COLLECTIVE SENSE

DEFENSIVE SECURITY

May the Data stay with U! Network Data Exfiltration Techniques.

•••

Leszek Miś - BruCON 2017

DEFENSIVE SECURITY

About me

- IT Security Architect and Founder @ Defensive Security
- VP, Cyber Security @ Collective Sense
- Offensive Security Certified Professional (OSCP)
- Red Hat Certified Architect/RHCSS/RHCX/Sec+
- Member of ISSA/OWASP Poland Chapter
- Speaker at OWASP Appsec USA, Brucon, Confidence ISSA and many others
- Mostly I am focusing on:
  - Linux & Web Application Security
  - Penetration testing / security audits
  - Threat hunting and Incident Response
  - Hardened IT Infrastructure (SSO/IdM)
  - Behavioral / statistic analysis → Machine Learning / Deep Learning

COLLECTIVE SENSE

DEFENSIVE SECURITY

What you need for this workshop?

- Kali VM
- your External VPS / Linux server
- Wireshark installed
- Internet connection

COLLECTIVE SENSE

DEFENSIVE SECURITY

What is Data Exfiltration?

- Part of post exploitation process
- Unauthorized copying, transfer or retrieval of data from a computer or server.
- Malicious activity performed through various different techniques, typically by cybercriminals over the Internet or other network
- Data theft, data exportation
- There is no silver bullet solution to detect it:
    - → Defence in Depth

COLLECTIVE SENSE

DEFENSIVE SECURITY

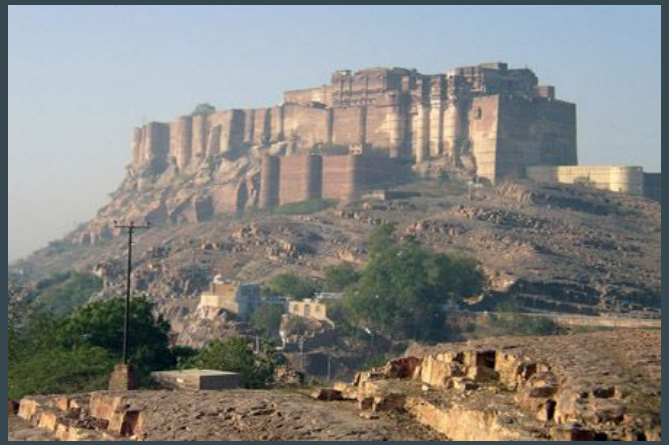
“Pre-post” exploitation process

- Sensitive information on public services
- Authentication bypass
- Admin access to administration panel → BF
- DNS subdomain takeover
- Docker image registry publicly accessible
- Source code disclosure, ex. publicly exposed GIT/SVN repos
- 0-day Unathenticated remote code execution
- Wget arbitraty file upload
- Client-side attacks
- Quake 3 server in corpo network

COLLECTIVE SENSE

Defence in depth

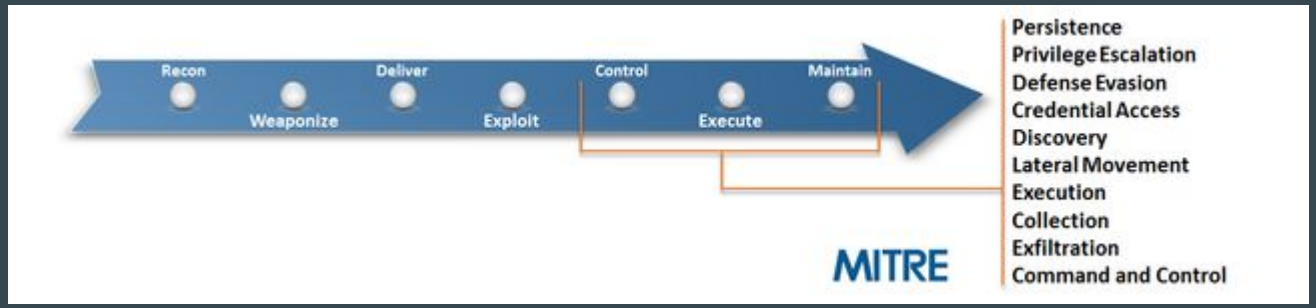
- Strategy of having layered security mechanisms:
  - if one fails, the other may still provide a protection
  - Network segmentation + deep network traffic analysis + host hardening + segregation of data + security culture + people + threat hunting
  - Question:
    - Which layers/devices does your external network packet pass?



