PROJECTING TA505 TRADECRAFT TO CUTTING EDGE SYSTEMS

FATIH OZAVCI

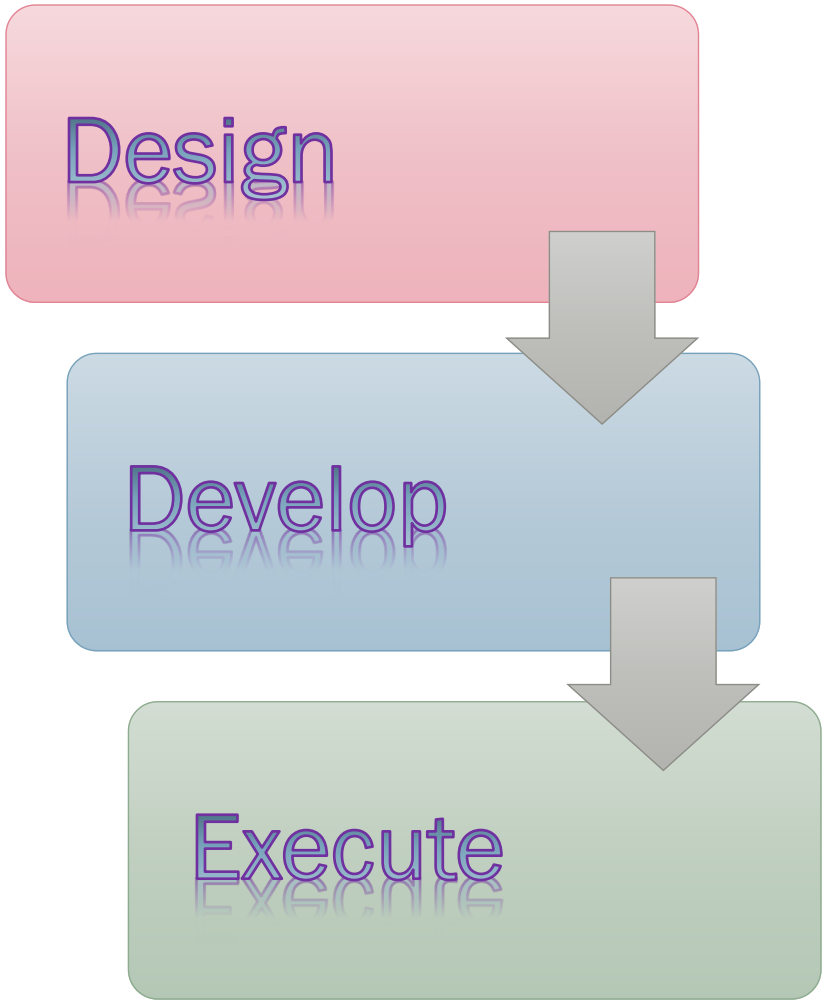
Fatih Ozavci

- Adversary Simulations and Research
- UNSW (ADFA) - Master of Cyber Security
- Security Researcher
  - *Vulnerabilities: Microsoft, Cisco, SAP*
- Speaker & Trainer
  - *Sessions: Black Hat USA, Def Con*
- Open Source Software Projects
  - *Petaq Purple Team C2 & Malware*
  - *Viproy VoIP Penetration Testing Kit*

https://linkedin.com/in/fozavci

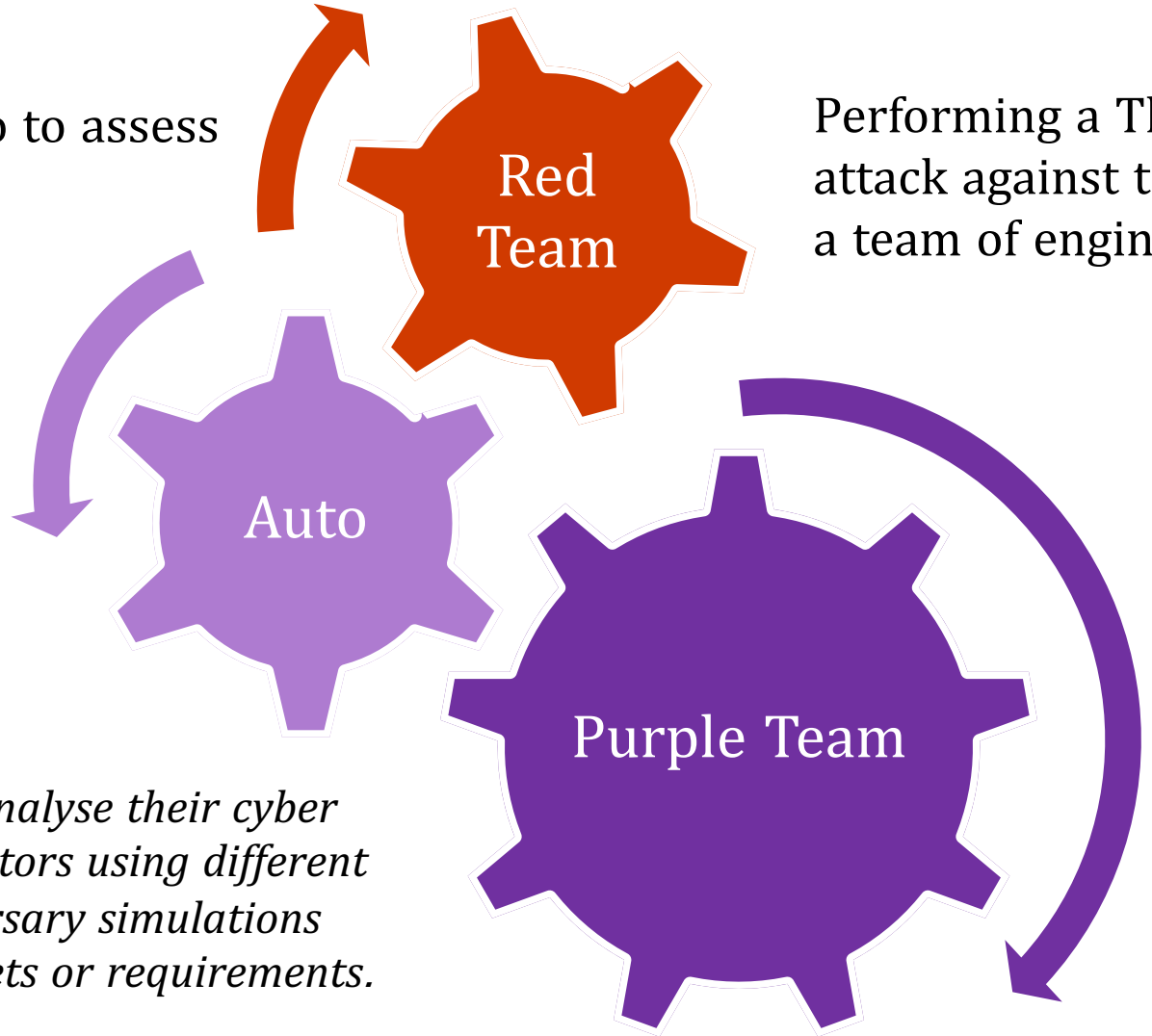
Agenda

- Adversary Simulations
- TA505 Tradecraft and Projections
- Implementation
  - *C2 & Malware Development*
  - *Customised New and Old Techniques*
- Execution
  - *Flags, Support Systems and Tips*
- Demonstrations



Adversary Simulation Types

Automating a scenario to assess the defence controls implemented (MITRE ATT&CK)



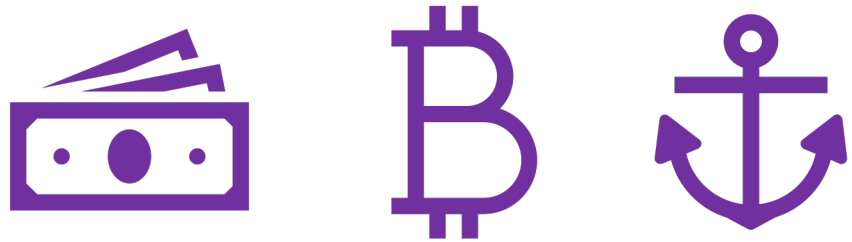
Performing a Threat Intelligence-Led cyber attack against the targeted environment with a team of engineers (CBEST, CORIE, ICAST)

Organisations desire to analyse their cyber defence against threat actors using different implementations of adversary simulations depending on their budgets or requirements.

