nmap, nessus, and snort

Vulnerability Analysis & Intrusion Detection

agenda

- Vulnerability Analysis Concepts
- Vulnerability Scanning Tools
    - nmap
    - nikto
    - nessus
- Intrusion Detection Concepts
- Intrusion Detection With snort

vulnerability assessment

- Vulnerability Assessment Process
  - Reconnaissance: Discover the Network
  - Enumerate the Devices on the Network
  - Determine the Services on the Devices
  - Verify Known Vulnerabilities
  - Report on Vulnerabilities
- Repeat this process, Over and Over

vulnerability assessment

- Vulnerability Assessment Practices
  - Perform Scans at a Regular Interval, ex. Weekly
  - Perform Emergency Scans for New Vulnerabilities
  - Provide PGP-signed e-mail on a Mailing List To Notify Customers of Upcoming Scans
  - Conduct Scans from a Well Known Source
  - Maintain a list of Admin Contacts for Notification

vulnerability assessment

- New Vulnerability Discovered Announcements

BugTraq, @Risk, CERT Mailing Lists

SecurityFocus Website
http://www.securityfocus.com/

SANS Top 20
http://sans.org/top20/

SANS Internet Storm Center News Summary
http://isc.sans.org/newssummary.html

Common Vulnerabilities and Exposures
http://cve.mitre.org/

vulnerability assessment

- Common Vulnerabilities At Universities
  - Phishing
  - Virus Infected E-mail
  - Buffer Overflows (HTTPD, SSHD, FTPD, RPC-DCOM)
  - Web Server Software (CGI's, PHP)
  - Client Browsers (XSS, Javascript, ActiveX)
  - P2P Download Viruses
  - Brute Force Password Attacks
  - Password Sniffing
- NOTE: Phishing is mostly an education problem. Also note that E-mail and the Web are very common attack vectors.

vulnerability assessment

Reconnaissance Tools

DNS (dig, nslookup)
Google
Whois

Enumeration Tools (Network Scanners)

nmap*	http://insecure.org/
scanudp	http://www.geocities.com/fryxar/
scanrand (paketto)	http://www.doxpara.com/

Vulnerability Scanners

nessus*	http://www.nessus.org/
nikto*	http://www.cirt.net/
nsat	http://nsat.sourceforge.net/
n-stealth	
hydra	
xscan/xspy	

nmap

nmap

- http://insecure.org/
- Supports Many different Types of Scans
- More than just a Port Scanner:
- OS Fingerprinting
    - Version of the Service Running
    - Additional NMAP Scripting Engine Capabilities

nmap

- nmap scan types
  - TCP SYN Scan -- I send a SYN, You send either a RST or a SYN/ACK,Most common type of scan, aka "TCP Half-Open"
  - TCP CONNECT Scan -- I send a SYN, You send RST or SYN/ACK, I send ACK
  - TCP Bad Flags Scan -- I send an Illegal TCP Flags Packet, You send a RST or Nothing
  - TCP ACK Scan -- I send an ACK, You send a RST or Nothing
  - UDP Scans -- I send a UDP Packet, You send back ICMP Unreachable, or Response, or Nothing

nmap

- nmap port options
  - Do You Reall Want to Scan All Of the Ports from 0-65535 ???
  - ex. -p 0-65535
  - Allows Mixture of UDP and TCP:
  - ex. -sU -sS -p U:53,111,137,T:21-25,80,139,8080
  - By default: 2300 Services Checked
  - /usr/share/nmap/nmap-services
  - ex. -p F

nmap

- nmap os and services detection
  - OS Version Determined by Observing Unique OS IP Behaviors. Features including: timestamps, sequence numbers, window size, ICMP, fragmentation
    - ex. -O
  - Service Version Matches Regular Expressions in Response Packets
  - /usr/share/nmap/nmap-service-probes
  - ex. -sV
  - ex. --version-light
  - ex. --version-all

nessus

nessus

The Grandaddy of OpenSource Scanners
http://nessus.org/
Unix, MacOS, Windows

Changed to Closed Source But Still Free
http://tenablesecurity.com/

Signature-Based Vulnerability Scanner
Signature Updates Vary Depending on the Customer