ATT&CK Framework

- Adversarial Tactics, Techniques, and Common Knowledge:
  - Threat Modeling Methodology for various phases of an adversary's lifecycle and platforms that are known to be targeted by cyber threats
  - Sections →
    - Collection
    - Exfiltration

https://attack.mitre.org



DEFENSIVE SECURITY

ATT&CK Framework - Collection

- Collection techniques prior to exfiltration:
  - Audio/Camera/Screen capture → BeEF & XSS
  - Automated collections
  - Clipboard data
  - Data from Local System / Data from Network Shares / Data from Removable Media → network/OS digging
  - Emails
  - Input Capture → keyloggers
  - Others

COLLECTIVE SENSE

ATT&CK Framework - Exfiltration

- Exfiltration techniques:
  - Data compressed
  - Data encoded
  - Data encrypted
  - Data Transfer Size Limits → data chunks
  - Exfiltration over Alternative Protocol
  - Exfiltration over C2 Channel
  - Exfiltration over other Network Medium
  - Exfiltration over Physical Medium
  - Scheduled Transfer

What does attacker want to collect?

What does attacker want to collect?

- Config files
- Password files
- Certificates & PKI keys
- Backup of critical infrastructure configs
- Bitcoins
- E-mails
- Source Codes + Data Files
- Office Documents
- DB Dumps
- Memory Dumps :>
- Custom Binary files

DEFENSIVE SECURITY

Why should we care? - offensive part

- Test Data Leakage Protection (DLP) solutions
- IDS/IPS Evasion
- Machine Learning Sensors Evasion
- Bypass a data whitelisting
- Bypass a “stricted” firewall rules
- Bypass a SSL forward proxies
- Hide my data & catch me if you can!

Check you \”Network Security Stack”\ for things we are going to talk about now!

COLLECTIVE SENSE

Why we should care? - defensive part

- Proactive event analysis:
  - Few questions:
    - Who? When? Where? What? Why? How?
  - Key points:
    - Active analysis of logs and system events
    - Behavioral analysis of user actions: user → IP mapping
    - Periodic vulnerability scanning
    - Attack paths identification
    - Periodic RAM memory analysis for critical systems → rootkit detection
    - **Multi-level network traffic analysis**

DEFENSIVE SECURITY

Multi-level network traffic analysis

- Packet Headers → Full Packet Capture
- Netflows → network billing
- Passive:
  - DNS
  - TLS
  - HTTP
  - SMTP
- Signatures / IP reputation / malware feeds
- SNMP + CVE search
- Active security scans → vuls
- GEO / whois / ipinfo
- Honey traps → canary tokens

COLLECTIVE SENSE

DEFENSIVE SECURITY

Top Protocols for Exfil!

- TCP
- UDP
- ICMP
- HTTP / HTTPS
- DNS
- SSH / SCP / SFTP
- POP3 / SMTP
- RDP
- FTP
- NTP
- BGP
  - + Powershell based
  - + TOR

COLLECTIVE SENSE

Top Cloud Services for Exfil!

- Twitter
- Gmail / Google Docs
- Slack
- Facebook → 25MB raw file
- Github
- Pastebin
- Skype
- LinkedIN → 100MB Office documents
- Youtube → 20GB as a video
- Vimeo → 5GB
- Flickr → 200MB as image
- Tumblr

ICMP

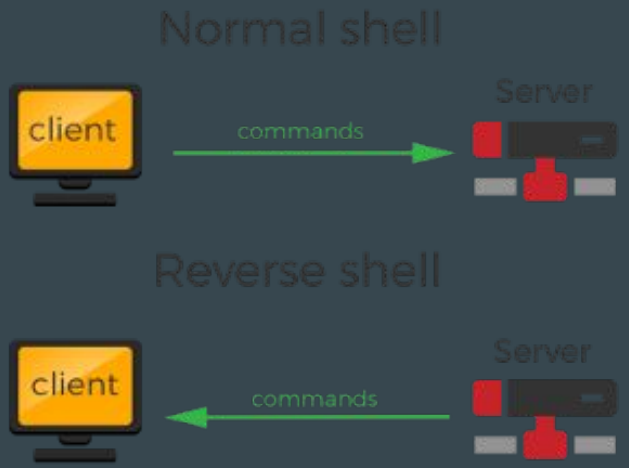
- ICMP → “ping”
  - echo request
  - echo reply
- ICMP:
  - icmptunnel
  - auxiliary/server/icmp_exfil
    - nping
    - exfiltrate-data.rb
  - icmpsh
  - hans