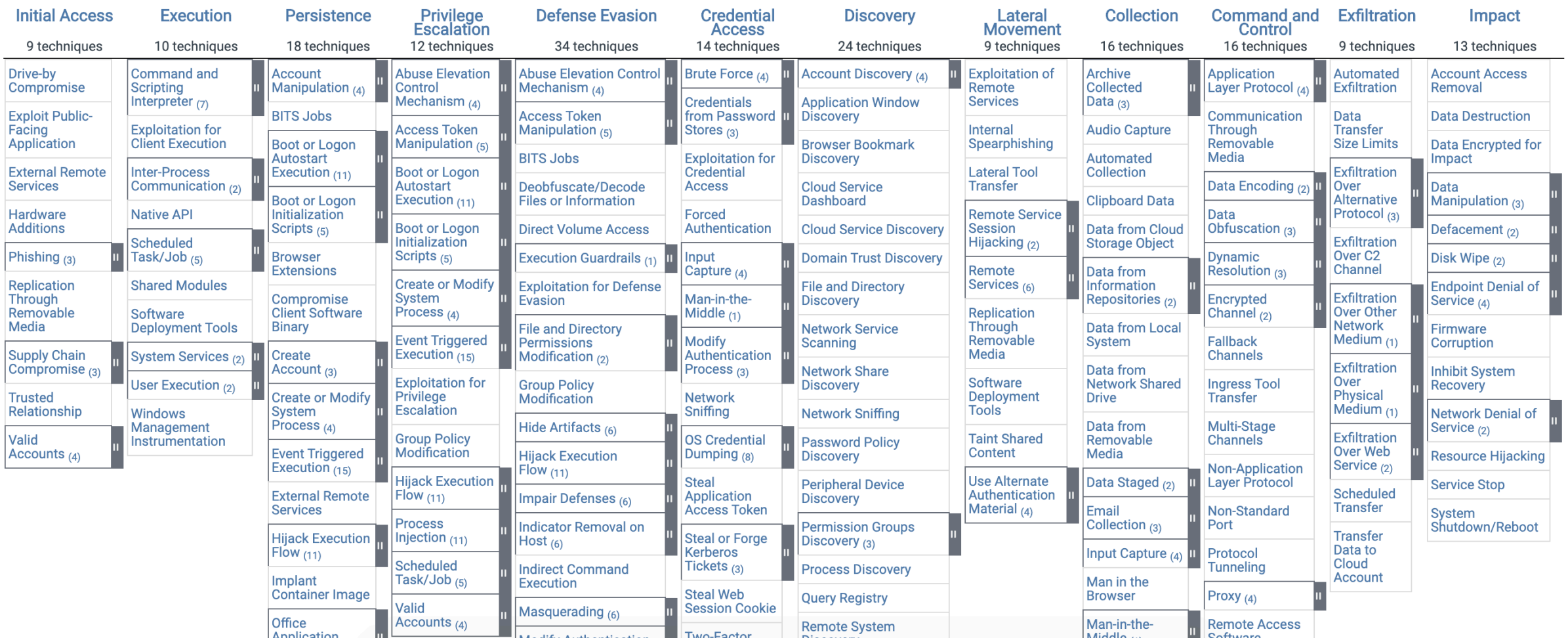
Performing a cyber attack with blue team collaboration to improve people and defence together (MITRE ATT&CK)

What Are We Simulating?

- Because, the regulation said so? (CBEST, CORIE, ICAST, MITRE)
- Security Breach Experienced
- External/Internal Red Team Exercise
- General Assessment of the Security Controls and Perimeter
- Threat Actor actively/potentially targeting the organisation
  - *Ransomware & Extortion*
  - *Blockchain Mining*
  - *Long Term Access*



Coverage: Mitre Att&ck



https://attack.mitre.org/

The Threat Actor (TA505+)

- TA505 is a threat group actively targeting financial institutions, including Australia, since 2014 using custom tools (e.g. FlawedAmmyy , ServHelper, SDBot) and offensive security tools (e.g. Cobalt Strike, TinyMet).

- They constantly changed/updated their RAT used as tradecraft. So, it's logical to assume that TA505 would start using .NET Tradecraft after Cobalt Strike received *execute-assembly* feature to run .NET assemblies with process injections.

- This adversary simulation is based on TA505 TTPs, but also additional .NET Tradecraft and custom C2 suites (e.g. Petaq C2). Therefore it's called TA505+ .

TA505+ Tradecraft Map

Mitre Att&ck ID	Malware	Description	Replacement
S0384	Dridex	HTTP C2, encrypted C2 traffic, VNC feature, P2P Relay	Petaq Implant
S0381	FlawedAmmyy	HTTP C2, WMI enumeration for AV, system information	Petaq Implant
S0383	FlawedGrace	Fully featured malware	Petaq Implant
S0460	Get2	Downloader for FlawedGrace, FlawedAmmyy, Snatch and SDBot	Petaq Dropper
S0039	Net	Internal Windows command, enum and mapping	No replacement
S0461	SDBot	TA505's new installer and loader	Petaq Dropper
S0382	ServHelper	TA505's new malware replacing the old ones in 2018	Petaq Implant
S0266	TrickBot	Spyware used against financial institutions, replaced Dyre. Used for mainly situational awareness and information collection.	.NET Applications

Mitre Att&ck ID	Malware	Description	Replacement
S0154	Cobalt Strike	Fully featured and commercial C2.	Petaq Service
	Metasploit Framework	Fully featured and commercial exploitation framework	No replacement

TA505+ Technique Map

Mitre Att&ck ID	Name	Implementation
T1087.003	Account Discovery: Email Account	Not Implemented
T1071.001	Application Layer Protocol: Web Protocols	Petaq Implant communicated with C2 using HTTP Web Sockets, Meterpreter used HTTPS
T1059.001	Command and Scripting Interpreter: PowerShell	PowerUp for privilege escalation enumeration
T1059.005	Command and Scripting Interpreter: Visual Basic	Not Implemented
T1059.007	Command and Scripting Interpreter: JavaScript/JScript	Not Implemented
T1059.003	Command and Scripting Interpreter: Windows Command Shell	Several situational commands run on CMD
T1555.003	Credentials from Password Stores: Credentials from Web Browsers	Not Implemented
T1486	Data Encrypted for Impact	Ransoblin used for ransomware simulation
T1568.001	Dynamic Resolution: Fast Flux DNS	Not Implemented
T1105	Ingress Tool Transfer	Petaq Dropper -> Implant -> Meterpreter
T1105.002	Inter-Process Communication: Dynamic Data Exchange	Replaced with Excel 4.0 Macro
T1078.002	Valid Accounts: Domain Accounts	Reusing the credentials extracted

TA505+ Technique Map

Mitre Att&ck ID	Name	Implementation
T1027	Obfuscated Files or Information	Excel file and Powershell to be obfuscated
T1027.002	Software Packing	.NET Tradecraft run inline, not required
T1069	Permission Groups Discovery	Situational awareness commands
T1566.001	Phishing: Spearphishing Attachment	Excel file is presented, but not mailed
T1566.002	Phishing: Spearphishing Link	Excel file link is presented, but not mailed
T1055.001	Process Injection: Dynamic-link Library Injection	DLL Injection via Petaq Implant
T1218.007	Signed Binary Proxy Execution: Msiexec	Msiexec command run via Petaq Implant
T1218.011	Signed Binary Proxy Execution: Rundll32	RunDLL32 called via Petaq Implant
T1553.002	Subvert Trust Controls: Code Signing	Not implemented
T1552.001	Unsecured Credentials: Credentials In Files	Implemented with a sample file on desktop
T1204.002	User Execution: Malicious File	Excel file is the malicious file for execution
T1204.001	User Execution: Malicious Link	Excel file is the malicious file for execution

Kill Chain Implementation for TA505+

1

Reconnaissance

- Collecting Threat Intelligence
- Tradecraft mapping for TA505

2

Weaponization

- Preparing Excel File
- Developing Petaq Loader
- Developing Petaq AMSI Patcher
- Developing Ransoblin

