

# RISHI OBEROI

DIPHE TECHNOLOGY | AZURE FULL-STACK ENGINEER

Rishioberoitechnology@gmail.com

LinkedIn

+44 7412 425242


SANS VoiceSecure - Global -

# AZURE SECURITY PORTFOLIO

# RISHI OBEROI

DIPHE TECHNOLOGY | AZURE FULL-STACK ENGINEER

Rishioberoitechnology@gmail.com

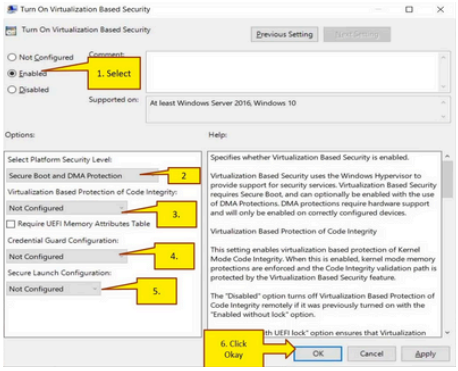
LinkedIn

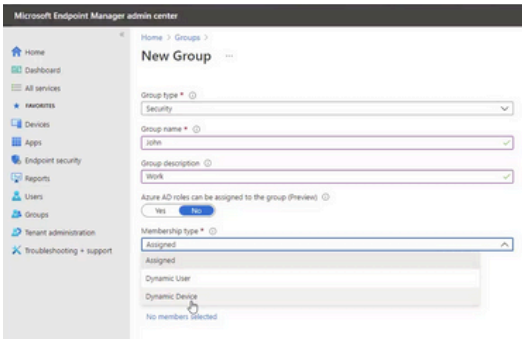
+44 7412 425 242


SANS VoiceSecure - Global -

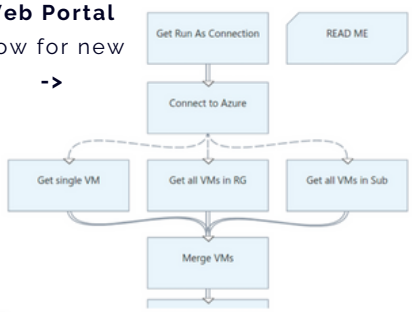
## MICROSOFT ACTIVE DIRECTORY, AZURE AND VM SECURITY

How to turn on virtualization based security on Windows 10 by enabling Credential Guard:

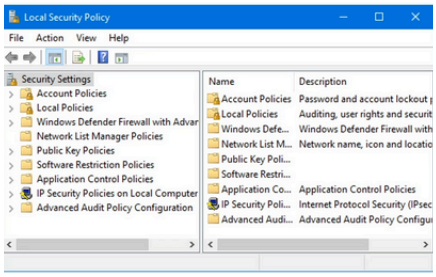


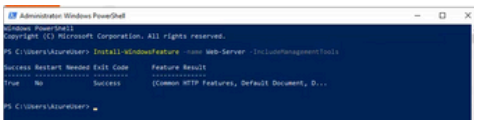




**Graphical Runbook: Azure Web Portal** allows me to create a workflow for new virtual machine systems. ->

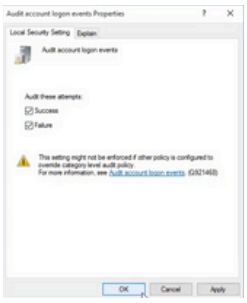



<- Creating a new group using Microsoft Endpoint Manager.

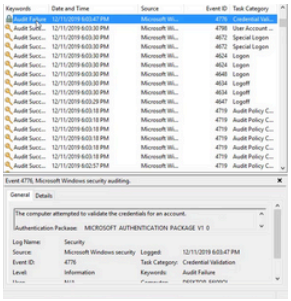



Installing an Azure Web Server on a VM using PowerShell.




(Screenshot 1).



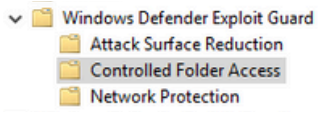

(Screenshot 2).

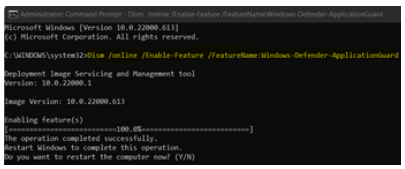
MMC -> Add snap-in. Local Security Policy: This allows administrators to set user privileges on local PCs that govern what users can do and automate if the system should track user activities in an event log.

Configuring the audit account management LGPO (screenshot 1) allows me to e.g. investigate the security log in Event Viewer (screenshot 2) which could give an indication to an attempted brute-force attack which can be mitigated by implementing MITRE ATT&CK M1036.