Client/Server Model, Server Runs as a Daemon,
Connect to Server using GUI Client from Anywhere

nessus

- http://nessus.org/plugins/
- In the Past, this was called "plugin updates":
- Registered Feed: DEFAULT (free, 7-day delay on new signatures)
- Direct Feed: ($1200/year, no delay on new signatures)

- Starting July 31st, 2008:
- HomeFeed: (free, targetted at Home users, a subset of signatures)
- ProfessionalFeed ($1200/year, no delay on new signatures)
- NOTE: Charitable, Teaching, and Training Institutions may receive the
- ProfessionalFeed free of charge.

nessus

Register To Receive Signature Updates:

Visit the Website: http://www.nessus.org/register
And Input the Registration Code:

```
% /opt/nessus/bin/nessus-fetch -,Äìregister <license code>
```

View Current License:

```
% cat /opt/nessus/lib/nessus/plugins/plugin_feed_info.inc
% sudo /opt/nessus/bin/nessus-fetch --check
```

Update Signatures:

```
% sudo /opt/nessus/sbin/nessus-update-plugins
```

Add Update Command to Cron:

```
% sudo -s
% crontab -e
28 3 * * * /opt/nessus/sbin/nessus-update-plugins
```

nessus

NASL - Nessus Attack Scripting Language

See: http://www.nessus.org/doc/nasl2_reference.pdf

See Also:

"Network Security Tools:
Writing, Hacking, and Modifying Security Tools"
By Nitesh Dhanjani, Justin Clarke

A Flexible Programming Language for Vulnerability Testing
Routines to handle Packet Generation, and Common Protocols,
And Sending and Receving Results

Example: Apache Chunked Encoding Vulnerability
http://www.nessus.org/plugins/index.php?view=viewsrc&id=11030

nessus

- nessus client gui options
    - /opt/nessus/bin/NessusClient
    - Connects to Server Daemon running on Port 1241 on Localhost
    - Must Have Credentials to Login to Server Daemon
    - Scan Settings Saved in User .nessus-client directory

nessus

- nessus client
  - Select "Connect" and Login To Server
  - Select "+" to define Scan Targets
  - Select "+" to create a "New Policy"
  - Share this Policy, To Allow Others to Use it As Well

nessus

- nessus scan options
  - Multiple Scanner Modules: SNMP, TCP, Netstat, Ping, SYN, Tarpit, Default: TCP and Ping Scanners
  - Scanners Run in Parallel, Default: 40 Hosts at a Time, 5 Checks at a Time
  - CGI, SQL, and SMB "Thorough" Scans Can Be Slow
  - Windows and SSH LocalUser Scan Capability
  - Recommendations in the Advanced User Guide
  - http://www.nessus.org/documentation/

nessus

- nessus reports
  - In the GUI Client, BY-IP, Color Coded By Severity
  - List of Open Ports/Protocols
  - List contains Link to the Plugin
  - Output Default is: /home/<user>/.nessus-client/report-XXXXXXXXX.nessus
  - Open File in GUI, Select "EXPORT" To Save As .html

intrusion detection

Detecting Unauthorized Activity on Your Network

- breakin attempts, successful breakins, suspicious traffic, known attacks, unusual traffic

Two Common Detection Methods:

- Signature Based, and Anomaly Detection

Two Common Applications:

- IDS -- Out-of-Band, Passive Monitoring IDS,
    - Notify Me When Something Bad Happens!

- IPS -- In-Line IPS, (Intrusion *Prevention* Systems)
    - But If I Know It is Bad, Why Not Block it!

See Also: Darknets, and HoneyPots

intrusion detection

- Signature Based
  - Like Anti-Virus, Not Protected Against Unknown Attacks
  - Processing Signatures is Resource Intensive
  - Maintaining Signature Updates Requires Management/Cost

- Anomaly Based
  - Require a "Learning Period"
  - Can produce false-positives, The Mother's Day Restaurant Effect
  - May Not Be As Effective On Certain Attacks

intrusion detection

- IDS challenges
  - It is difficult to distinguish "good" traffic from "bad"traffic in many cases.
  - The closer you are to the Host, the more accurate your detection is going to be. For example, local system event logs, file system change logs, much more reliable, ex. Linux "incrond", inotify kernel file system event viewer
  - Firewalls, System Integrity, Anti-Virus... May Take Priority
  - IDS -- It's Not a Panacea, But Used Selectively It Can Help You Identify Problems

intrusion detection

Deploying the Monitor

- Central Monitor, Report Database, Management Console
- Remote Monitors (Probes)