3

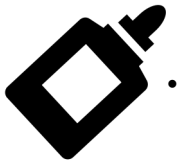
Delivery

- Assume Breach (User executes)
- Delivering the Excel file via Web
- Petaq Implant lands as stages
- Petaq Service used for delivery

4

Exploitation

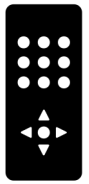
- Excel file gets executed by User
- Petaq Loader runs AMSI patch
- Petaq Loader runs Petaq Implant



5

Installation

- Petaq Implant adds itself to Registry



6

Command & Control

- Petaq Service drives Petaq Implant
- Runs .NET Applications in memory
- Forks Metasploit Framework sessions

7

Actions on Objectives

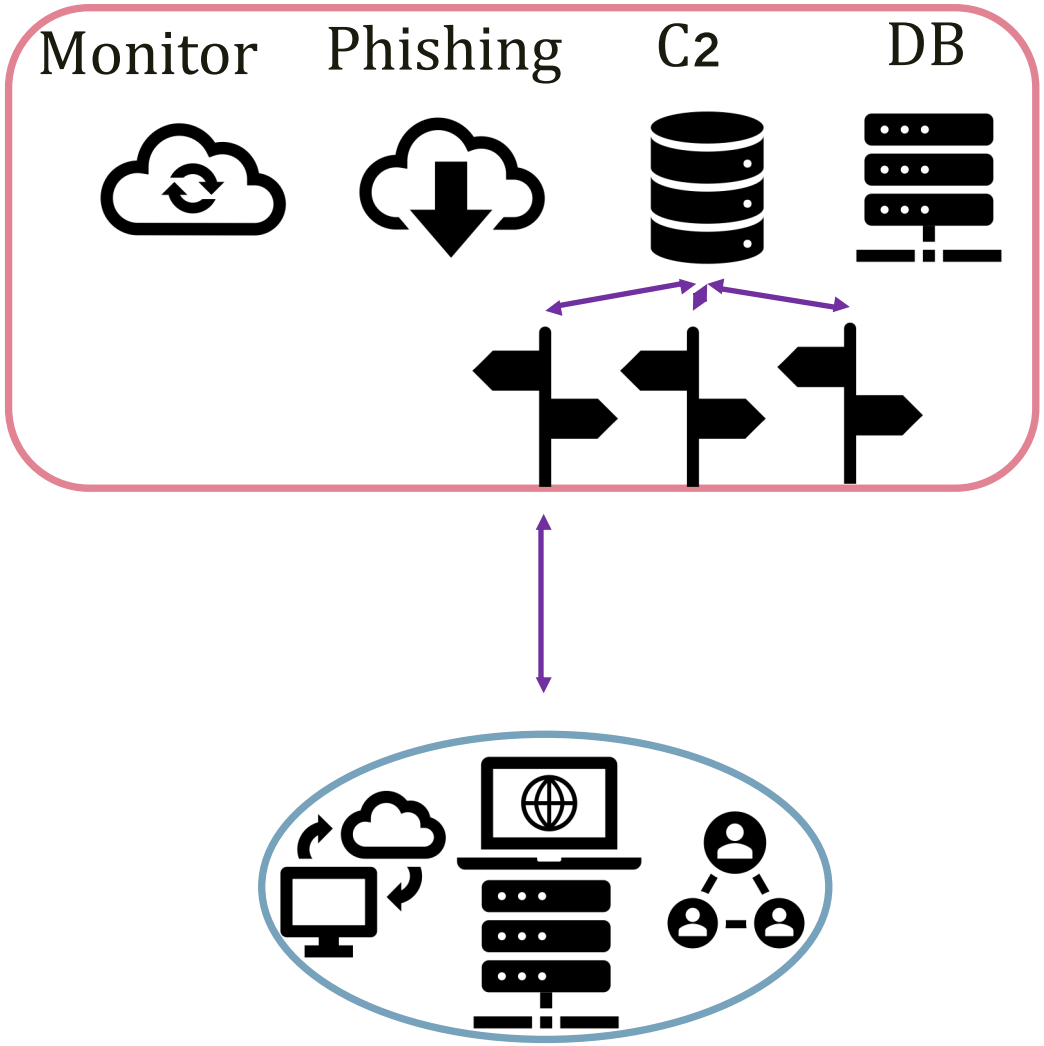
- .NET and PowerShell Applications
- Ransoblin runs for ransoming files
- Metasploit Framework used for exploits, VNC, RDP

Lockheed Martin – Kill Chain: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Platform

➢Cloud Deployment

- *Provider Selection*
- *Services: Storage, DB, VM, OS*
- *Domains: Fronted, Aged, Classified*

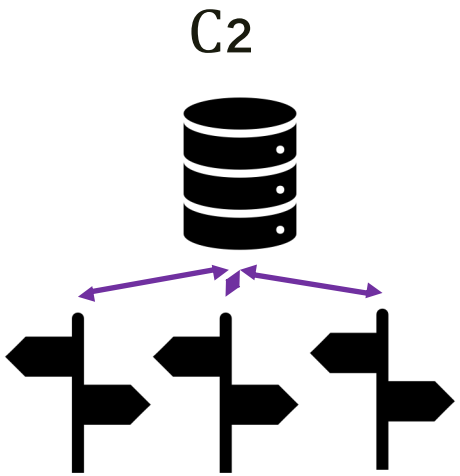


➢Operational Security

- *Real-Time Monitoring*
- *Encrypting Data in Transit and at Rest*
- *Implement Compliance Requirements*

Software: Command & Control

- Command & Control Service Selection
  - *What does the threat actor use?*
  - *What operating systems are targeted?*
  - *Multi Instance: Long Term, Short Term, Interactive*
  - *C2 Protocols, Cloud Native, Multi User, Logging…*
- Safer C2 Choices
  - *Scythe (Commercial, Safer and Flexible for Automation)*
  - *Cobalt Strike (Commercial, Favorite of Threat Actors and Red Teams)*
  - *Covenant (C#, Open Source, Mostly Stable)*
  - *SilentTrinity (.NET and Python, Open Source, Stable)*



Software: Petaq C2

- Petaq Purple Team Command & Control Server (MIT License)
  - *P'takh (petaQ) is a Klingon insult, meaning something like "weirdo"*
  - *Protocols : HTTP(S), WebSocket, SMB Named Pipe, TCP, UDP*
  - *Execution : CMD, .NET Assembly, Source, Shellcode Injection, PowerShell*
  - *Features : WMI Lateral Movement, Nested Implant Linking, Encryption*
  - *Scenario Based Automation and TTP Support*

- Petaq is suitable to interactive and scenario based exercises

https://github.com/fozavci/petaqc2

Applications Developed & Customised

Petaq Dropper

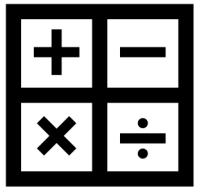
- C# Application
- Loads .NET Assemblies (Implant & AMSI patcher)
- https://github.com/fozavci/ta505plus

Petaq Implant

- C# .NET 4.5 Application
- Fully featured malware, all essential features
- Runs commands, powershell, .Net, shellcode
- Llinks other remote implants as nested implants
- https://github.com/fozavci/petaqc2

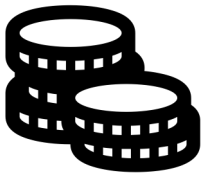
Petaq Service

- C# .NET Core 3.1 Application
- C2 running through HTTP Websockets
- https://github.com/fozavci/petaqc2



Malicious Excel File

- Excel 4.0 Macro
- Generated using ExcelntDonut
- https://github.com/fozavci/ta505plus



Ransoblin

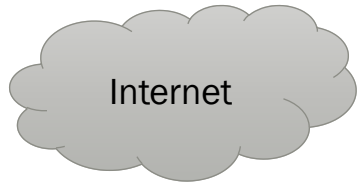
- C# .NET 4.5 & Core 3.1 Application
- Safer Ransomware implementation
- https://github.com/fozavci/ransoblin

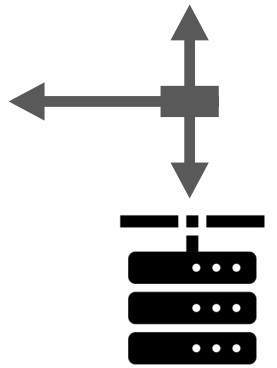
Petaq AMSI Patcher

- C# .NET 2.0 Application
- Patches AMSIScanBuffer
- https://github.com/fozavci/petaq_amsi