LAB1 - ICMP

- Lab 1:
  - ICMPtunnel
    - exfiltrate-data.rb
  - Meterpreter
  - tcpdump / wireshark

TCP - Metasploit / meterpreter

- Meterpreter
  - bind / reverse shell:
    - upload / download
  - pivoting:
    - route
    - portfwd



LAB2 - Metasploit / meterpreter

- Lab 2:
  - metasploit / meterpreter
  - tcpdump / wireshark

TCP - simple Linux tricks / “one-liners”

- Tools:
  - nc
  - netcat
  - socat
  - curl
  - rsync
  - ssh
  - ftp
  - scp / sftp
  - /dev/tcp
  - xxd
  - host , dig, nslookup
  - others

TCP - simple Linux tricks

- LAB3:
  - one-liners
  - linux tools
  - wireshark

DNS

- Core of the communication
- UDP vs TCP
- Requests and responses

DNS record types

	Type	Name	Function
Zone	SOA	Start Of Authority	Defines a DNS zone
	NS	Name Server	Identifies servers, delegates subdomains
Basic	A	IPv4 Address	Name-to-address translation
	AAAA	IPv6 Address	Name-to-IPv6-address translation
	PTR	Pointer	Address-to-name translation
	MX	Mail Exchanger	Controls email routing
Security and DNSSEC	DS	Delegation Signer	Hash of signed child zone's key-signing key
	DNSKEY	Public Key	Public key for a DNS name
	NSEC	Next Secure	Used with DNSSEC for negative answers
	NSEC3[a]	Next Secure v3	Used with DNSSEC for negative answers
	RRSIG	Signature	Signed, authenticated resource record set
	DLV	Lookaside	Nonroot trust anchor for DNSSEC
	SSHFP	SSH Fingerprint	SSH host key, allows verification via DNS
	SPF	Sender Policy	Identifies mail servers, inhibits forging
	DKIM	Domain Keys	Verify email sender and message integrity
Optional	CNAME	Canonical Name	Nicknames or aliases for a host
	SRV	Services	Gives locations of well-known services
	TXT	Text	Comments or untyped information[b]

DNS

- DNS responses:
  - NOERROR → DNS Query completed successfully
  - FORMERR → DNS Query Format Error
  - SERVFAIL → Server failed to complete the DNS request
  - NXDOMAIN → Domain does not exist
  - NOTIMP → Function not implemented
  - REFUSED → The server refused to answer for the query
  - YXDOMAIN → Name that should not exist, does exist
  - XRRSET → RRset that should not exist, does exist
  - NOTAUTH → Server not authoritative for the zone
  - NOTZONE → Name not in zone

DEFENSIVE SECURITY

DNS

- Allow for querying a internal DNS servers only
- No one should send TXT resolve request to the DNS except MX servers
- Track down number of NXDomain responses → DGA
- Profile your devices against DNS traffic → generate notification if there is a one who reach the threshold
- Watch out for a:
  - lot of requests to restricted domain
  - lot of requests to one domain
  - lot of requests to fast flux domains
  - DNS replies have private addresses
  - lot of DNS traffic going to bad guy country
  - DNS replies have patterned encoding
  - Packet size outside the normal distribution
  - Spike in DNS byte count across normal traffic patterns

COLLECTIVE SENSE

DNS

- Tools:
  - DET
  - OzymanDNS
  - DNS2TCP
  - Iodine
  - SplitBrain
  - TCP-over-DNS
  - YourFreedom
  - Heyoka
  - DNScat2 → remote shell
  - NSTX
  - DNScapy
  - VPN over DNS
  - MagicTunnel
  - Element53

DNS

- Lab 4:
  - dnscat2 → remote shell
  - DET → DNS
  - Passive dns analysis

HTTP / HTTPS

- It is all about HTTP methods, requests and responses, right?