## MICROSOFT SENTINEL, AZURE AND DEFENDER SECURITY

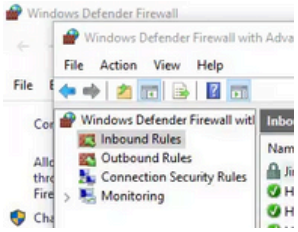
- DEFENDER EXPLOIT GUARD (SERVERS): GPO Management.
- Attack surface reduction,
- Controlled folder access
- Network protection.



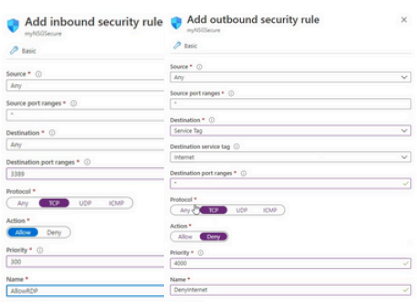



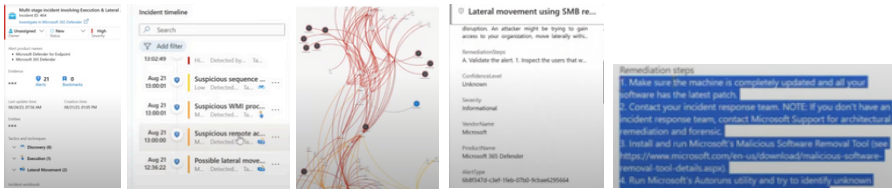

- DEFENDER APPLICATION GUARD App & Browser control deployment with DISM.

- Using Windows Defender Firewall Advanced Settings to configure a new TCP inbound rule in Defender: "Allow the connection if it is secure. "Authorize Users and Exceptions."




Configuring Azure virtual machine network firewall rules to e.g. allow inbound traffic from RDP port 3389 to enable technical support or an outbound security rule: "DenyInternet" allowing destination port ranges "*" with priority 4000 in case of a quarantine scenario.




- Monitoring: MS Sentinel to respond to multi-stage incidents involving execution & and lateral movement using e.g. SMB port 139 for suspicious remote access.
- Using the Incident Timeline for remediation steps and the incident activity log to document information for each step of the incident to hand over to fellow investigators.
- Responding to event classification when an IDS identifies data as benign when, in fact, it is malicious: A false negative does not generate an alert for the analyst and therefore these can be dangerous because the analyst cannot take action. This type of event classification has the most potential to be a serious event when missed.

# RISHI OBEROI

DIPHE TECHNOLOGY | AZURE FULL-STACK ENGINEER

Rishioberoitechnology@gmail.com
LinkedIn
+44 7412 425 242


SANS VoiceSecure Global

## HASH-BASED FILE INTEGRITY VERIFICATION

```
File  Edit  View  Search  Terminal  Help
giac@gsec_f03:~$ sha1sum /opt/snmpcheck/snmpcheck.p
83e60ceaf66096e402295521a3927cc55450b0bd  /opt/snmp
giac@gsec_f03:~$
giac@gsec_f03:~$ sha256sum /home/giac/GSECHashing/GS
43e864944d6563afb3ba080e04ecfe86c32aad9168cfbbfba5f0
```

Using the Linux terminal or PowerShell to find the digits of an MD5, SHA-1 or SHA256 hashed file to ensure files are not corrupt by comparing the file's hash value to a previously calculated value. If these values match, the file is presumed to be unmodified (reading fingerprints of digital evidence) (file integrity checking). NIST SP 800-86. This technique can be used during the remediation stage of a ransomware attack to verify the correct files have been decrypted SP 1800-25. SP 1800-26.

## AIRODUMP-NG WIRELESS SECURITY

```
root@slingshot:~# airodump-ng  wlan0mon

CH  4 ][ Elapsed: 0 s ][ 2020-03-02 13:36

 BSSID              PWR  Beacons #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
 E8:FC:AF:FC:95:66   20    2     0     0      9  54e  WPA2 CCMP  PSK  AD Net
 E0:46:9A:5A:9D:20   22    3     0     0      2  54.  WEP             NETGEAR15
 6E:8F:E0:BB:A4:62   58    2     0     0      1  54e. OPN             xfinity
 74:85:2A:3D:6B:69   58    2     0     0      1  54e. WPA2 CCMP  PSK
 00:24:B2:67:0E:50   51    3     3     1      1  54 . WPA  CCMP  PSK  VITAL

 BSSID              STATION            PWR   Rate    Lost  Packets  Probes
 E0:46:9A:5A:9D:20  8C:29:37:C6:68:5D   39    0 -24      1    30    NETGEAR15
 00:24:B2:67:0E:50  FC:DB:B3:DA:21:0B   42    0 - 1     22     8    VITAL
```