Target Environment

Production Server
- Windows 2008
- Metasploitable 3
- 172.28.128.2



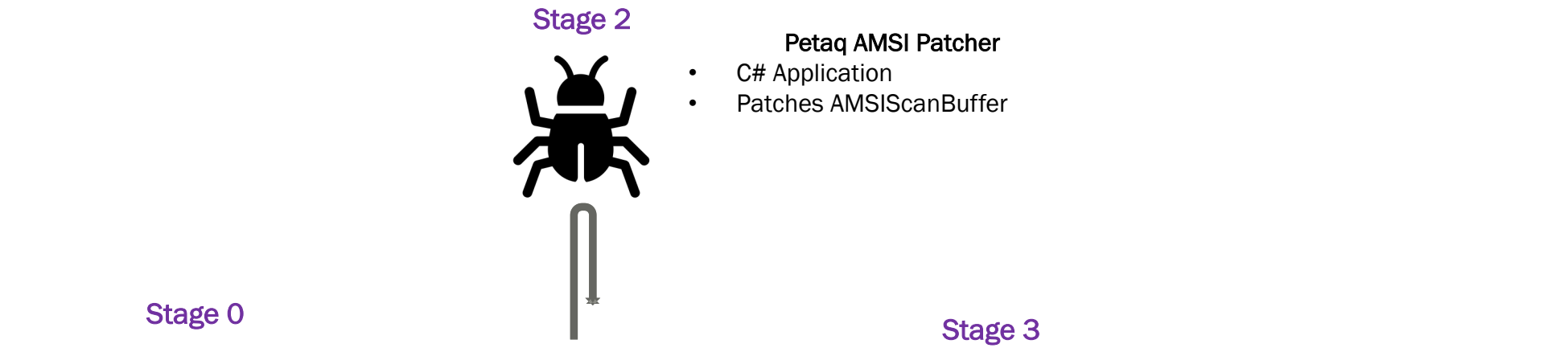


Attacker
- Kali Linux 2020.2
- Petaq Purple Team C2/Malware
- Metasploit Framework
- 172.16.168.134

Employee Laptop (Protected)
- Up-to-date Windows 10
- Up-to-date Windows Defender
- Up-to-date Office 2019
- 172.16.168.198
- 172.28.128.254

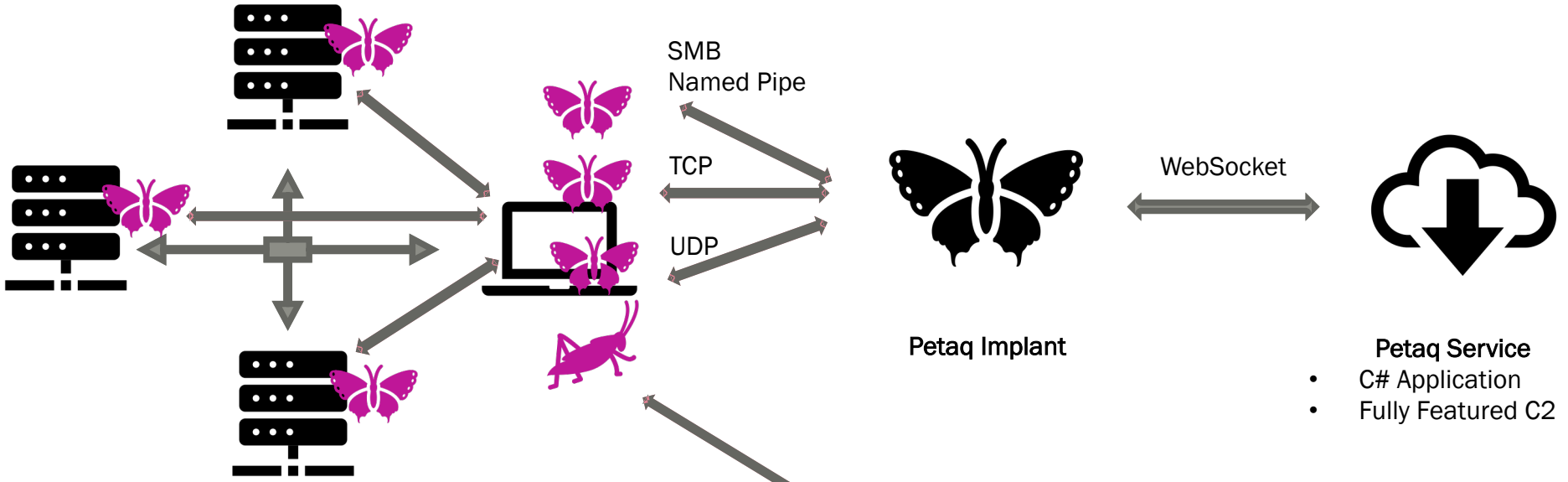
Application Server
- Ubuntu Linux 14.04
- Metasploitable 3
- 172.28.128.3

Initial Compromise & Defence Evasion



No Initial Windows Defender Detection + Patched/Bypassed Windows Defender + Fileless Malware

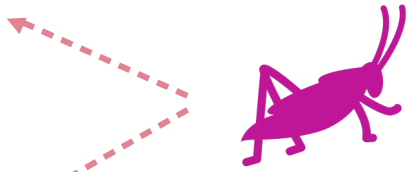
Internal Implant Communications



Actions on Objectives

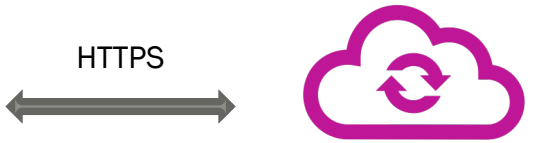
Remote Access
Tunnelling, VNC, RDP, Actions

Exploitation
Lateral Movement, Exploits



Meterpreter
Fully Featured Malware

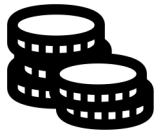
HTTPS



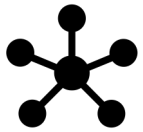
Metasploit Framework
- Traffic tunnelling
- Exploitation
- Known attacks

Petaq forks Meterpreter for interactive actions

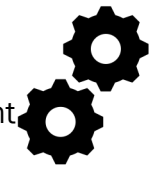
Ransoblin
Safer Ransomware Implementation



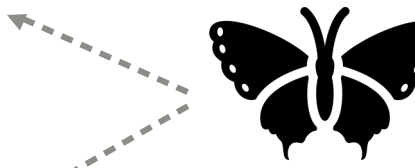
.NET Applications
Situational Awareness, Credentials Dump, Privilege Escalation Analysis



Fundamental Actions
File operations, System commands, Implant linking, Persistency

