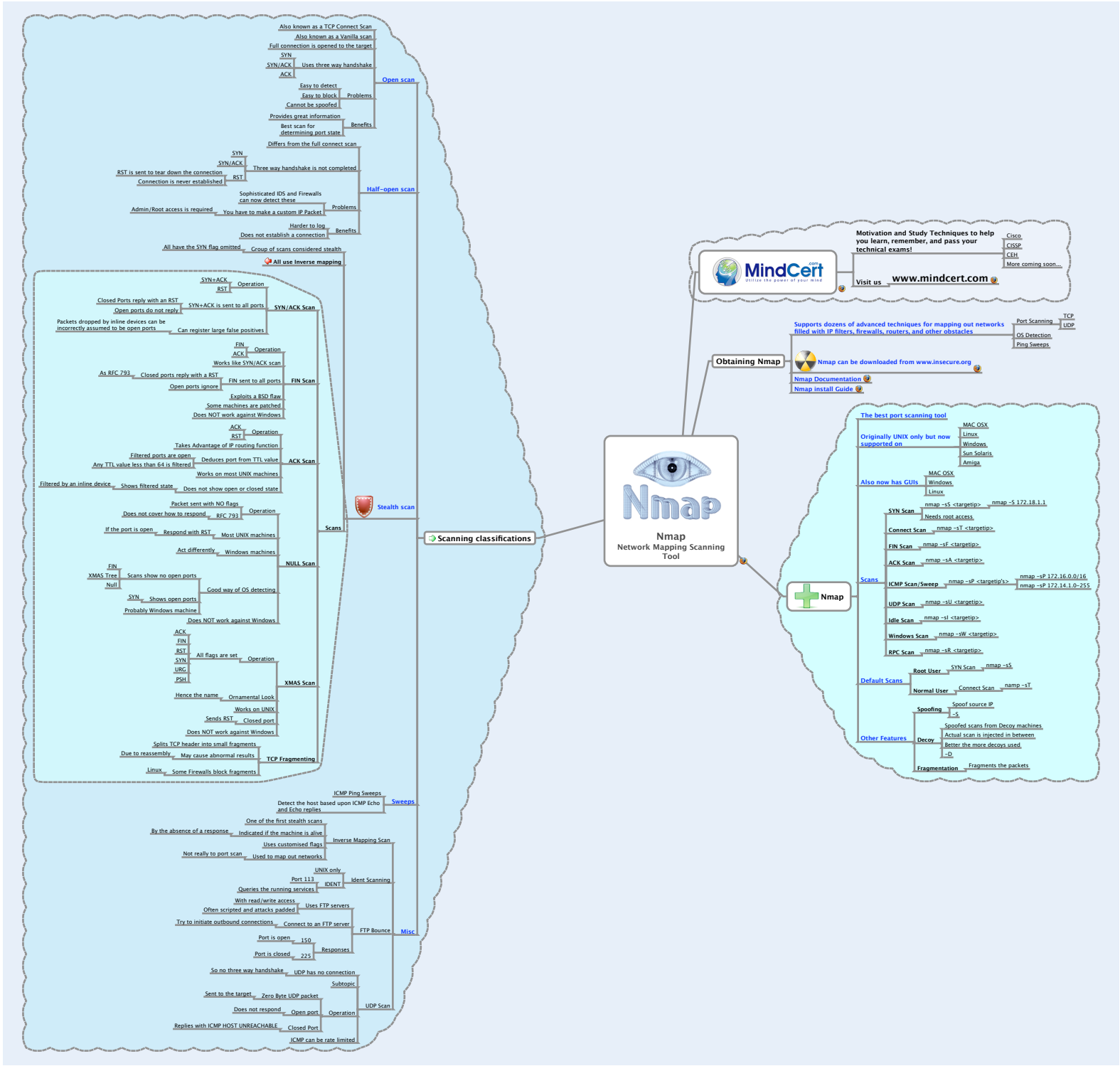
Nmap
Network Mapping Scanning Tool
Scanning classifications
Open scan
Also known as a TCP Connect Scan
Also known as a Vanilla scan
Full connection is opened to the target
Uses three way handshake
SYN
SYN/ACK
ACK
Problems
Easy to detect
Easy to block
Cannot be spoofed
Benefits
Provides great information
Best scan for determining port state
Half-open scan
Differs from the full connect scan
Three way handshake is not completed
SYN
SYN/ACK
RST
RST is sent to tear down the connection
Connection is never established
Problems
Sophisticated IDS and Firewalls can now detect these
You have to make a custom IP Packet
Admin/Root access is required
Benefits
Harder to log
Does not establish a connection
All use Inverse mapping
Group of scans considered stealth
All have the SYN flag omitted
Stealth scan
Scans
SYN/ACK Scan
Operation
SYN+ACK
RST
SYN+ACK is sent to all ports
Closed Ports reply with an RST
Open ports do not reply
Can register large false positives
Packets dropped by inline devices can be incorrectly assumed to be open ports
FIN Scan
Operation
FIN
ACK
Works like SYN/ACK scan
FIN sent to all ports
Closed ports reply with a RST
As RFC 793
Open ports ignore
Exploits a BSD flaw
Some machines are patched
Does NOT work against Windows
ACK Scan
Operation
ACK
RST
Takes Advantage of IP routing function
Deduces port from TTL value
Filtered ports are open
Any TTL value less than 64 is filtered
Works on most UNIX machines
Does not show open or closed state
Shows filtered state
Filtered by an inline device
NULL Scan
Operation
RFC 793
Packet sent with NO flags
Does not cover how to respond
Most UNIX machines
Respond with RST
If the port is open
Windows machines
Act differently
Good way of OS detecting
Scans show no open ports
FIN
XMAS Tree
Null
Shows open ports
SYN
Probably Windows machine
Does NOT work against Windows
XMAS Scan
Operation
All flags are set
ACK
FIN
RST
SYN
URG
PSH
Ornamental Look
Hence the name
Works on UNIX
Closed port
Sends RST
Does NOT work against Windows
TCP Fragmenting