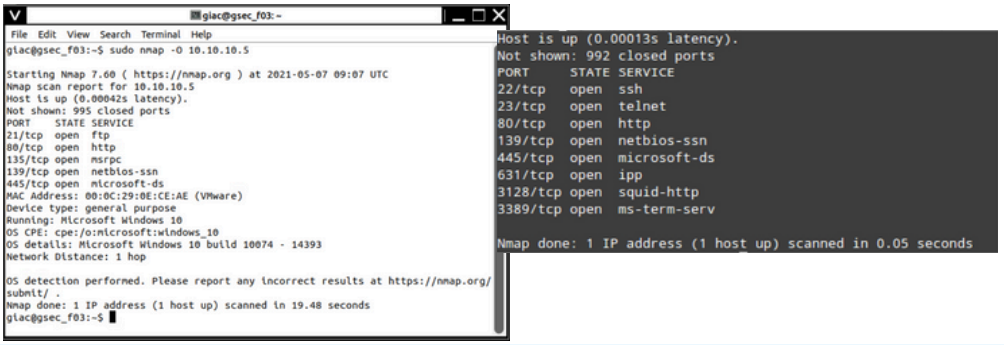
How to use Airodump-ng to find out with which wireless security algorithm a host with a specific MAC address is connected to its access point with.

Match the row of the MAC address to the Probes column:
E.g. MAC: VITAL.
Match the now identified ESSID column to the ENC column:
E.g. VITAL: WPA.

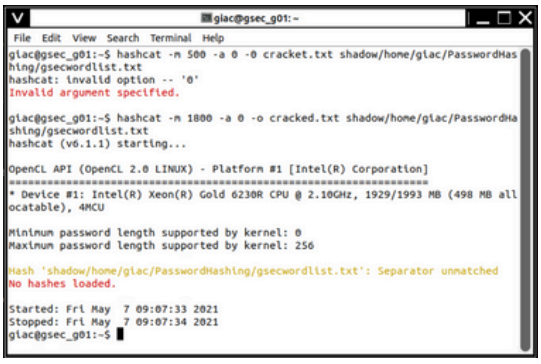
## NMAP TO SCAN AND FINGERPRINT OPEN PORTS OR OS DETAILS

Perform an OS Fingerprinting nmap scan against 10.10.10.5 to find out the OS details:
$ sudo nmap -O 10.10.10.5

Investigate which ipv4 address and port show a STATE value of e.g. "filtered" or "open" to display system vulnerabilities:
$ nmap 10.10.10.0/24


## SECURITY TESTING WITH HASHCAT




Using Hashcat for Linux and Bitcoin wallet hash cracking to security test for critical system vulnerabilities open to OS credential dumping attacks ID: T1003.002.

Mitigate this dictionary-combinator attack by restricting access to NTLM MITRE ATT&CK M1028 and implementing user training M1017.

Detection: monitoring for the "SAM" HKLM key dump being created in the Windows registry. MITRE ATT&CK DS0024