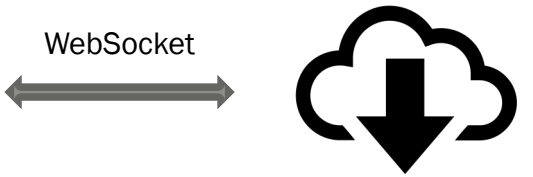


Native Shellcode
Meterpreter fork, Process Injections



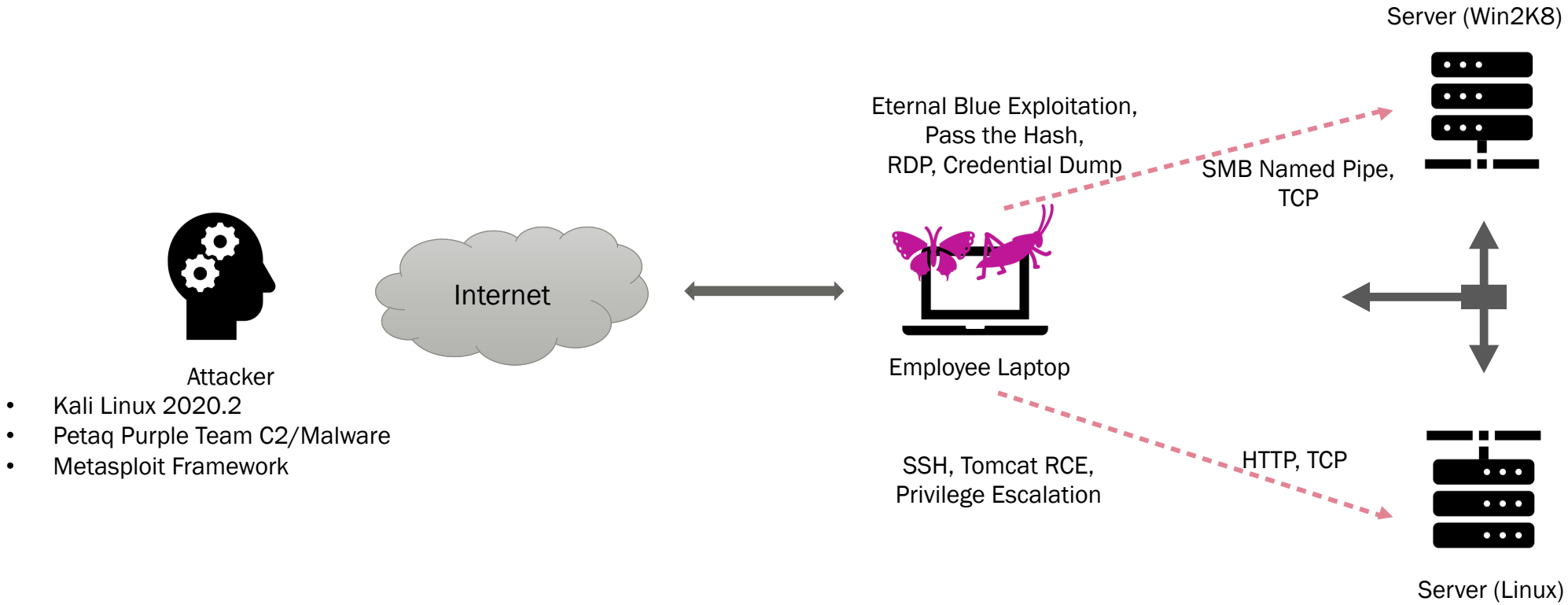
Petaq Implant
Fully Featured Malware

WebSocket



Petaq Service
- C# Application
- Fully Featured C2

Lateral Movement



Attacker

- Kali Linux 2020.2
- Petaq Purple Team C2/Malware
- Metasploit Framework

Defence Evasion Techniques

- Anti-Malware Scan Interface (AMSI)
  - *Used by Anti-Virus software such as Windows Defender*
  - *Bypass PoC: https://s3cur3th1ssh1t.github.io/Bypass_AMSI_by_manual_modification*
  - *Bypass PoC: https://github.com/rasta-mouse/AmsiScanBufferBypass/blob/master/ASBBypass/Program.cs*
  - *Old Bypass PoCs were prevented as Windows Defender updates detect them*
  - ***Marshall.Copy replaced with WriteProcessMemory API for patching AMSI scan buffer***
- Event Tracing for Windows (ETW)
  - *Used by Endpoint Detection and Response software such as Sysmon*
  - ***Bypass was not implemented due to time constraints, but can be added in a later date***
  - *Bypass: https://modexp.wordpress.com/2020/04/08/red-teams-etw/*
  - *Detection: https://gist.github.com/Cyb3rWard0g/a4a115fd3ab518a0e593525a379adee3*
- Kernel Security
  - *Kernel Driver Utility for driver exploitation & manipulation,* ***not implemented nor used by TA505***
  - *Bypass: https://github.com/hfiref0x/KDU*

Execution Tips

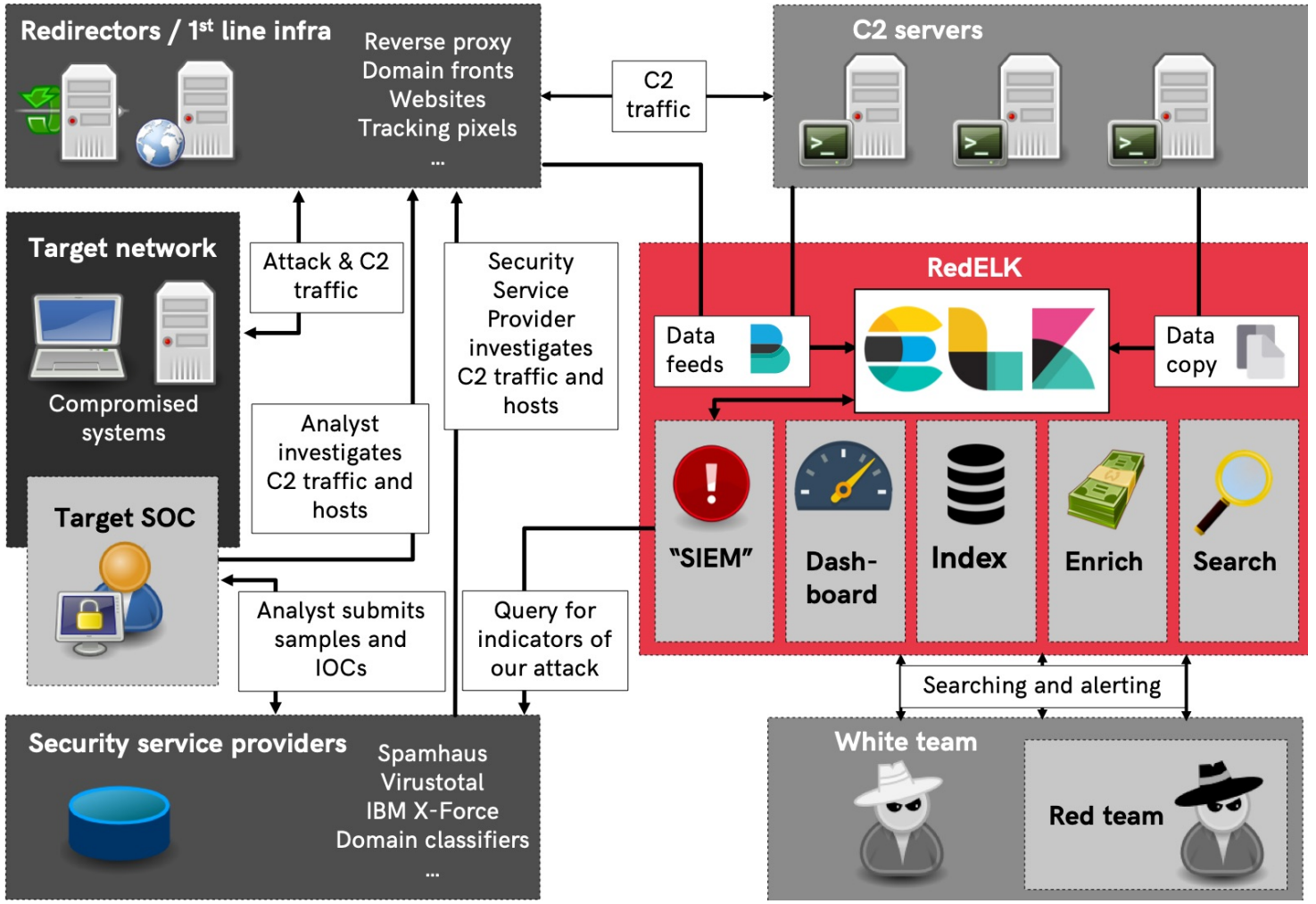
- Attacks take time to show up on SOC monitors and alerts.
  - *Run the attacks or scenario, and give a grace period*
  - *The exercise duration may be 2-3 days due to scope*
- Use a CTF or reporting software to give a metric to all parties.
- Assign a facilitator to the exercise.
  - *Maintain the pressure like the real life exercise*
  - *It's not a race, but a friendly competition*
- Blue team should receive all tradecraft, logs and IOCs

Planting the Flags

- Flags are useful to assess the team capabilities such as reverse engineering, malware analysis and utilising the security controls.
  - *Phishing email (e.g. headers, content)*
  - *Initial malware stages (e.g. command, dropper, stage1, stage2)*
  - *C2 communications (e.g. profile, protocol)*
  - *Persistency options (e.g. registry, file IOCs, services)*
  - *Lateral movement (e.g. remote service, WMI query, creds)*
  - *Data exfiltration (e.g. fake DLP flags, C2 channels, WebDAV)*
- Use a Capture the Flag scoring website or application

