Network Forensic

Network Forensic

Section 1

Web Proxy

also waf bypass, we are have log

1-squid

2-nginx(reverse)

3-bluecoat

4-barracuda

Squid Proxy Server

1-debian or redhat

2-squid installation

3-/etc/squid/squid.conf

Http_access deny all

Http_port

Acl `name` src `ip rage`

Http_access allow `name`

4-restart services

5-access log -> /var/log/squid -> forensic

6-cache dir -> /var/spool/squid -> forensic

7-User-Agent and Referer Must be enabled

8-logformat combined

9-access_log combined

Squid Access Log

1-Unix TIme -> date --utc -d @UTime

Head -1 -> first

Tail -1 -> last

Grep -r(recursive)-i(case sensitive)-a(ascii),-l(list)

Squid Log Analytic Tools

sarg->/etc/sarg/sarg.conf->sarg -x->server_url/squid_report

Squidview

calamaris

Squid Cache Forensic

Cache Extraction

/var/spool/squid -> grep -rial File Name

Hex Editor(bless)->open object->Delete anything till header file->save as

Tcpdump Refresher

Network Protocol Analyser

Capture->cap,pcap,pcap-ng

Read

-i->interface

-w->output

-r->read

-s->all packet(full)->for example -s0,-s100

-n->not dns resolve

“Host `ip` and port `port`”

“Not Port `port`”

“Not Net `Range`”

Tshark Refresher

Wireshark command line

-w->write

-r->read

-qnz tcp.conv

-e ip.addr,....

-T Fields

-E separator=’||’

-O->protocol->for example -> -O http

-Y->Search in data->for example->-Y “http.server contains Apache”

Wireshark Refresher

Name Resolution->resolve MAC,resolve IP,resolve Transport

Time

Packet->Flag->Auth Select->Scan Signature

Follow TCP Stream->Follow packet

Wireshark->export object->save as file

Tshark --export-objects”http,destdir”

Network Evidence Acquisition

1-Full packet capture->by rich assets(1..10)->wireshark,tshark,tcpdump

Core sw->port spanning->capture

2-Logs: 1-event 2-syslog->successful

3-Netflow: ipfix->network->device:L4(ip header,tcp header)

Omni pack

EMC/RSA

Emulex

Network Challenges and Opportunities

1-NAT

*** Before Nat Should be Important Logg***

2-Encryption

Ssl offloading->private key->decrypte->plain traffic

HIPS->per client Sll traffic

4-VPN

1-pptp->mppe(microsoft point to point encryption)

2-l2tp->ipsec(pre shared,kerberos,cert(asy))

3-sstp->ssl->public/private key=>not selected

4-Vlan

port-trunk->must be enabled

Section 2

Http: Protocols and Logs

http/1.1

http/2.0

http/3.0

Request/Response dissection

Request

method->(get,post,connect(tunnel))