# RISHI OBEROI

DIPHE TECHNOLOGY | AZURE FULL-STACK ENGINEER

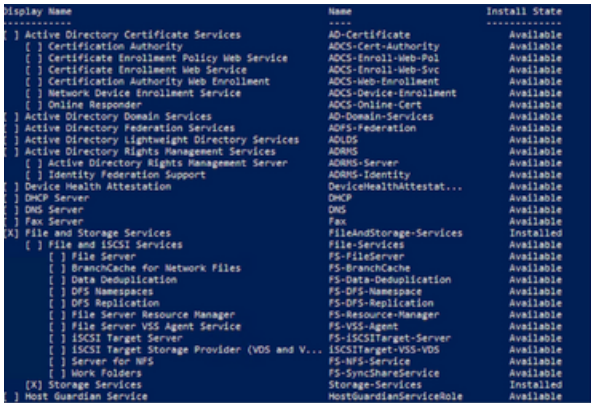
Rishioberoitechnology@gmail.com

LinkedIn

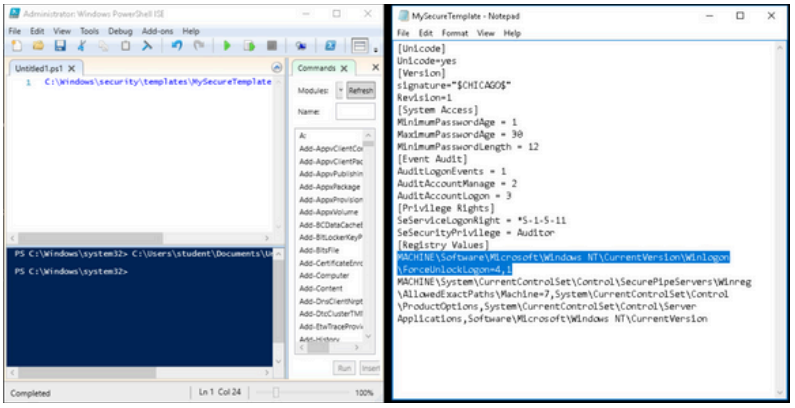
+44 7412 425 242


## WINDOWS POWERSHELL ISE TO READ & ANALYSE .INF SECURITY TEMPLATES

1.)




2.)

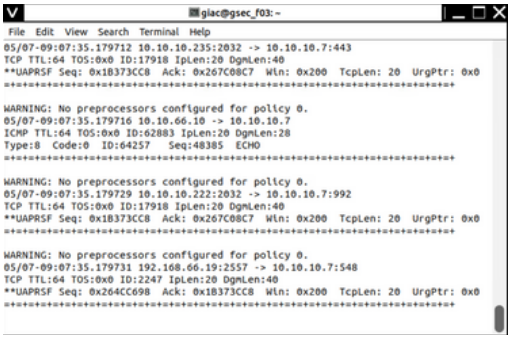


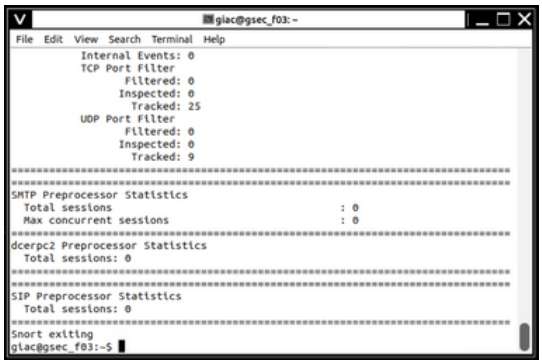

To analyse services and values in Windows Powershell run the command:
Get-Service -Name fdPHost | Select-Object DependentServices (first screenshot).

To find out how settings are configured in a Microsoft security template run the command:
ise .\Windows\security\templates\MySecureTemplate.inf (second screenshot).

If the INF file is opened in another tool such as using the MMC, different names and setting formats will be seen such as Success or Failure auditing policy rather than a numerical assignment.

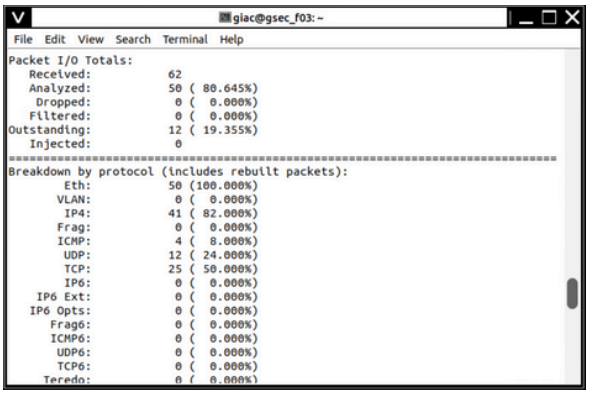
## SNORT IDS TO GENERATE INTRUSION ALERTS BASED ON INCOMING TRAFFIC




To generate intrusion alerts with Snort based on incoming traffic this rule can be used.

Automated snort IDS detection rule: alert tcp any any -> 192.148.1.1/24 80 (content: "/cgi-bin/test.cgi";mesg:"Attempted CGI-BIN Access, Warning!! Check server role modificaiton.";




How to investigate what the source IP address or source port of a host triggering an alert with a specific SID is.

Investigate the source port of a host triggering a specific alert message:

Command: sudo snort -c /etc/snort/snort.conf -i etho -A full
cat /var/log/snort/alert

Now use the Search button (top left) for what you need.