RedELK – Operational Security and Metrics

- RedELK
  - *Open Source*
  - *Processing C2 Logs*
  - *Processing Proxy Logs*
  - *Check IOC Websites/Feeds*
- Benefits
  - *Protect the Platform*
  - *Observe the Blue Team*
  - *Avoid Unwanted Victims*

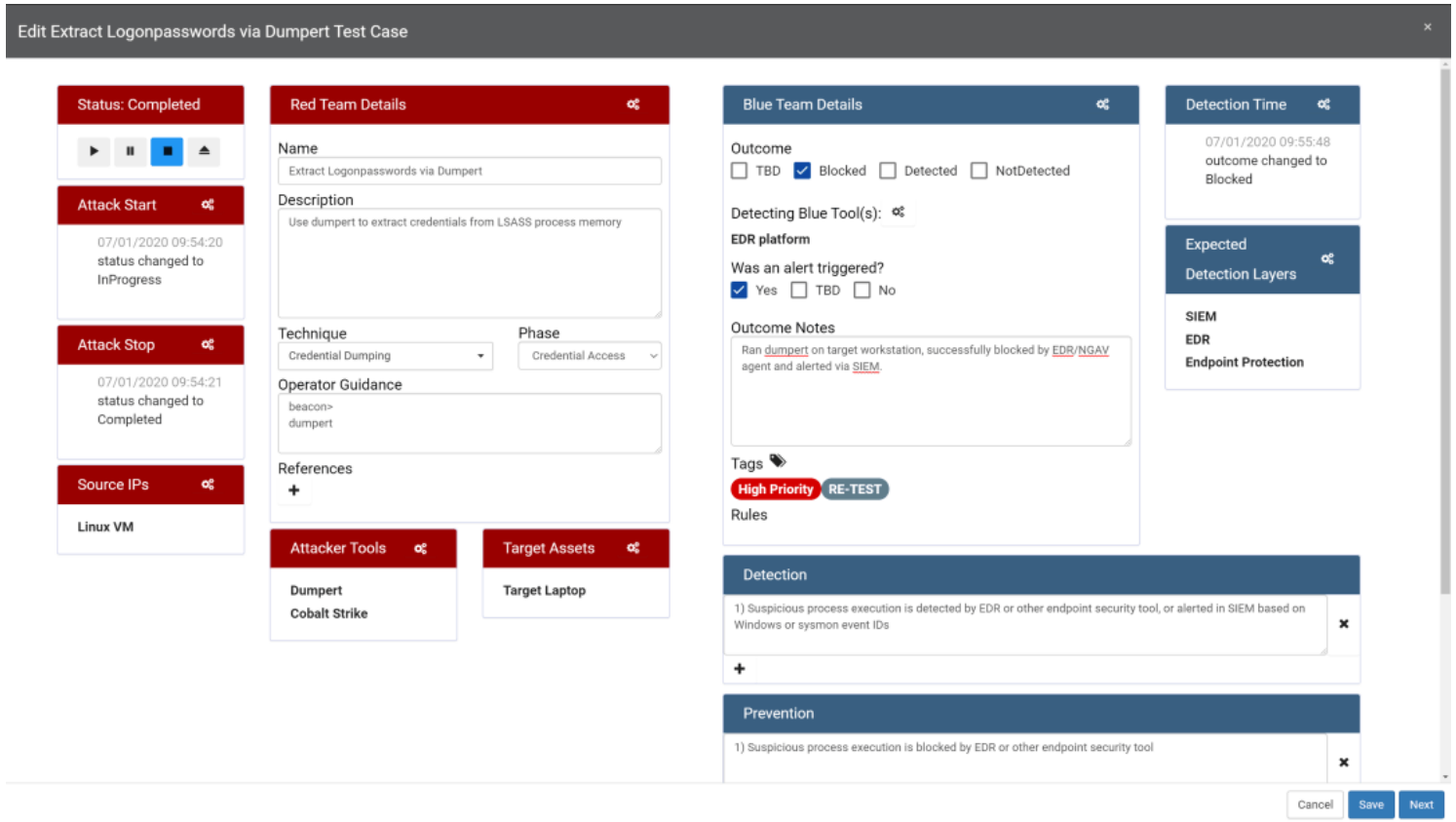


https://github.com/outflanknl/RedELK

Vectr – Monitoring and Reporting

➢Vectr is designed to provide metrics to the Red and Blue teams during the Purple Team exercises.

- *TTP Details*
- *Mitre Att&ck Mapping*
- *Detection/Prevention*
- *Response/Flags*



https://vectr.io/

Uplift the Game

➢Add Variations to Command & Control

- *Cloud Native C2s (e.g. Serverless Apps, Direct DB Connections, JavaScript Everywhere)*
- *C2 Traffic Cloud to Cloud (e.g. Deploying the C2 in another tenant of target cloud)*
- *Domain Fronting (e.g. Leveraging Cloud Fronting services with Domain/SNI masking)*
- *Newest HTTP Protocols (e.g. Mobile push on HTTP/2 or HTTP/3, WebRTC, WebSocket)*

➢Improve Evasion Techniques

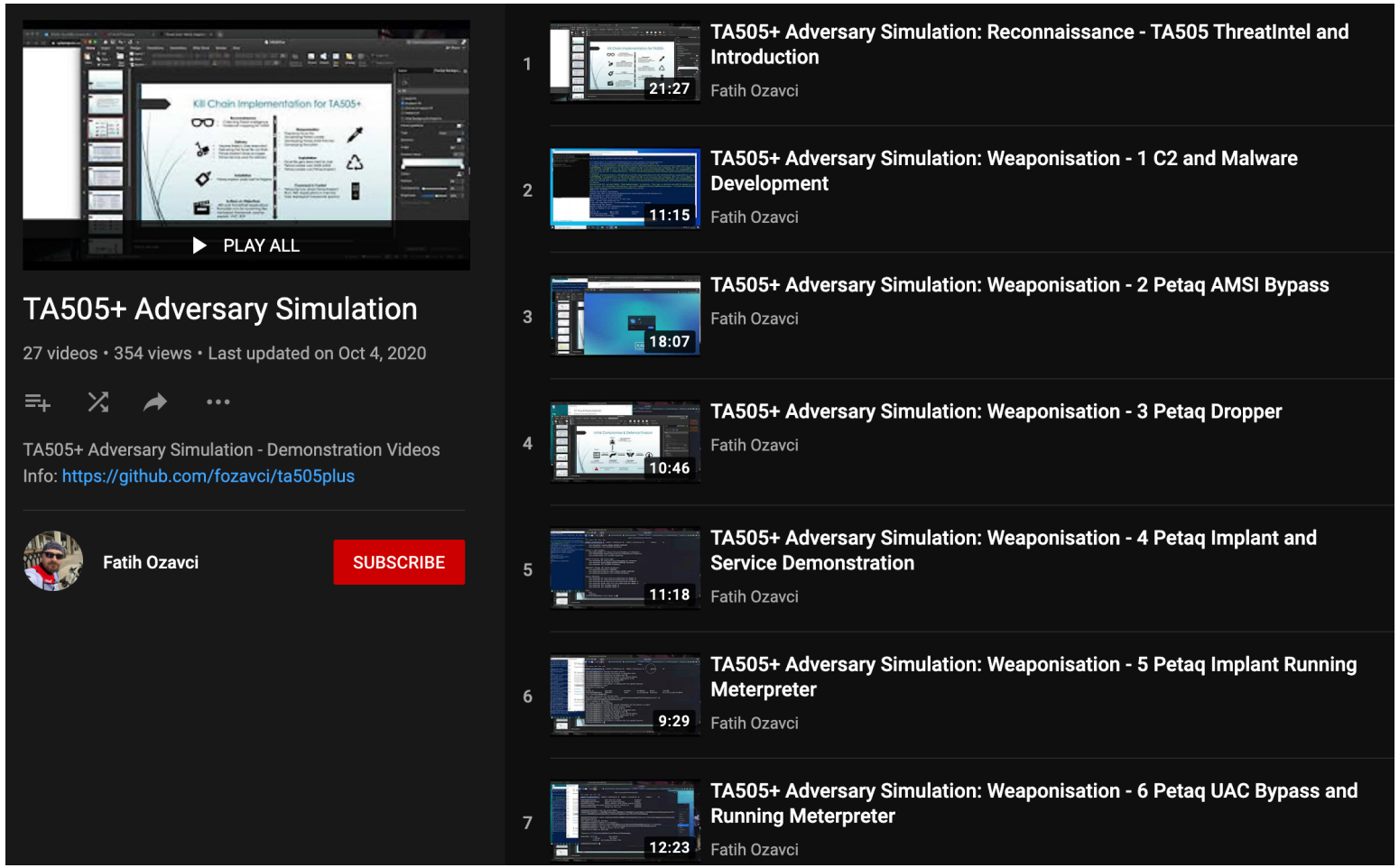
- *Reloading a clean NTDLL and remapping API Calls*
- *Protecting the processes with Parent ID spoofing, Microsoft Process Tags and Hollowing*
- *Disabling the EDR monitoring in Kernel Space*