Splits TCP header into small fragments
May cause abnormal results
Due to reassembly
Some Firewalls block fragments
Linux
Sweeps
ICMP Ping Sweeps
Detect the host based upon ICMP Echo and Echo replies
Misc
Inverse Mapping Scan
One of the first stealth scans
Indicated if the machine is alive
By the absence of a response
Uses customised flags
Used to map out networks
Not really to port scan
Ident Scanning
UNIX only
IDENT
Port 113
Queries the running services
FTP Bounce
Uses FTP servers
With read/write access
Often scripted and attacks padded
Connect to an FTP server
Try to initiate outbound connections
Responses
150
Port is open
225
Port is closed
UDP Scan
UDP has no connection
So no three way handshake
Subtopic
Operation
Zero Byte UDP packet
Sent to the target
Open port
Does not respond
Closed Port
Replies with ICMP HOST UNREACHABLE
ICMP can be rate limited
Obtaining Nmap
Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles
Port Scanning
TCP
UDP
OS Detection
Ping Sweeps
Nmap can be downloaded from www.insecure.org
Nmap Documentation
Nmap install Guide
MindCert.com
Utilize the power of your mind
Motivation and Study Techniques to help you learn, remember, and pass your technical exams!
Cisco
CISSP
CEH
More coming soon...
Visit us
www.mindcert.com
Nmap
The best port scanning tool
Originally UNIX only but now supported on
MAC OSX
Linux
Windows
Sun Solaris
Amiga
Also now has GUIs
MAC OSX
Windows
Linux
Scans
SYN Scan
nmap -sS <targetip>
nmap -S 172.18.1.1
Needs root access
Connect Scan
nmap -sT <targetip>
FIN Scan
nmap -sF <targetip>
ACK Scan
nmap -sA <targetip>
ICMP Scan/Sweep
nmap -sP <targetip's>
nmap -sP 172.16.0.0/16
nmap -sP 172.14.1.0-255
UDP Scan
nmap -sU <targetip>
Idle Scan
nmap -sI <targetip>
Windows Scan
nmap -sW <targetip>
RPC Scan
nmap -sR <targetip>
Default Scans
Root User
SYN Scan
nmap -sS
Normal User
Connect Scan
namp -sT
Other Features
Spoofing
Spoof source IP
-S
Decoy
Spoofed scans from Decoy machines
Actual scan is injected in between
Better the more decoys used
-D
Fragmentation
Fragments the packets