Host:dst

Cookie:tracking

Response

Status code

Server

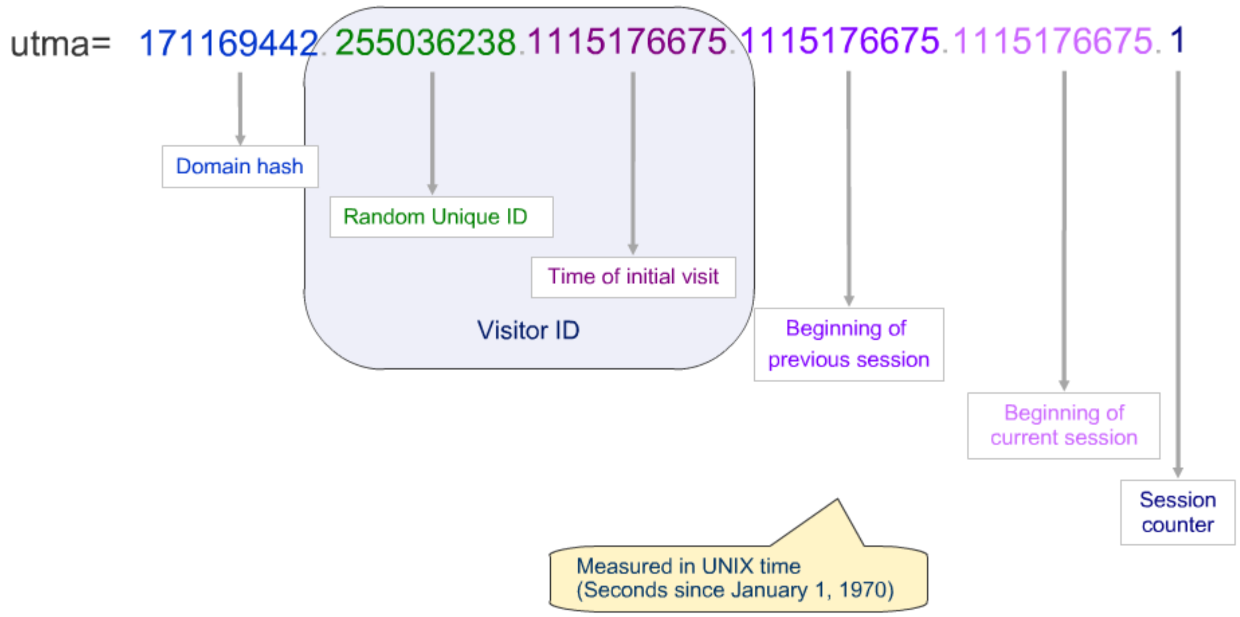
Content-type

Etag

Google Analytic field

--utma

__utma – Visitor Identifier


utma= 171169442.255036238.1115176675.1115176675.1115176675.1
Domain hash
Random Unique ID
Time of initial visit
Visitor ID
Beginning of previous session
Beginning of current session
Session counter
Measured in UNIX time (Seconds since January 1, 1970)

--utmb

--utmc

Http Log Format

1-NCSA

2-w3c

Filter for Detecting Web Attack

“Http.host matches “url””

“Http.request.method == “POST””

“Http.request.uri contains “;ls””

“Http.request.full_uri contains “../””

“Http.authbasic”

Http.cookie

Http.time

Mime_

“Http and png”

“Http and mp4”

“Http contains “\x52\x51”” -> 5251->attack sign

File upload->tshark -r http-attack-1.pcapng -T fields -e http.host -e ip.src -e ip.dst "mime_multipart.header.content-disposition matches \"(\(.php|aspx|jsp))\""

XSS->tshark -r http-attack-1.pcapng -T fields -e http.host -e http.request.uri -e ip.src -e ip.dst -e http.cookie "http.request.uri matches \"(\(script|h1))\""

DNS

:53

Http request==dns query(len=255)->-question=1>type=mx,ptr->dns.qry

Http response==dns response->question=1,answer=1

DNS Filter

dns.a->a record->ip v4

dns.aaaa->a record->ip v6

Dns.mx

Dns.ns

Dns.qry.name contains com

Dns.qry.name.len > 25

DNS as Tunnel Transport

Tunnel protocol

1-dns

2-http

3-icmp

4-ssh

Data send with dns tunnel should be like fqdn

encoding->base64,hex,ascii

Filter Flux DNS

attacker->increase time->attack mechanism

Query: c2.evil.org

Reply: ip1

Query: c2.evil.org

Reply: ip2

ttl=3600ms

Attack ttl: <=300ms

Fast flux single= change A Record

Fast flux double=change ns record

DGA

Automatic domain generation algorithm

For example

Algorithm1->10 domains

Algorithm2->10 domains

Fast Flux Detection

single=dns.resp.ttl<300 && domain1->ip1,ip2,ip3

double=dns.count.answer>12

DNS Amplification Attack

DNS Redirection->DDos->dns spoof->request1,request2->src10

Detection DNS Amplification

Network block=src,src;tshark->tcp.conv->network block

Firewall, IDS and NSM Logs

Enterprise : cisco

Sotto:linksys, dlink

Software: iptable,pfsense

fw->rule->deny any deny->action

Action:1-reject,2-accept,3-drop,4-log

Intrusion Detection System(IDS)

