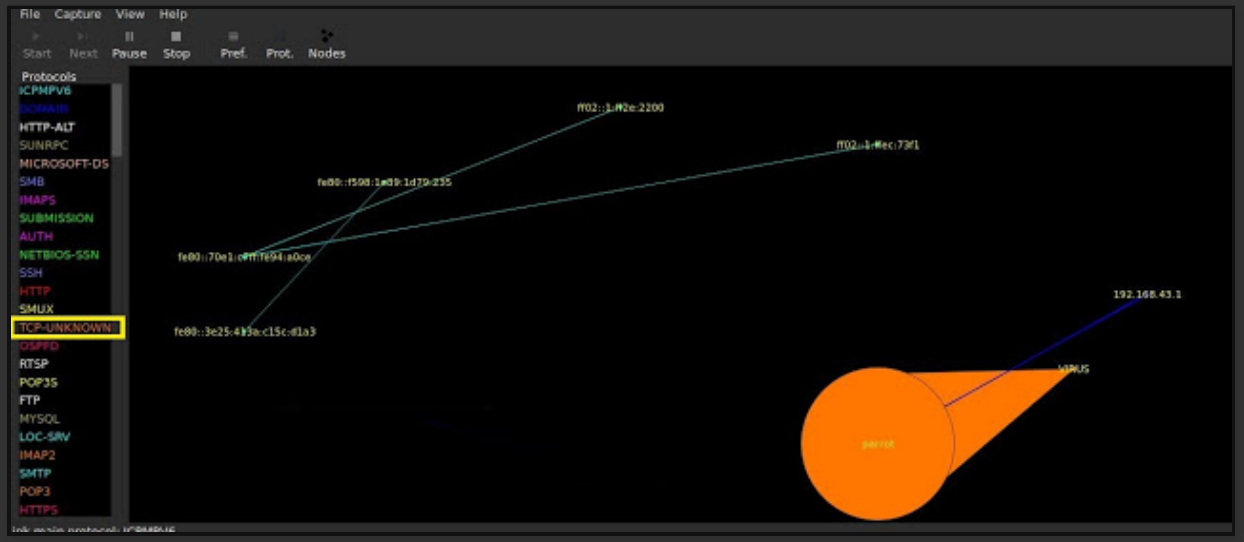
```
Specify MAC address from a Vendor  --spoof-mac Dell/Apple/
Generate a random MAC address      --spoof-mac 0
Specify your own MAC address   --spoof-mac 00:01:02:25:56:AE
```

Ping Suppression

Often security administrators block ICMP (echo request, echo reply) ping on firewall to keep outside attackers from being able to find active hosts.

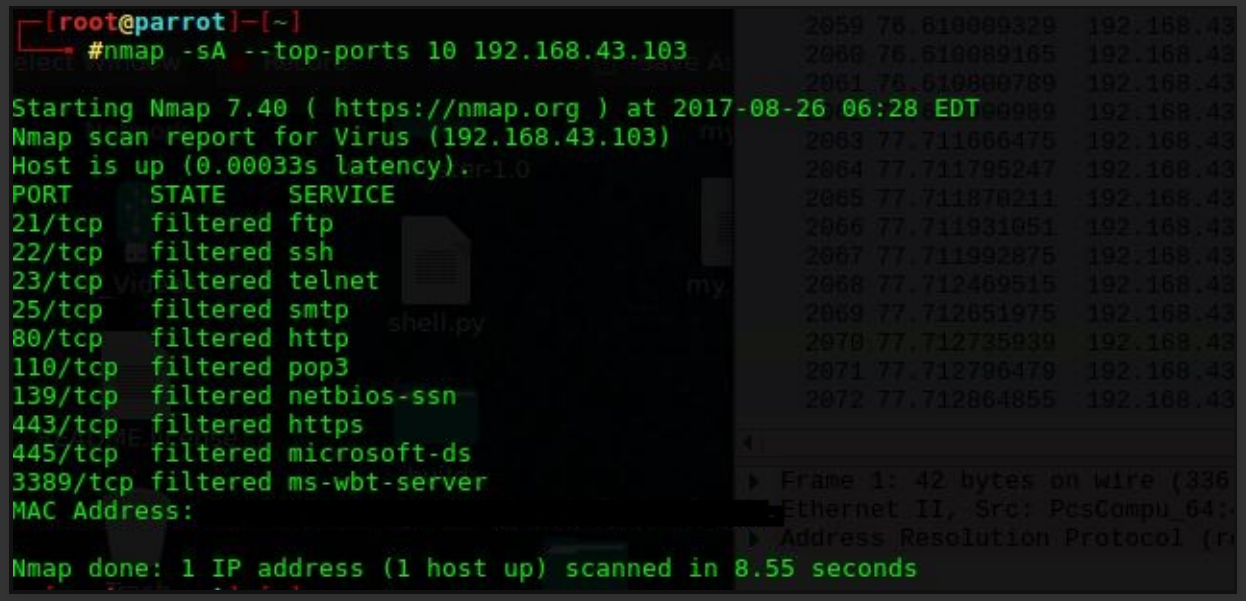
When we Scan With Nmap it sends out an ICMP Request to see if the host exists and is up. If it doesn't receive a response, it will report back that the host is down. By using the -Pn switch we can scan our target without sending the default ICMP.

```
nmap -Pn 192.168.43.103
```