Accessing The Traffic

- Passive Optical Splitter
- Backbone Switch Monitor Port/SPAN Port
- Aggregation Switch Monitor Ports
- Multiple Monitor Interfaces

Preparing To Handle the Output (Incident Handling)

intrusion detection

- Commercial and OpenSource Products

Commercial -- 3COM Tipping Point, IPS
HighSpeed Switch Signature Matching

Commercial -- Juniper IPS, Cisco IPS
Client/Server/Manager Signature Matching

Commercial -- Proventia (ISS)
Protocol Analysis

OpenSource / Commercial Support
SNORT IDS, or SNORT In-Line
http://snort.org/

OpenSource
BRO IDS
http://bro-ids.org/

snort

snort

- Started as a Sniffer, a better "tcpdump"
- Developed by Martin Roesch, 1998
- http://www.snort.org/ <--- The OpenSource Origin
- http://www.sourcefire.com/ <--- The Commercial Side
- Signature Based Detection
- Highly Customizable Configuration Language
- Current Version: 2.8.2
- http://www.snort.org/dl/current/snort-2.8.2.tar.gz

snort

- signature updates

SourceFire Rule Updates provided by
Sourcefire Vulnerability Research Team (VRT) On a subscription Basis
At Fairly Reasonable Price

Other Signature Updates Available From
http://www.bleedingthreats.net/
http://oinkmaster.sourceforge.net/

snort

- modes of operation

SNIFFER Mode -- on the command line as a tcpdump replacement

```
% sudo snort -dave
```

PACKET LOGGER Mode --

```
% sudo snort -b -l /logdir   <--- binary output, single file TCPDUMP output
% sudo snort -l /logdir      <--- logdir, creates per-IP directories, TEXT output
```

IDS Mode --

```
% sudo snort -c /etc/snort/snort.conf -h localnetaddress/localnetmask
```

snort

- Configuration File
  - /etc/snort/snort.conf
  - Global Variables Defined At Beginning of Configuration File
    - Defines Local Network and Local Well-known Services Hosts
  - "include" statements used to bring in configuration sections
  - Common Run Syntax:
    - snort -c /etc/snort/snort.conf -h localnetaddress/localnetmask -l /logdir -b -A fast

snort

- alert output

Lots of Flexibility in Sending Alert Outputs

Output Options Can be Set in the Configuration File

-s	<--- Syslog (auth.alert)
-A full	<--- Full Packet Headers
-A fast	<--- Abbreviated Packet Headers
-A console	
<sockets>	
<winpopup>	

snort

- preprocessors: plugins
  - Protocol Analysis Feature
  - Application Level Analysis
  - Attack Detection Plugins

snort

- snort rule syntax

Packet Headers
[action protocol source direction destination]
simple actions: alert, log, or "pass" (ignore)

Packet Contents
[packet matching attributes, alert messages]
IP/TCP/UDP/ICMP/strings, etc.

snort

- snort rules files

Default RULE_PATH is /etc/snort/rules

```
include $RULE_PATH/web-attacks.rules
include $RULE_PATH/backdoor.rules
include $RULE_PATH/community-bot.rules
include $RULE_PATH/community-virus.rules
```

Constructing Rules:
http://www.snort.org/docs/snort_htmanuals/htmanual_2.4/node14.html

snort

Example: Apache Chunked Encoding Rule in "web-misc.rules"

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS
(msg:"WEB-MISC Apache Chunked-Encoding worm attempt";
flow:to_server,established; content:"CCCCCCC|3A| AAAAAAAAAAAAAAAAAA"; nocase;
reference:cve,2002-0392...; classtype:web-application-attack; sid:1809; rev:9;)
```

```
action:      alert
protocol:    tcp
source:      any-non-local-address
destination: our-webservers
flow:        to_server,established   <--- TCP connection has been established
content:...                          <--- string match, hex 3A match
```

snort

- additional tasks
    - Database Integration
    - ACID, BASE, Etc.