HTTP Methods

GET	Retrieve a resource from the provided URL
HEAD	Like GET, but retrieve head only
POST	Send information as a block of data
PUT	Store information in the provided URL
DELETE	Delete the specified resource
TRACE	Echo back request, audit changes made by intermediate servers
OPTIONS	Return supported HTTP methods
CONNECT	Enter “dumb” mode, convert to a transparent TCP/IP tunnel
PATCH	Apply partial modifications to a resource

Only GET, POST, HEAD, and OPTIONS are typically enabled

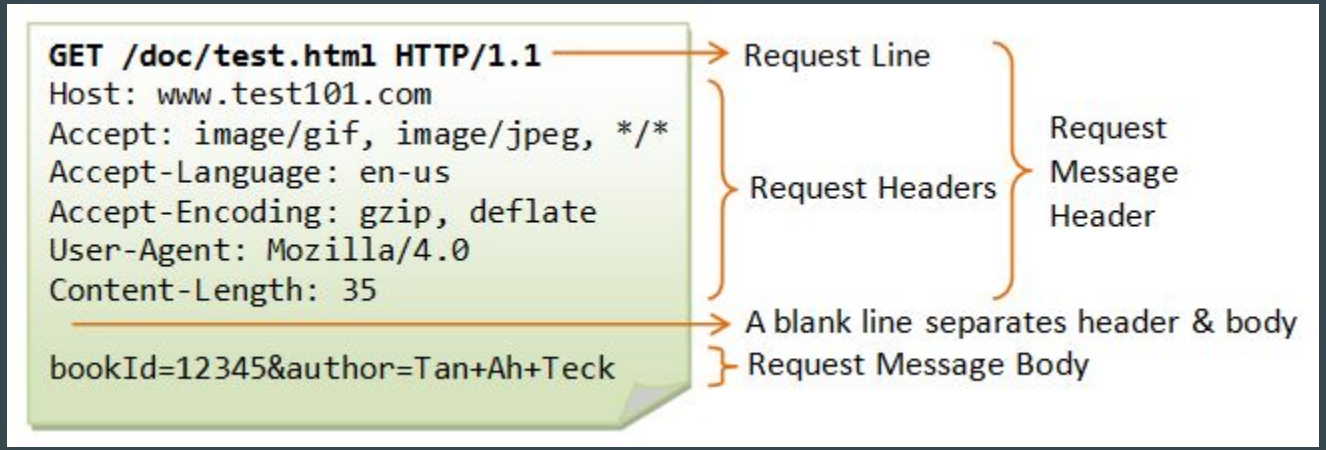
HTTP / HTTPS

- It is all about HTTP methods, requests and responses, right?

Header	Type	Contents
User-Agent	Request	Information about the browser and its platform
Accept	Request	The type of pages the client can handle
Accept-Charset	Request	The character sets that are acceptable to the client
Accept-Encoding	Request	The page encodings the client can handle
Accept-Language	Request	The natural languages the client can handle
Host	Request	The server's DNS name
Authorization	Request	A list of the client's credentials
Cookie	Request	Sends a previously set cookie back to the server
Date	Both	Date and time the message was sent
Upgrade	Both	The protocol the sender wants to switch to
Server	Response	Information about the server
Content-Encoding	Response	How the content is encoded (e.g., gzip)
Content-Language	Response	The natural language used in the page
Content-Length	Response	The page's length in bytes
Content-Type	Response	The page's MIME type
Last-Modified	Response	Time and date the page was last changed
Location	Response	A command to the client to send its request elsewhere
Accept-Ranges	Response	The server will accept byte range requests
Set-Cookie	Response	The server wants the client to save a cookie

HTTP / HTTPS

- It is all about HTTP methods, requests and responses, right?



HTTP / HTTPS

- Incoming HTTP POST payload analysis at server side:
  - you need WAF (Web Application Firewall) → ex. modsecurity:
    - SecRequestBodyAccess
    - SecResponseBodyAccess
- Outgoing HTTPS traffic analysis:
  - you need SSL Forward Proxy for TLS inspection → logs
    - internal PKI CA:
      - → passive TLS inspection
- Corporate NTLM HTTP proxy as a gateway (only 443/tcp allowed) →
  - rpivot
  - cntlm
  - OpenVPN
- Detection of HTTP traffic sent directly to IP (without domain name in use)