Half Open Scan (ACK Scan)

When the TCP three-way handshake establishes(SYN, SYN-ACK, ACK), every packet sent subsequently in the communication will have the ACK bit set. Firewall will assume that this ACK packet is part of an established communication between the client and server and, thereby, let it pass.



- Only provides "filtered" or "unfiltered"
- Useful in reconnaissance for a more detailed scan

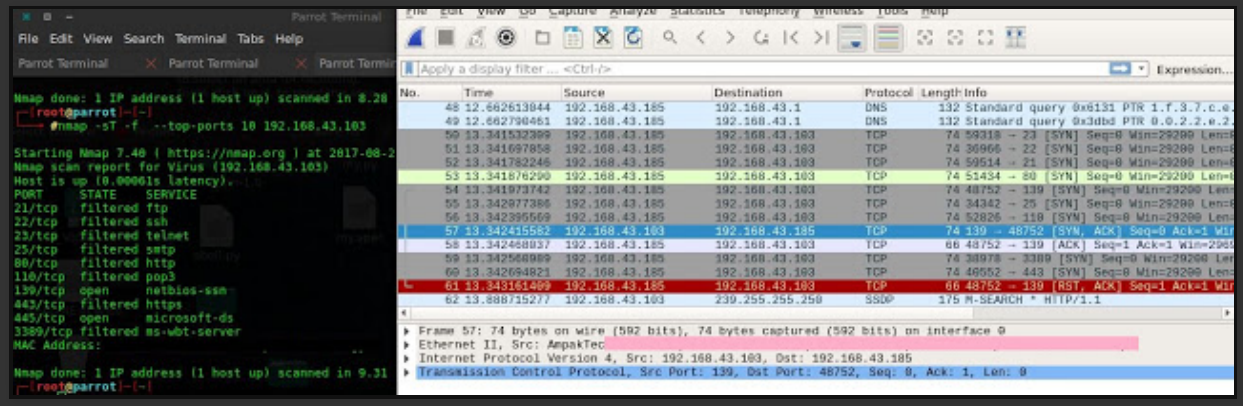
Fragmentation

In this attack nmap will break the IP header into many small pieces to evade the IDS. The pieces are then reassembled at

the destination. Since IDS's relys on signatures very similar to AV software the pieces would not match the signature the IDS is looking for. This would allow the pieces to traverse the network where they would be reassembled at the destination machine and do their dirty work.

For increasingly more smaller fragments use the -ff switch.

```
nmap -sT -f --top-ports 10 192.168.43.103
```



Timing (--Scan_delay, -T0-T5, -ttl)

Most IDS's only alert on threshold level of scans takes place. For instance, Snort on the default setting only alerts on scans when 15 or more ports are scanned per second. If we can slow down the speed of our scan, it can go right past the IDS without alerting the administrator.

Using the --scan_delay We can set the minimum amount of time between each probe that nmap sends to the target.

```
nmap -sS --scan_delay 5s Target
```

We can also use use built in -T timing switch to slow down our scan

```
 nmap -sS -T0 Target
```

```
 nmap -sS --ttl <value> Target
```

ttl is useful if you are in a slow network and you don't want your scan to be time out early.

ttl sets the IPv4 time-to-live field in sent packets to the given value in milliseconds.