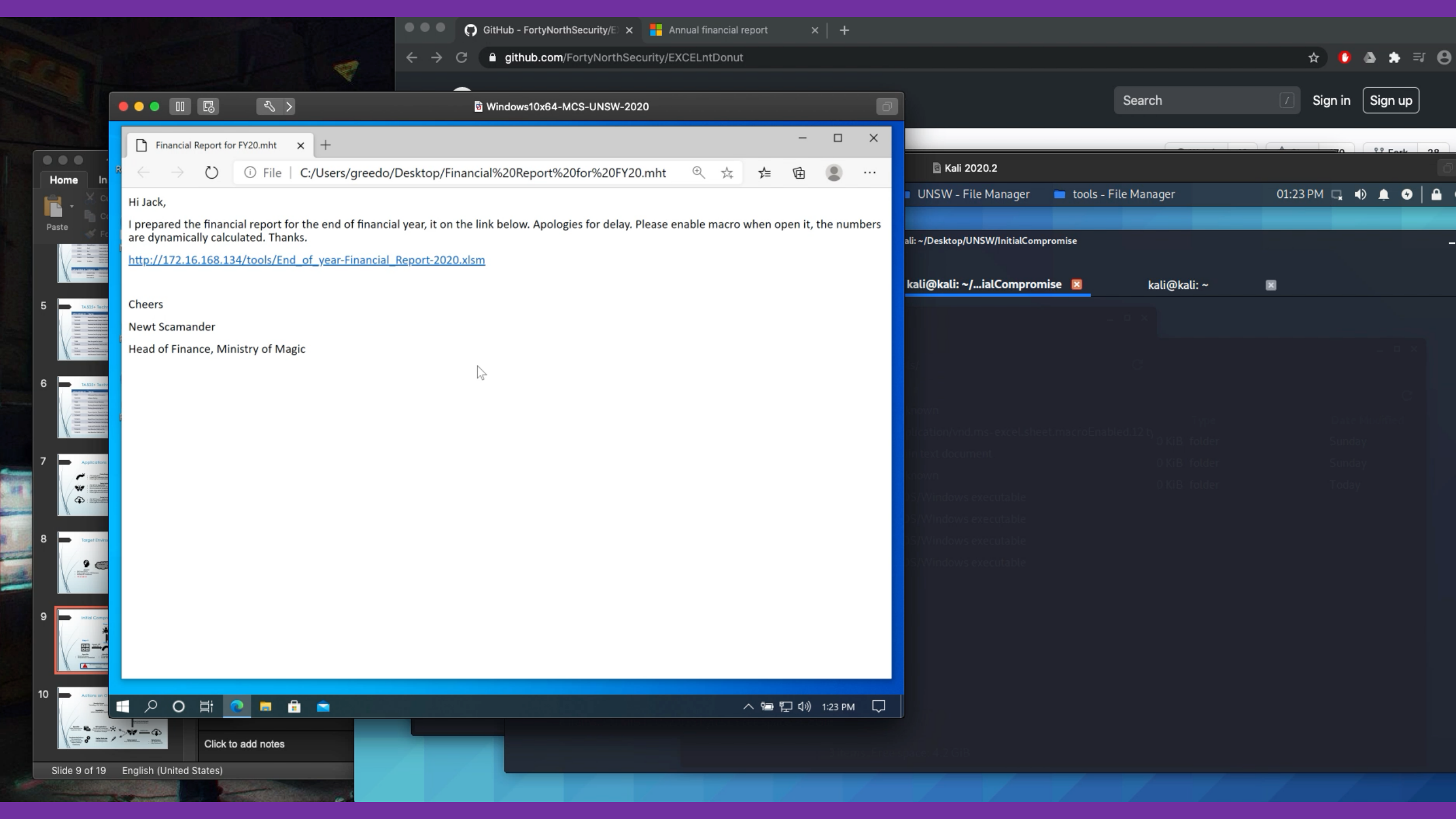
➢Adjust the Pace of Exercise for the Scenario Requirement

DELIVERY & EXECUTION DEMO

4h+ Development and Execution Videos

https://www.youtube.com/playlist?list=PL-o-7RjmFOAUOBb_eZDL__9yM7YOMX-6c

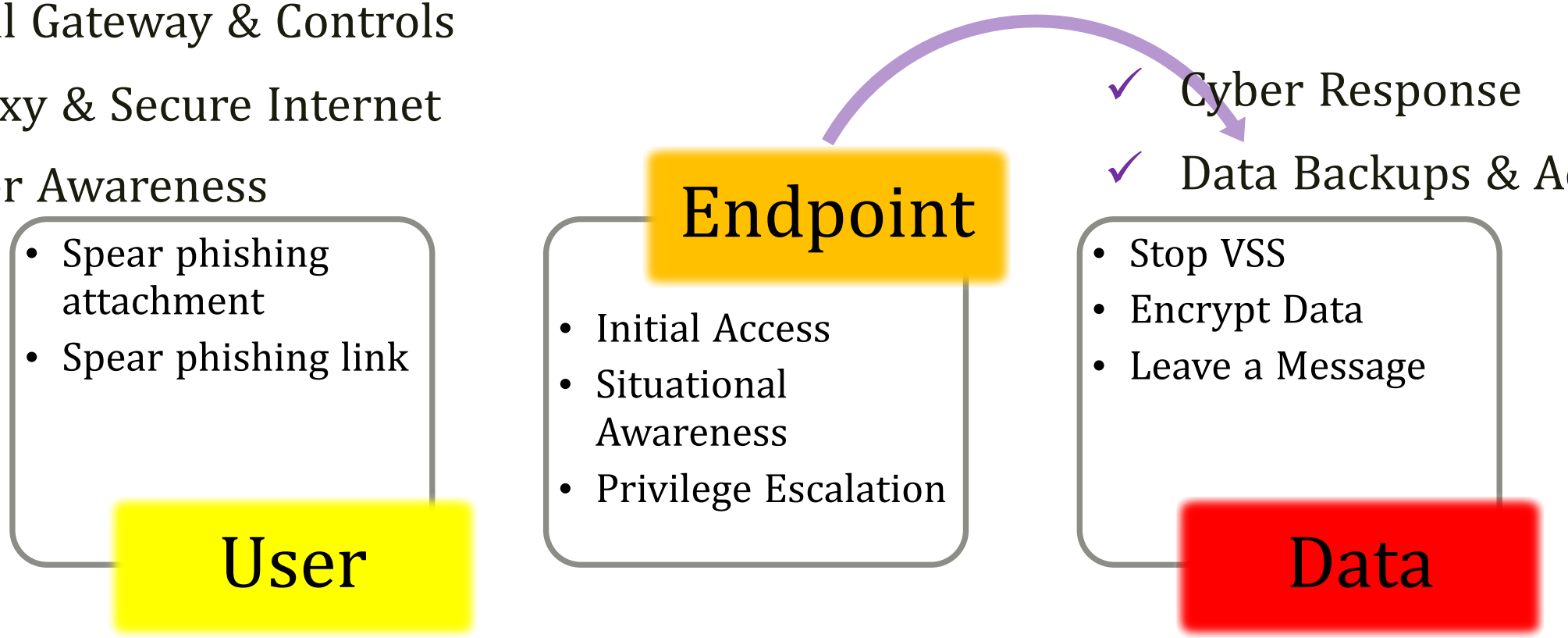



GitHub - FortyNorthSecurity/E
Annual financial report
github.com/FortyNorthSecurity/EXCELntDonut
Search
Sign in
Sign up
Windows10x64-MCS-UNSW-2020
Financial Report for FY20.mht
File | C:/Users/greedo/Desktop/Financial%20Report%20for%20FY20.mht
Hi Jack,
I prepared the financial report for the end of financial year, it on the link below. Apologies for delay. Please enable macro when open it, the numbers are dynamically calculated. Thanks.
http://172.16.168.134/tools/End_of_year-Financial_Report-2020.xlsm
Cheers
Newt Scamander
Head of Finance, Ministry of Magic
1:23 PM
Kali 2020.2
UNSW - File Manager
tools - File Manager
01:23 PM
kali@kali: ~/Desktop/UNSW/InitialCompromise
kali@kali: ~/...ialCompromise
kali@kali: ~
Home
Paste
Click to add notes
Slide 9 of 19
English (United States)