ids:d->detection->n(network-based)ids,h(host-based)ids

ips:p->prevention

sensor->traffic->signature->match=>attack

Software: 1-snort,2-suricata

Network security monitor(NSM)

All packet by protocol

By not sign

Software: bro->zeek:1-live,2-postmortem->after attack

Zeek: network protocol,file metadata,inventory,special cases

conn.log->connections

protocol.log->id

pe.log->unknown

x.502->cert issuer

Zeek -Cr pcap

securityonion=zeek+dashboard+...

Log Protocol and Aggregation

syslog->udp->514

Sources: router,switch,access point,fw,...

Syslog srv=linux(syslog)+access point(syslog)+win(kiwi)

Facility: service->/var/log/auth.log,/var/log/kern.log

Serverity: alert,critical,errors

Microsoft Eventing 6.0

centralized->event viewer->subscriptions->collector(source,source),cert(domain),api(connections)

Comprehensive Log Aggregation

SIEM Tools: splunk,arch sight

Enhanced Aggregators: ELK Stack,lorythm

ELK

Elasticsearch+logstash+kibana

Mode:

1-live(syslog->514->5514+netflow->9996->9995)

2-offline(extract log in /logstash/syslog/YYYY/)

Query->discover->add filter

Section 3

Netflow and file access protocol

Flow: sequence of packet

Netflow: protocol->collect->analyze->v1..v10->v5 popular->template base

Netflow->call as ipfix:1-ip header,2-transport header

Netflow Architecture

Enable netflow before nat

Nat: lan to dmz

Snat: lan to internet

Dnat: internet to dmz

Tools

Nfcapd: collector

-p: port

-l: dir

-w: write

-d: daemon

Nfdump: analyze

-R: reader dir

-s: srcip,bytes

-t: date and time | “2019/10/12.15:33-2019/11/12.15:33”

-o: extended tcp

-c: count

“Host <ip> and port <port>”

“Proto <tcp>”

“Not proto <icmp>”

Follow BAT

Big data->SILK,Flowbat(3000)->quick,query builder

/data/sensors.conf

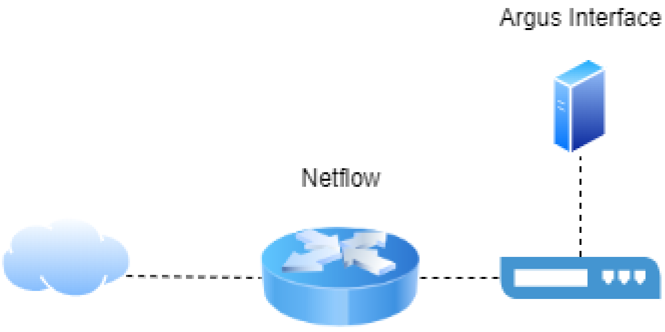
Export by fields

Section 3

Argus

Spanning port->raw->argus->flow(netflow)

argus->convert raw to flaw



Connect to server: ratop -S ‘ip:port’

Analyse-> ra -r packet.ra -s time saddr proto sport dport

Analyse-> ra -a -nnr packet.ra - “port 3389”

Internal: nf.ipv4_src_ip:[ip to ip]

External: !nf.ipv4_src_ip:[ip to ip]

TCP Flag

s->syn

S->syn ack

R->reset

E->established

f->finish

F:finish ack

Attack Architecture

Send, receive-> file transfer

src1,dst1->brute force

ipX->port1-> internal scanning

File Transfer Protocol(FTP)

Status code:

530->access

230->success

Command:

List: LIST

Get file: RETR

Put file: STOR

Rename file: RNFT

ftp.request.command == RETR

Microsoft Protocol(SMB)

smb->cifs->1.0,2.0,3.0

Header->(Last boot,..)

smb2.cmd==0x73->session established

smb2.cmd==0x75->access request

smb2.cmd==0x74->logoff

Smb2.boot_time

File Transfer: (smb2.cmd==5)&&(smb2.flags.response==1)

File Name: smb2.filename==”example.jpg”

File Name: smb2.filename contains “example.jpg”

File Delete: smb.share_access==0x00000004

File Create: smb.options==0x00000064

Edit File: smb.create_options==0x00200000

Zone Identifier in header: file from?

Section 4

Commercial tools, wireless and full packet hunting

Simple mail transfer protocol

Commands:

MAIL->from

RCPT->to

DATA->content

VRFY->verify email

Status code:

220->service ready

250->action okay->verify

251->user not local

550->mailbox unavailable

Scenario

Employee send info mail to out of scope with personal laptop(laptop may be dell)

Eth.addr contains <vendor ID>

Dhcp ack->ip

```
Ngrep “Suspect Name” -N -t -q -I *.pcap “ip.src==ip and tcp.srcport==port and dst.src=ip and tcp.dstport==port”
```

Follow TCP Stream= full message

Mail attachment->base64->bless(delete header)->base64 remove space and break line with fromdos

```
Tofrodos -b “attach”
```

```
Base64 -d file > example.doc
```

Commercial Forensic Network Tools

Full packet capture:

RSA Netwitness or moloch(free)

Netflow collection

Qradar,manageengine

Analyst Supporting Tools:

Network miner,steelcentral

Wireless Network Forensics

ids->nids->wids

wlc(wireless lan controller)->access points

Convert access point to nids

Decompile: binwalk

Change embedded os: openwrt+kismet+tshark

Access point->enable spanning->tshark

List,Brand,SSID: tshark -r .pcap -Y “wlan.fc.sub_type==0x08”

Traffic encrypted | plain: -Y “wlan.fc.protected==1”

List connected systems: -Y “(wlan.bssid==MAC)” -T fields -e wlan.sa -e wlan.da -e frame.time

Connection Time: -Y”((wlan.bssid==MAC) && (wlan.fc.protected==1)) && (wlan.sa==MAC)” -T fields -e frame.time -e frame.len | cut -d “ “ -f4

Section 5

Encryption, protocol reversing, OPSEC

Encoding, encryption and ssl

Encoding: base64(/==.),html char(#&),hex(0-9,a-f)

Encryption: symmetric(aes,rsa),asymmetric(public key)

Hash: md5(32),sha1-512(48,64),NTLM(microsoft)(32)

SSL Decrypt

wireshark->preferences->protocols->ssl->rsa key list->src ip address->key

Perfect forward secrecy

Public key,per session

SSL Forensic

Bluecoat,palo alto | bettercap,Dsniff

Network protocol

For example:

Smb per 64 byte contains @smb

Identifying undocument protocol feature

For example:

Icmp malicious data,http response by \n

Investigating OPSEC and Threat Intelligence

Advanced persistent attack->permanently

Incident Response->find & Forensic attack

Open source Intelligence

OSINT->public/private database->info

The attacker is watching

All-in-one privacy

Premature Traffic block

All ip block reject

All ip target reject

Risk mitigations

1-Use separate network access:

For example: forensic and pentest

2-alternate access path

3-isolate vm

Establishment Steps

1-installing and configuring elk

2-enable syslog(network,firewall,ips,ids,access point)->elk

3-enable netflow->elk

4-installing and configuring moloch->elk

5-determine FPC(full packet capture) zone

6-installing beats on microsoft os

7-installing and configuring web proxy->squid->elk

8-installing and configuring zeek

Resource

- noorasec.com