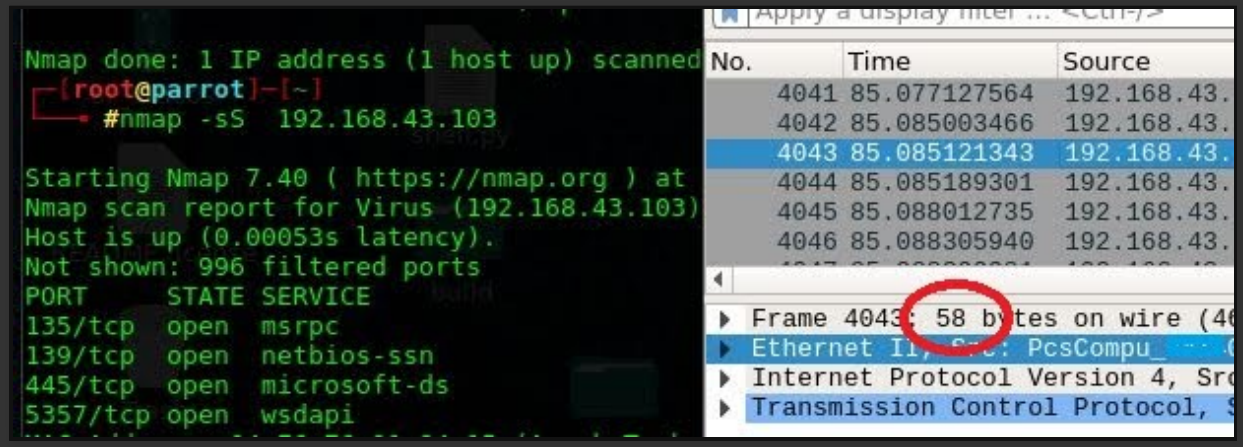
Changing Data length

Some firewalls and IDS's have signatures of nmap scans based upon the length of the packet. These signatures include the default data length of nmap's scanning packets. These packets are generally very small (TCP scan is 40 bytes and an ICMP scan is just 28 bytes). If we can change the length of these packets by appending random data to it we can at least get past this signature component and may be able to get past the

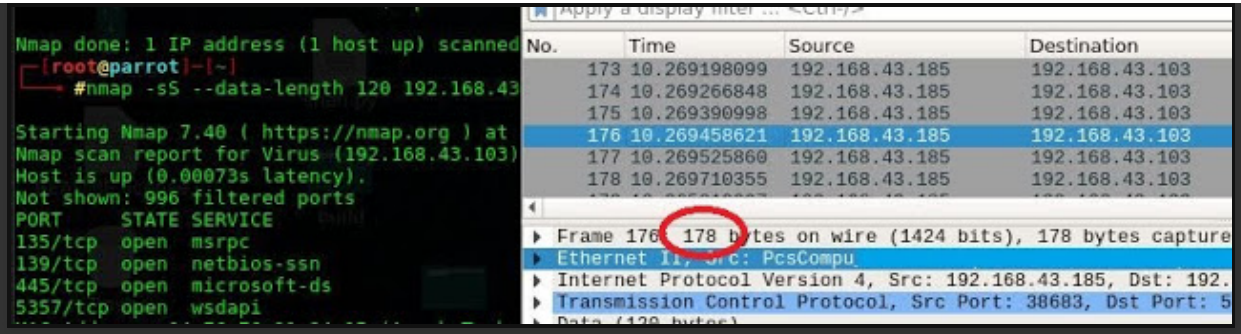
IDS to the network.

By choosing a data length other than the default, nmap will pad the packet so that it doesn't look like a typical scanning packet and hopefully, more like a legitimate packet.

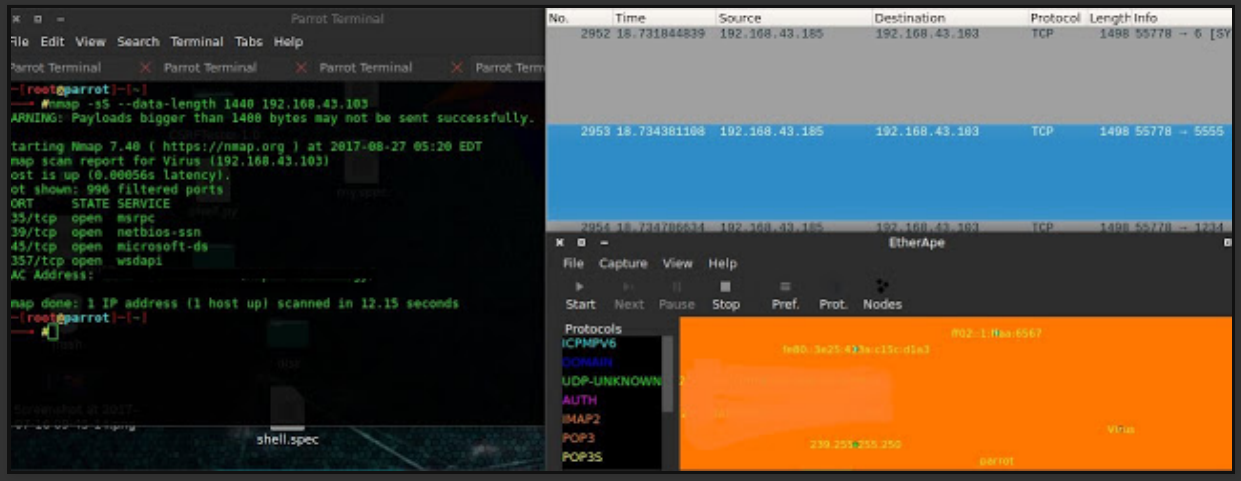
Before



After Adding --data-length 120 58+120=178



Note that payloads larger than 1400 bytes are NOT allowed.