HTTP / HTTPS

- Tools:
  - httptunnel
  - tunna
  - XSSshell-XSStunnel
  - DET → HTTP
  - curl
  - rpivot
  - cntlm
  - Proxytunnel
  - corkscrew
  - connect-proxy
  - meterpreter

Cloud based apps

- Gmail → DET:
  - "gmail": {
    - "username": "cda262cdwe3a6c345046af3f9734d9ebdwdqwf@gmail.com",
    - "password": "Give_me_some_B33rs!",
    - "server": "smtp.gmail.com",
    - "port": 587

    }

Text-based steganography

- Cloakify:
  - transforms any filetype (e.g. .zip, .exe, .xls, etc.) into a list of harmless-looking strings
  - hide the file in plain sight, and transfer the file without triggering alerts.
  - defeat data whitelisting controls - is there a security device that only allows IP addresses?
  - example: you can transform a .zip file into a list of Pokemon creatures or Top 100 Websites.

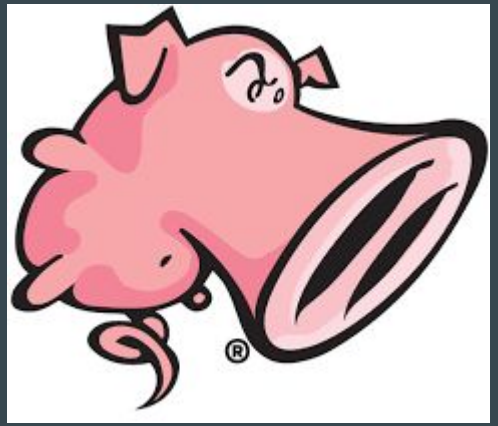
Text-based steganography

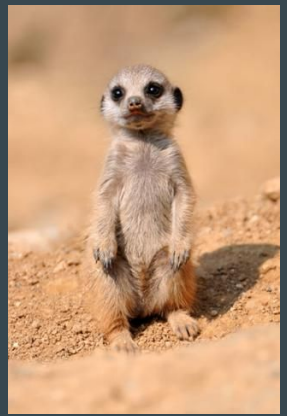
- Lab

DEFENSIVE SECURITY

IDS / IPS (not only signature-based)

- Open Source:
  - Suricata - http://suricata-ids.org
  - BRO IDS - https://bro.org
  - Snort - https://www.snort.org





COLLECTIVE SENSE

IDS / IPS

- Suricata is an engine for NIDS, NIPS, NSM:
  - IDS → passive → TAP or SPAN port
  - IPS → active → inline → router/bridge
- Features :
  - IPV4/IPV6, defrag, TCP tracking
  - Stateful HTTP, SMTP, DNS, TLS
  - Lua scripting
  - ET Ruleset / VRT/Talos

DEFENSIVE SECURITY

Amsterdam

- Provide features of Suricata+ELK via docker containers
  - Objective is super fast installation
  - Amsterdam provides
    - Latest ELK and suricata
- Basic setup sniffing traffic on physical host:
  - pip install amsterdam
  - amsterdam -d ams -i wlan0 setup
  - amsterdam -d ams start
  - firefox http://localhost:8000

COLLECTIVE SENSE

Summary

- Try also:
  - PyExfil → https://github.com/ytisf/PyExfil
  - IPv6DNSExfil → https://github.com/DShield-ISC/IPv6DNSExfil
  - QRCode-Video → https://github.com/Neohapsis/QRCode-Video-Data-Exfiltration
  - udp2raw-tunnel → https://github.com/wangyu-/udp2raw-tunnel
  - XFLTReaT → https://github.com/earthquake/XFLTReaT
  - sound-poc → https://github.com/iiamit/data-sound-poc
  - sneaky-creeper → https://github.com/DakotaNelson/sneaky-creeper
  - corkscrew → https://github.com/elia/corkscrew
  -

Questions?

lm@defensive-security.com

lm@collective-sense.com

Twitter: @cr0nym

LinkedIN: https://www.linkedin.com/in/crony/

Open Source Defensive Security Training

https://defensive-security.com

@DeepSec → November 14-15, Vienna

@Brucon 2018 Spring Training Session - hope so :)

COLLECTIVE SENSE

- Excellent visibility based on many collectors
- Behavioral analysis of network traffic
- Hybrid ML / DL based anomaly detection
- Active 0-day protection module
- Modular, responsive web interface

https://collective-sense.com