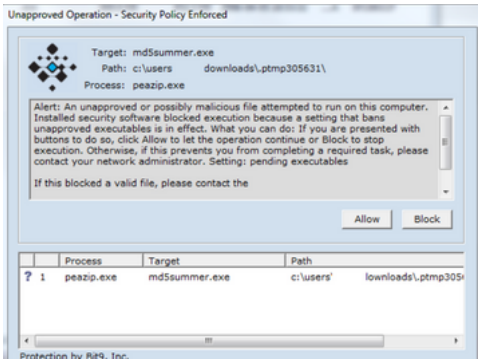
# RISHI OBEROI

DIPHE TECHNOLOGY | AZURE FULL-STACK ENGINEER

Rishioberoitechnology@gmail.com
LinkedIn
+44 7412 425 242


SANS VoiceSecure Global

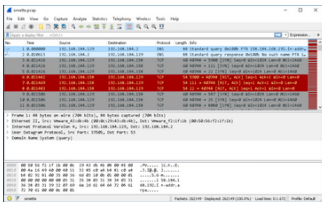
## HIPS APPLICATION BEHAVIOUR MONITORING

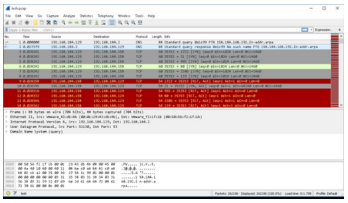


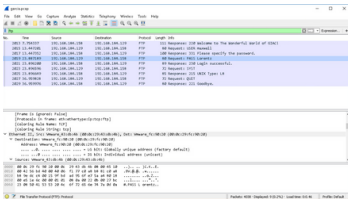

Unapproved Operation – Security Policy Enforced.

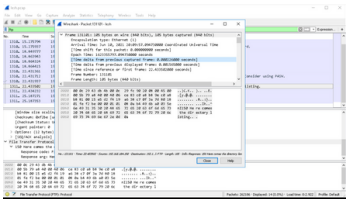
The system that generated this alert should be classified as: Host-based intrusion prevention. Application behaviour monitoring is a feature of HIPS software where a manufacturer selects a supported application, and records the intended functionality of the application in normal use. NIST SP 800-94.

## WIRESHARK FOR NETWORK TRAFFIC MONITORING. DETECTING NETWORK ANOMALIES ACCORDING TO THE SYSTEM BASELINE. CONFIGURATION MANAGEMENT









Monitoring network traffic (sniffing) T1040 to detect DS0029 baseline dependent [RST, ACK] TCP 3-way handshake (transport layer) packets indicating failed transmissions. This could be a piece of evidence for network misconfigurations or an attempted layer 5 session hijacking attack ID: T1185.

Mitigation: Data loss prevention M1057 and filter network traffic M1037.
Detection: Application log monitoring DS0015
data exfiltration indicator xxx
mitigation xxx
Intercepting FTP messages (layer 7) to discover unencrypted passwords inside packets. Adversary-in-the-Middle Attack T1557. Takes place on the application layer and layer 3 (network layer)

Mitigation: This type of attack be mitigated by decrypting sensitive network traffic ID: M1041 and segmenting the network into protected enclaves M1030 (vector-oriented DiD).
Detection: Identify network anomalies DS0029 and Windows registry key modifications to the DNSClient "EnableMulticast" DWORD value DS0024.

## TCPDUMP TO ANALYSE SAVED PACKETS (.PCAP)

```
glac@gsec_f03:~/pcaps$ ls
1989.pcap   blueteam.pcap   elephant.pcap   pheasants.pcap   woodward.pcap
apple.pcap  cass_tech.pcap  flex.pcap       test.pcap        zero.pcap
beats.pcap  deleteme.pcap   hackathon.pcap  thunderbay.pcap
glac@gsec_f03:~/pcaps$ tcpdump -r elephant.pcap
reading from file elephant.pcap, link-type EN10MB (Ethernet)
18:09:54.347036 IP 192.168.1.4.62449 > 107.162.133.105.http: Flags [S], seq 2544572039, win 65535, options [mss 1460,nop,wscale 6,nop,
K,eol], length 0
18:09:54.379827 IP 107.162.133.105.http > 192.168.1.4.62449: Flags [S.], seq 142857004, ack 2544572040, win 4380, options [mss 1460,s
18:09:54.379877 IP 192.168.1.4.62449 > 107.162.133.105.http: Flags [.], ack 1, win 65535, length 0
18:09:54.379922 IP 192.168.1.4.62449 > 107.162.133.105.http: Flags [P.], seq 1:73, ack 1, win 65535, length 72: HTTP: GET / HTTP/1.1
glac@gsec_f03:~/pcaps$
```

A tcpdump file reading .pcap recorded packet data to investigate recorded HTTP traffic (Layer 7 Application).
This allows me to find out e.g. when a packet was transmitted, who the host entities were and if the transmission was successful.