Transmission Unit (--mtu)

It is an extension of nmap's fragmentation options. A fragmentation option of -f is the same as specifying an --mtu of 8, and a fragmentation option of -ff is the same as an --

```
mtu of 16. The Maximum Transmission Unit (mtu) must be a
multiple of eight (8,16,24,32. . . ).

nmap -sS --mtu 24 Target

Scan with Random Order (--randomize-hosts)

Shuffles each group of up to 16384 hosts before it scans them.
This technique combined with slow timing options in nmap can
be very effective when you don't want to alert firewall.

nmap --randomize-hosts 192.168.1.60-74

Sending Bad Checksums (--badsum)

Checksums are used by the TCP/IP protocol to ensure the data
integrity. By sending packets with incorrect checksums can
help you to discover information from systems, Because Some
firewall or IDS will respond if they are not properly
configured.


nmap -sS --badsum Target

Using Multiple Techniques

To make sure that your scans are not detected, you may want to
use several of these techniques combined. For instance, you
```

may want to slow the scan to T1, fragment the packets (-f), lengthen the packet to 1200 bytes, use proxies, such as this;

```
nmap -sS -T1 -f --badsum --data-length 1200 --proxies
sock4://176.57.216.214:80,http://213.85.92.10:80 Target
```

Scans, such as this, will be very slow, but nearly undetectable.

Countermeasures:

- Configure IDS, IPS & Firewall Properly
- Manage system, IDS, IPS logs
- Filter inbound ICMP Request & Response
- Filter all outbound ICMP type 3 unreachable messages
- Check how IDS Reacts on heavy traffic & handles fragmented IP packets
- Be aware of all Evasion techniques & bypass techniques
- Perform Scanning From Internet to your system & check available ports
- Monitor traffic

Tools:

- Nmap
- Wireshark
- EtherApe

References

Etutorials.org

Hackers-arise

Best Open Source IDS

By Himanshu - September 27, 2017

Ph?n ?ng: funny (0) interesting (0) cool (0)

Labels: Badsum, Decoy scan, Evasion Techniques, Firewall Evasion Countermeasures, frag, MAC Spoofing, mtu, Proxy scan, scan-delay

1 comment

Google+

Add a comment

Top comments

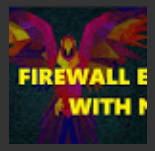
Himanshu shared this via Google+ 8 months ago - Shared publicly

+1 · Reply

Newer Post Home Older Post

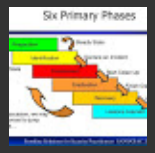
Subscribe to: Post Comments (Atom)

Popular Posts



IDS, IPS AND FIREWALL EVASION USING NMAP

NIDS – Network Intrusion Detection System • It Uses a network tap, span port, or hub to collect packets on the network • Attempts t...

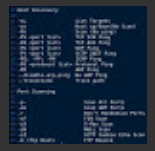


INCIDENT RESPONSE PLAN

An incident response plan (IRP) is a set of written instructions for detecting, responding to and limiting the effects of an information...

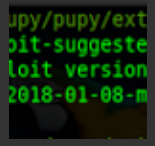
INSTALLING PRESISTENCE BACKDOOR IN WINDOWS

USING METASPLOIT windows/local/s4u_persistence windows/local/vss_persistence windows/local/registry_persistence windows/manage...



NMAP CHEAT SHEET

Target Specification 192. 168. 100. 1-50 IP Range 192. 168. 100. 1/24 CIDR Spec. -iL Filename IP Addr File - iR...



WINDOWS-EXPLOIT-SUGGESTER

./windows-exploit-suggester.py --update This will download latest ms bulletin xls file pip install xlrd --upgrade to download xl...

PUPY (RAT, POST EXPLOITATION TOOL)

Installing pupy git clone https://github.com/n1nj4sec/pupy.git pupy cd pupy git submodule init git submodule update pip install -r pu...

Exploit Office 2016 using CVE-2018-0802

If you don't have Empire download from here Just run ./setup/install.sh to install Also Download Exploit for CVE-2018-0802   Cr...

Comment