SCENARIO AUTOMATION DEMO

Scenario Automation

- ✓ Mail Gateway & Controls
- ✓ Proxy & Secure Internet
- ❑ User Awareness



- ✓ Endpoint Detection & Response
- ✓ Vulnerability & Patch Management
- ✓ Command & Control Detection

Running Scenarios Through Petaq

```
{
    "threat_actor":"Demo Threat Actor!",
    "ttps":[
        "T1087.001",
        "T1087.002",
        "T1059.001",
        "T1127.001-v2",
        "T1041",
        "Seatbelt",
        "ShellcodeInvoke",
        "InlineCSharp",
        "T1562.004",
        "T1047",
        "T1571"
    ]
}
```

Threat Actor

TTP IDs (Filenames)

Preparing TTPs for Petaq

```
{
    "name": "Enumerate users and groups",
    "mitreid": "T1087.001",
    "description": "Getting the users and groups via net command.",
    "instructions": [
        "exec cmd /cnet users",
        "exec cmd /cnet groups"
    ]
}
```

Name

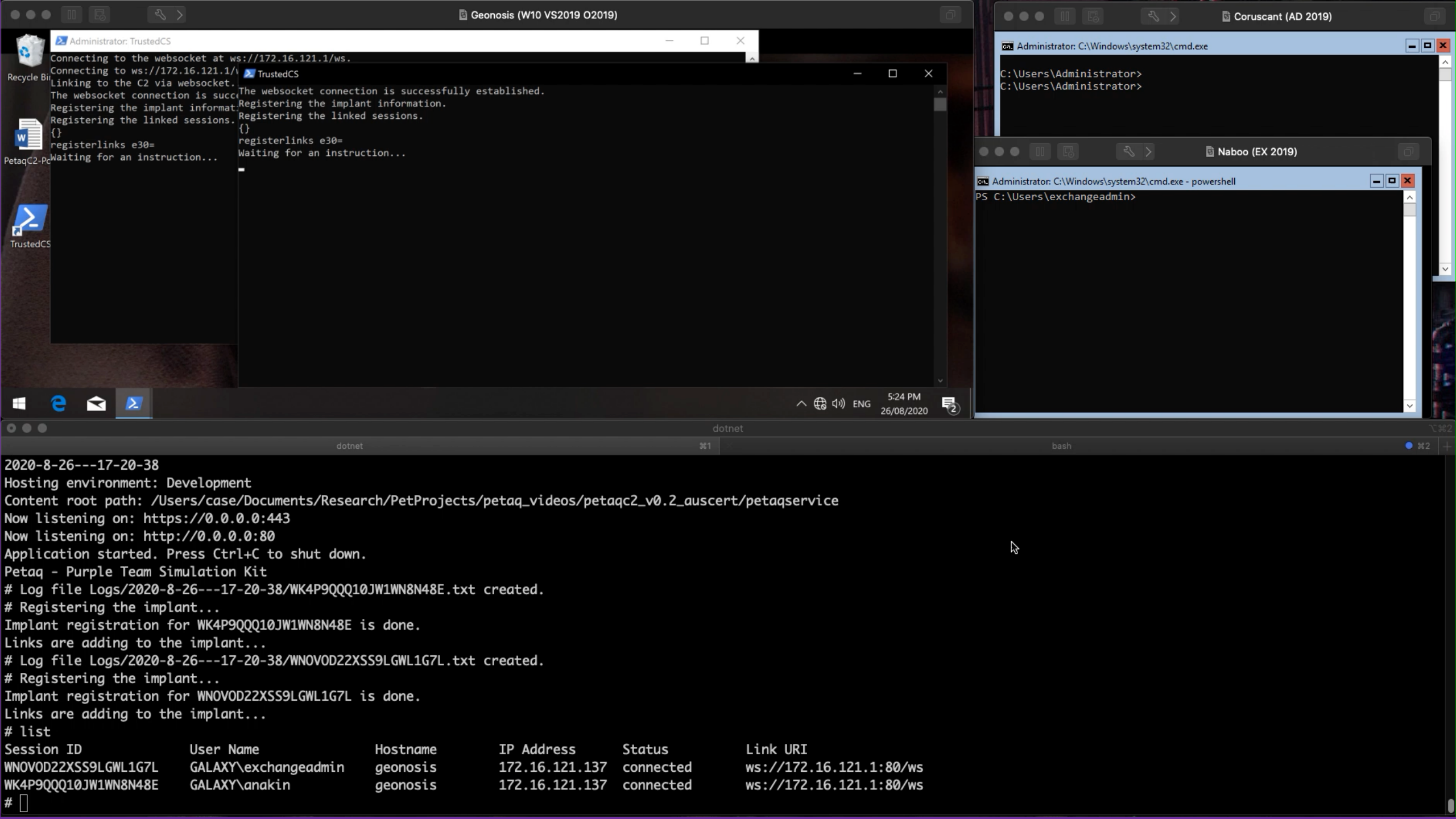
Mitre Att&ck ID

Description

Instructions

Execute Process Command	Upload Download Link Sleep	Execute .NET Assembly .NET Source Code .NET Direct	Execute PowerShell via System Management	Execute Shellcode (Raw Assembly)	Lateral Movement (WMI)

Use real tradecraft such as PowerUp, Mimikatz, Seatbelt, SharpMove, WMI, SC, PSExec



dotnet

dotnet ⌘1 bash ⌘2

```
2020-8-26---17-20-38
Hosting environment: Development
Content root path: /Users/case/Documents/Research/PetProjects/petaq_videos/petaqc2_v0.2_auscert/petaqservice
Now listening on: https://0.0.0.0:443
Now listening on: http://0.0.0.0:80
Application started. Press Ctrl+C to shut down.
Petaq - Purple Team Simulation Kit
# Log file Logs/2020-8-26---17-20-38/WK4P9QQQ10JW1WN8N48E.txt created.
# Registering the implant...
Implant registration for WK4P9QQQ10JW1WN8N48E is done.
Links are adding to the implant...
# Log file Logs/2020-8-26---17-20-38/WNOVOD22XSS9LGWL1G7L.txt created.
# Registering the implant...
Implant registration for WNOVOD22XSS9LGWL1G7L is done.
Links are adding to the implant...
# list
Session ID              User Name              Hostname       IP Address      Status       Link URI
WNOVOD22XSS9LGWL1G7L    GALAXY\exchangeadmin   geonosis       172.16.121.137  connected    ws://172.16.121.1:80/ws
WK4P9QQQ10JW1WN8N48E    GALAXY\anakin          geonosis       172.16.121.137  connected    ws://172.16.121.1:80/ws
#
```

Conclusion

- Various exercise types exist, find/develop a tailor fit exercise
- Exercise development and customisation improves efficiency
- TA505 can still walkthrough newer systems with minor updates
- Benefits of Purple Team Exercises
  - *Overall defence level for certain threats*
  - *Security weaknesses or vulnerabilities*
  - *Uplifting the existing skills sets and resources*
  - *Measuring software and solution efficiency*

- <u>Specialists first, software later…</u>

References

- *TA505+ Repository (https://github.com/fozavci/ta505plus)*
- *Petaq C2 (https://github.com/fozavci/petaqc2)*
- *Petaq AMSI Patch (https://github.com/fozavci/petaq_amsi)*
- *Ransoblin (https://github.com/fozavci/ransoblin)*

THANKS