OODA Security

Taking back the advantage!
About Me

• Kevin Fiscus
• Owner – Cyber Defense Advisors
• 24 Years in IT
• 13 Years in security
• SANS Certified Instructor
• GIAC Security Expert
• Cyber Guardian Red/Blue Team
The Bad News

• The average company finds out about a breach from a third party
• The average company has been breached for a year before detection
• Those are averages, meaning roughly half of companies are breached for more than a year before detection
• That is a problem!
First - OODA

- Concept developed by USAF Colonel John Boyd for fighter pilots
  - Observe
  - Orient
  - Decide
  - Act
- Complete the loop first and fly home
- Complete the loop last, take a short trip down
Information Security?

• What do fighter pilot concepts have to do with information security?
Let’s Change the Venue

• Close your eyes
• Think about your home
• It’s night and a sound wakes you
• Think about all of the normal sounds
  – Your furnace, the steam heat, your cat
• Assume it is NOT normal
  – How quickly would you be able to determine what and where
It’s a Bad Guy

• OK, so it’s a bad guy in your house
• You know your house, he doesn’t
• You know where to hide, or where he could be hiding
• You know how to get out
• You know where your phone (gun) is
• Assuming minimal preparedness, chances are that you win because you complete OODA first
Another Situation

• You get home late at night
• You walk in your house
• There are lights on you turned off
• Things have been moved
• Someone has gone through your “stuff”
• Things are missing
• Obvious, right?
The Point?

• In familiar environments, we have the OODA loop advantage
• Why is it then, that most organizations only find out about a breach via a 3rd party?
• Why is the average company breached for a year before detection?
• Why do we fail to complete the OODA loop?
Attackers Are Super Sneaky

• Ah, no! Not really
• Attackers do not behave like legitimate users
  – They attempt to learn the environment
• Legitimate users (and often admins) know where they need to go and go only there (for the most part)
Standard Attack Methodology

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks
Sneaky Bits

• Gaining Access can be difficult to detect
  – IDS/IPS may detect exploit
  – Application logs may show crashes or service restart

• Covering Tracks is meant to be difficult to detect

• Recon often never touches the target

• But what about scanning?
Scanning is EASY to Detect

• Every firewall log is filled with scanning
• External IDS/IPS systems constantly alerting to scanning
• The problem is not detecting scanning but rather filtering through the noise
• As a result, detecting scanning at the network perimeter is not usually reasonable
• Maybe there is a better way…
Users are Predictable

- Users don’t need to understand the network
- They know what buttons to push to do their jobs
  - Sending email, accessing corporate applications, storing files on the “S” drive (whatever that is)
- Almost all traffic is from end user computer to some servers or from server to server
- Virtually no traffic from end user system to other end user systems
Attackers are Blind

• Imagine you walk into a new house blind
• You learn the environment by bumping into things
Most attackers do the same things
  – Gain access inside the network
  – Ping sweep, port scan, DNS recon, vul scanning
  – Not activities of normal users and easy to spot, if we are looking
But Monitoring is HARD

• HARD = expensive, time consuming, resource intensive, etc.
  – Deploying a NIDS or NIPS to cover your entire internal network
  – Deploying HIPS or HIDS throughout your entire environment
  – Purchasing SIEM solutions and configuring logging everywhere

• Difficulty is relative to size
  – Large organizations may have budget but massive complexity
  – Small organizations have simple environments but no budget
There is an Easier Way

• Let us start very simply - netcat

    nc –l –p 80

• Assume this is run on your laptop

• Should anyone be connecting to your laptop on port 80?

• Check the listener, if it’s not running, someone did something unexpected and your OODA loop starts
Getting A Little More Complex

• How about this:

   nc –l –p 80; date >> trigger.txt

• Now you know when the connection happened

• Using the “-L” option on Windows or a loop in Linux establishes a persistent listener
• [root@lOCM ~]#while [ 1 ]; echo "started"; do IP=`nc -v -l -p 2222 2>&1 1>/dev/null | grep from | cut -d[ -f 3 | cut -d] -f 1`; iptables -A INPUT -p tcp -s ${IP} -j DROP; done
Let’s Expand the Coverage

• Egress filtering on the firewall
  – Allow anything required for business but block everything else
  – Log all blocked traffic

• Not perfect
  – Attackers will often use common ports (80, 53, 443, etc.)
  – Good egress filtering is uncommon so often attacker will use FTP, TFTP or other ports to download their tools
  – Attackers will often use one victim to scan for others
  – Don’t forget about malware
Even Better

• Break your network into VLANs
  – Does require a managed switch
• VLANs should largely mirror the business
• Allow all necessary traffic between VLANs
• Block and log all else
  – Any blocked traffic is an attacker, a user doing something wrong, a misconfiguration or a bad block rule (all are things you want to know about)
But That Is Difficult!!!

- Yes, and no
- Depends on the level of granularity
- Consider 2 VLANs; servers and users
- Expand to 3 VLANs; servers, standard users and IT users
- Incremental steps are perfect
Other OODA Accelerators

• Create common but unlinked pages on web sites
• Rename the “Administrator” account then create a fake account named “Administrator”
• Create fake but sensitive sounding documents
• Log access to all of the above
• Creativity leads to more ideas – this is not an exhaustive list
Benefits

• Easy to set up
• Fairly low maintenance
• Fairly low false positives
• Accelerates out OODA loop
• If done carefully, difficult for an attacker to detect
How?

• First, understand what is normal
  – Required to define what needs to be allowed
  – Necessary because detecting abnormal is extremely difficult if you don’t know normal

• Consider the difficulties of configuring NIDS
  – They are designed to detect bad, not deviations from good
  – Require a LOT of tuning
  – Basically, blacklisting technology so difficult to managed
Limitations

- OODA acceleration is not designed to be 100% effective
- Based on the fact that the vast majority of attackers walk around your network “blind” and thus run into a lot
- That is OK because the attackers only need to trip one “sensor”
Not All or Nothing

• Designed to improve over existing controls
• Incremental improvements are wonderful
• A single NetCat listener can make the difference between detection and undetected compromise
• Ideas can scale from the largest environments to the smallest – but those in the middle will benefit the most
Questions

• Kevin Fiscus
• http://www.cdasecurity.com
• http://www.facebook.com/CyberDefenseAdvisors
• http://www.facebook.com/kevinbfiscus
• http://www.linkedin.com/in/kevinbfiscus
• kfiscus@cdasecurity.com
• kfiscus@sans.org