chapter 6: PACKET STRING DATA

packet string data: imp human readable data
-considered as partial packet capture
-collected from same source fro, which nsm sensor gathering other data
-collect as much app layer data from clear text protocols as long term storage will permit

---

fpc data rentention is in terms of hours and days,
session data in terms of quarter years or years
pstr is in between that is weeks or months.

-no of freee and open source tools available for pstr data collection and generation.

-- in pstr only data you care about is human readable

URL SNARF

-part of d sniff suite
-passivley collects HTTP request data and stores it in common log format(CLF)

-passivley listen on interface and dump collected data to stdout, visible in terminal window

defualt listen on tcp
port 3128\8080\80
interface eth0

HTTPRY

-specialized packet sniffer for displaying and logging http traffic only.
-allow for capture and output of any http header in any order.
-ability to customize output.

JUSTNIFFER

-full fledged protocol analysis tool that allow for completely customizable output.

-includes python script, which extract files transffered during http communication
-can be extended to do perfromance measures ,response times and connection times.

VIEWING PSTR DATA

-potential solution that can parse view and interact to pstr data are:
*logstash
***Raw text parsing with bash tool**

logstash

-log parsing engine
-allow both single and multiline logs
-also a powerful log collector
-can confgiure logstash to parse log that are collected with url snarf
-logstash 1.2.2 includes kibana interface for viewing logs.

Raw text parsing with bash tool

-parsing raw data using **sed , awk, and grep** can sometimes carry a mystical aura of fear that is not entirely desrved
-we can search for every host seen in the data by simply performing search for host field.

CHAPTER 7: DETECTION MECHANISMS, INDICATORS OF COMPROMISE AND SIGNATURES

DETCTION MECHANISMS

-detection is function of software that parses through collected dtaa to generate alert data, this is refferd to as detection mechanism

2 primary categories:
1)signature based detection
2)Anamly based detection

SIGNATURE BASED

-we look for matches of specfic patterns in data .
-patterns can be simple like ip, text string
-patterns can be complex like specified numjber of null bytes occuring occuring after a specific string.
-when these pattens are broken down into objective platform independent pieces of data they become **INDICATOR OF COMPROMISE**
-when they are expressed in form of platform specific language of detectin mehcnaism , they becoime signatures.

ANAMOLY BASED DETCTION

-relies upon observing anamoulous traffic through heuristics and statistics.
-ability to recognize attack patterns that deviate from normal network beahviour.
-a new evolving subset of this is honey pot based detection mechanisms.

IOC'S AND SIGNATURES

-IOC is a piece of info , that objectively describe a network intrusion , expressed in platform idependent way.
-could be simple indicator like IP address of command and controls server,
-could be complex like mail server is being used as a malicious SMTP relay.
-When IOC is taken and used as platform sepcifc language i.e snort rule it becomes part of signature.

IOC AND SIGNATURES

-signature can contain 1 or mores IOC .
-indicators can be classified as
-host and network indicators
-static indicators
-variable indicators

-host and network indicators

-basic level of classfication helps frame the indicator to plan detection mechanism it will be used with.

-host based ioc is piece of info that is found on host and objectively describes and intrusion, common examples
-registery key
-file name
-text string
-process name
-mutex
-file hash
-user account
-diectory path

examples of network based IOC are
-ipv4/ipv6 address
-x509 certificate
-domain name
-text string
-protocol
-file name

STATIC INDICATORS
-for which values are explicitly defined
-3 variations

*atomic
*computed
*behavioural

atomic indicators
-smaller and specific
-cannot be broken down to smaller components
examples are:
-ip
-text string
-host name
-email address

computed indictors
-derived from incident data
-examples
-hash values
-regular expressions
-statistics

behavioural indicators
-collection of computed and atomic indicators
-paired together often with some form of logic, to provide useful context
-examples include
*filename with hash values
*combination of text string and regular expression

variable indicators
-indicators for which values are not known.
-examines thoratical attack rather that one already occured

indicatos and signature evolution
- they have shlef life

immature
mature
retired

immature indicator:
that is newly discoverd as a result of some form of inteligence
-also include variable indicators,that are not yet evealated fully.
-confidence upon them may vary depending upon source
-may change frequently

Mature indicator:
-once an indicator or signature is proven that it is useful in NSM enviroment , it is considered to be mature.
-considered as reliable and stable
-combine with other indicators in order to make more granular behavioural indicators resulting in advance signature.
-any change to them should be documented

Retired indicator:
that is no longer being actively used is considered retired.
-it isn't currently used by a detection mechanism.

TUNNING SIGNATURES

-ensures that signatures on which indicators rely are being used reliably and effectively
-while determining maturity and confidence level of a signature 4 data points should be considered
true/false positive/negative

TP: alert that correctly identifies an activity
FP: alert that incorrectly identifies an activity
TN: alert is incorrectly not been generated when a specific activity has not been occured

FN:alert is incorrectly not being generated when specific activity has occurred.

PRECISION

-precision of signature refers to ability to identify positive results.

-can be determined by proportion of tp against all positive results.

precision = tp /(tp +fp)

-can also help us to find probabilty that,given an alert being generated , activity that has been detected has truly occured.

-signature has high precision, alert is genrated , then activity is very likely occured

CRITICAL INDICATOR AND SIGNATURE CRITERIA

-indicator or signature without context is not useful.

-on receiving alert analyst examine supporting context of indicator and signature